Digitally signed by Culicov Iuri
Date: 2021.06.18 14:30:16 EEST
Reason: MoldSign Signature
Location: Moldova

The procurement of Instant payments software solution

National Bank of Moldavia

SMARTVISTA

TECHNICAL OFFER

17 June 2021

Notice

BPC AG
Neuhofstrasse 5a
6340 Baar
Switzerland

Phone: +41 (41) 760 64 70

Email: info@bpcbt.com

Web: www.bpcbt.com

I. Contents

II. Understanding of the scope 8

III. Executive summary 9

IV. Proposed IPS solution 11

Diagram & description of the components 11

Interfaces 11

SmartVista Instant Payments Overview 13

SmartVista Instant Payment System at a glance 14

General Architecture 15

ISO 20022 Messaging Standard 16

Instant Payment Platform Core Services 19

Credit Transfer 19

Bulk Payment Flow 22

Payment Exception Flow 25

Payment Return/Refund 27

Direct Debit (optional service) 28

Instant Payment Platform Overlay Services 29

Request-To-Pay 29

Addressing Service 35

E-Mandate Management (optional) 37

Instant Payment Platform Value-Added Services 42

Fraud and Risk Management System (optional) 42

Reports and Analytics 45

Billing and Statement 47

Participant Portal 53

Participant Types and Account Management 62

Participant Status 62

Participant Account Hierarchy 62

Liquidity Management 64

Settlement and Reconciliation 72

Disputes Management 75

Customer claims registration 76

Case flow 77

SmartVista Technology & Security Architecture 79

SmartVista Integration Platform 79

Core module 81

Channels 81

Business Process Engine 82

Services 84

Stand-in and Stand-alone module 84

Authorization module 85

Dictionaries module 85

UI Rest module 85

Admin module 85

Front-end component (user interface) 85

Component-Based Architectural Style 86

Layered Architectural Style 87

Service-Oriented Architectural Style 89

Supported Platforms 90

Reliability, Availability and Scalability 91

Active-Passive Configuration 91

Active-Active Configuration 92

SmartVista Testing Tool 92

Setting up of PKI 98

Root Certification Authority 98

SmartVista Security Architecture 103

SmartVista Secure Application Development 107

PA DSS certificate 109

ISO 9001:2015 certificate 110

V. Working hypothesis 111

VI. Project Management; Approach, Deliverables & Tools 114

Description of Working Principles 114

Implementation strategy 116

Project Organisational Chart 117

BPC Team Structure, Roles & Responsibilities 117

Customer Team Structure, Roles & Responsibilities 123

Project management plan 126

Purpose 126

Project Overview 128

Project Management Approach 129

Scope Management 132

Project Scope 133

Requirements Management 135

Requirements Development and Documentation Plan 135

Integration Management 136

Schedule Management 137

Project Schedule 137

Project Deliverables 138

Project Milestones 139

Cost Management 140

Quality Management 141

Document Deliverables 142

Software Quality 142

Services Quality 143

Resource Management 143

Basic responsibilities of BPC's team members 144

Communications Management 146

Stakeholders 149

Communications Matrix 150

Risk Management 153

Activities 154

Schedule for Risk Management Activities 156

Procurement Management 157

Stakeholder Management 158

Change Management 159

Change Request 159

Change Process Roles and Responsibilities 159

Overall Change Management process 160

Operational Change Management Process 162

Commercial change management process 162

Travel Logistics 163

Visa and Border Formalities 163

Working Environment 163

Meeting Environment 163

Approach, Deliverables & Tools 163

Deliverables 168

Approach, Deliverables and Tools used for Analysis phase 170

Approach, Deliverables and Tools used for Design Phase 170

Approach, Deliverables and Tools used for Implementation / Build phase 171

Approach, Deliverables and Tools used for Testing phase 174

Approach, Deliverables and Tools used for Go live and Final Acceptance Phases 178

Approach to the Change Management Process 179

Development policy 179

Quality Assurance 180

Version Management 180

VII. Answers to section F4.4 182

FUNCTIONAL REQUIREMENTS 182

NON-FUNCTIONAL REQUIREMENTS 242

IMPLEMENTATION REQUIREMENTS 271

CONDITIONS FOR WARRANTY, MAINTENANCE AND POST-IMPLEMENTATION SUPPORT 304

VIII. Users training approach 307

Training philosophy and requirements 307

Proposed approach 307

NBM involvement 308

Processing system fundamentals 308

Processing fundamentals (T-01) 308

Working with EMV (T-02) 308

SmartVista suite training 308

SmartVista essentials (T-03) 308

SmartVista configuration (T-05) 309

SmartVista credit card management (T-06) 309

SmartVista administration (T-07) 309

Transaction processing (T-08) 310

SmartVista training for trainers (T-09) 310

Dispute management (T-10) 310

Encryption and keys (T-11) 311

ATM scenarios (T-12) 311

Supplementary modules training 312

Access control server (T-13) 312

E-commerce solution (T-14) 312

Fraud management (T-17) 312

SmartVista Integration Platform user training (T-21) 312

SmartVista Integration Platform configuration training (T-22) 312

System Monitoring user training (T-23) 313

IX. Recommended platform 314

Software 314

Hardware 314

Production 314

Development / Test 315

OVM Manager & Monitoring Server 315

PKI 316

X. Proposed SLA 317

XI. Appendices 319

Model of standard maintenance and support agreement 319

Model of standard licensing agreement 319

Model of product warranty 319

Model of escrow agreement 319

Contact details

“Please contact us if you have any queries to address.”

Vasily Volynskiy
Senior Vice President
volynsky@bpcbt.com
+41 79 138 4239

BPC AG
Neuhofstrasse 5a
6340 Baar
Switzerland
Tel: +41 (41) 760 64 70
Fax: +41 (43) 508 04 10
www.bpcbt.com

II. Understanding of the scope

Based on analysis of NBM public RFP, BPC understood the scope of the project is to modernize the Automated Interbank Payments System (AIPS), which is the only interbank payment system in the country and offer Consumer and Business payments infrastructure to member Banks and PSPs.

Two settlement components are available by NBM, namely; Real Time Gross Settlement (RTGS) system for large-value and time-critical payments, and the Designated-time Net Settlement (DNS) system for low value (retail) payments, available for bank or non-bank members of the Moldavian payment eco-system.

The estimated volume of monthly transactions is 5,000.000, while availability level is set at the level of 99,99% and TPS capacity up to 100.

Native ISO 20022 messaging is mandatory between NBM Instant Payments Platform and members, including complementary services like CAS, RTP, time-out handling, dispute management, amongst others, in-line with SCT Instant Rulebook, tightly integrated to RTGS system.

The expected delivery lead time for the project is 20 months, with a warranty period of 12 months, in a way to provide the best optimum service to NBM members (banks and PSPs).

The main delivery components are; Software licenses for IPS solution, Implementation services, and Post implementation services. A cap of 300 man-hours has been specified for any required Change Requests are dimmed necessary during project implementation and delivery.

Organizational change management and procurement of the infrastructure platform needed to run the IPS solution, are considered as out-of-scope topics.

The project location is NBM's headquarters, Chisinau, Republic of Moldova, where the project activities will be conducted, except those that do not require NBM's team involvement and could be performed remotely.

III. Executive summary

BPC would like to thank **National Bank of Moldavia** for inviting us to provide a proposal for a "The procurement of Instant payments software solution".

The scope of the RFP is for the Bank to select an innovative and proven digital payment platform is to provide clearing and instant settlement of retail payments, initiated by individuals, corporates and government. The IPS system shall become a cross platform, that offer interoperability for all PSP in the local market, by processing their payment messages originated from different channels and devices namely PC, mobile acceptance networks.

Choosing **SmartVista,** BPC's world known payments platform, PA-DSS certified and PCI-DSS ready, is a strategic move to a market leading solution. SmartVista, our own-build platform, is scalable, high performing, highly functional, extremely flexible, reliable and proven and represents the best in class and the best value on the market.

310+

97

"and growing"

20+

National Switches & IP schemes

BPC is continuously growing on a global range and **National Bank of Moldavia** could only benefit by this growth.

BPC as a trusted technology partner has vast experience in executing and implementing national instant payment projects and helping central banks to materialize their vision, strategy and long term financial inclusions plans. Several regulators and central banks have already shown their trust on BPC in many countries in the region. SmartVista is implemented in over twenty-two National Switch and third-party processors all around the world. The Yemen Financial Services, which is the technology subsidiary of the Central Bank of Yemen has deployed National Instant Payment system via SmartVista. Today there are more than seven banks connected to the Instant Payment scheme and availing services like P2P transfers, Alias Management and Request-To-Pay. With over 90% unbanked population in the country, the National Instant Payment scheme is playing a central role in addressing the financial inclusion challenge.

Last month the National Bank of Ethiopia selected BPC's SmartVista to power the National Instant Payment Scheme called NBM. The NBM will offer innovative services like instant P2P transfers, Direct Debits, Bulk Credit Payments, Central Alias Scheme, Request-To-Pay, Real-time fraud prevention and Dispute management. The project is set to go live by Q2 2022.

We are proud of our **SmartVista** platform, of the clients we have, and of the business we have built over decades. SmartVista technology, is used and trusted by more than 310 clients, in 97 countries globally, managing more than 2 million POS, 120 thousand ATM terminals and 1 billion credit / debit cards. Among our customers, are global and regional brands like HSBC, ING, BNP Paribas, OTP Group and ERSTE, the leading and most innovative national players, national switches and instant payment schemes in more than 20 countries.

<u>Ready made functionality</u>

SmartVista Instant Payments System is able to map the the scheme organization and it meets the requirements set out in SCT Instant Rulebook. Central alias service (CAS) and request to pay (RTP) features are included out of the box, while it is easy to configure new functionalities as the payment market evolves. SmartVista is using all open new technologies,

thus securing the feature and investment of National Bank of Moldova. It is closely integrated with a number of RTGS systems globally.

Simple and flexible to implement

Based on market recognized SmartVista technology, **SmartVista** can interact with virtually any external system via built-in integration APIs. A simple interface makes it easy for customer service staff to manage customers and makes setup and configuration straightforward for issuing teams. The product includes out-of-the box support for all IPS clearing interfaces and built-in interchange forecasting. SmartVista works seamlessly alongside other products within a broader payments' solution.

Easy to operate and maintain

Relying on open standards and tailored for automated operations with the extensive self-diagnostics, **SmartVista** is not demanding in terms of operational staff. Most of our clients allocate quite limited resources for operational and support tasks.

Future proof choice

BPC is also looking to the future; we realize that the world of payments is changing. We adapt our technology and our "Mind Set" to the digital and Mobile age. Our offering is able to accommodate those changes. PSD2, Open API's, Open platform, etc. force us to have a solution that is substantially more open and interoperable. SmartVista product suite, is a future proof solution that is already prepared for digital era challenges and may enable PSD2 compliance and instant payments capabilities for your initial and subsequent projects. BPC's ability to innovate is reflected in the fact that we won back-to-back awards from IAIR for "Best Company for Innovation in Payment Technologies". This is in addition to a number of other awards.

High Availability & Complete Reliability

SmartVista fully utilizes the high availability and fault-tolerance options offered by the underlying UNIX systems and Oracle databases and certified hardware platforms: IBM, HP, Oracle and others.

We would appreciate the further opportunity to show you the capabilities and strengths of the **SmartVista** platform, as part of your selection process and look forward to continuing this "journey" with you.

IV. Proposed IPS solution

Diagram & description of the components

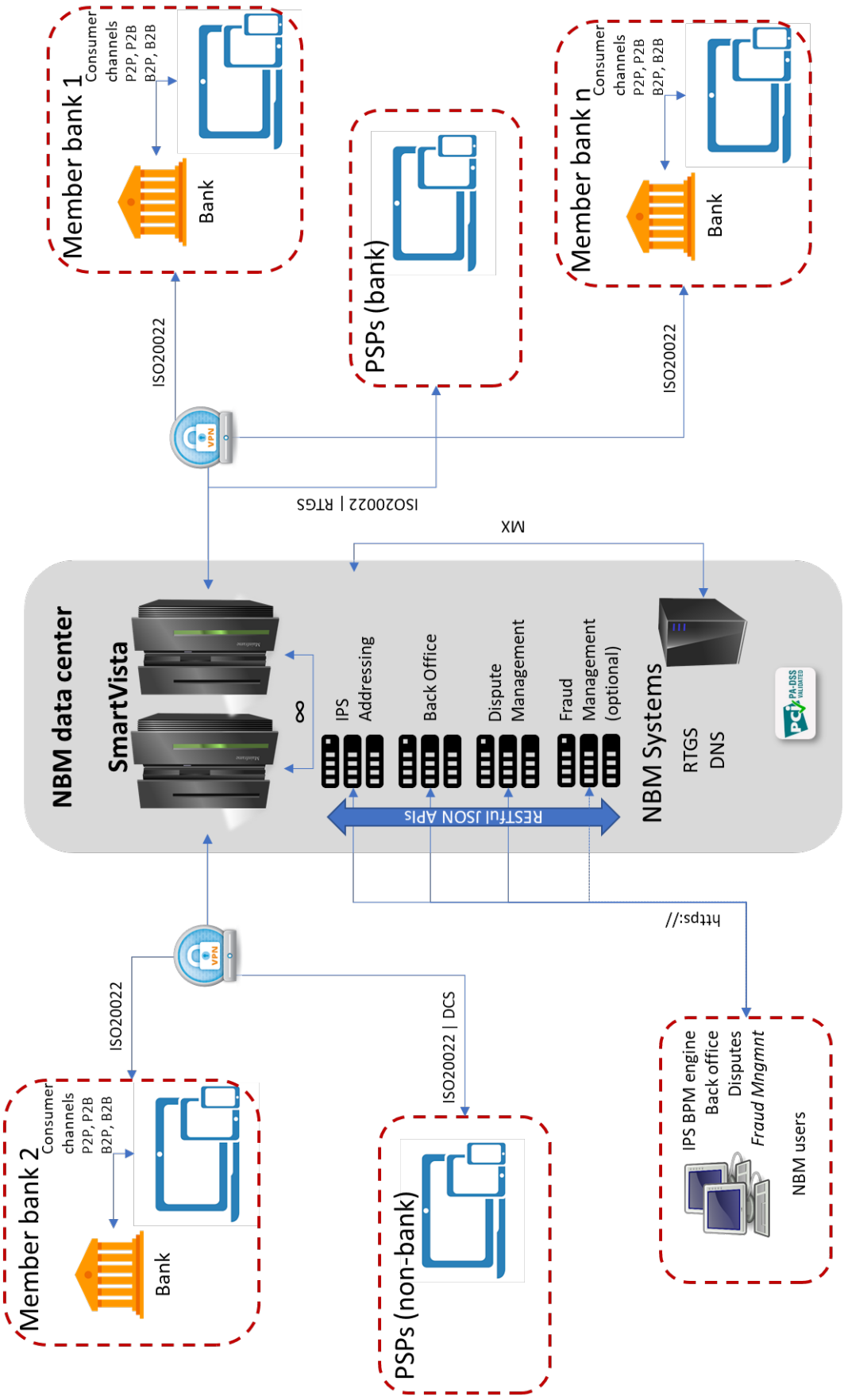
To address the business and operational requirements we propose the following SmartVista modules, for on-premise operational model at National Bank of Moldova Data Center.

SmartVista components

- Integration Platform (IPS)
- Addressing
- Back Office
- Dispute Management
- Fraud Management (optional)

Interfaces

Interface	Description
ISO 20022	Participant Banks, bank-PSPs and non-Bank PSPs
MX	RTGS & DNS



SmartVista Instant Payments Overview

In today's fast-paced world, getting an instant service is expected. As such, instant payments are becoming the new norm set by the growth of e-commerce worldwide that drive new payment habits. Traditional wire payments that take business days to reach an account are no longer acceptable. Consumers and businesses alike expect instant payment for goods they purchase or sell.

An electronic instant payment means that the payment function is available 24/7/365 and results in the immediate or close-to-immediate interbank clearing of the transaction and crediting of the payee's account with confirmation to the payer (within seconds of payment initiation).

BPC' SmartVista Instant Payment System (SVIPS), is a real-time payment processing, clearing and settlement solution for central banks, national switches and payment service providers that offers immediate payment functionality to their end customers. SmartVista allows banks, fintechs, payment services providers, bill aggregators, agency banking providers to interconnect seamlessly and offer complete interoperability of payments across various payment verticals.

Benefits

Interoperability

Wide range of payment methods

Unparalleled Security

Instant Payment Interoperability is the key

Adopting instant payments for the first time can be challenging as no system works in isolation, and the key is to ensure efficient interoperability for the service in order to demonstrate value to the end user and all participants. This is where BPC SmartVista comes to play. BPC is the best partner for instant payment projects as it has a proven success rate in delivering green field and transformation projects that required instant payment enablement. Beyond instant payment, BPC's SmartVista has been designed to answer interoperability, expandability and robustness challenges. From interoperability between banks, telecom operators and their national switch, from interoperability between large financial institutions or multi-country operations, to efficient connections with international card schemes or third party services, and the integration with government retail and business online services, BPC has experienced it all.

The widest range of Payment Methods

Customers, retail and businesses alike, expect to pay for goods and services the way they want to. Any payment, whether e-commerce, salary transfer, social benefit payment, tax collection, person-to-person can be instantly paid and settled in real-time without the requirement of going through

long clearing and settlement cycles. SmartVista promises a platform where any payments player in a country whether bank or not, can connect and send and receive payments in real-time, which are final and irrevocable. End-user can make payments using easy to remember aliases offered via the Addressing Service, that work as a proxy to IBAN, making it easy to send and receive payments without remembering or key-in long account numbers.

Unparalleled Security

SmartVista offers a real-time fraud and risk management solution that is built into the payment infrastructure, ensuring peace of mind to the payment providers from fraudulent activities. SmartVista provides an interoperable payment platform allowing regulators to make digital payments reachable to every segment of the population, benefitting all stakeholders from real-time instant payments and settlement.

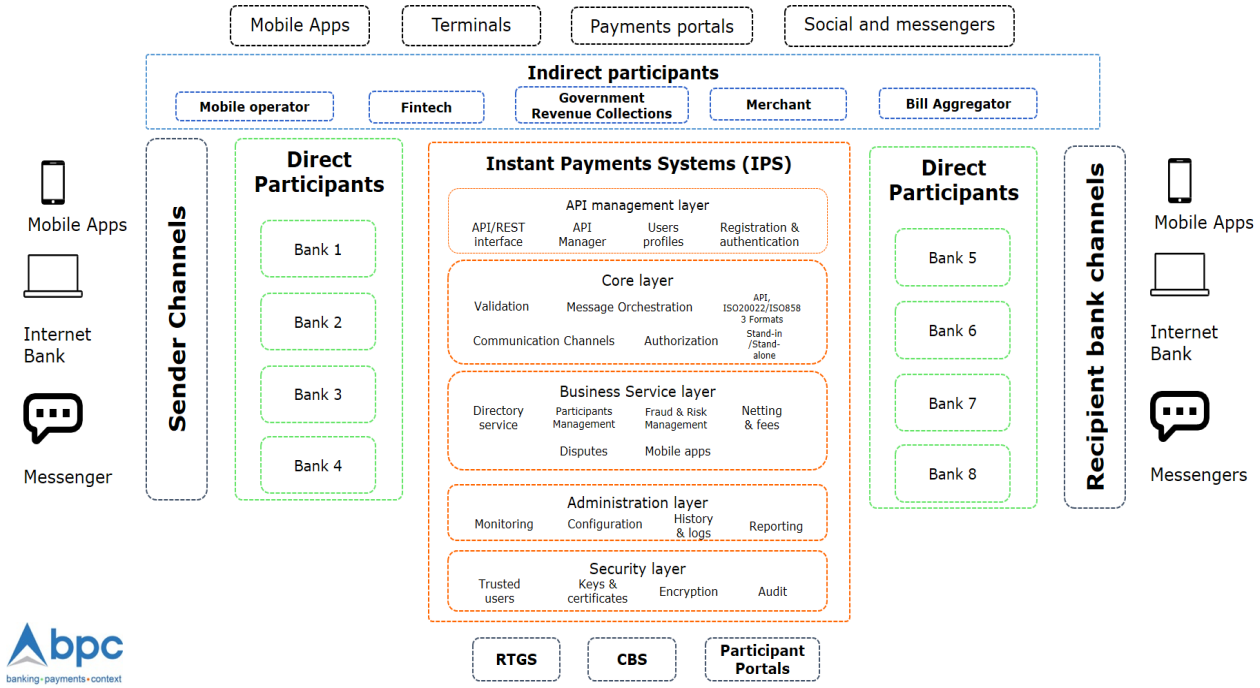
SmartVista Instant Payment System at a glance

Key Features	Payment Types by segment
Inbound and outbound instant payments 24/7/365 in less than 5 seconds Management of different message formats and CSMs Support for recalls and returns Time out management Pre-integrated with internet and mobile banking and fraud Easy integration into existing bank infrastructure Fully API enabled and, ISO 20022 compliant	**Retail customers & Businesses** **P2P** Mobile or alias peer to peer payment Cross border remittance **P2B** e/m commerce in –store POS/mPOS bill payment **B2P** salary transfer expenses, school fees, housing allowance **B2B** request for payment Cross border remittance **Governments** **P2G** tax and revenue collection **G2P** social benefits, grants health benefits **B2G** tax and revenue collection **G2B** subsidies, incentives

Payment Methods							
Online	Web	Mobile	Wallet	Wearable	ATM	NFC contactless	QR Codes

Offline	Cheque	Stand-in	Bulk File Upload

General Architecture



The SVIPS is built on layered service oriented architecture with following internal components:

API Management Layer
The SVIPS enables connectivity of Direct and In-direct participants. Both direct and indirect participants can connect to the system via the API management layer which exposed the functional APIs in any messaging framework (SOAP XML, JSON).

Core Layer
This is the core processing engine of SVIPS that provide message authentication, validation, routing and authorization features (online/Stand-in etc). The core layer is built on top of SmartVista Integration platform that provide the extensibility framework whereby clients can create or modify a business flow via user interface using Business Process Model and Notation (BPMN) tool. The core engine provide connectivity and message mapping/transformation framework whereby participant can connect using ISO 20022 or legacy format (ISO 8583).

Business Service Layer
The Business Service Layer provide participant management features. These are related to participant on-boarding, liquidity management, fee/interchange structure, settlement and dispute management. This layer provides overlay services like Addressing Service, Request-to-Pay etc. Also

the business service layer provide real-time Fraud Management and AML screening of transactions performed via the core layer.

Administration Layer
The administration layer provides monitoring and user management, audit logging, role based access control to the participant portals and internal backoffice system of SVIPS. The SVIPS reporting engine is exposed via this layer to allow operators and participant to print and export various reports.

Security Layer
SVIP offers state-of-the-art security protection of the payment platform by providing confidentiality, integrity and non-repudiation checks of real-time transaction messages exchanges among participants. The complete PKI keys lifecycle management is offered from this layer.

ISO 20022 Messaging Standard

Since the adoption of ISO 20022 international standards, the world has experienced faster cross border remittance interoperability. SmartVista is built to support ISO 20022 messaging standards and is capable to support both instant and bulk payments. The system is built on a proven technology platform with high scalability, availability and reliability endorsed by industry analyst and customers. The underlying platform supports configuration of business process on the fly where any transaction can be built by using Business Process Model and Notation (BPMN) tool. This creates a lot of flexibility for the end user to extend the system without the involvement of a vendor, which drastically reduces the time to market of new business cases and overlay services.

SmartVista is capable of processing and routing different types of ISO 20022 based transactions. The table below provide list of some of the important message types necessary for instant payments supported by the system.

Message Type	Purpose	Description
Pacs.008	FI-To-FI Credit Transfer	The financial institute to financial institute credit transfer request send from sender participant to receiver participant
Pacs.002	FI-To-FI Payment Status Report	The financial institute to financial institute payment status report is sent by the receiver party to the previous party in the payment chain informing the status of the request
Pacs.003	FI-To-FI Customer Direct Debit	The financial institute to financial institute customer direct debit is sent from receiver participant to sender participant and it is used to collect funds from sender account for a receiver
Pacs.004	Payment Return Message	The Payment Return message is sent by the receiver participant to the sender participant when the original payment request cannot be processed. This message is initiated after the settlement has taken place

Pacs.028	FI-To-FI Payment Status Request	The financial institute to financial institute payment status request is sent from participant to find the status of original transaction that was either sent or received by it
Camt.029	Resolution of Investigation Message	The Resolution of Investigation Message is sent from case assignee to case creator to inform the resolution of the case
Camt.056	FI-To-FI Payment Cancellation Request	The financial institute to financial institute payment cancellation request message is sent by case creator (receiver participant) to case assignee (sender participant) and is used to request the cancellation of original payment instruction
Pain.013	Creditor Payment Activation Request	The Credit Payment Activation Request is sent by Creditor sending party to the Debtor receiving party to request movement of funds from debtor account to creditor account. This is also known as Request-To-Pay initiation
Pain.014	Creditor Payment Activation Request Report	The Creditor Payment Activation Request Report is sent by any party that receive Creditor Payment Activation Request about the positive and negative status of its request
Acmt.023	Identification Verification Request	The Identification verification request is sent from a participant to a participant to verify an account identification information
Acmt.024	Identification Verification Report	The Identification verification report is sent in response to the Identification Verification Request message
Pain.009	Mandate Initiation Request	The MandateInitiationRequest message is used to set-up the instruction that allows the debtor agent to accept instructions from the creditor, through the creditor agent, to debit the account of the debtor
Pain.010	Mandate Amendment Request	A Mandate Amendment Request message is used to request the amendment of specific information in an existing mandate.
Pain.011	Mandate Cancellation Request	A Mandate Cancellation Request message is used to request the cancellation of an existing mandate
Pain.012	Mandate Acceptance Report	A Mandate Acceptance Report message is used to confirm the acceptance or rejection of a Mandate Request message.

Using these message types, the payment scheme proposes business flows of various uses cases.

Instant Payment Platform Core Services

Credit Transfer

The SVIPS offers credit transfer service for the following use cases:

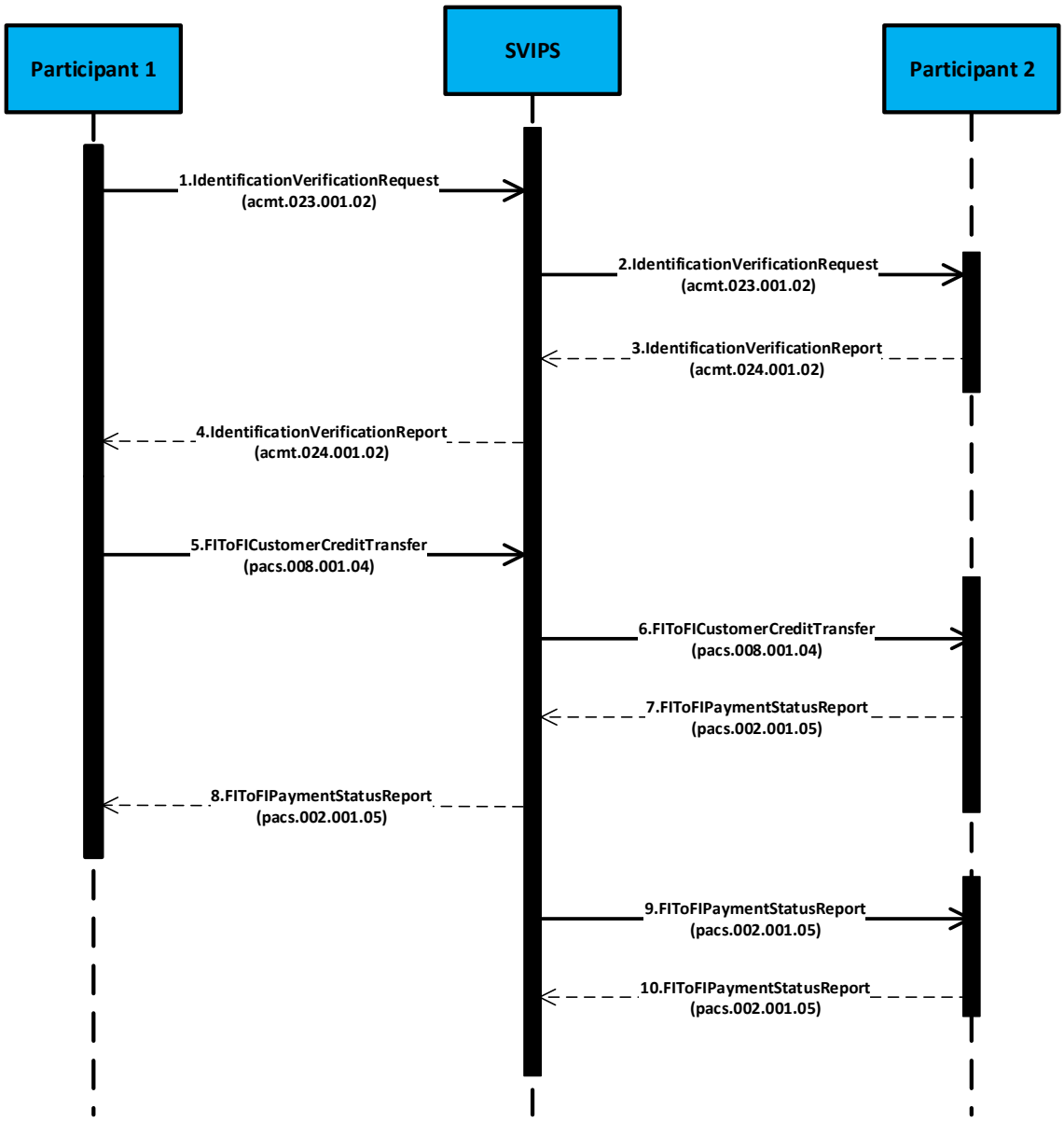
- Credit Transfer from Direct Participant to Direct Participant
- Credit Transfer from Direct Participant to Indirect Participant
- Credit Transfer from Indirect Participant to Direct Participant
- Credit Transfer from Indirect Participant to Indirect Participant

The Credit transfer end-to-end business flow initiates with account validation request which is invoked by the payer. The account validation request is initiated on either payee bank account/IBAN or if the payee participant has subscribed to the addressing services, then on his/her alias. The account validation confirms the existence of account as well as the readiness of the payee to receive funds and it returns the payee name (either full text or truncated) from the payee participant. The payer participant displays the payee name on the user channel for the customer to verify that they are about to send funds to the correct beneficiary. This validation step is necessary as it reduces the risk of payment credit to incorrect beneficiary.

If in case the payee participant has subscribed to the Addressing service then the name of the account is fetched from the service itself, rather than from the payee participant. As per CBUAE requirements, in case of bulk transfers, there are payee participants who can neither validate account status nor return account name in response. For such participants, SVIPS would return "No name" account name in response to the account validation request from the payer participant. This will provide indication to the payer that the payee participant has not verified the payee.

After account validation request, the end user initiates credit transfer request. It is routed to the payer participant from the payer channel where the customer account is debited and then a credit payment is initiated to the SVIPS. The SVIPS validates the request and forwards it to the payee participant which credits the end user account and return response (in case of a positive flow). On receiving positive acknowledgement, the SVIPS performs settlement by updating balances of respective participants and sends the payment status report to them.

The sequence flow of ISO 20022 message types is explained below:

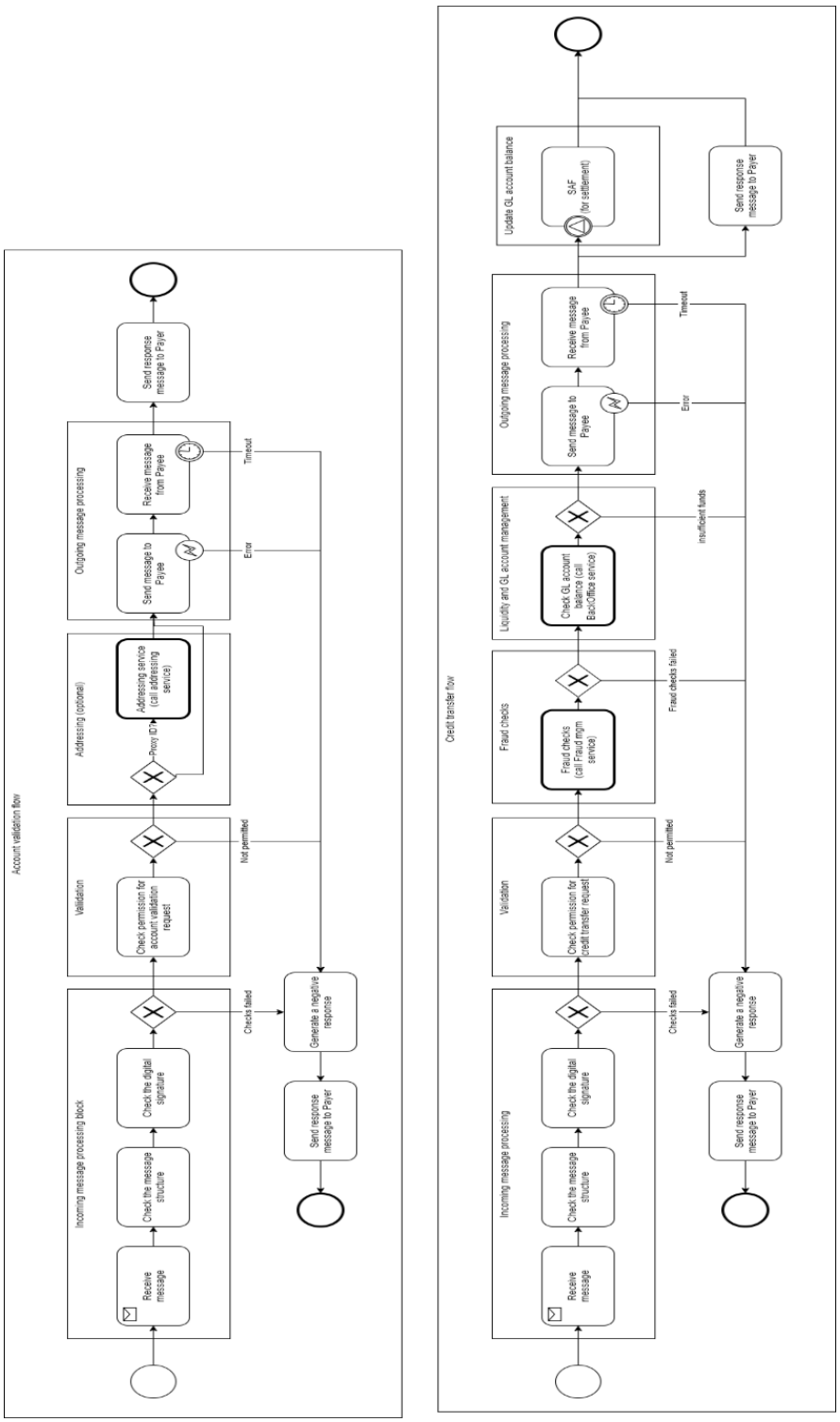


No.	Description
1	Participant 1 sends request of account verification to SVIPS
2	SVIPS identifies the alias/account, resolve the destination via BIC (bank identification code) and forwards account verification request to Participant 2
3	Participant 2 validates the account and return account details (name) to SVIPS
4	SVIPS forwards account details to Participant 1
5	Participant 1 sends Credit transfer request to SVIPS
6	SVIPS identifies the destination, validate Participant1 balance and liquidity limit and forwards request to Participant 2
7	Participant 2 credit end customer account and return positive payment status report to SVIPS
8	SVIPS update the balance and liquidity limit and forwards the payment status report to Participant 1
9	SVIPS notifies to Participant 2 indicating the settlement of funds
10	Participant 2 acknowledges the payment status report

The dataflow of how SVIPS processes a credit transfer business flow is depicted below.

1. On receiving account validation request SVIPS checks the message structure and digital signature.
2. The transaction permission is verified whether payer can initiate such request and whether payee has permission to receive this request.
3. If payee has subscribed to Addressing service then alias is verified and destination payee is identified.
4. Outgoing message is constructed and send to the payee.
5. Response is received from payee and sent to payer participant.
6. The payer proceeds with credit transfer and submits credit transfer request to SVIPS.
7. SVIPS first checks message structure and message signature.
8. SVIPS checks transaction permission of payer to send such message type.
9. SVIPS submits message to Fraud management module to check the fraud score. If fraud check fails then transaction is rejected and returned to the payer.
10. SVIPS checks liquidity balance of payer participant to verify that it has enough funds to complete this transaction. It places amount hold on the payer participant balance.
11. Outgoing message is constructed and sent to the payee participant.
12. The payee responses and if the message is successfully processed then SVIPS park settlement advice to the settlement module to post transaction amount in respective participant accounts for final settlement.

The payee acknowledgement is forwarded to the payer and optionally payment status report sent to payee informing that settlement has been completed.



Bulk Payment Flow

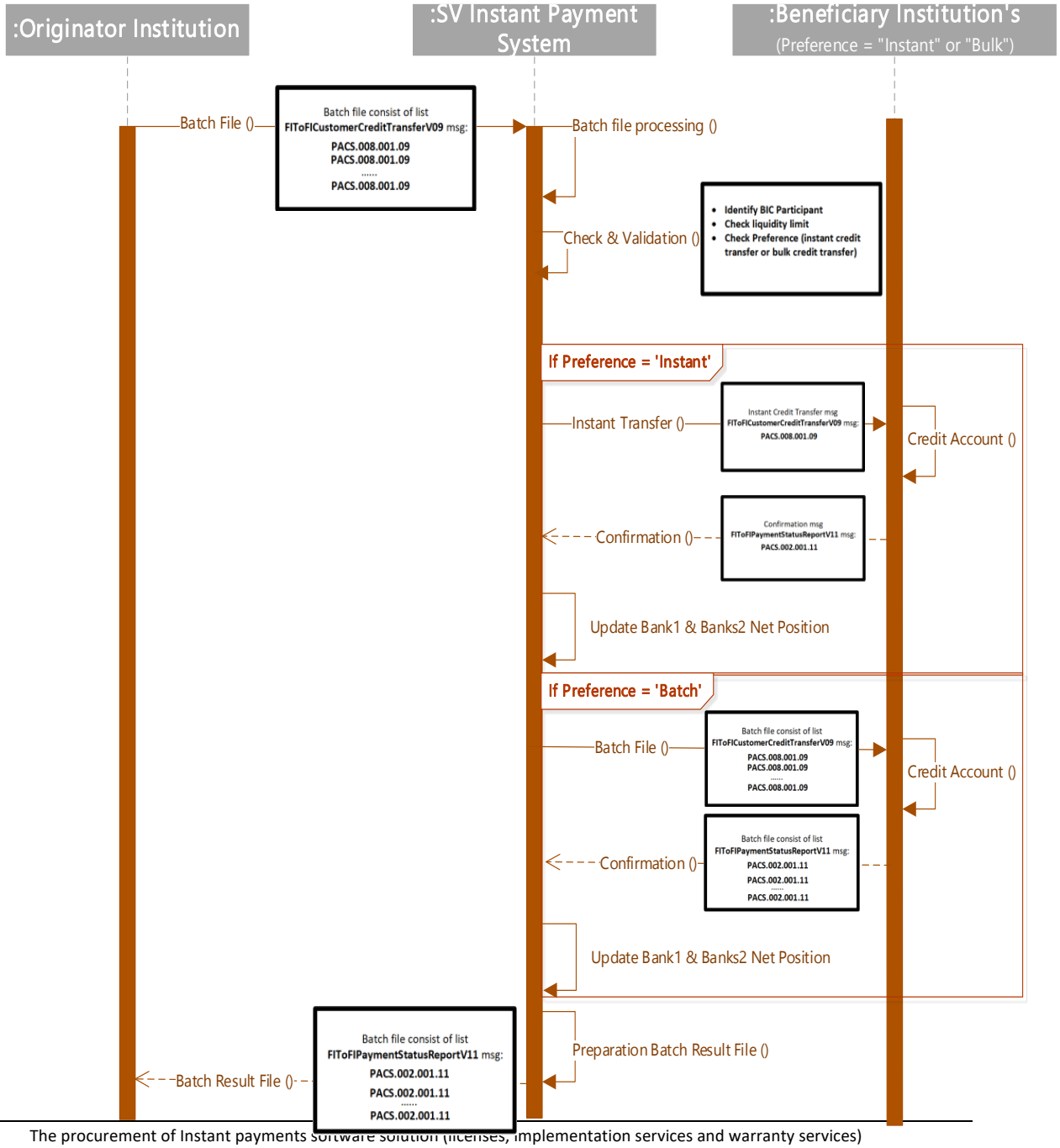
SVIPS supports payment transmission in bulk from all types of participants. The bulk messages are initiated as a file from payer participant (in case of credit transfer) or payee participant (in case of direct debit). The file is processed in SVIPS where the format specifications and business logic is checked and verified. SVIPS enable participants to choose messages transmission mechanism either as online message transmission or in a form of a bulk file transfer. Hence participant preference is checked before transmitting a message to the destination participant. The preference is enabled via the participant portal where the option to select this parameter is

available to the operator. The participants can choose on the following method to receive messages:

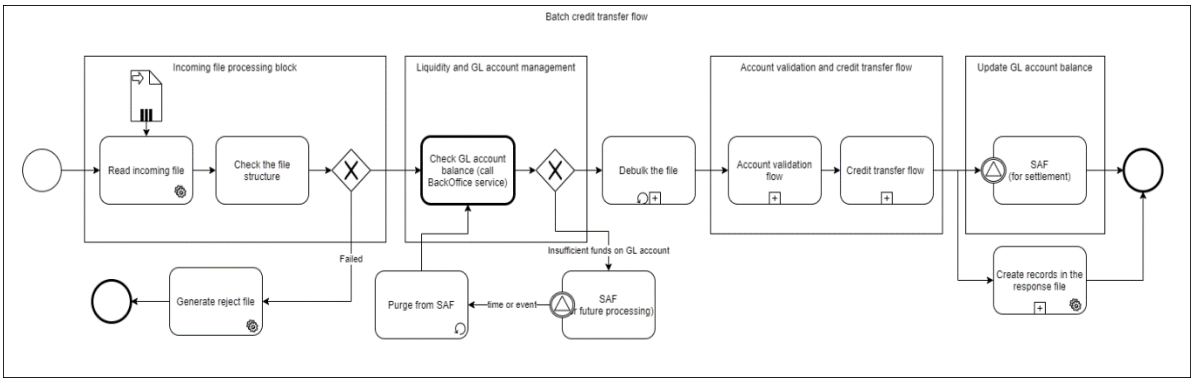
- Send Single online request
- Send Bulk request in a file
- Receive Single online request
- Receive Bulk request in a file

The bulk batch can be managed as a single transaction to the end participant or it can be de-bulked in to individual payments and transmitted. The system also allows configuration of whether to accept of reject a complete batch if few transactions in it could not be processed successfully.

The transaction sequence flow in case of bulk transmission is described below:

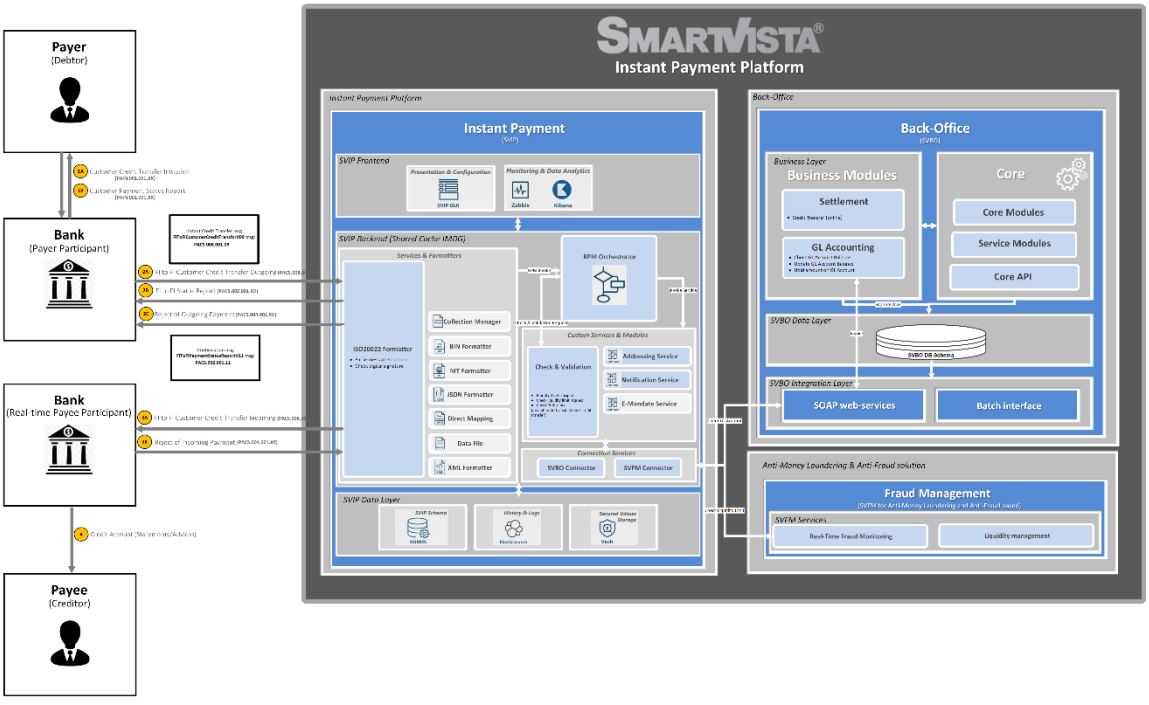


If in case the liquidity limit check returns insufficient funds in the originator account, then SVIPS places the bulk credit request in a queue waiting for the liquidity to reach sufficient level. The message is placed in a queue and then it is retried periodically waiting for the liquidity to reach optimum level of the originator. Once it reaches the level where it can be transmitted then it is sent to the destination participant.



1. The SVIPS reads the incoming file and validates its structure
2. The payer total amount in the batch is calculated and checked against the account balance. If balance is not sufficient then batch is moved in to waiting queue(SAF) and periodically checks the liquidity status.
3. Once enough liquidity is realized to run the batch then it is de-bulked and same process of account validation and credit transfer is followed for each credit instruction as described in Credit Transfer section.
4. After settlement a return file is created to the payer indicating the transactions successfully processed by the batch.

Here is a dataflow of Credit transfer transaction within SmartVista functional modules:



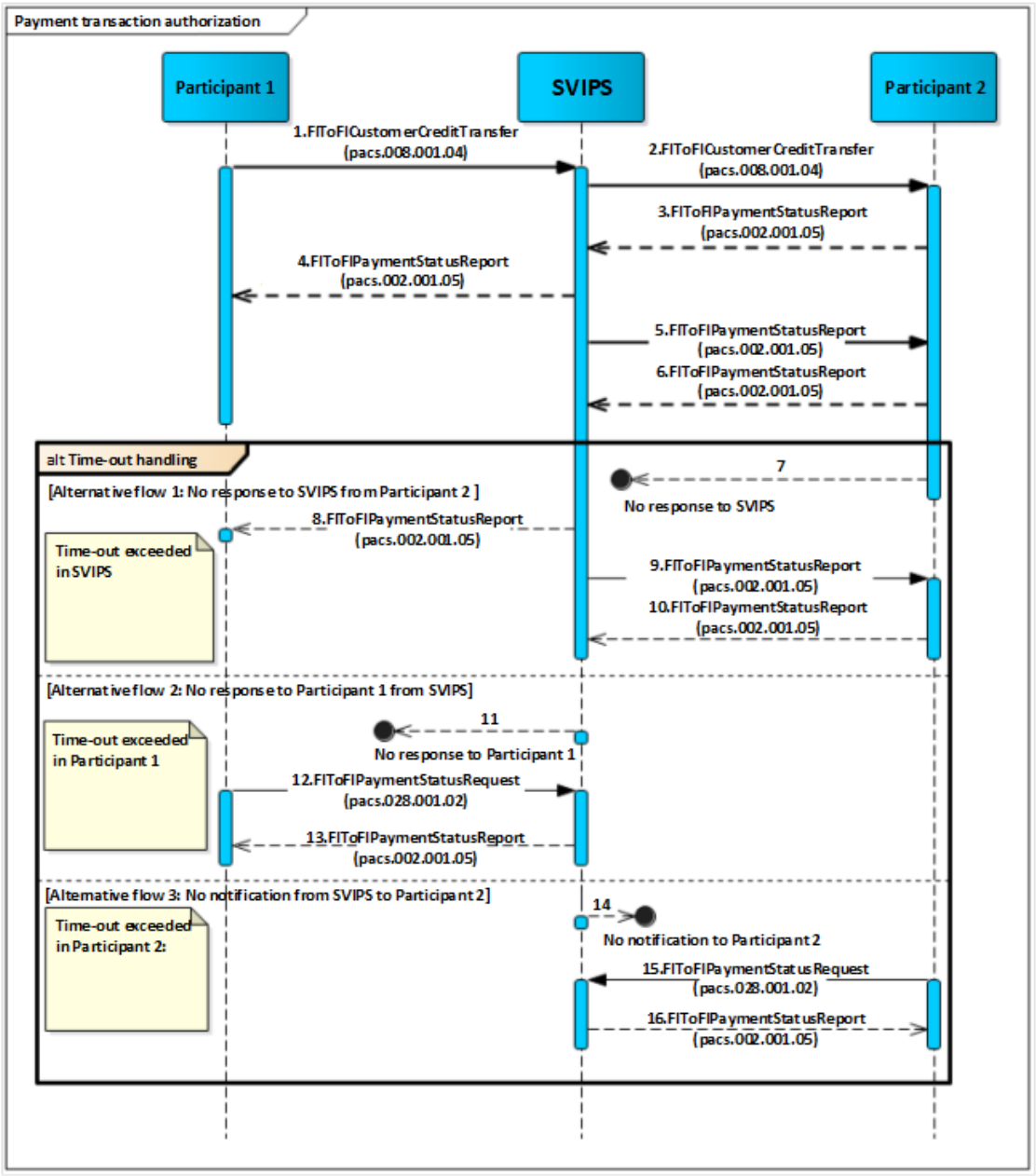
Payment Exception Flow

There can be several time out condition that needs to be managed gracefully by the system to reduce the risk of incorrect account settlement. SVIPS has robust exception flow management where the chances of settlement exceptions, are minimal. Some of the exception scenarios are:

- Payee participant credited but settlement not performed as no response received at SVIPS
- Settlement performed but payer participant could not receive payment status report
- Settlement performed but payee participant could not receive payment status report

These conditions are gracefully managed by specifying timeout values among various transaction steps. Hence, whenever a timeout condition is encountered, then as per scheme rules the exception management is triggered by relevant parties involved in the transaction.

Below is the payment exception flow description:



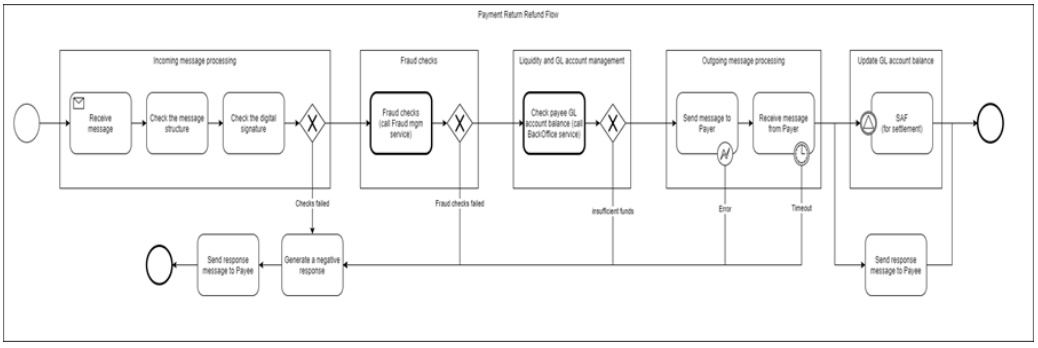
No.	Description
Main Flow Successful	
1	Participant 1 sends Credit transfer request to SVIPS
2	SVIPS identifies the destination, validate Participant1 balance and liquidity limit and forwards request to Participant 2
3	Participant 2 credit end customer account and return positive payment status report to SVIPS
4	SVIPS update the balance and liquidity limit and forwards the payment status report to Participant 1
5	SVIPS notifies to Participant 2 indicating the settlement of funds
6	Participant 2 acknowledges the payment status report
Alternative Flow 1	
7	Message from Participant 2 fails to reach SVIPS due to network problem
8	SVIPS waits for a particular timeout and then send negative Payment Status Report to Participant 1
9	SVIPS sends negative Payment Status Report to Participant 2 so in case it has credited customer account then it can reverse it
10	Participant 2 acknowledges Payment status report
Alternative Flow 2	
11	Message from SVIPS fails to reach Participant 1 due to network problem
12	Participant 1 sends Payment Status request to SVIPS inquiring about the status of the original message sent in Step 1
13	SVIPS responds with the status of the original transaction
Alternative Flow 3	
14	SVIP notification to Participant 2 does not reach it due to network problem
15	Participant 2 sends Payment Status request to SVIPS inquiring about the settlement status of the original message sent in Step 1
16	SVIPS responds with the status of the original transaction

Payment Return/Refund

Participant may request a return or refund of payment which can be triggered by the customer or merchant due to reasons defined by the scheme. Some of the typical cases are:

- incorrect amount received or sent
- amount sent to incorrect beneficiary
- fraudulent transaction performed on user account

In such cases these transaction are initiated as a result of a dispute management lifecycle where the case reaches its conclusion as per the scheme rules. Usually a direct participant(settling participant) operates the payment return service on behalf of its indirect participant (clearing participant) to settle a disputed transaction. However SVIPS also allows indirect participant to initiate return with proper permissions and limits on their usage of this service.



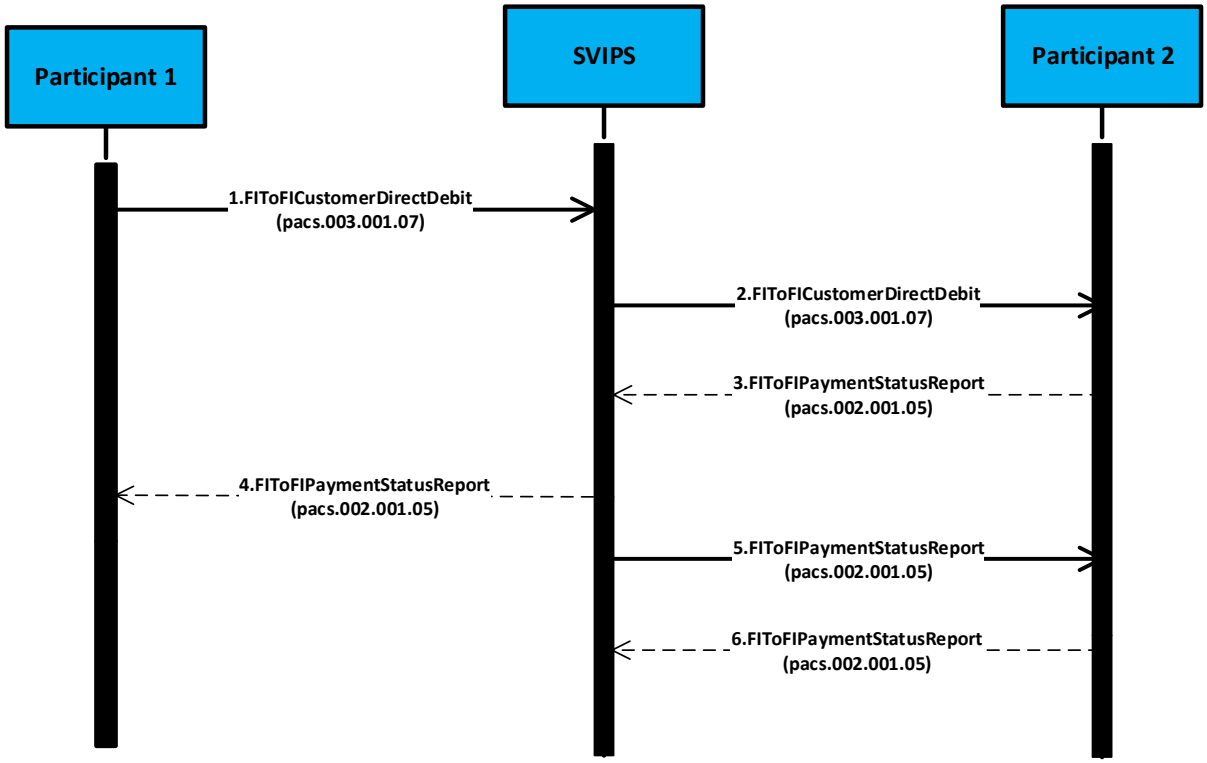
he Payment return follows similar flow as credit transfer. The only difference is that the return is initiated by the original payee to the original payer. The message is initiated using either ISO20022 pacs.004 or camt.056 message types

Direct Debit (optional service)

SVIPS offers Direct Debit service for both direct and indirect participants. The service requires that participant establish a mandate whereby both creditor and debtor has agreement on the purpose, frequency and duration of the direct debit instruction. Using the permission set in SVIPS, a participant can initiated Direct Debit directly through the platform without having an E-Mandate registered in the system. E-Mandate as an overlay service is optional feature for participant subscription. In absence of E-Mandate defined on the central infrastructure, the scheme would mandate participant to agree on the terms bi-laterally. If in case participant subscribed to eDDA service then SVIPS would perform the business logic check on the existence of E-Mandate and special conditions associated with it and on validation would proceed with the direct debit instruction.

The Direct Debit would not check the terms of E-mandate when it is invoked, as it would be the domain of the creditor and debtor.

Direct Debit service can be invoked a single real-time request or in a form a batch file that can be uploaded in SVIPS for processing.

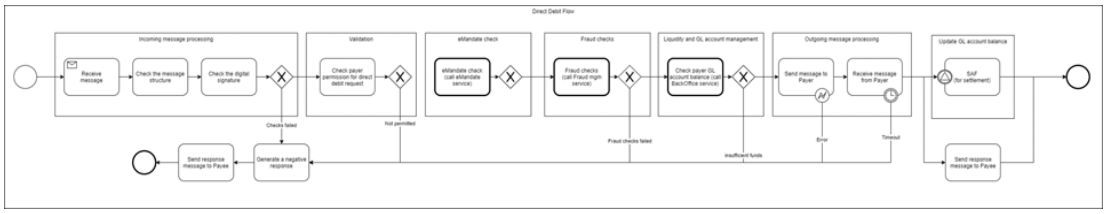


No.	Description
1	Participant 1 sends Direct Debit request to SVIPS

2	SVIPS identifies the destination, validate Participant2 balance and liquidity limit and forwards request to Participant 2
3	Participant 2 debits end customer account and return positive payment status report to SVIPS
4	SVIPS update the balance and liquidity limit and forwards the payment status report to Participant 1
5	SVIPS notifies to Participant 2 indicating the settlement of funds
6	Participant 2 acknowledges the payment status report

The business process flow is described below:

1. SVIPS first checks message structure and message signature.
2. SVIPS checks transaction permission of payer to send such message type.
3. SVIPS checks the existing of E-mandate against the direct debit transaction. If all business logic checks passed validation then would proceed to next step.
4. SVIPS submits message to Fraud management module to check the fraud score. If fraud check fails then transaction is rejected and returned to the payer.
5. SVIPS checks liquidity balance of payer participant to verify that it has enough funds to complete this transaction. It places amount hold on the payee participant balance.
6. Outgoing message is constructed and sent to the payer participant.
7. The payer responses and if the message is successfully processed then SVIPS park settlement advice to the settlement module to post transaction amount in respective participant accounts for final settlement.
8. The payer acknowledgement is forwarded to the payer and optionally payment status report sent to payer informing that settlement has been completed.

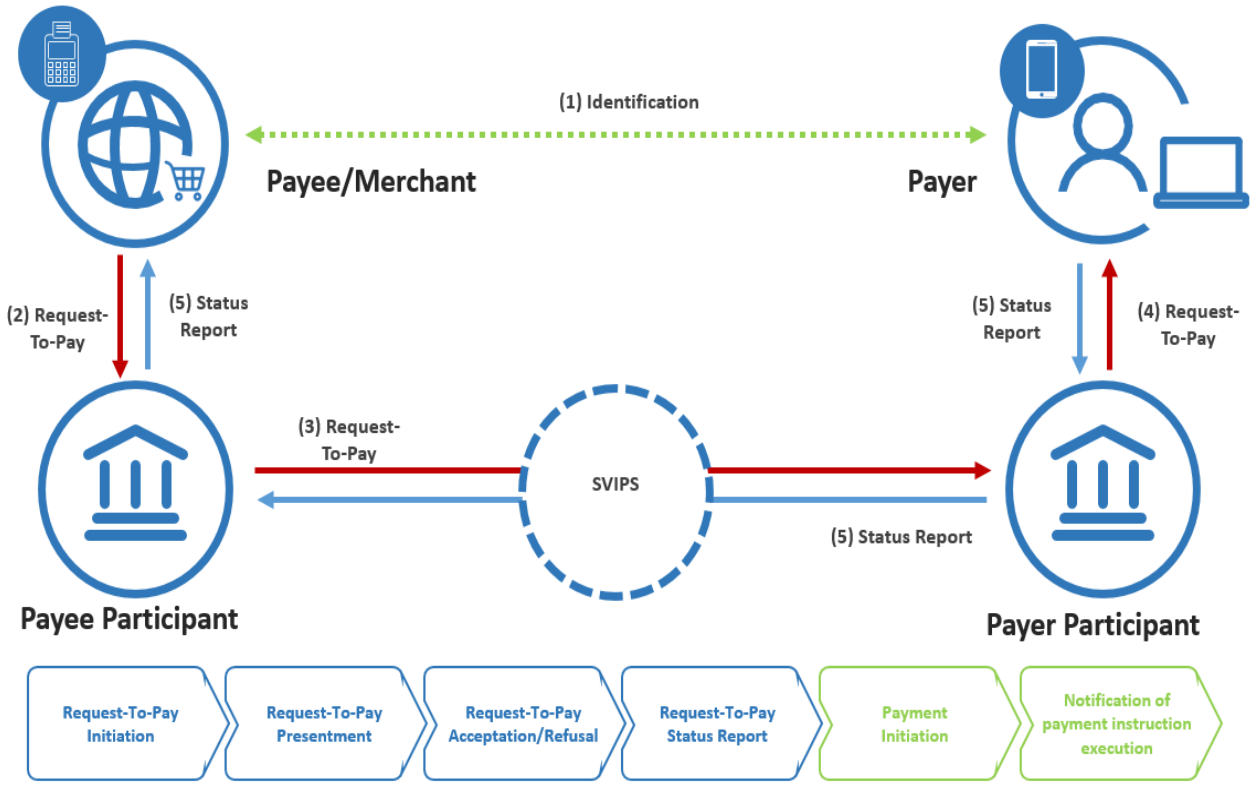


Instant Payment Platform Overlay Services

Request-To-Pay

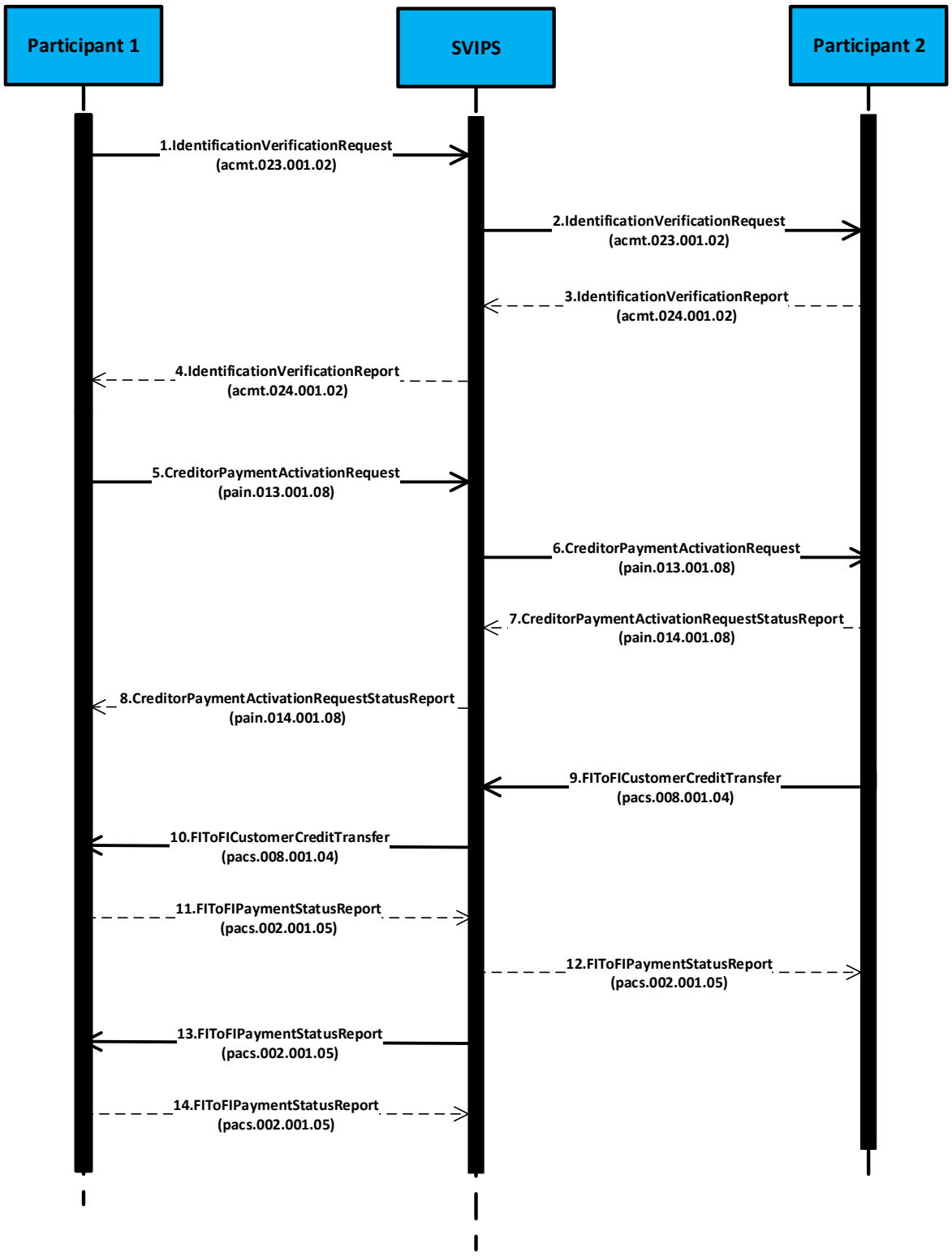
Request-To-Pay is a highly innovative overlay service that enables payee to request for funds from the payer. In other words payee can pull funds from the payer account after authorization and authentication from the payer end-user.

SVIPS follows a typical 4-corner model for Request-To-Pay overlay service.



The end-to-end business flow starts with payee verifying account information of the payer by initiating account validation request. In response, the payee receives the payer confirmation of account status indicating that it is active. The next step is for the payee to initiate Request-to-pay message to the payer participant, which is then notified to the payer end user. The payer participant sends acknowledgement of receipt and subsequently the acceptance of Request-to-pay from the payer end-user.

After the transmission of Request-to-pay acknowledgement, the payer participant initiated credit transfer to the payee participant. The same process flow of single credit transfer transaction is initiated to complete the Request-to-Pay business flow.

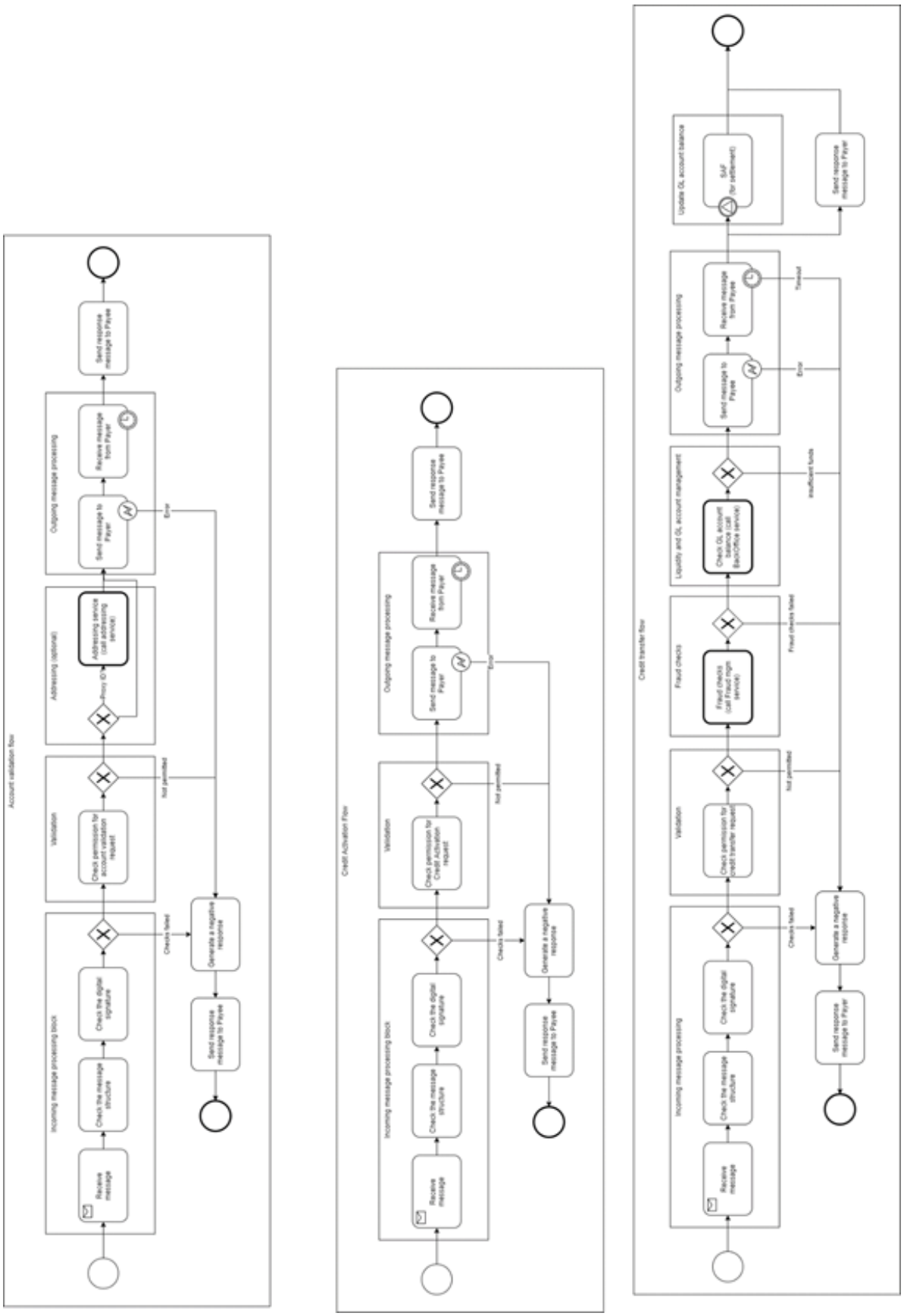


No.	Description
1	Participant 1 sends request of account verification to SVIPS
2	SVIPS identifies the alias/account, resolve the destination via BIC (bank identification code) and forwards account verification request to Participant 2
3	Participant 2 validates the account and return account details (name) to SVIPS
4	SVIPS forwards account details to Participant 1

5	Participant 1 sends Credit Payment Request to SVIPS requesting funds
6	SVIPS validates request and forwards it to Participant 2
7	Participant2 acknowledges Credit Payment Request to SVIPS, allowing funds transfer
8	SVIPS forwards Participant 2 acknowledgment to Participant 1
9	Participant 2 sends Credit transfer request to SVIPS
10	SVIPS identifies the destination, validate Participant 2 balance and liquidity limit and forwards request to Participant 1
11	Participant 1 credit end customer account and return positive payment status report to SVIPS
12	SVIPS update the balance and liquidity limit and forwards the payment status report to Participant 2
13	SVIPS notifies to Participant 1 indicating the settlement of funds
14	Participant 1 acknowledges the payment status report

The business process flow of Request-To-Pay is depicted below:

1. SVIPS checks the message structure and digital signature
2. The payee validates the payer account via Account validation request
3. The transaction permission is verified whether payee can initiate such request and whether payer has permission to receive this request.
4. If payer has subscribed to Addressing service then alias is verified and destination payer participant is identified.
5. Outgoing message is constructed and send to the payer.
6. Response is received from payer and sent to payee participant.
7. The payee initiated Credit activation request to SVIPS
8. SVIPS check the message structure and digital signature
9. The SVIPS checks message permission of payee for initiating Credit activation request; whether payee and payer has subscribed to the Request-To-Pay overlay service
10. The message is constructed and sent to the payer
11. The payer acknowledges the request and initiated credit transfer message
12. The same credit transfer business flow is initiated as described in Credit transfer section but without payee account validation



Payment Acceptance and Transmission Criteria:
There is a number of options to accept and transmit Request to Pay service in SmartVista.

Request now and Pay Now	Request now and Pay Later	Request later and Pay now	Request later and Pay later
The payee requests for the payment and the payer immediately accept the request and transfer funds	The payee request for the payment and the payer immediately accepts the request. The transfer of funds takes place later	The payee request for the payment. The payer does not accept immediately but later based on some business criteria. Once accepted the payment is immediately made to the payee	The payee request for payment. The payer does not accept the request immediately but later based on some business criteria. The payment is scheduled to be initiated later

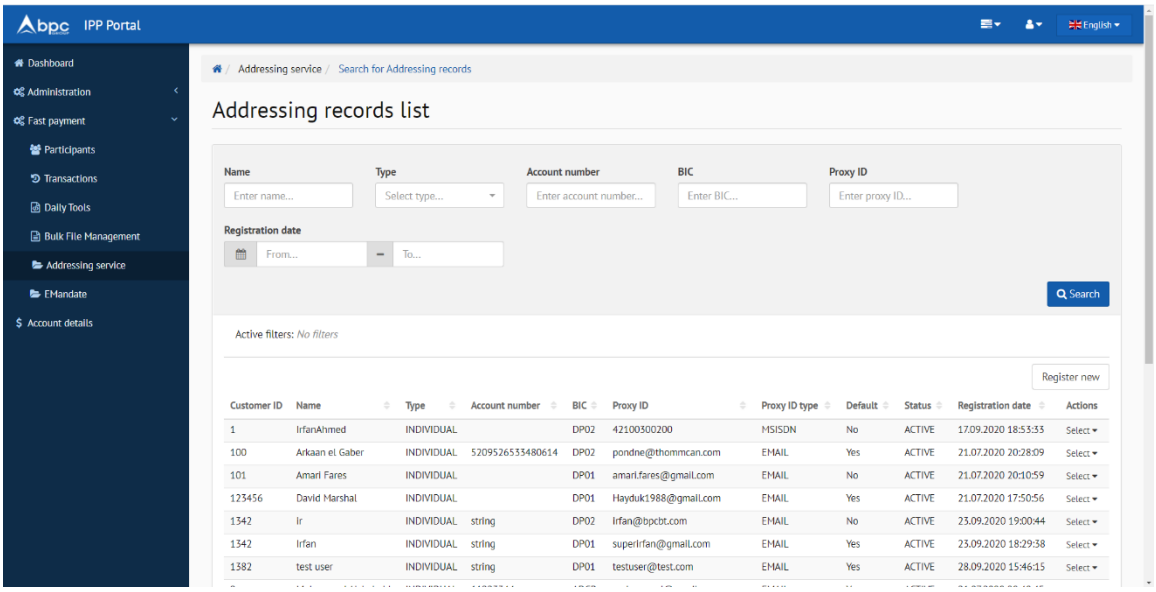
Various uses cases of Request to Pay can be offered to participants considering the above acceptance and transmission criteria. For example

- Instant payment from merchant to customer
- Payment Guarantee from merchant to Customer
- Pre-authorization request from merchant to customer
- Payment in installments
- Payments in the future
- Change of amount of a payment

Addressing Service

Addressing services also known as Directory Service is one of the overlay services offered by SVIPS. The Directory service is used to resolve destination bank and customer credentials based on an easy to remember alias defined by a customer. The SVIPS Directory service support the definition of easy to remember Aliases whereby customer can choose their mobile number, email address, social media ID, National ID, or any open text that they desire as their alias. The alias however, should be unique for a participant institute. The types of aliases supported are:

- Bank ID
- Account ID
- Card Number
- Mobile Number (MSISDN)
- Mobile Wallet
- Email
- Passport ID
- Social Security ID
- E-Wallet ID
- Free Text



The Directory services let a customer define a single alias to several banks. For example if a customer has account in Participant A and Participant B, then a single alias (eg. mobile number) can be used as an identifier to both of these participants. However customer is required to set a default record so that when a transaction reach SVIPS with the alias belonging to two different participants then it can decide which destination it should be routed.

Types of Directory Service Schemes

SVIPS offers following types of Directory services scheme:

- **Centralized Directory Service** – Customer information like alias, customer ID, Participant Identification code, Account number, Customer Name is stored in the directory. A record

is registered once by the customer using participant channels and it can be modified as well. All verification is taken centrally via the Directory service without the need to inquire with the participant about the validity of an alias

- **Federated Directory Service** – Minimal information of customer like alias, Participant Identification code is stored in the Directory service. For any further verification of customer credentials (Name, Customer ID, etc) the information is fetched from the participant

SVIPS Directory service allows participant end users to change their alias by sending a modification request through participant channels. A customer can also request to move its alias from one participant to another. Such request needs to be verified by the participant before invoked to the SVIPS. Alias can have following statuses:

- Active – Alias is active and return customer information
- Frozen – Alias is not active but return positive response on the availability of customer. The customer information is not returned
- In-active – Alias is inactive and cannot be reactivated

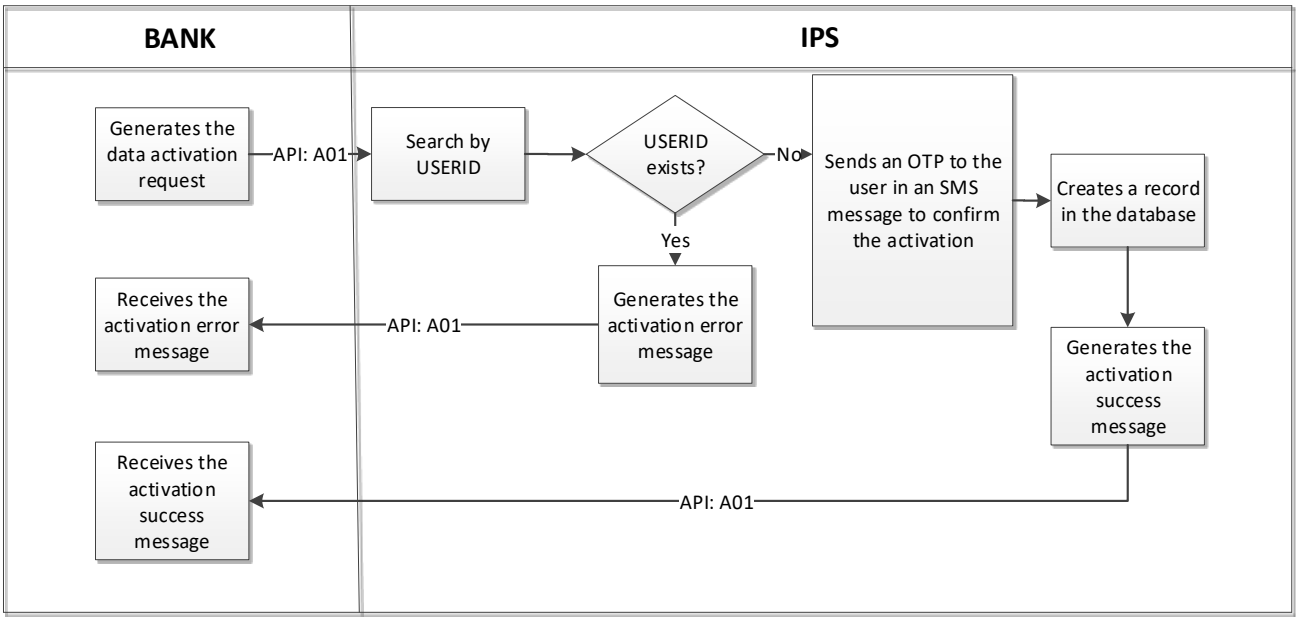
Alias Expiry and Non-usage

SVIPS Directory Service offers usage tracking of aliases used by customer. The system has a parameter which defines the number of days since alias was used. In case of no usage for a specified period the alias status can be set as not active. Directory service also maintain an expiry period where in case alias is not used till the expiry it is marked in-active and can be purged from the service allowing it to be available for registration.

Alias Registration Process

The following process is typically followed when customer registers an alias on Directory Service:

1. Using a particpant's channels and tools provided by the bank, the user sends the registration request to the participant. The user must include a user identifier that is going to be used as a user simplified identifier in the request.
2. The bank redirects this request to SVIPS (operated by the IPP scheme).
3. SVIPS checks if the received user identifier already exists in its Directory service database.
4. If the user identifier does not exist in the database (i.e. the user is not registered), SVIPS associates it with the BIC of the bank that redirected the registration request. At this point, the user identifier becomes the user simplified identifier that has the default BIC associated with it. Next, SVIPS sends a one-time password to the user's mobile phone to confirm the registration. If the user registration is successful, the user can only change the BIC that is associated with his user's simplified identifier via the participant channel.
5. After the registration data verification is completed, SVIPS informs the requesting participant about a successful registration. Now, whenever participants use the Addressing Service for the user simplified identifier, SVIPS will provide the default BIC associated with it.
6. The registration data modification flow is provided below:



Specific Use Aliases

SVIPS Directory service has a feature that maintains a list of aliases that are reserved for specific end users. For example aliases that resemble short code of a bank, corporate bodies, and regulatory authorities can be reserved for their respective owners and may not be made available. This special list is maintained in the Directory services allowing alias creation other than the one listed in it.

Directory Service Housekeeping

The Directory service maintenance is available from the participant portal where participant operation staff can perform housekeeping tasks on their aliases defined by their customers. Operations like adding an alias, modification and deletion is supported from the portal. Also changing alias from one user to another is also provided. Participants can inquire the complete addressing relationship of its customer within its institute via the participant portal that list all the existing aliases of customers registered.

All the housekeeping functions of directory management are exposed as APIs to the participant so that their channels can initiate these requests and perform any maintenance task that they require.

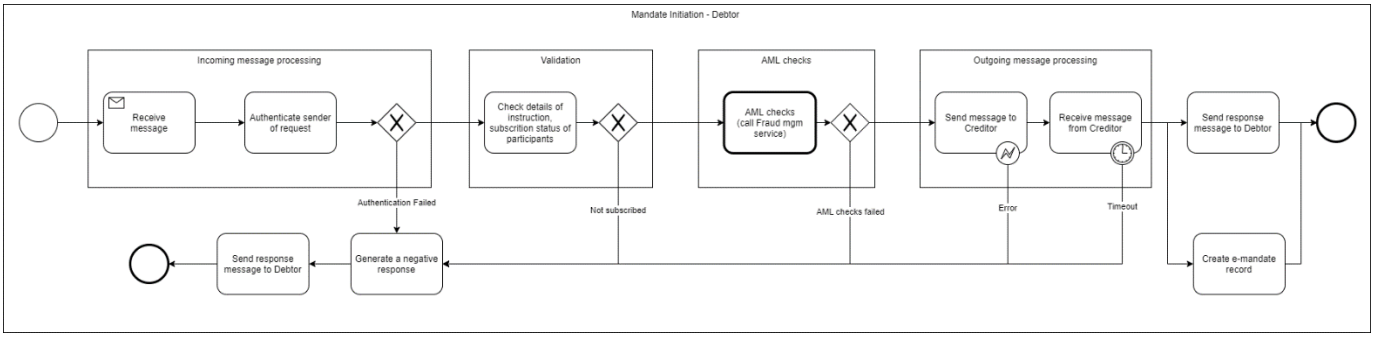
E-Mandate Management (optional)

The E-mandate Management is part of SVIPS overlay services that manages the processing of Direct Debit Authority mandate creation, modification, suspension and cancellation. Mandates are used for further direct debit flows and guarantees that the Payer has an agreement and approves debiting of it funds on its behalf. E-Mandate service is built based on the ISO20022 specifications.

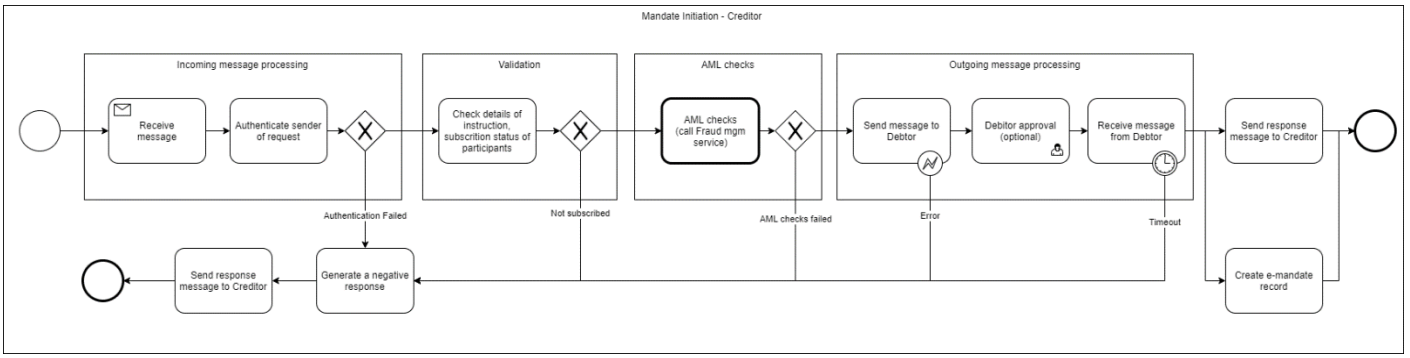
E-Mandate Initiation

E-Mandate can be initiated by the Creditor participant (Mandate Initiation Request by Creditor - Simplified mode in CBUAE terminology) and confirmed by the Debtor participant end-user. It can also be created by the Debtor end-user (Mandate Initiation Request by Debtor - Standard mode in CBUAE terminology).

Business process of E-Mandate creation from Debtor:



Business Process of E-Mandate creation from Creditor:



E-Mandate Amendment

E-Mandate can be amended if the party wants to change the information of existing mandate (with the unique reference to it). The amendment can be initiated both by creditor or debitor. However any amendment requires authorization from the debitor.

E-Mandate cancelation / suspension

E-Mandate cancellation and suspension actions are used when the party wants to cancel the existing mandate ((with the unique reference to it) or suspend it for a while. The initiator of a Mandate Suspension can be either the debtor or the creditor.

E-Mandate acceptance report

E-Mandate acceptance report is used as a response to the mandate request messages of all types, as it returns the confirmation or rejection of the request.

E-Mandate Processing Types

SVIPS supports of two types of E-Mandate management

- Single request
- Multiple request (batch with the de-bulking)

E-Mandate statuses and tracking

SVIPS provides a holistic view on the mandates status and keeps record of all the changes which were done with the mandate (lifecycle). It also has a pre-configured set of statuses, which can be extended by configuration:

- Valid / Active
- Suspended
- Cancelled
- Rejected
- Expired

E-Mandate Expiration principles

E-Mandate record can have an expiration date which can be defined by the E-mandate owner or can have default value. Expiration can be extended with the Amendment request.
For the mandates which were not used for the certain period of time, they can be suspended for reaching the expiry date.

E-Mandate Types

- one time
- recurrent

E-Mandate data structure (fields)

SVIPS stores a set of mandatory fields related to the mandate. Fields can be extended by configuration. Set of standard fields configured in the system

- Message related information
  - MessageIdentification
  - CreationDateTime
- Initiator information
  - InitiatingParty
  - Name
  - PostalAddress
  - StreetName
  - BuildingNumber
  - PostCode
  - TownName
  - Country
- Mandate related information
  - Mandate Name

- MandateIdentification
- MandateRequestIdentification
- Type
- ServiceLevel
- Code
- LocalInstrument
- Code
- Occurrences
- SequenceType
- Frequency Type
- FirstCollectionDate
- FinalCollectionDate
- CollectionAmount
- TrackingIndicator

- Creditor related information
  - Creditor
  - Name
  - CreditorAccount
  - Identification
  - IBAN
  - CreditorAgent
  - FinancialInstitutionIdentification
  - BICFI
- Debtor related information
  - Debitor
  - Name
  - DebtorAgent
  - FinancialInstitutionIdentification
  - BICFI
  - Ultimate Debtor
  - Name
- Document information
  - ReferredDocument
  - Number
  - RelatedDate
- Amendment details
  - UnderlyingAmendmentDetails
  - AmendmentReason
  - Originator
  - Name
  - Reason
  - Proprietary
  - Mandate

  - MandateIdentification
  - TrackingIndicator
- System related information
  - Unique Record ID
  - LastUpdate
  - ChangeHistory
  - LastUsage
  - UsageHistory
  - Status

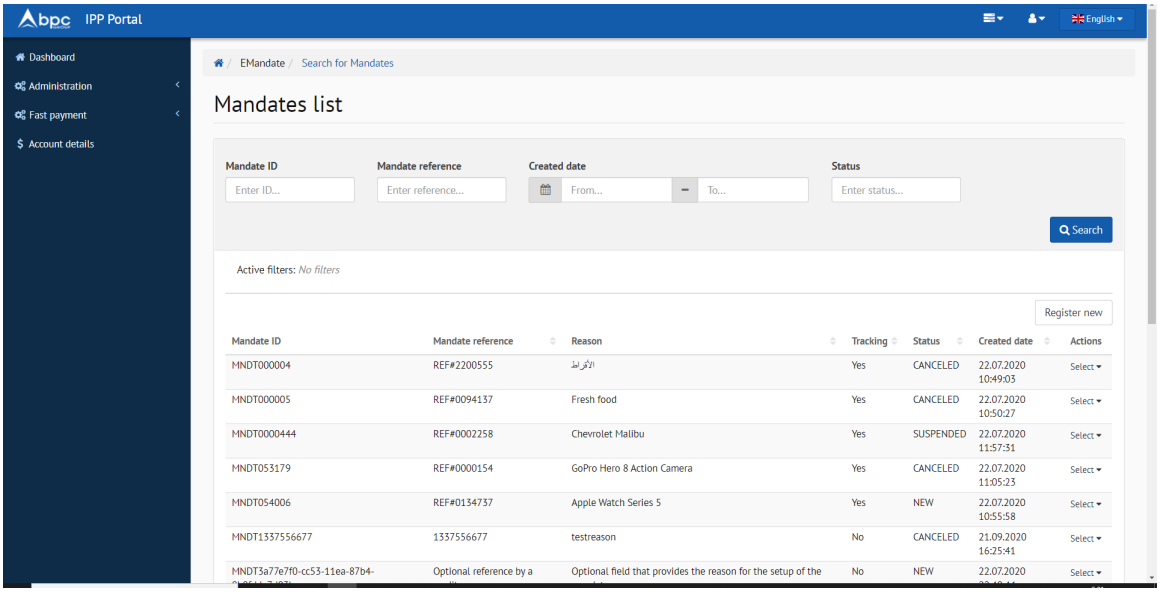
E-Mandate Service Reporting

SVIPS has an embedded reporting engine, which allows creating user-defined reports out of the information stored in the database. System comes with the set of standard reports like:

- List of active mandates with the statuses
- List of newly created mandates
- List of updated mandates
- List of unused and suspended mandates

E-Mandate GUI

SVIPS offer user screens which allow to view and manage E-mandates create by participant from the participant administrator portal.



Instant Payment Platform Value-Added Services

Fraud and Risk Management System (optional)

BPC's Fraud Management module helps participants detect and prevent fraud across all payment channels, in real-time.

Fraud Management module covers real-time transaction monitoring and allows performing statistics profiling on any level – customer, terminal, card, merchant or device. The analytics tool includes a robust business-driven rules engine for transaction scoring and applies machine learning techniques for fraud analytics and modeling. A dashboard gives an operator real-time insights into key statistics. When transactions are identified as fraudulent, the system operator can use the enterprise case management capability to handle fraud cases. SmartVista Fraud Management supports alerts generation through multiple channels, including SMS or e-mail.

Fraud Management module comes with a powerful rules engine. **Each transaction is validated against a set of user defined business rules, which can monitor hundreds of parameters – ranging from simple checks such as transaction location to more sophisticated validations based on the card's historic transaction profile.** Rules can be created at any level, from individual customers to customer segments, for groups of merchants or groups of channels. The outcome of each validation is a value – indicating the risk level of the transaction.

- Powerful and Easy to Use Rules Engine
- Streamlined Case Management
- Supporting online (realtime) prevention, near-online and offline fraud detection
- Covers PSD2 requirements and ensures RBA
- Omni channel fraud management
- Alerting and reporting capabilities
- Optional neural capabilities
- Up to 2,000 transactions per second

Deployable as a stand-alone module, or as part of a larger project, Fraud Management can be deployed extremely quickly, speeding the return on your investment.

In the following table you may observe the general areas and functions offered, which will allow better control in way to reduce payment-related fraud and financial loss.

Area	Function
Prevention and detection functionality	Our fraud management service provides functionality for checking, analysing, and handling authorizations in the • online • near-online • offline modes and transactions in offline mode
Channels and transaction types	Following channels and type of transactions can be monitored • Direct Participants • Indirect Participants • payments on all types • card-based • non-card based Supported types on interfaces for online interactions: • ISO 20022 • ISO-8583 • SOAP • HTTP/JSON For offline interactions: • XML
Comprehensive analysis	Transactions and events analysis against • black and white lists • custom configured fraud lists • rules • statistics profiles • machine learning (ML) models
Models management	Before applying a rule to production environment, it can be tested against historic data with following outputs: • testing data set statistics • rule triggered • detected fraud • false positive Statistics profile structure can be changed via GUI. Machine learning models (ML) built externally can be uploaded to the system in the supported format and used for transactions scoring.
Alert and case management	Handling of suspicious and fraudulent transactions by operators via web interface. Features of the case management: • all information on a monitored entity is shown at one form

	• actions can be taken right from the case management form, incl. data export, sending SMS/email notifications, adding a card to black list etc. • operator can work with all alerts and transactions of the alerted entity • data from different channels is aggregated and shown at the form • actions taken by operators during investigation are logged and saved to the investigation history • marking fraudulent transactions • based on fraudulent transactions lost money and prevented losses are calculated
Custom configuration	Users can change parameters and do custom configuration for different objects in the system at any time, including • online channels • transaction attributes • rules • reactions • lists • statistics profiles • filters and displayed columns, sorting • transactions colouring
Notification interfaces with external systems	Templates and recipients for SMS and email notifications in automatic or manual modes are fully customized
Multi-institution and multi-channel support	Data for analysis can be obtained via different channels with support for data separation between institutions
Report generation	Built-in reporting engine provides functionality for executing default and custom reports
Analytical tools	Dashboard and widgets for data visualization and showing key business metrics for proper decision making, including • fraud intensity • fraud MCCs • fraud MCC groups • fraud by terminals • fraud by merchants • fraud by countries • fraud by type • performance monitor • rule efficiency (for fraud detection) • saved/lost money • fraud detection metrics • actual fraud detection metrics
Machine Learning and Neural Networks	As fraud detection becomes more complex due to the increasingly complex payments ecosystem and more data becomes available, the evolution towards Machine Learning for fraud detection is a logical next step. Statistical and Machine Learning based risk scoring improves throughput and improves scalability when running in an environment of vast data. This does not completely eliminate the need for a human interference, which is still required for investigations and spot checks.

	SmartVista Fraud Management can apply Machine Learning to analyse payment transactions in (near) real time. Once the machine is trained to identify suspicious transactions, based on an extensive set of historical data, it can be used to analyse payment transactions across multiple axis.

Anti Money Laundering Module

Anti-money laundering (AML) module is part of SmartVista Fraud Management (SVFM). It helps banks in preventing the use of the financial system for the purposes of money laundering or terrorist financing.

SVFM provides checking of a payment transaction against different pre-loaded lists according to compliance regulations, including UN, EU, OFAC sanctions lists. Any new list (for ex., sanctioned persons and organizations, terrorists, politically exposed people (PEP), local state lists) can be configured via the SVFM web-interface and can used in rule checks. This does not require any online interfaces with external data sources.

SVFM in combination with SmartVista Integration platform (SVIP) can provide online interfaces to external databases and services, like Dow Jones, Thomson Reuters, Spark Interfax and others. In this case a payment processed by SVIP first, enriched with the data from external sources, and then goes to SVFM for analysis and scoring. The advantage of the approach is that data for analysis is always updated in the 3-rd party databases and services and not managed by the bank, while logic of checks and decision making is on bank's side thanks to SVFM.

Reports and Analytics

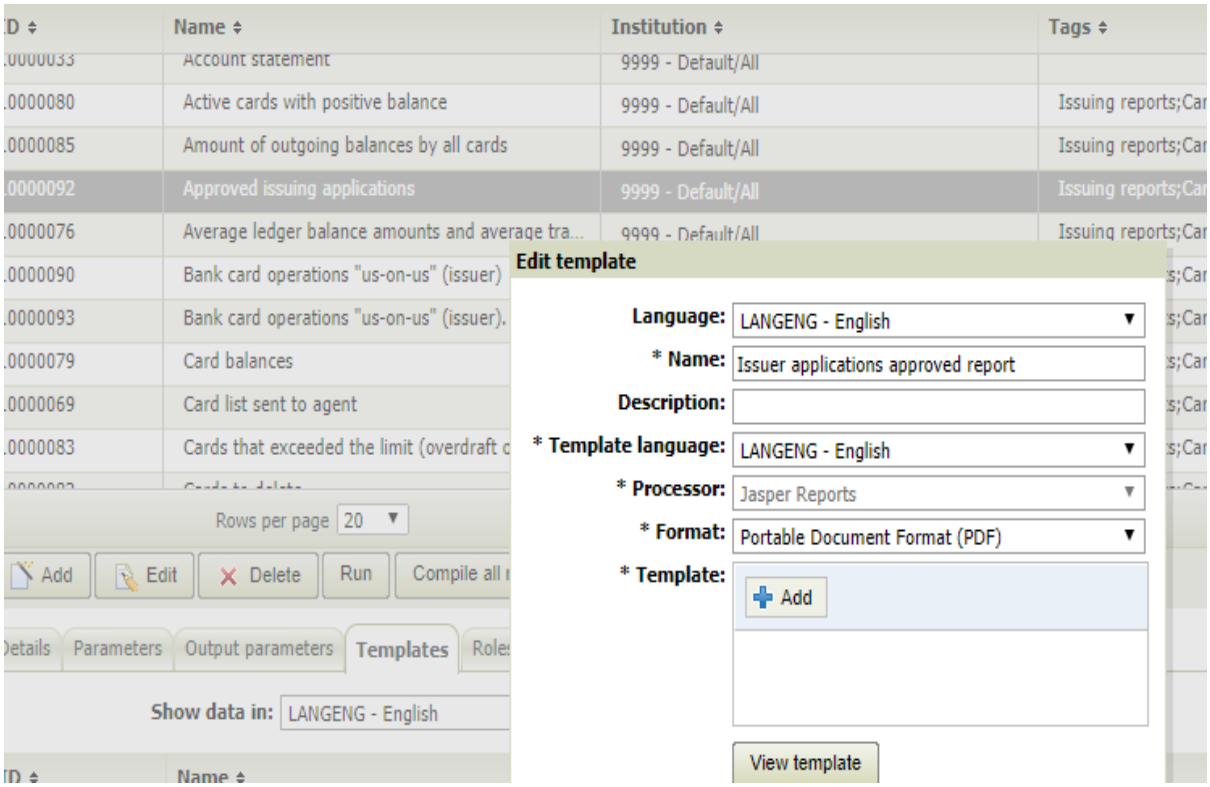
SmartVista comes with a large set of standard reports that have been designed using the Oracle Reports tool, that fully complies with client's business and operational requirements.

SmartVista contains two independent reporting engines:

- JasperReports
- Frozen Queries (optional component)

Due to the openness of the solution, our clients can effectively create its own reports, based on the SmartVista Database Dictionary and 4GL tools like Oracle Reports, or by using SmartVista Frozen Queries built-in special report tool, which allows to create direct SQL-requests to database and to store the results as standard format files.
SmartVista Frozen Queries tool allows creating ad-hoc arbitrary reports by using direct SQL-requests to SmartVista database. Embedded HTML code can be used for creation report headers and trailers. Report results can be exported to standard file formats – PDF, XLS, CSV, plain text, etc. and also be sent to an e-mail address. The saved queries (reports) can be set up for automatic run from a system job scheduler (supports daily, weekly, monthly, quarterly and annual reporting).

JasperReports is an open source Java reporting tool that can write to a variety of targets, such as: screen, a printer, into PDF, HTML, Microsoft Excel, RTF, ODT, Comma-separated values or XML files. It can be used in Java-enabled applications, including Java EE or web applications, to generate dynamic content. It reads its instructions from an XML or .jasper file. The JasperReports Engine has been tightly integrated with SmartVista. For users with more sophisticated report management requirements, reports designed for JasperReports can be easily imported into the JasperServer - the interactive report server.



The above screenshot shows how a report template can easily be imported into SmartVista via its Web GUI

Detailed SmartVista Database dictionary, systems audit logs and transactions logs are available for reporting facilities. There are no technical restrictions for composing and generating any specific reports.
A system of user role definitions managed by the SmartVista administrator user can grant or deny rights to a particular report for any authorized user. Batch report files are stored at different locations. The time of report production and storage location are configurable. The places for file storage are configurable for each report and for each institution to ensure reliable and secure storage. Also reports can be accessed online or downloaded in CSV and XLS format (other formats are also possible).

Billing and Statement

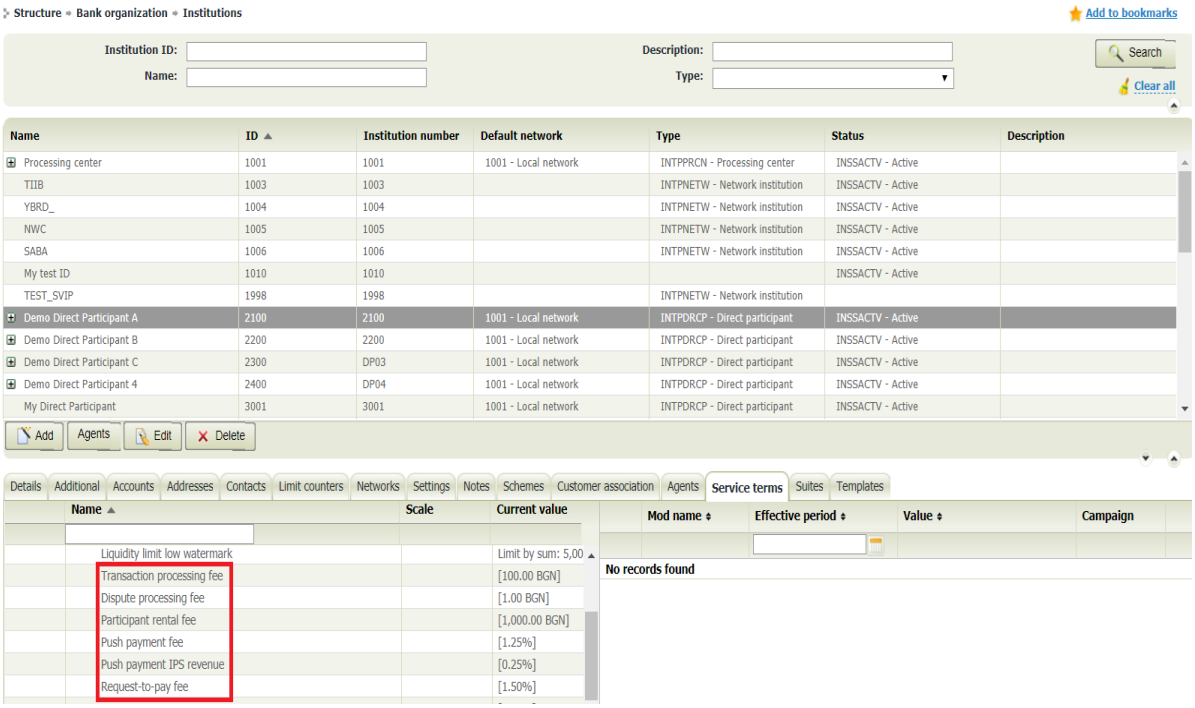
SVIPS has a sophisticated and highly parametrized billing module that offers configuration of fee/ interchange and other billing parameters in almost any business requirement of a participant. SVIPS Billing module provide following hierarchy on which billing parameter can be configured:

- Institution
- Participant
- End user
- Channel

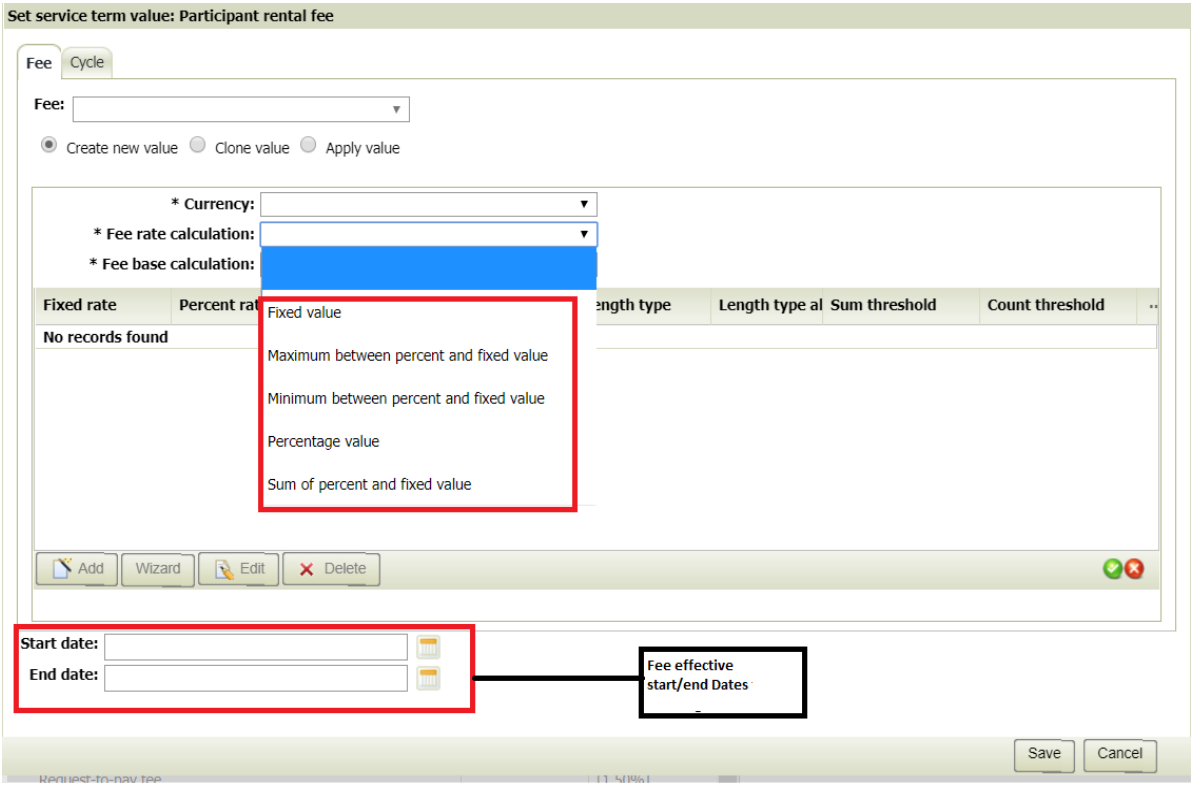
For example if a billing parameter of Monthly Rental fee needs to be configured then that can be defined at the Participant level. At every level any type of billing parameter can be defined. For interchange its amount can be defined at the participant level where any bilateral arrangement can be enforced without impacting other participants of the scheme. Example of billing parameters at participant level are:

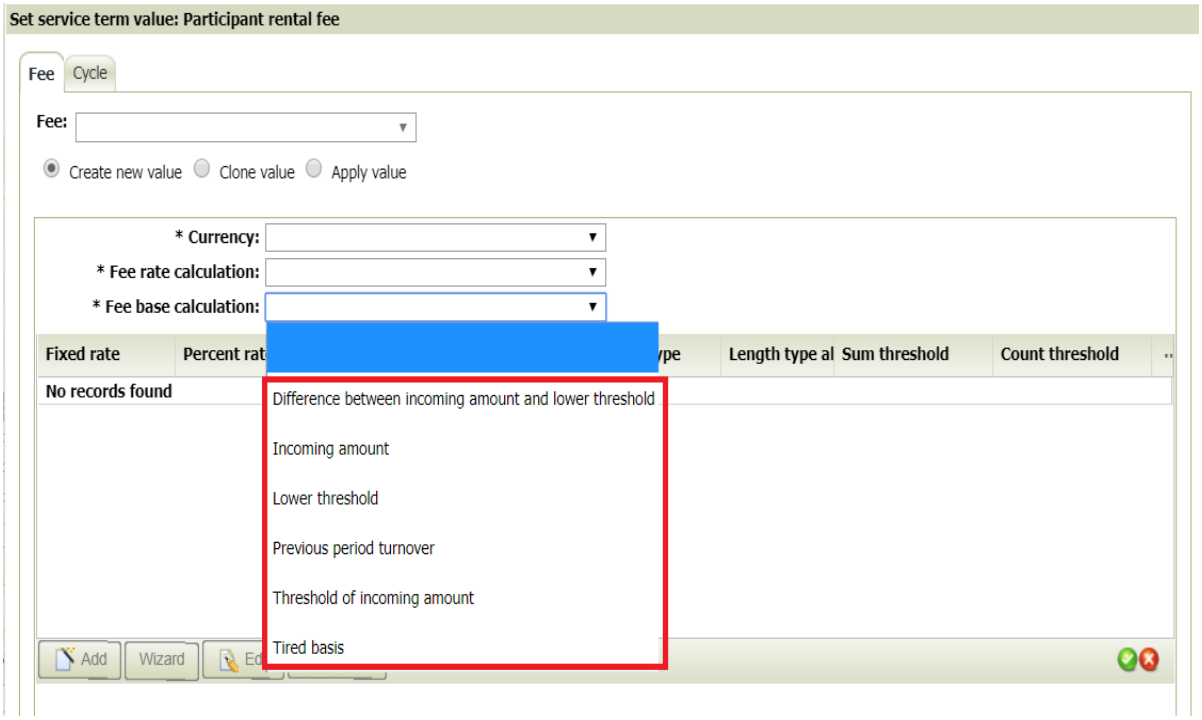
- Monthly scheme usage fee
- Transaction volume based charge
- Transaction value based charge
- Charge based on a campaign (first 100 transactions free per month)
- Charge based on duration
- Interchange defined as per percentage of the transaction value or turnover of a week, month, year etc.
- Interchange or transaction fee defined as a fix value per transaction
- Charge holiday where it is not applied on certain days of the year

Here is the screen shot of billing parameters applicable at the participant institution level:



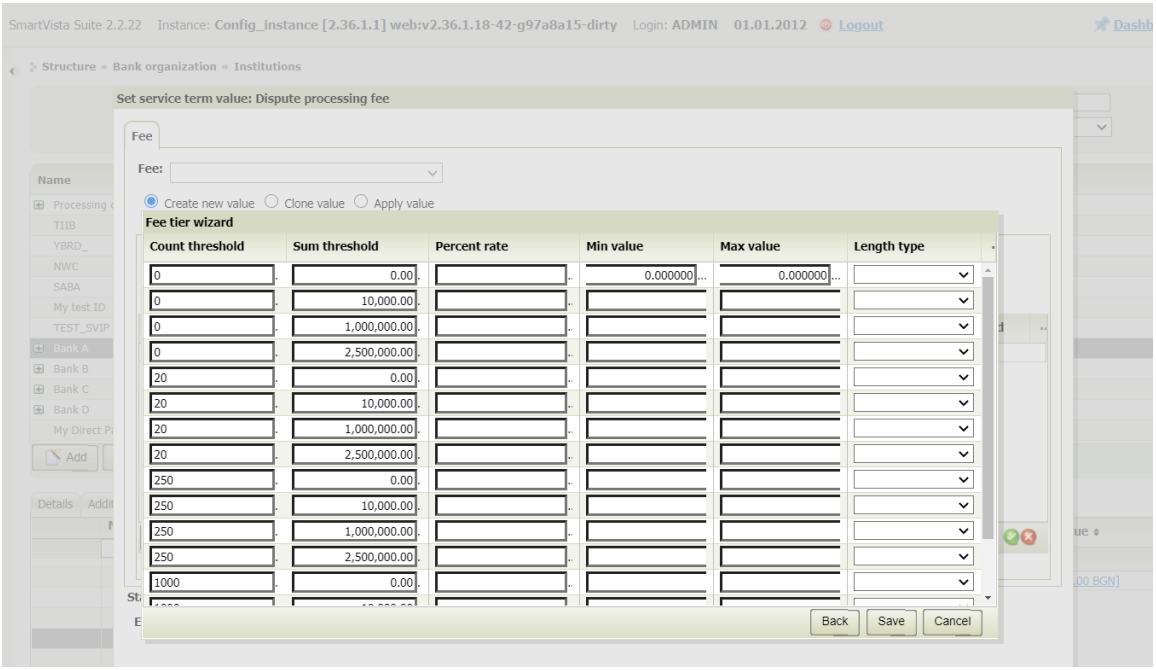
The SmartVista Fee and interchange definition wizard provides a lot of options to select a fee calculation criteria applicable on a large set of business rules. Here is a snapshot of the fee wizard:





The wizard allows selection of various fee rate calculation criteria and fee base calculation. The base calculation criteria derives the fee algorithm and the fee is applied on the fee rate calculation criteria. The fee wizard offers to establish fee campaigns with an effective start and end date. The fee on effective dates is activated and on expiry reverts back to the previous value before the start of the campaign.

Various combination of value based and volume based thresholds can be configured allowing unlimited capability to calculate fee on any tier.



Participant wise statements are configured and can be generated as per schedule or on demand from the billing module. The statement can be build using the user interface via Jasper reporting tool.

Fee Calculation Methods

The fee calculation module operates in real time and uses a number of predefined and user configurable algorithms for fee calculation. Operators can use web based interface to set predefined or user configured fee algorithm. The fee calculation algorithm is one or several sets of parameters that are used for calculation of the fee according to the specific formula. The module supports tiered fees by default.
The module provides the following predefined fee calculation algorithms:

#	Description	Formula
FA01 FA03	Used for participant fee calculation · FEE_AMNT - The calculated fee amount. · TRX_AMNT - The transaction amount in subunits of the basic transaction monetary currency unit. · K - The percentage part of the fee. The unit used is a hundredth of percent, for example, 100 is 1%. · C - The constant part of the fee in the minor denomination, for example, cents.	$FEE\_AMNT = \frac{TRX\_AMNT * K}{10000} + C$ $MIN < FEE\_AMNT < MAX$

	· MIN - The minimum fee amount in the minor denomination. · MAX - The maximum fee amount in the minor denomination. · For FA03 currency is explicitly set	
FA02 FA04	Used for participant fee calculation · FEE_AMNT - The calculated fee amount. · TRX_AMNT - The transaction amount in minimal currency units. · L - The threshold value of the transaction amount in the minor denomination. · K1, K2 - The fee percentages that are used depending on the transaction amount. The unit used is a hundredth of percent, for example, 100 is 1%. · C1, C2 - The constants that are used depending on the transaction amount. · For FA04 currency is explicitly set · Fpr FA05 fee amount depends on the number of transactions performed during a certain period	$TRX\_AMNT < L \Rightarrow FEE\_AMNT = \frac{TRX\_AMNT * K1}{10000} + C1$ $TRX\_AMNT > L \Rightarrow FEE\_AMNT = \frac{TRX\_AMNT * K2}{10000} + C2$
FA05	Used for participant fee calculation · FEE_AMNT - The calculated fee amount. · TRX_AMNT - The transaction amount in minimal currency units. · L - The threshold value of the transaction amount in the minor denomination. · K1, K2 - The fee percentages that are used depending on the transaction amount. The unit used is a hundredth of percent, for example, 100 is 1%. · C1, C2 - The constants that are used depending on the transaction amount. · N - The number of a record inside of the algorithm. · Li - The threshold for amount of withdrawn cash for the current 24 hours (−1 is the maximum value, infinity). · Ki - The fee percentage for a threshold. · Ci - The constant for a threshold.	$TRX\_AMNT + TOT\_AMNT \le L \Rightarrow FEE\_AMNT = \frac{TRX\_AMNT * K}{10000} +$ $TRX\_AMNT + TOT\_AMNT > L \Rightarrow FEE\_AMNT = FEE\_AMNT1 + FEE\_AMNT$ $FEE\_AMNT1 = \frac{(L - TOT\_AMNT) * K}{10000}$ $FEE\_AMNT2 = \frac{(TRX\_AMNT - L + TOT\_AMNT) * K}{10000} + C$

FA06	Used for Payer fee calculation · FEE_AMNT - The calculated fee amount. · TRX_AMNT - The transaction amount without acquirer fees in the account currency. · L - The transaction amount threshold. · K1 - The fee percentage if the transaction amount is below the threshold. · K2 - The fee percentage if the transaction amount is above the threshold. The unit used is a hundredth of percent, for example, 100 is 1%. · C1 - The constant to be used if the transaction amount is below the threshold. · C2 - The constant to be used if the transaction amount is above the threshold. · CONV_FEE - The conversion fee specified in hundredths of percent.	$TRX\_AMNT < L \Rightarrow FEE\_AMNT = \frac{TRX\_AMNT * K1}{10000} +$ $TRX\_AMNT \geq L \Rightarrow FEE\_AMNT = \frac{TRX\_AMNT * K2}{10000} +$ $TRX\_AMNT < L \Rightarrow FEE\_AMNT = \left(\frac{TRX\_AMNT * K1}{10000} + C1\right) + \left(\frac{TRX\_AMNT * CONV\_FE}{10000}\right.$ $TRX\_AMNT \geq L \Rightarrow FEE\_AMNT = \left(\frac{TRX\_AMNT * K2}{10000} + C2\right) + \left(\frac{TRX\_AMNT * CONV\_FE}{10000}\right.$
FA07	Used for Payer fee calculation · FEE_AMNT1 - The amount of the base fee. · FEE_AMNT2 - The amount of the fee for Exceed Limit usage. · TXN_AMNT - The transaction amount in the account currency. · EXCEED_AMNT - The used amount of Exceed Limit. This value is variable and is calculated for every transaction. · ABAL - The available balance (customer's own funds added to the exceed limit value). · EXCEED_LIMIT - The value of the Exceed Limit for the customer. This is the maximum threshold. · K1 - The base fee percentage. · K2 - The exceed limit fee percentage. · C - The constant in the minor denomination. · MIN - The minimum amount for the base fee in the minor denomination.	$FEE\_AMNT = FEE\_AMNT1 + FEE\_AMNT2$ $FEE\_AMNT1 = \frac{TRX\_AMNT * K1}{10000} + C$ $(MIN < FEE\_AMNT1 < MAX)$ $FEE\_AMNT2 = \frac{EXCEED\_AMNT * K2}{10000}$ $\begin{cases} EXCEED\_AMNT = (TRX\_AMNT + FEE\_AMNT1) - (ABAL - EXCEED\_LIMIT) \\ если\ (TRX\_AMNT + FEE\_AMNT1) \leq ABAL \\ EXCEED\_AMNT = EXCEED\_LIMIT \\ если\ (TRX\_AMNT + FEE\_AMNT1) > ABAL \end{cases}$
FA09	Used for fee calculation on adding additional service	FEE_AMOUNT = N * RATE_AMT

	· N - The number of days until the card expiry date. · RATE_AMNT - The rate for using the service for one day in the minor denomination.	
FA11	Used when multilevel commission fee is required · C - Fee percentage. · data_ent - This can be the amount of the transaction or a threshold value for the current phase. · Amount - Fee base amount. · Tier - Sum of the fees calculated before the current phase. · K - Constant in the minor denomination.	$\text{Fee} += (\frac{C}{10000}) * (data\_ent \rightarrow amount - tier) + K$
FA12	Used when it is required to add value added tax (VAT) to the amount · Fee - Total calculated fee amount. · amount_with_fees - Transaction amount including fees. All other fees that are applicable for this transaction. The FA12 fee is applied as the last one. · Percent - Value added tax (VAT). It is applied to the result amount after all other fees have been applied.	$\text{Fee} = (amount\_with\_fees) * (1 + \frac{percent}{100})$

Participant Portal

SVIPS offers a web portal as an operator portal for participant (both direct and indirect) to perform various operational functions related to the following areas:

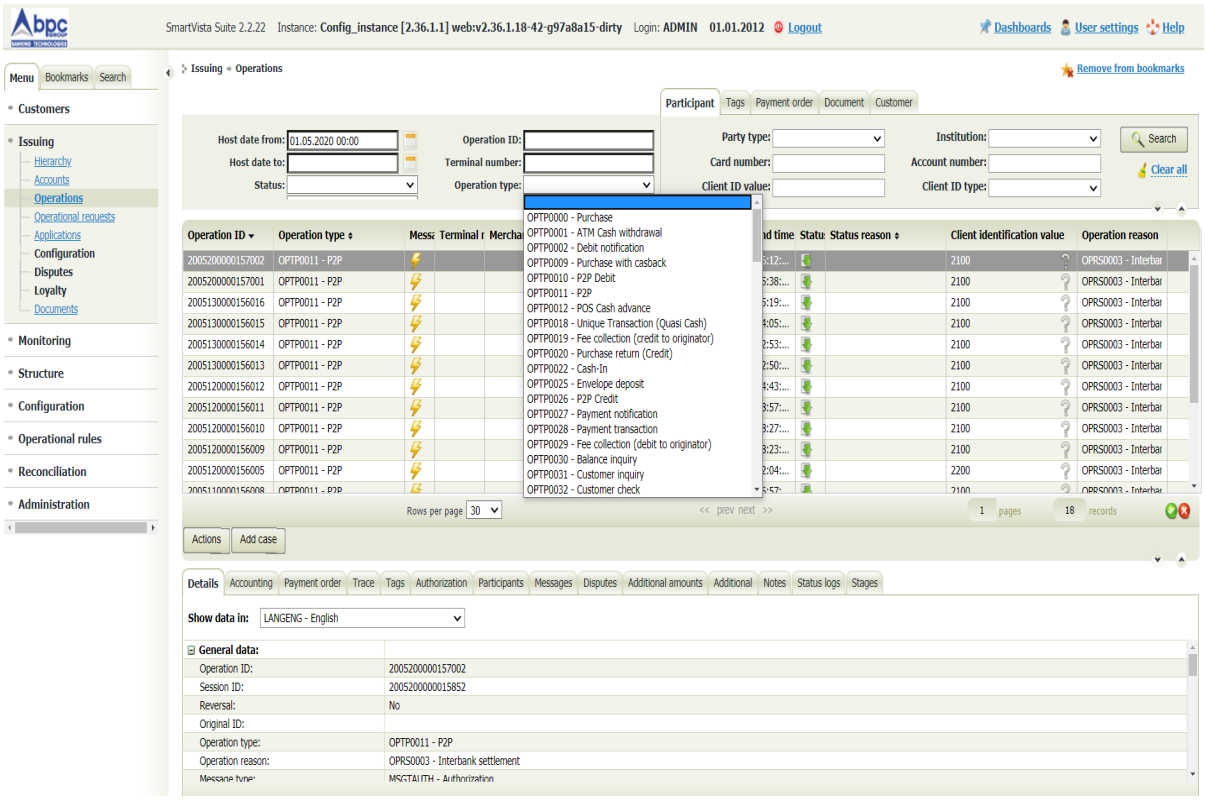
- **Liquidity Management** – Setting up net debit caps, requesting funding/defunding
- **Addressing Service Management** – Housekeeping of customer aliases, activation, deactivation, movement from one institute to another etc.
- **Transaction Monitoring** – Monitor their transaction records performed by their customers
- **Dispute Management** – Raise a dispute against a transaction and manage its complete lifecycle
- **Fraud Management** – View potential fraud cases and manage their operations
- **Bulk Payment File Management** – Upload bulk payment file for bulk payment to participant and view status of the batch
- **Dashboard and Reports** – View dashboard over various filters and extract statistics reports of transactions processes, billing data, directory services usage etc.

The portal provides administrator management console where participant can define their uses as per Role Based Access Control (RBAC) principle. A maker/checker 2 factor authentication is

enabled in any workflow of the portal, allowing participants to manage their operations in a secure manner. Participant portal can also integrate with enterprise 2FA solutions that offer hard and soft tokens as a second factor authentication method to perform any sensitive operations.

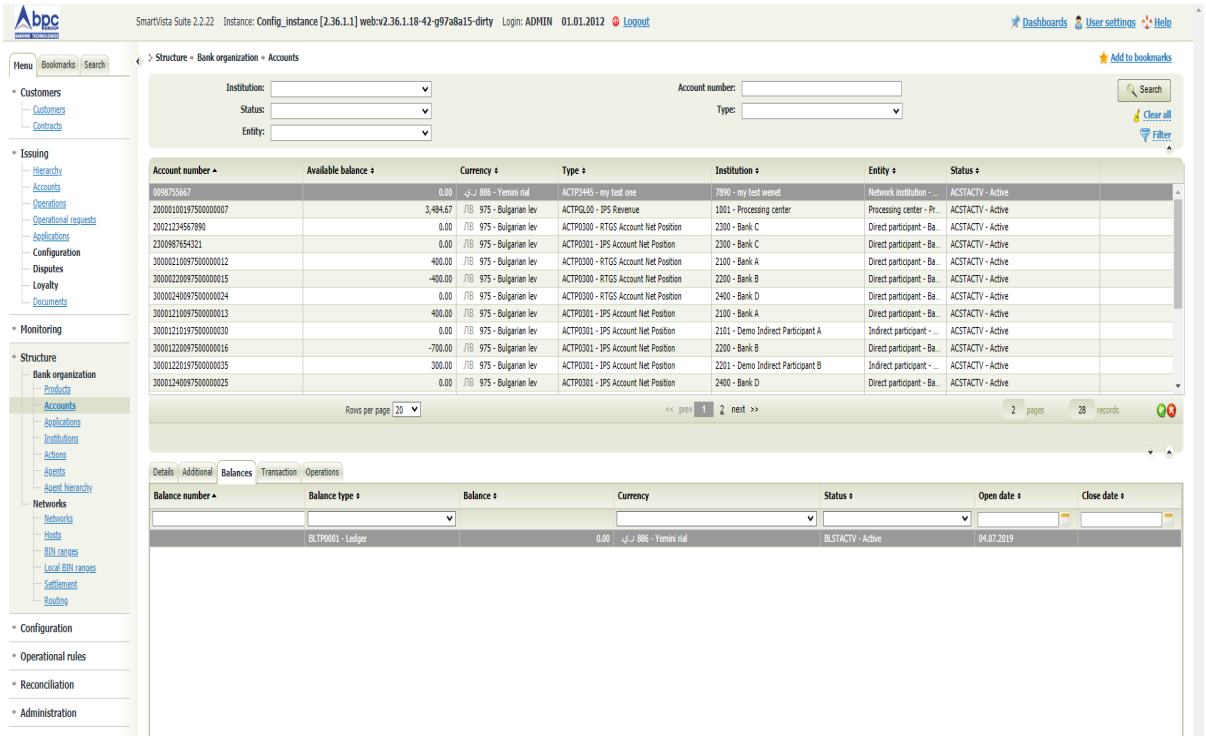
Payment Status and Summaries

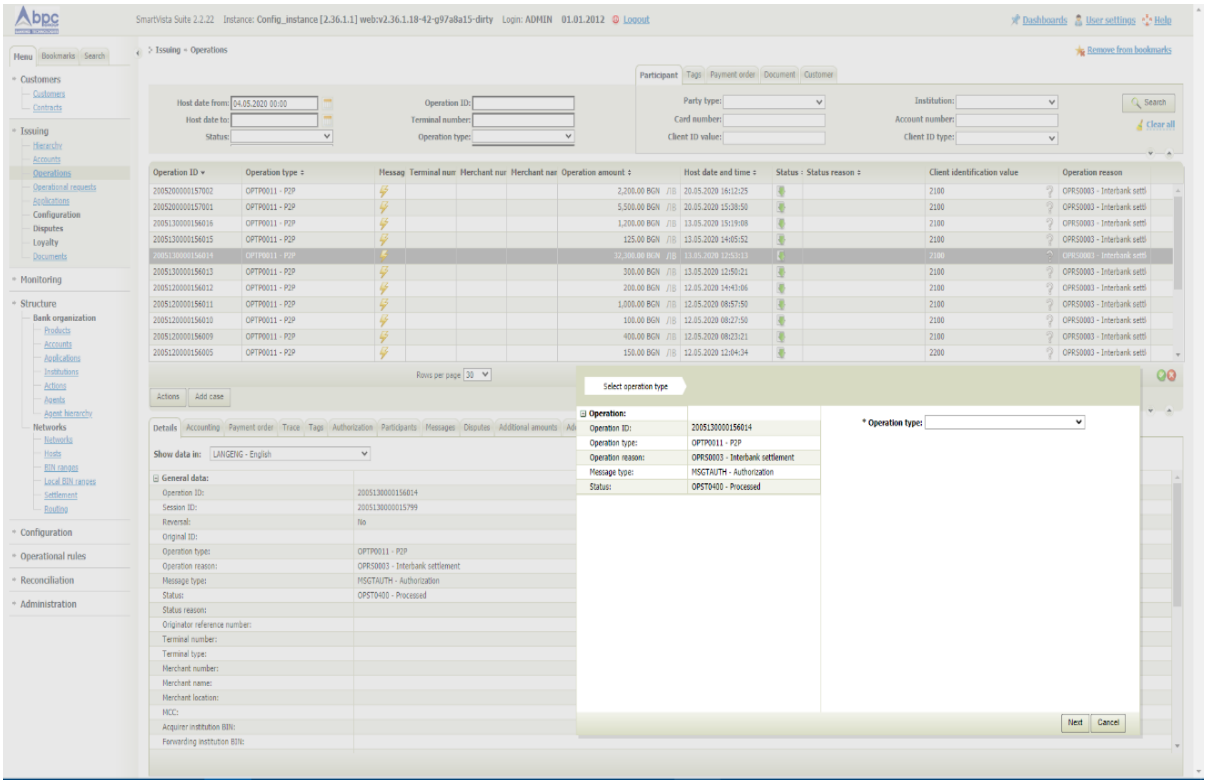
The portal provides tracking for all payment transactions captured by the system including successful and unsuccessful ones. There is a flexible transaction search filter that supports many parameters including transaction type, source and destination, date and time, status and others. Additionally, the search filter support logical expressions to search for a specific transaction based on a combination of the non-traditional or rarely used search values. The system also support multi-mode processing and able to process the transaction instantly, deferred or in batch.



Account Information

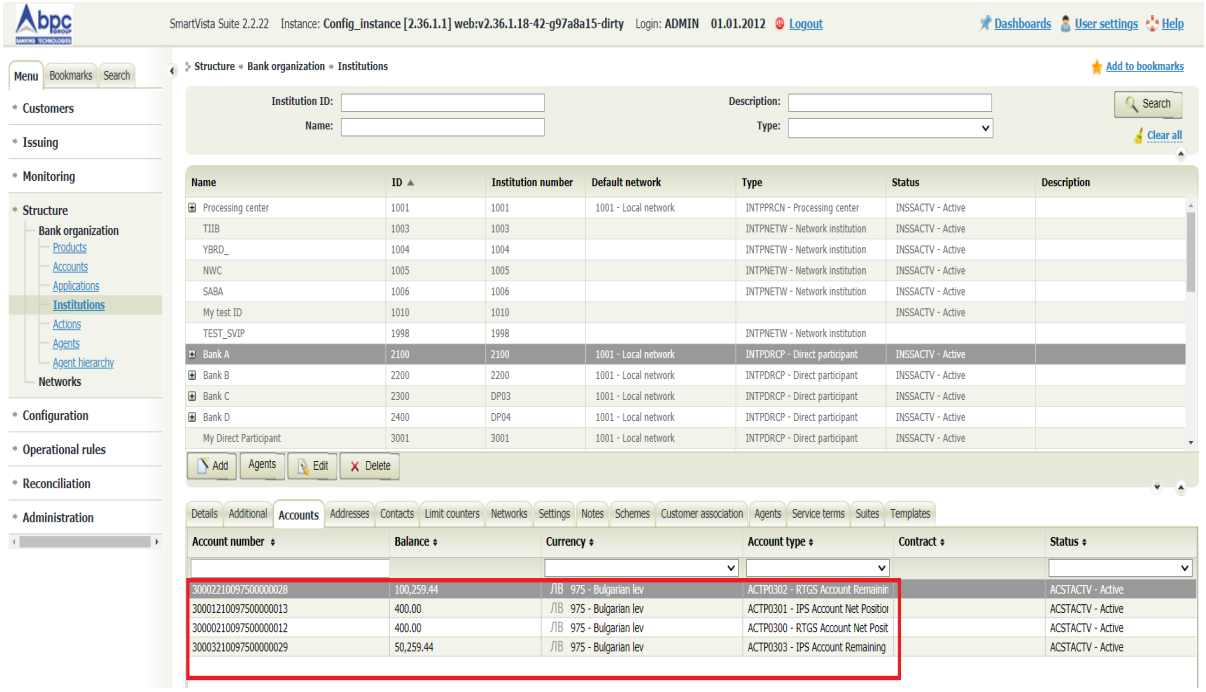
The portal provides full participant/member account configuration with the corresponding balance information. The system supports manual balance sweeping transactions directly from the operator screen and provides full reconciliation and reporting capabilities.





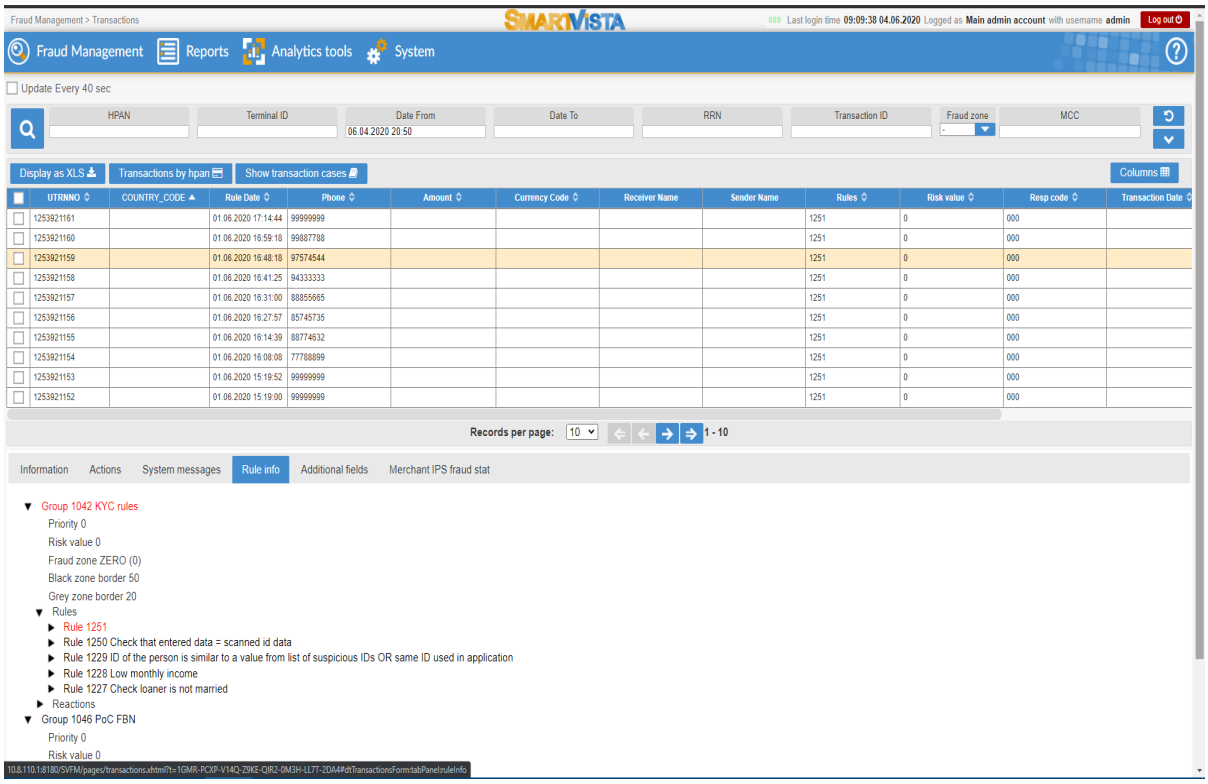
Liquidity Status

The portal provides participant/member configuration with the liquidity management features indicating participant/member name, current liquidity value, net position, liquidity limit and some other parameters. It is also possible to dynamically change the limits upon request and manage the participant/member configuration.



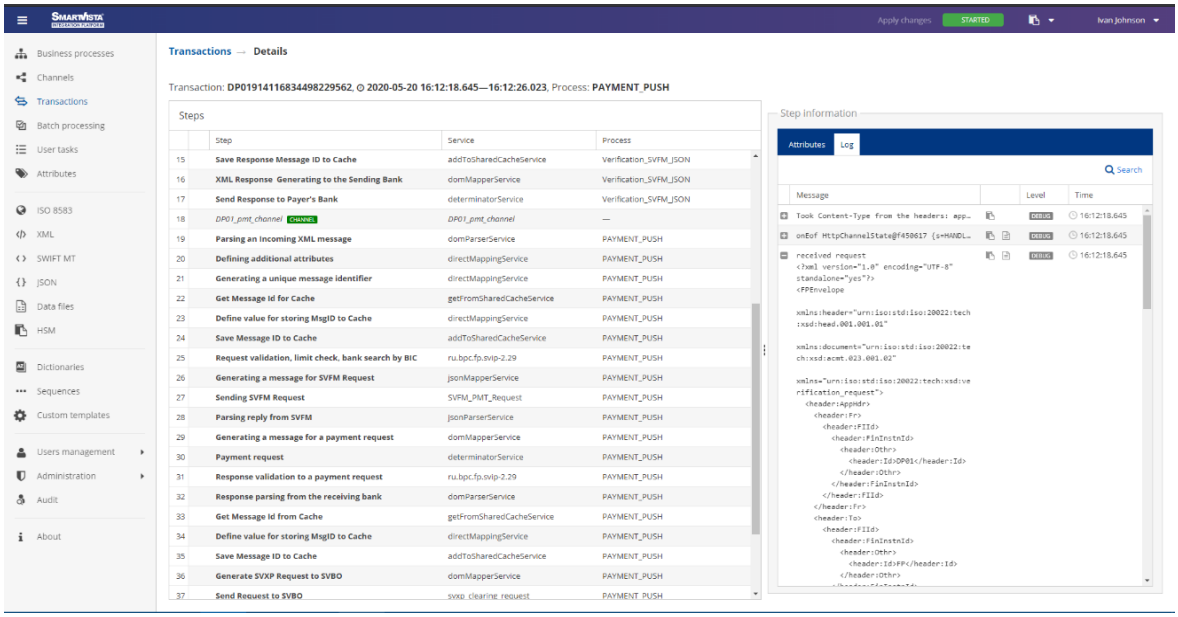
Fraud Screening (optional)

The portal provides participant/member fraud screening with full transaction summary, alerts triggered by the fraud event, case management, investigation history, entity profile visualization.



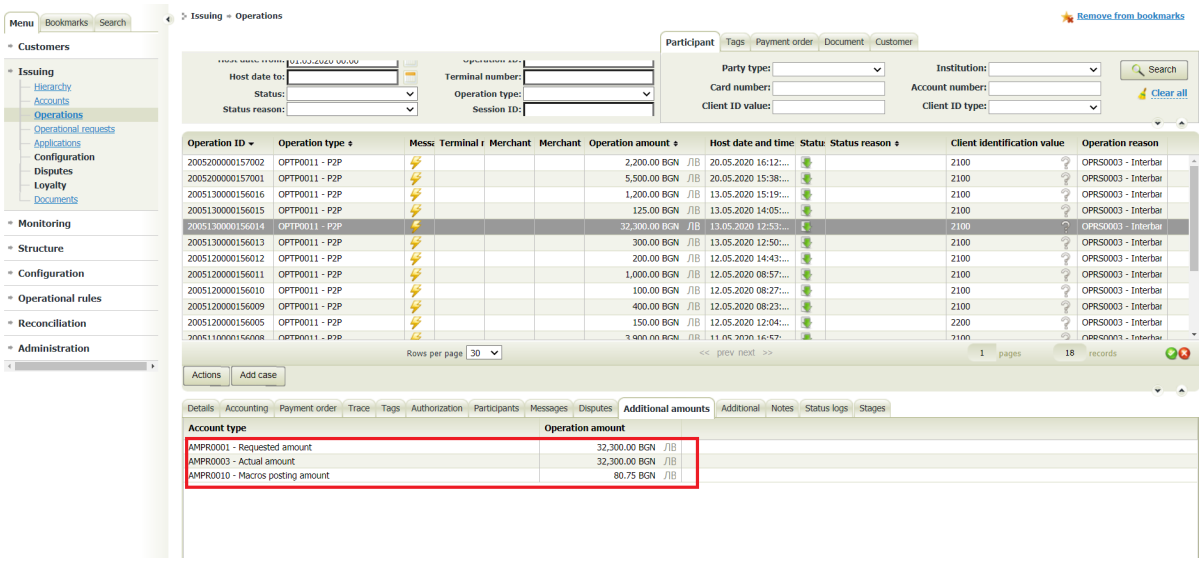
Message Enquiries

The portal provides complete logging of the incoming and outgoing messages including full step-by-step breakdown of the message processing flow. It is possible to see the original message contents and review the message if needed.



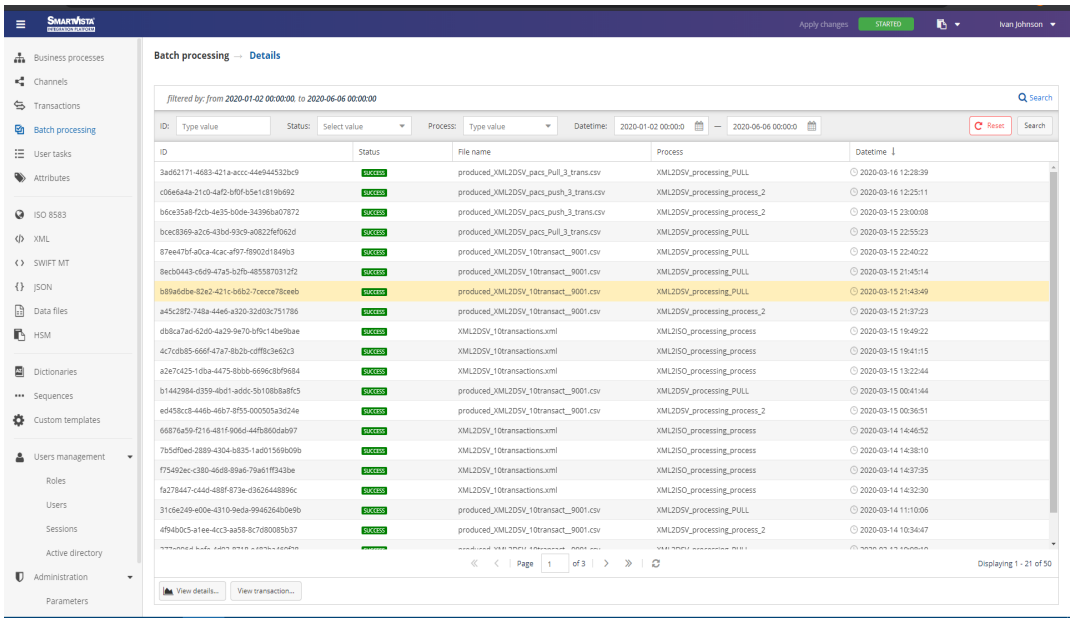
Billing Information

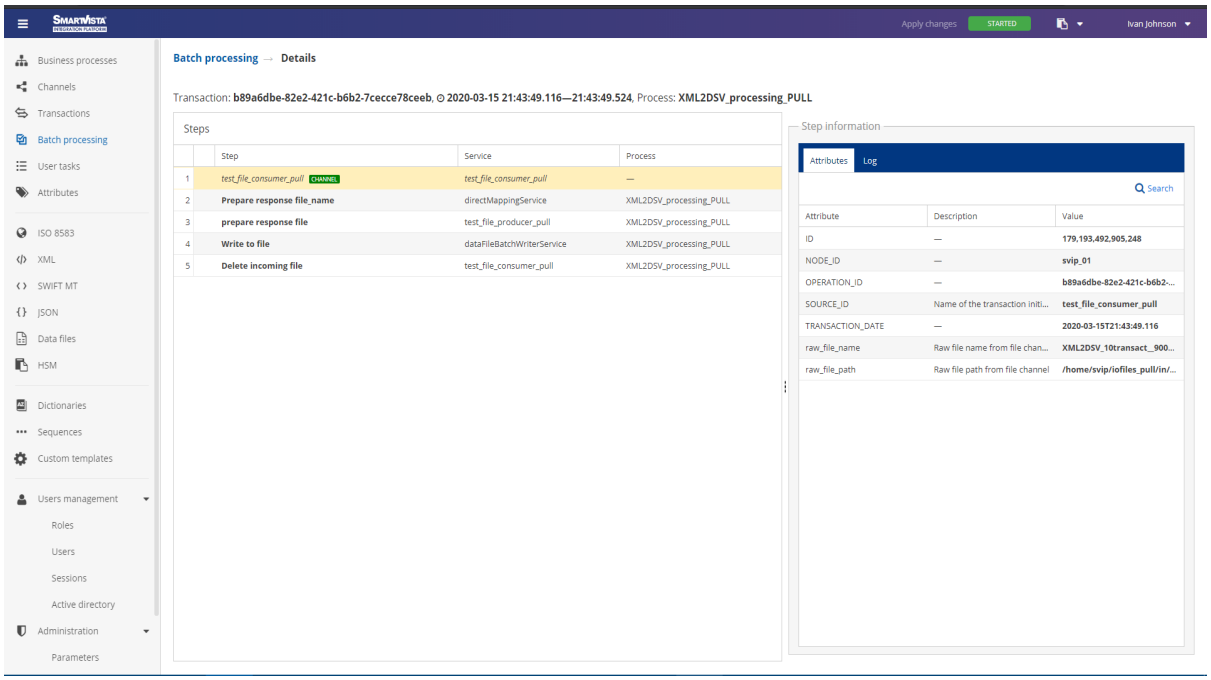
The portal provides full visibility about the fees charged for every transaction and the corresponding parties that should receive the applicable fees. The fees can be calculated for all parties involved in the transaction as originating, processing or receiving entities depending on the fee configurations.



File Management

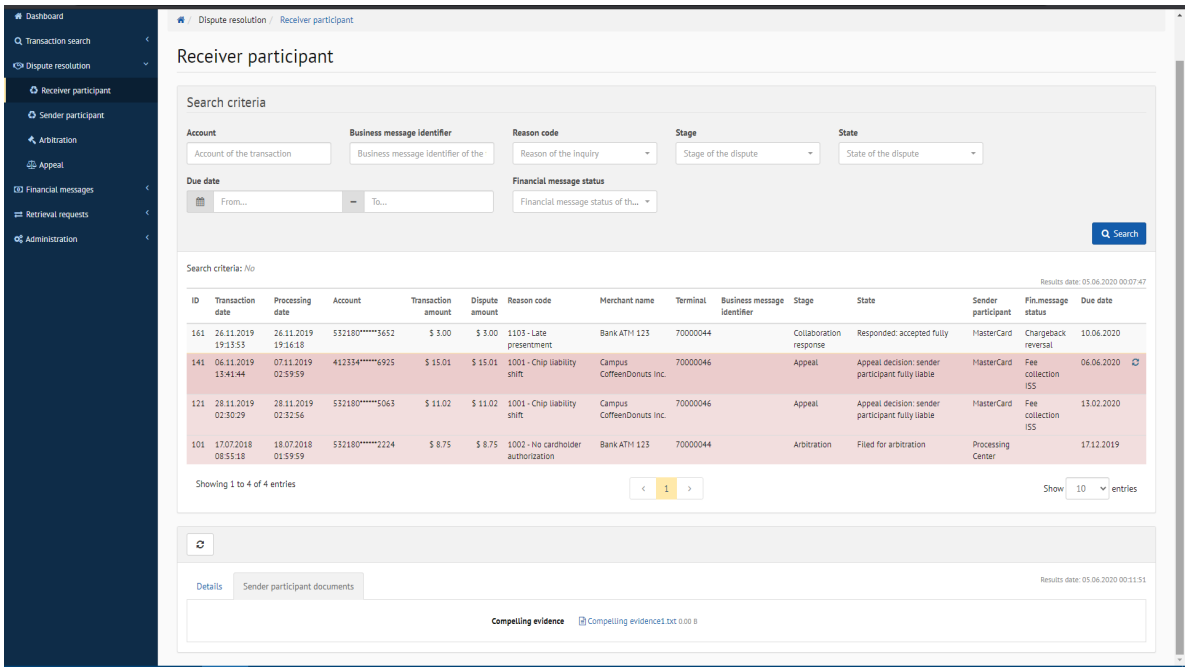
The system supports batch file processing and batch consolidation and synchronized delivery. The batch processes are run in parallel with instant payment processing and can be performed on the time of the received batch or by schedule. There is also full batch processing tracking capabilities and notifications based on the batch processing events.

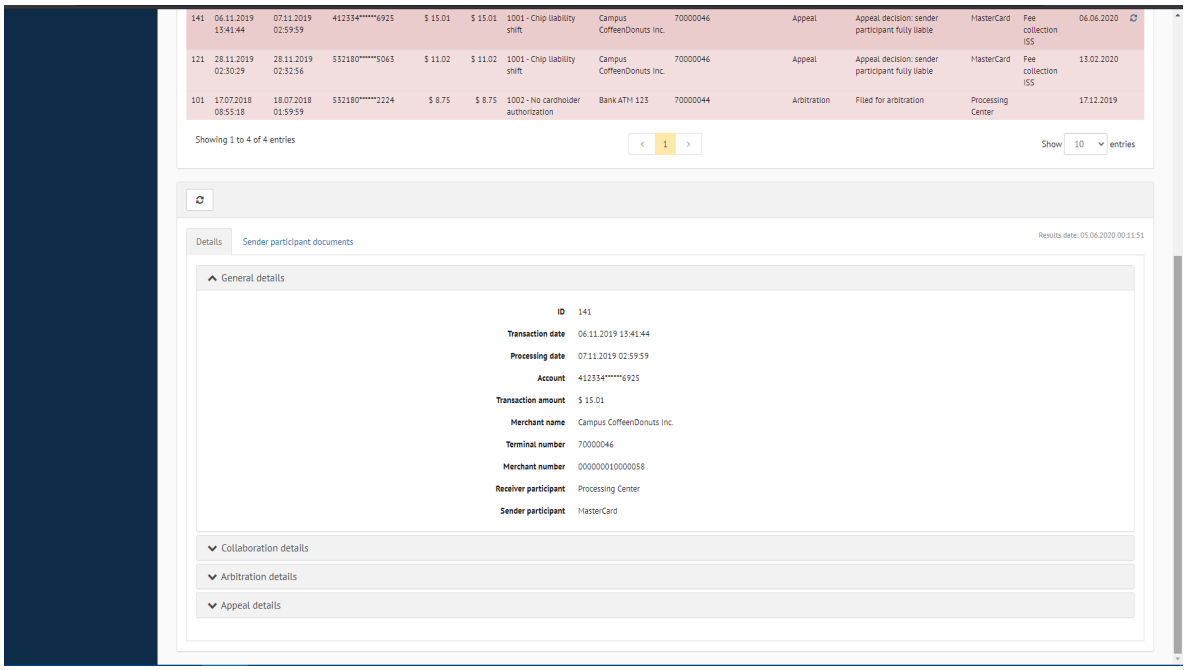




Dispute Management

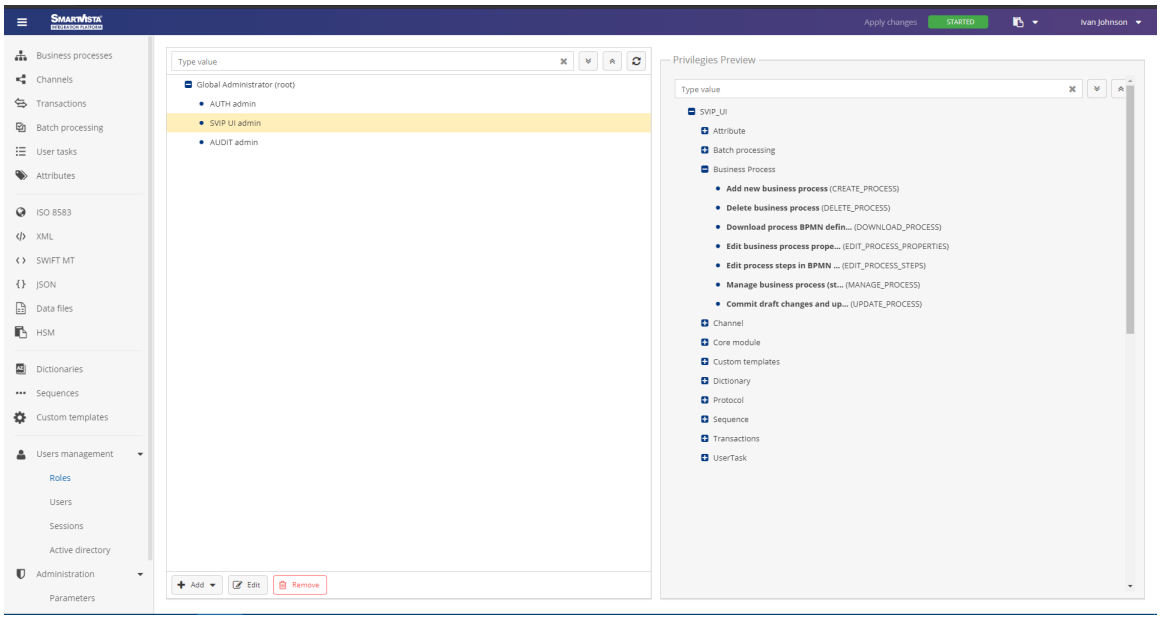
The portal provides dispute management features for sender and receiver participants. These include transaction search and investigation claim registration and case management, activity tracking, documents attachments, manual and automatic delegation.

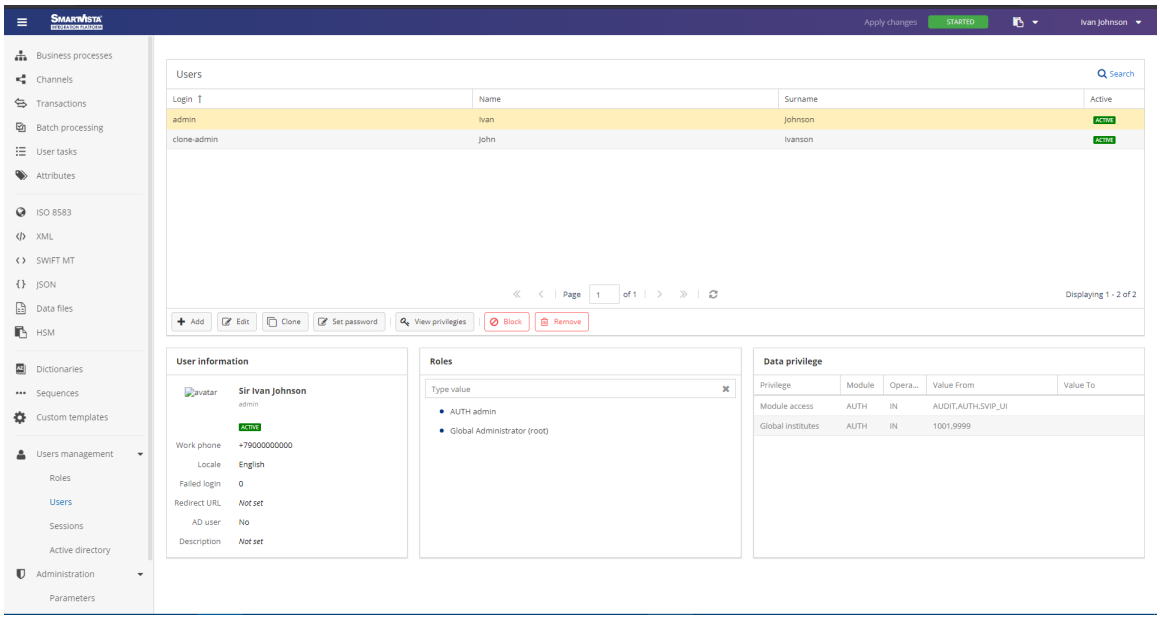




User Management

The portal supports RBAC approach and maintains the user hierarchy based on the corresponding roles associated with registered staff. There is a full administration capability including user creation/blocking/deletion, role configurations, user session management and audit functions.





Participant Types and Account Management

The SVIPS supports the following types of participants:

- Direct Participant – Participants that hold a settlement account in the central bank
- In-Direct Participant – Participants that do not hold a settlement account in the central bank and rely on the Direct Participant to perform settlement on their behalf

Within In-Direct Participants, there are several participant categories that are supported in SVIPS:

- InDirect Participant that hold settlement account in SVIPS – These participants can manage their own liquidity limit and balance in SVIPS, however the main settlement with central bank take place via Direct Participant settlement account in SVIPS and central bank
- In-Direct Participant that do not hold settlement account in SVIPS – These participants do not hold settlement account in SVIPS and hence dependent on their settlement agent (Direct participant) to manage their liquidity limits

Participant Status

SVIPS maintains participant status of each participant that connects to it. The participant status is tagged to the type of transactions they are allowed to initiated and process. Below are the typical participant status and their transaction permissions for a single and bulk credit transfers:

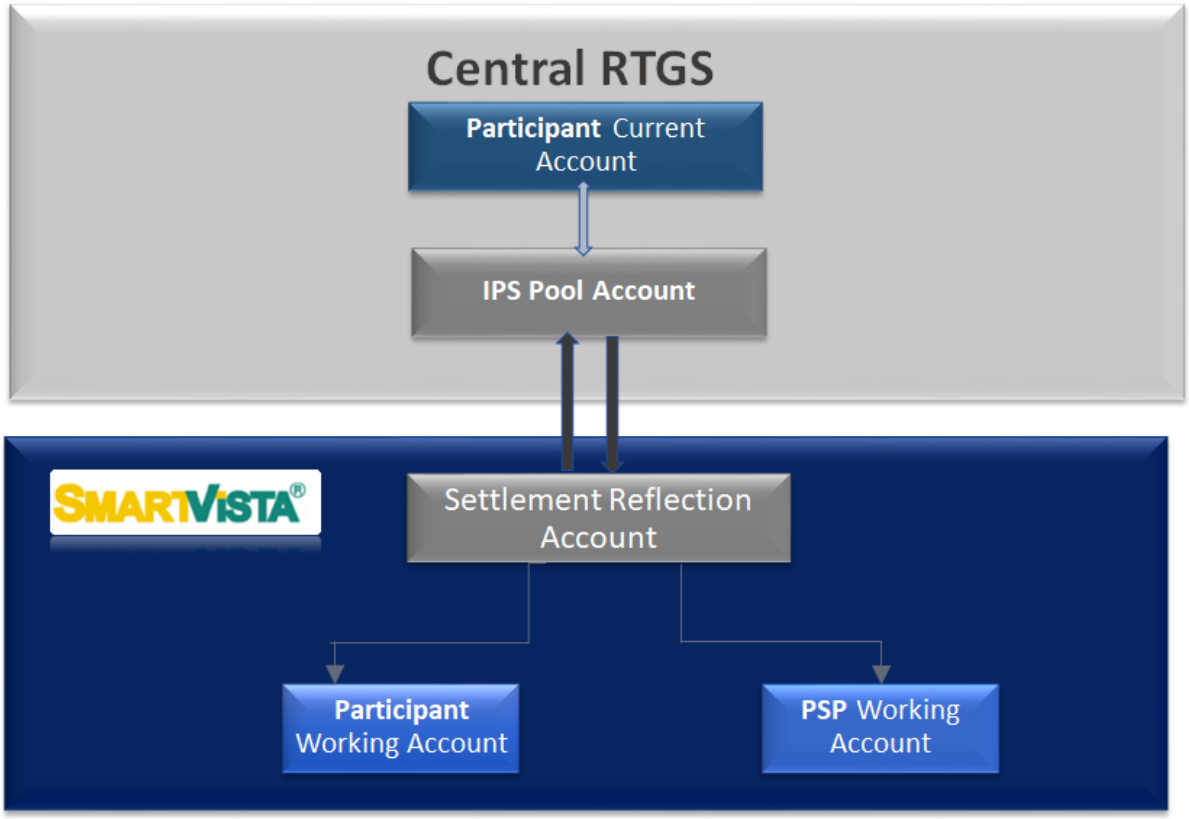
Status	Message Type	Incoming	Outgoing
Active	Credit Transfer	Allowed	Allowed
Active	Bulk Credit Transfer	Allowed	Allowed
In-active	Credit Transfer	Allowed	Not Allowed
In-active	Bulk credit transfer	Allowed	Not Allowed
Closed	Credit Transfer	Not Allowed	Not Allowed
Closed	Bulk Credit Transfer	Not Allowed	Not Allowed

Participant Management list is maintained in SVIPS and shared with all participants at a scheduled time. The list contains the BIC of the participant along with their current operating status and the permitted transactions set. Using the list all the participant get the latest status of the scheme members, which they can use to allow or deny transaction initiation from their respective channels. The participant list can be transmitted as a push notification to end participants. SVIPS also support pull method where participant request for the participant list by calling an API exposed by the SVIPS core.

Participant Account Hierarchy

SVIPS provides highly configuration and sophisticated two-level participant account hierarchy. This hierarchy provides a lot of flexibility to manage any type of participant account and liquidity management, supported by the scheme. In this hierarchy:

- Direct participants have their settlement reflection account which are synchronized with central bank instant payment pool account maintained in Core banking or RTGS.
- Under this reflection account, every participant can have their working accounts with the balance as a subset or equal to the amount maintained in the reflection account. This acts as the participant net position limit. Participant can choose not to define this limit so that all transactions are settled using the main reflection account balance
- In the same hierarchy the direct participant which act as a settlement agent to a PSP has a PSP working account. Just like participant working account, the PSP working account limit can be defined by the settlement agent as a subset of the balance maintained in the main reflection account
- In order to keep instant payment settlement separate from other payments, a settlement agent creates a pool account in central bank core banking or RTGS, which provides guarantee of settlement of the transactions that take place in the instant payment scheme. This pool account gets funding from the main current account of the settlement agent maintained in central bank.
- In this setup, a direct participant can manage unlimited number of indirect participants under the hierarchy of its reflection account



Liquidity Management

The Direct participant defines its maximum limit in the reflection account and can also choose to define a sublimit in its working account. Likewise, the direct participant acting as a settlement agent sets up maximum limit of its PSP spending in the respective PSP working account. Prior to this setup it is assumed that PSP must have opened a funding account in the respective Direct participant bank and have instructed the settlement agent to setup its main limit. The sum of the limits defined under a reflection account hierarchy may exceed the balance maintained in it. However this does not results in a shortage of liquidity because during the clearing process the balance in the reflection account is also checked along with the limit in the working account.

If a transaction take place between one direct participant to another then the following procedure takes place:

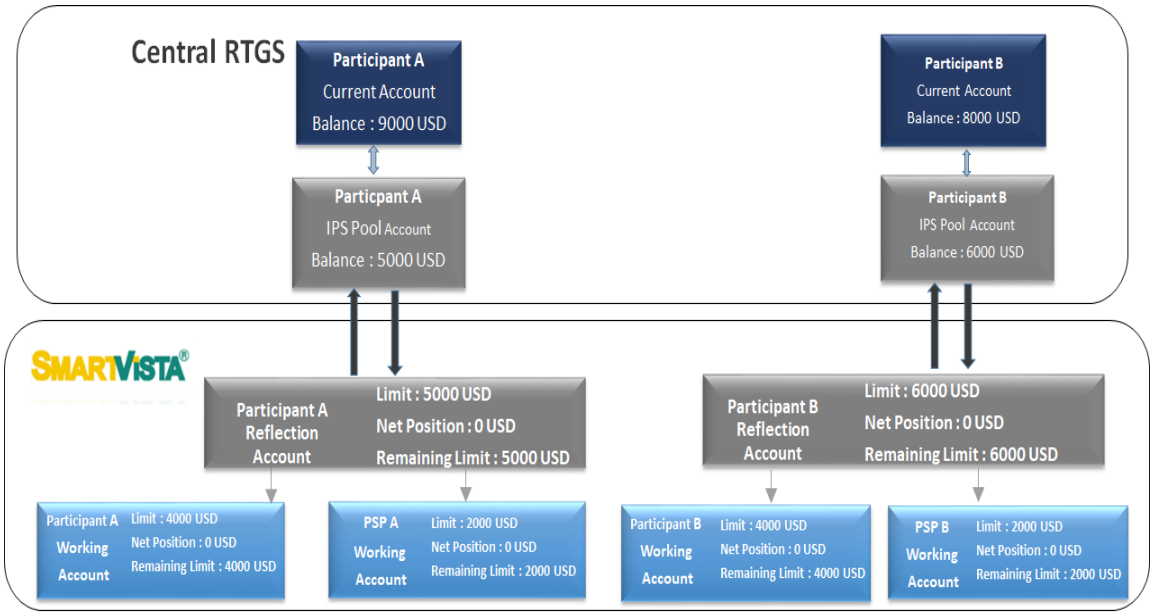
- Limit in the sender working account is checked and if found adequate then the balance in the reflection account is checked.
- If both limit and balance hold adequate amount then the transaction is allowed to clear. The respective limit, balance and net position of sender working account, sender reflection account, receiver working account and receiver reflection account is updated.

If a transaction take place within the same hierarchy, that is among a PSP and a Bank sharing same reflection account then:

- Limits in the sender working account are checked and if adequate then transaction is allowed to clear.
- As a result of clearing the limit of working account of sender participant is deducted with the transaction amount, its net debit position is updated and then the net position of receiver working account and its remaining limit is updated.
- No update take place in the reflection account balance as the movement of funds happen within the same hierarchy.

If a transaction take place between two PSPs that fall under different hierarchies of their respective settlement agent then their fund movement follow same procedure as explained for the movement between two different direct participants above. The only difference is that instead of movement of funds in the working account of the direct participant, it takes place in the working account of PSP, and the respective reflection account is also updated.

Here is an example of participant liquidity setup:



In the above example there are two direct participants (Participant A and Participant B) and two indirect participants (PSP A and PSP B). Participant A is the settlement agent of PSPS A and Participant B is the settlement agent of PSP B.

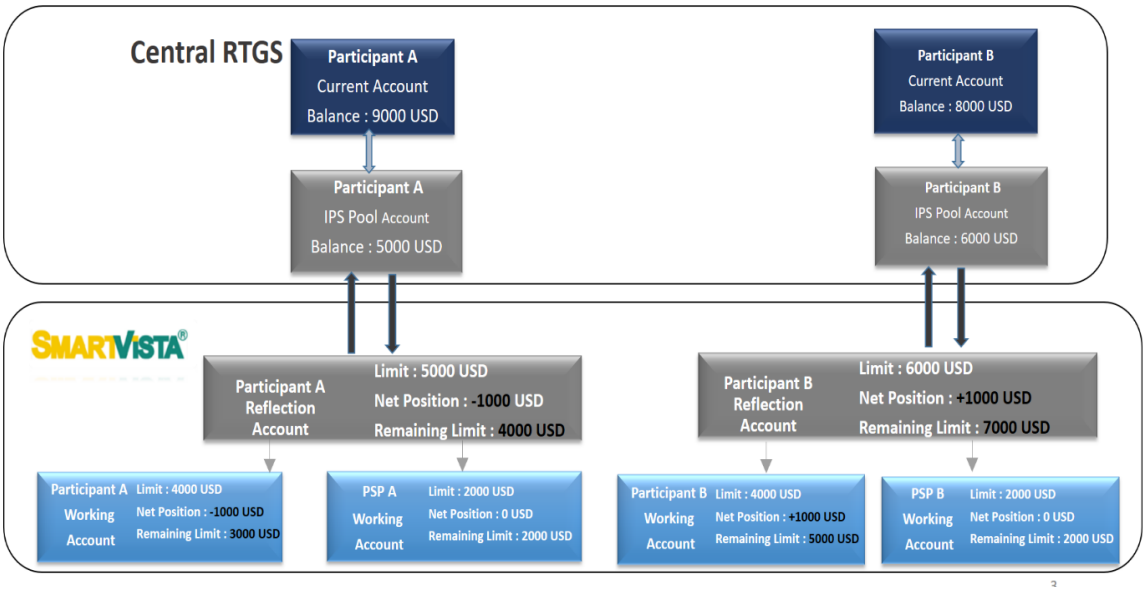
Participant A current account has a balance of USD 9000 and its IPS Pool Account which dedicated for Instant payment settlement has a balance of USD 5000. This balance is derived from the Current Account. In the SVIPS there is Participant A Reflection Account which 'reflects' the balance and position of IPS Pool Account held in the central bank RTGS or core banking system. In other words the balance of Reflection account is synchronized with the balance of IPS pool account. Similarly, the account and limit is set in the Participant B IPS account in central bank RTGS and its reflection account in SVIPS.

In the hierarchy of a Reflection account of Participant A there is Participant Working Account which holds a limit of USD 4000 and in the same hierarchy there is PSP A Working Account with a limit of USD 2000. The PSP A is acting as an indirect participant with Participant A playing a role of its settlement agent in the scheme. Same hierarchy with respective balance and limit is defined for Participant B.

Note that in the Participant A hierarchy, the accumulative limit of Participant A working account and PSP A working account is more than the limit defined in the reflection account. This does not result in liquidity shortage because the clearing process ensures that the reflection account has sufficient limit to process a transaction.

Let us walk through a few clearing scenarios to understand this account hierarchy.

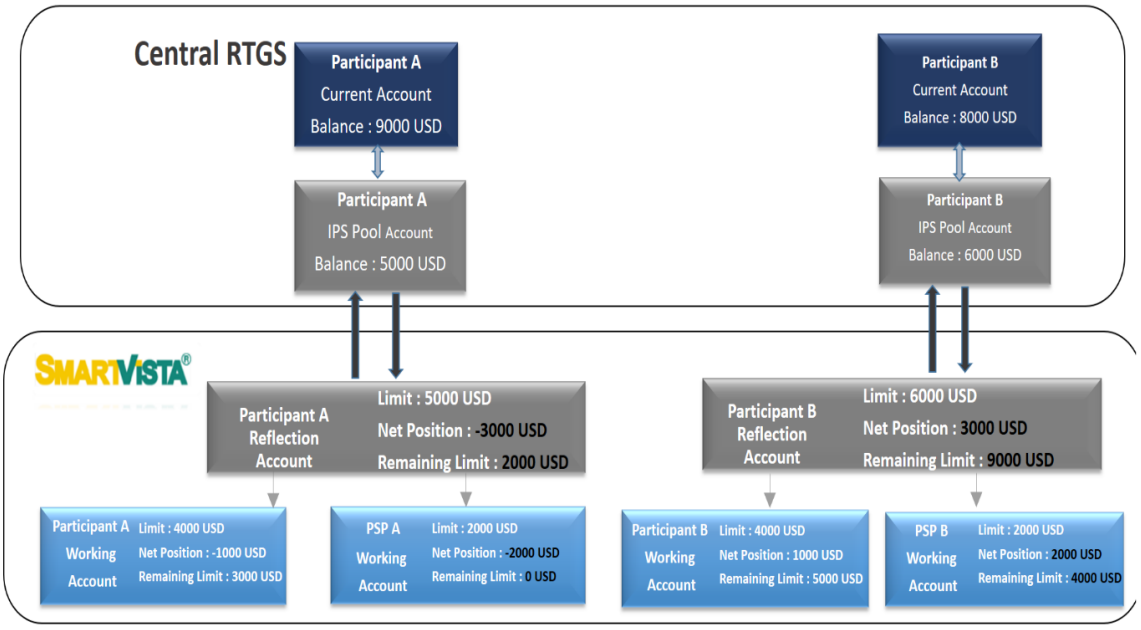
Push Payment of USD 1000 from Participant A to Participant B



In the above clearing message a push payment of USD 1000 took place from Participant A to Participant B. The following process is followed:

- The Participant A Working Account limit is checked and since the transaction amount is less than the limit this validation is successful
- The Participant A Reflection Account Limit is checked and since the transaction amount is less than the limit this validation is successful
- Once the above two checks pass their validation then the Working account net position and its remaining limit is debited by the transaction amount
- The Participant B working account net position and remaining limit is credit with the transaction amount
- The Participant B Reflection Account remaining limit and its net position is credited with the transaction amount

Push Payment of USD 2000 from PSP A to PSP B

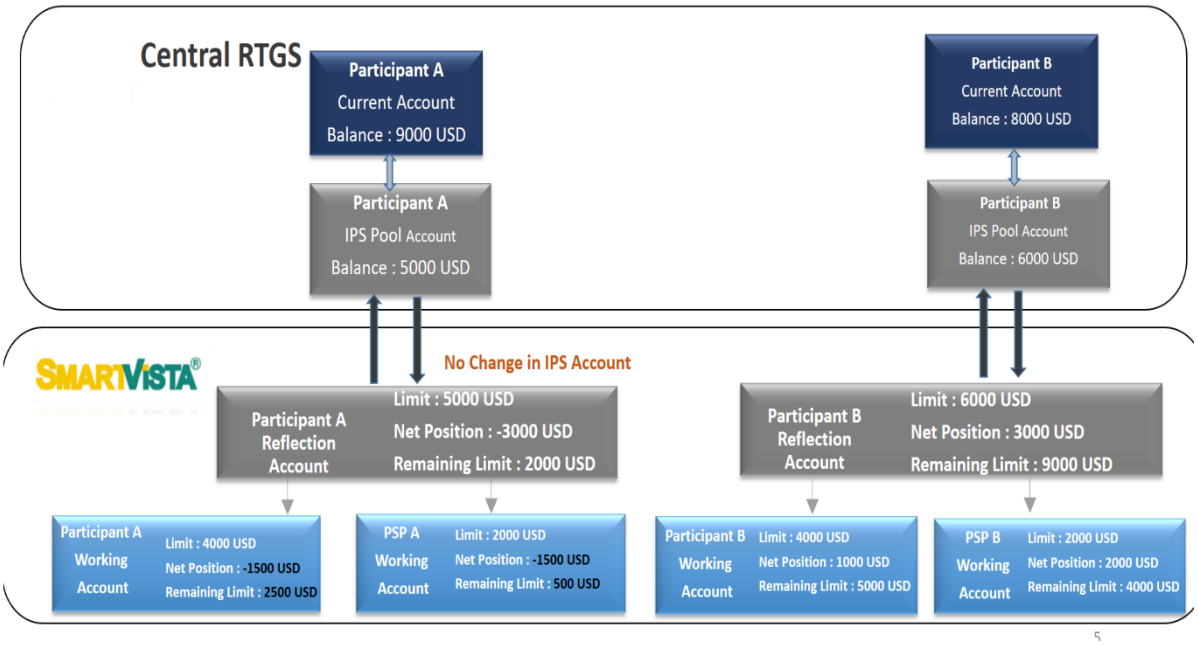


In the above clearing message, a push payment of USD 2000 took place from PSP A to PSP B. The following process is followed:

- PSP A working account limit is checked which is greater than the transaction amount
- Participant A Reflection account limit under which the PSP A account is maintained in the hierarchy is checked and it is greater than the transaction amount
- After successful validation of both of these checks, the PSP A working account is debited with the transaction amount and its remaining limit is also reduced with the same amount
- PSP B working account net position and remaining limit is increased by the transaction amount

Note that the Participant A working account and Participant B working account remain untouched because they have no role in the clearing process between PSP A and PSP B. However the respective reflection account that are maintaining the PSP accounts in their hierarchy are updated respectively.

Push Payment of USD 500 from Participant A to PSP A

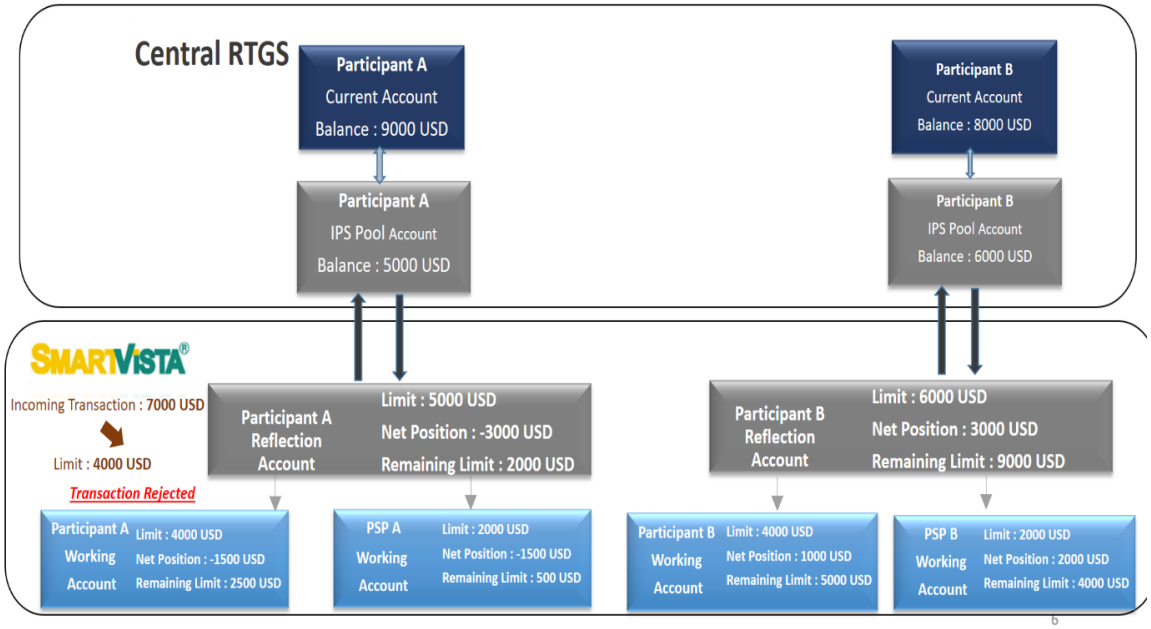


In the above clearing example, a Push payment messages is sent from PSP A to PSP for an amount of USD 500. The following process if followed:

- Limit of PSP A is checked against the transaction amount. Also, the limit of Participant A reflection account is checked against the amount.
- If both passes the check then the net position of Participant A working account is debited by the transaction amount and its remaining limit is also reduced
- The net position and remaining limit of PSP A is increased respectively by the transaction amount

Note that no movement of position take place in the Participant A reflection account. This is because the clearing process involve movement of funds between participants falling under same hierarchy hence there is no need to debit/credit net position or limit of reflection account.

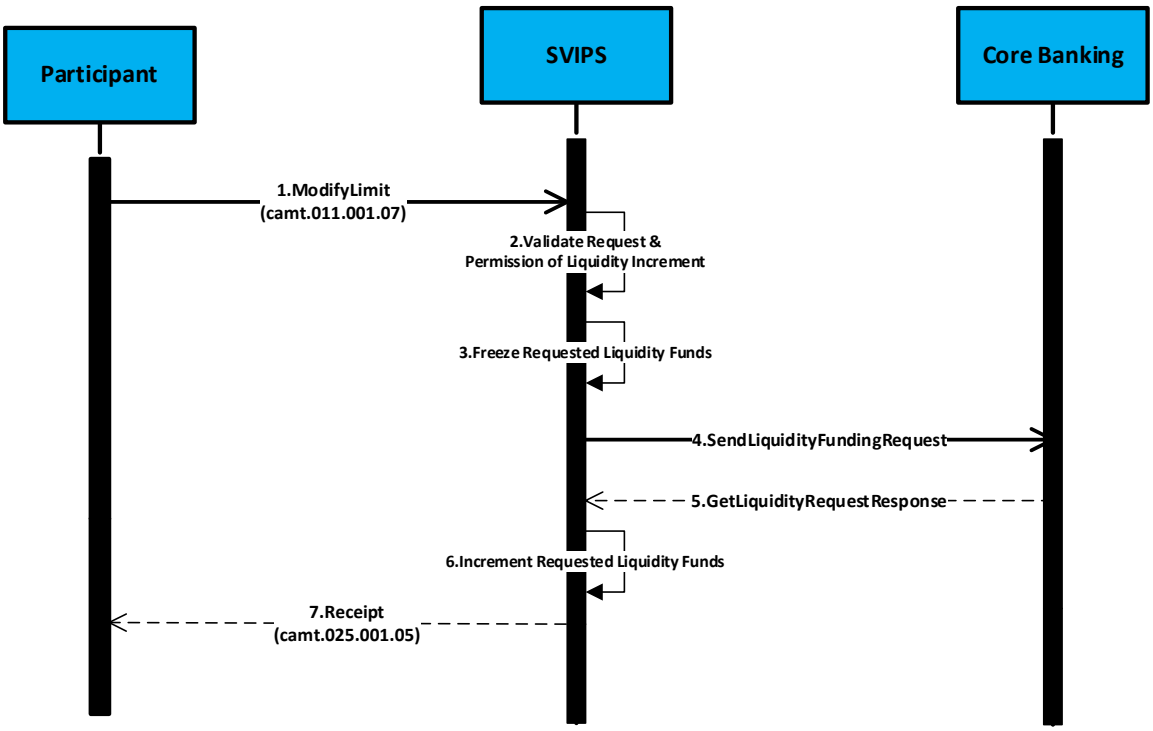
Push Payment of USD 7000 from Participant A to Participant B



In the above example a transaction of USD 7000 is attempted from Participant A to Participant B. The transaction is rejected because the Participant A working account limit is less than the transaction amount. Even if that limit would have been greater than transaction amount, the transaction would have been rejected because the Participant A reflection account limit would not be enough to process it.

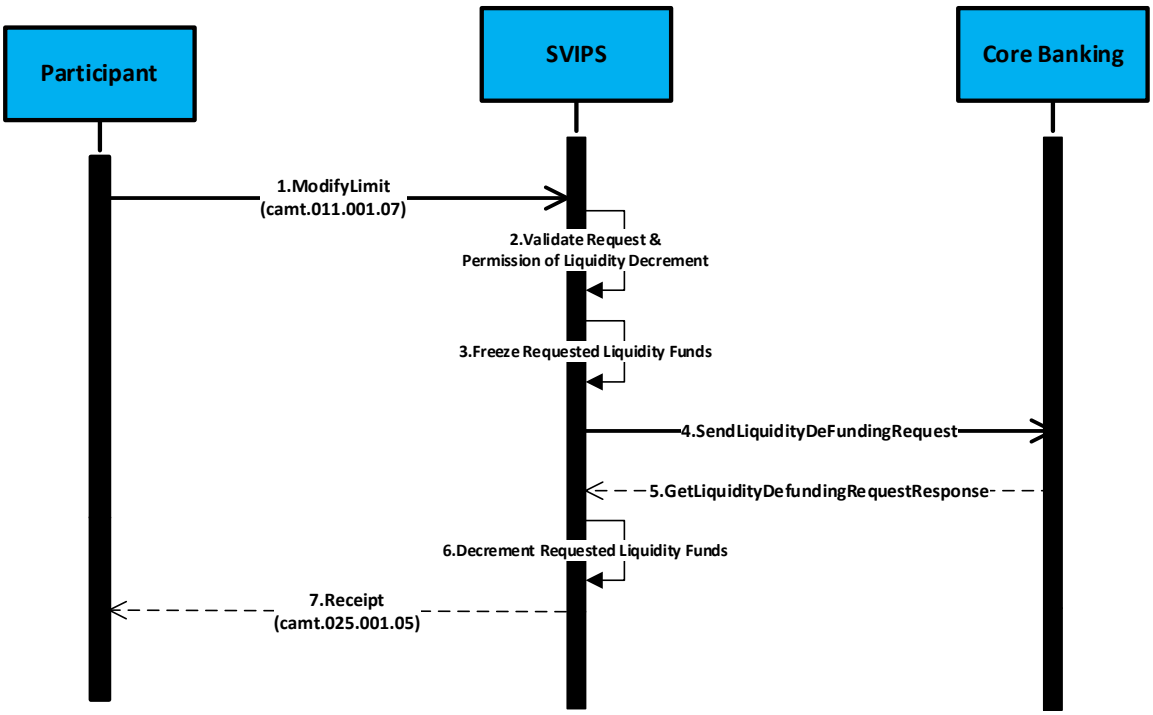
Liquidity Increment and Decrement

Participants (both direct and indirect) can request for manual liquidity increase and decrease at any time of the day since SVIPS is always online and functions 24 hours a day. Using ISO 20022 camt.011 and camt.025 message types a participant can request SVIPS to set limit higher than the current value or it can request to decrease the limit. In case of request of higher limit a topup request is sent to the central bank RTGS, or core banking system to reserve the required amount in their accounts. After successful validation at central bank the respective reflection account of participant limit is increased by the desired amount.



No.	Description
1	Participant sends request of Liquidity Increment to SVIPS
2	SVIPS validates request and permission of participant
3	SVIPS freeze the requested liquidity topup amount from participant limit
4	SVIPS forwards Liquidity topup request to core banking
5	Core banking sends response of liquidity topup request
6	SVIPS increments liquidity amount
7	SVIPS sends receipt of liquidity increment request

Similarly, in case of liquidity decrement a defunding request is initiated by the participants which is validated by central bank. On successful validation the limit is decreased from SVIPS reflection account and balance are increased at the central bank settlement accounts.



No.	Description
1	Participant sends request of Liquidity Decrement to SVIPS
2	SVIPS validates request and permission of participant
3	SVIPS freeze the requested liquidity defund amount from participant limit
4	SVIPS forwards Liquidity defund request to core banking
5	Core banking sends response of liquidity defund request
6	SVIPS decrements liquidity amount
7	SVIPS sends receipt of liquidity decrement request

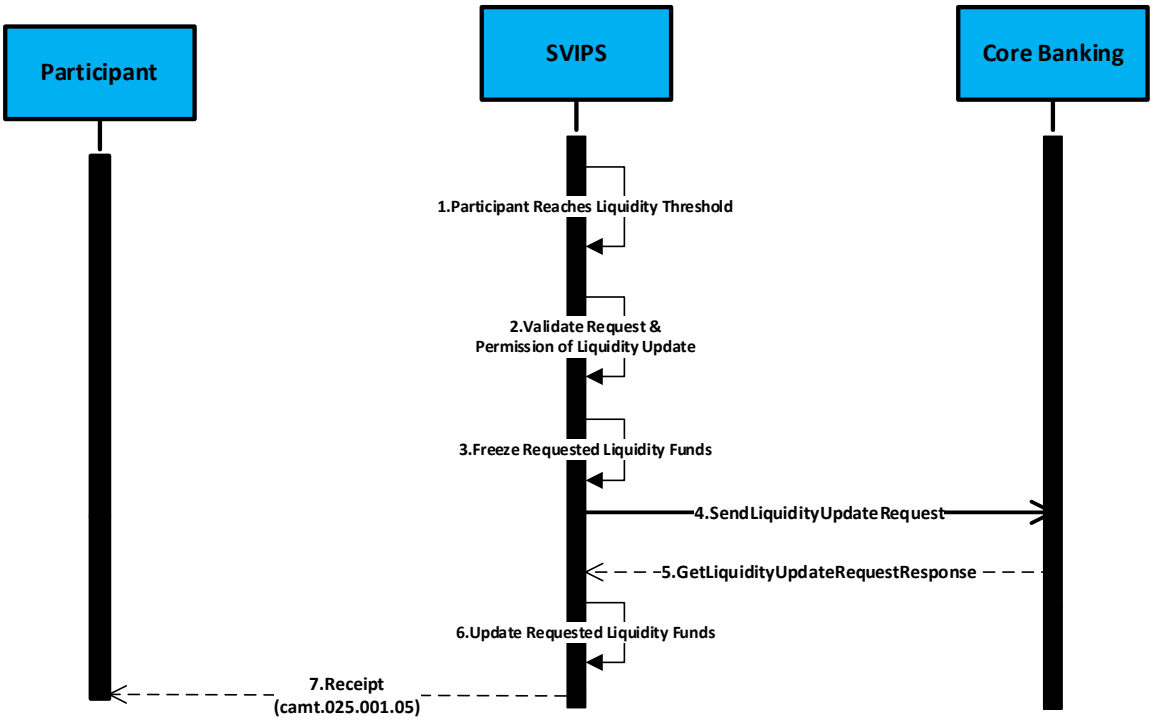
The request to manually increase or decrease liquidity can be set from the participant portal which is part of SVIPS module.

Automatic Funding and De-Funding Request

SVIPS has provision to define high and low liquidity watermark threshold. This is managed by participants through the participant portal where they can choose to set automatic or manual liquidity increment/decrement option along with high/low and optimal liquidity watermark.

Once liquidity reaches high watermark, the SVIPS can automatically generate a defunding request to the central bank core banking or RTGS system and update the respective participant limits to the optimal level defined in the system. Likewise when liquidity threshold reaches low watermark, the SVIPS request for liquidity topup from the participant pool account in central bank and credit the limit in the reflection account of the SVIPS.

For indirect participants the request for liquidity increment/decrement is carried out by the direct participant which acts as a settling participant for an indirect of clearing participant. Via notifications initiated by SVIPS, a direct participant is notified for a need for liquidity change for itself or an indirect participant. Using the participant portal the direct participant can act on the request to increase the liquidity limit for a clearing participant.



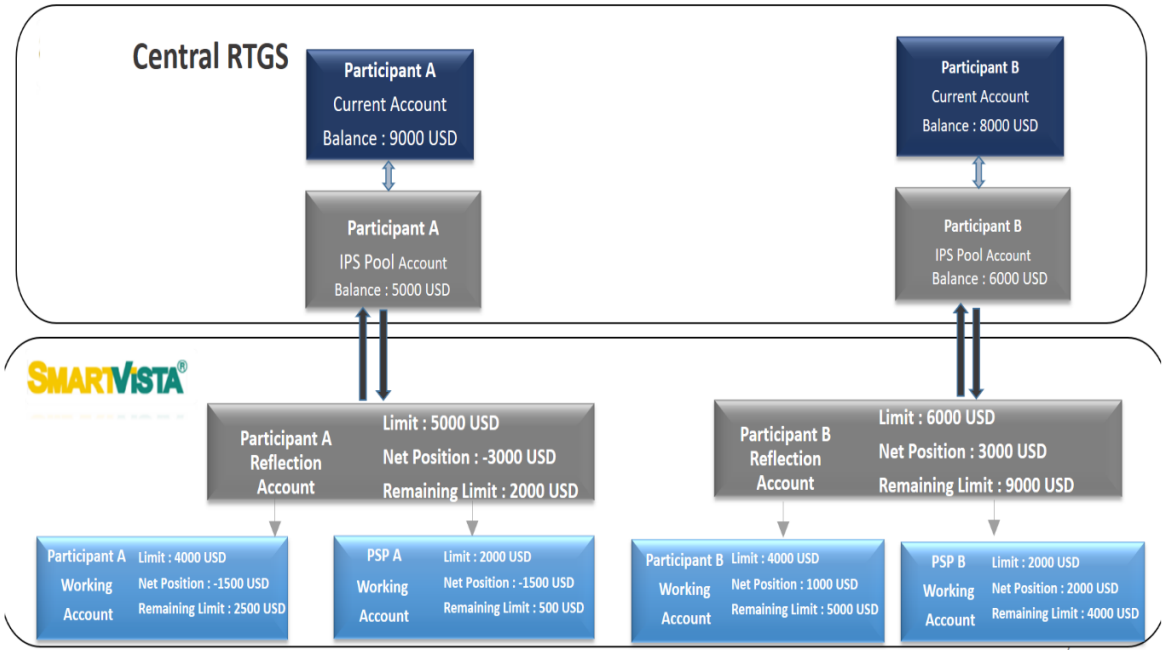
No.	Description
1	Participant reaches Liquidity threshold (either high or low)
2	SVIPS validates permission whether participant is allowed auto liquidity setup
3	SVIPS freeze the requested liquidity amount to the optimum amount set for the participant
4	SVIPS forwards Liquidity update request to core banking
5	Core banking sends response of liquidity update request
6	SVIPS updates liquidity amount
7	SVIPS sends receipt of liquidity update notification to Participant

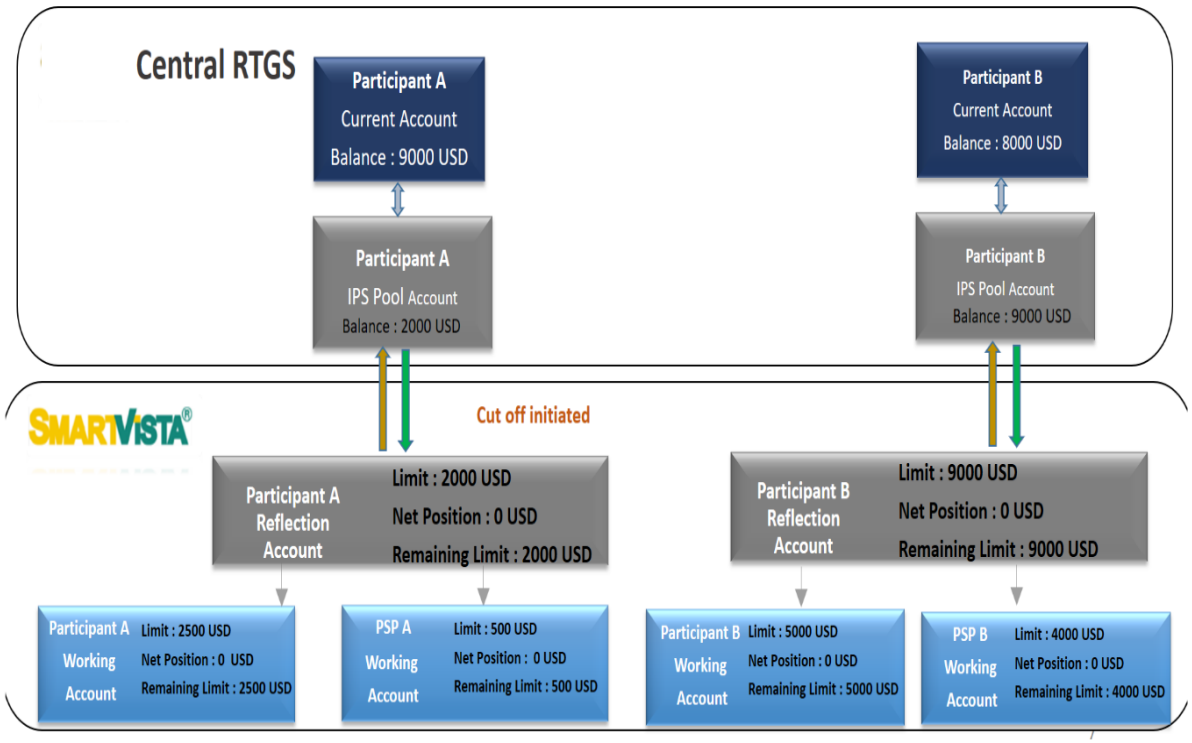
Settlement and Reconciliation

SVIPS support multilateral net settlement among all participant of an instant payment scheme. The net positons are updated in real time after every clearing message. At a particular time defined by the central bank (and usually during RTGS working hours), a net settlement is initiated from SVIPS to the RTGS. The decision to initiate net settlement can be based on a time of of day, or on the liquidity threshold defined by the participants. For example if certain

number of participant liquidity limit reach high/low watermark then SVIPS can decide to initiate net settlement to counter the liquidity risk.

Considering the clearing example in previous section let us see how the net position is updated after net settlement is triggered. This is the position just before net settlement is triggered:





After the net settlement, the following position is reflected:

The new settlement limit is updated in all account heads. Starting from the Central bank RTGS where the consolidated net position is transmitted, the IPS pool account is updated by the last remaining limit in the Participant reflection account. The net position is reset to zero and the new limit becomes the last limit of the reflection account as well as working accounts residing under its hierarchy. The net settlement is followed by their statement and reports to the respective participants for their reconciliation.

Disputes Management

The SmartVista Dispute Management solution helps financial institutions process dispute messages and resolve customers' claims. It enables users to register, investigate and make final decisions on dispute claims within one system. The solution provides a full-function case management system with the ability to initiate any dispute message of the basic dispute cycle; to run various dispute reports; and to log any users' actions in the history. It also enables users to receive automatic email notifications after predefined events, and automatically set the case due date, helping users to investigate dispute claims faster and more efficiently. The key features of the SmartVista Dispute Management solution are listed in the table below:

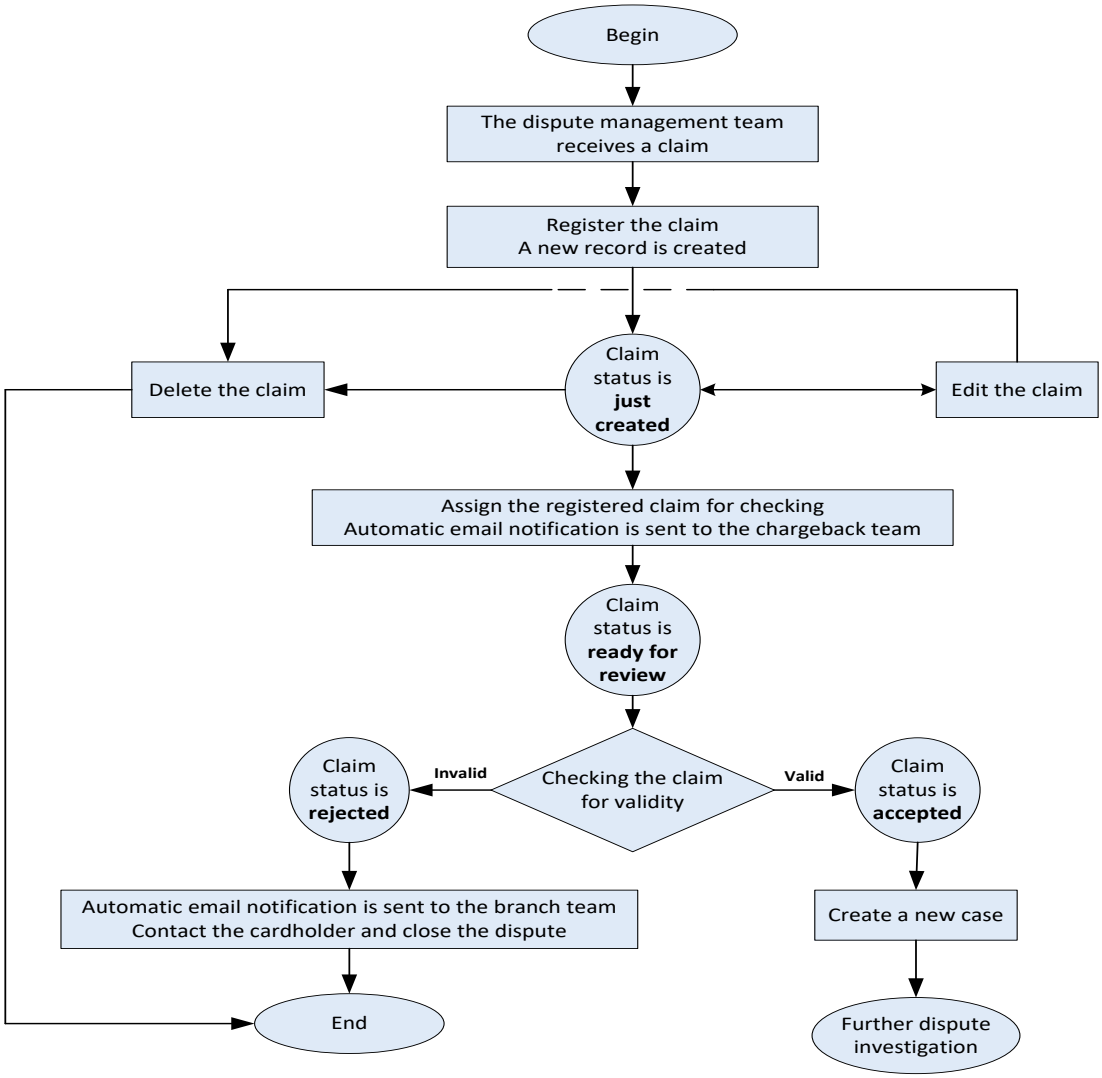
Feature	Description
Customer claims registration	The solution enables registering customer's claims and handling the acceptance of the claims process. Claims serve further as the basis for the creation of *cases*.
Case management	A *case* is a set of information about a dispute, including a customer claim, an original transaction, supporting documents, and processed dispute messages (incoming and outgoing). The solution supports the case management requirements of both parties to a dispute: issuers and acquirers. The case management feature is a set of cases with various functionality including: Case handling actions Case statuses and resolutions handling Case creation Bulk actions with cases Time management for cases Case history logging Dispute messages management
Automatic case creation	The solution supports automatic or semiautomatic case creation based on specific predefined events. A case can be created based on the following: Dispute messages from an incoming clearing file Manual matching of dispute transactions (unpaired items) received in incoming clearing files that were not automatically matched Details of the original transaction Not settled transactions (loss advice transactions) from an incoming clearing file
Bulk actions with cases	The solution enables case handling actions to be performed on multiple selected cases. Example bulk actions include: Case taking, refusing and reassigning Case hiding and unhiding Case closure and reopening Changing a team responsible for case investigation Adding comments and attachments
Due date handling	The solution supports time management for cases, in accordance with the specific time frames for initiating dispute messages, responding to incoming dispute messages and resolving disputes. If a case does not include dispute messages, the solution enables the due date to be set manually. Five calendar days prior to the due date, an automatic email notification is generated and sent to the team investigating the case.
Adding comments to cases with	The solution provides a wide range of predefined comments that can be added to a specific case. Users can also add their own comments. The addition of particular

automatic system reaction	comments can trigger relevant actions in the system, for example, transitions between case statuses or case resolutions.
Item management	*Items* are dispute messages that form part of dispute cases. The solution supports validation rules for outgoing items, and item handling, including editing, cancelling and reversing items.
Automatic email notifications	The solution provides the automatic delivery of notifications for a predefined list of users when some predefined event has occurred or is about to occur. The supported delivery channel is email.
Letter templates	The solution provides letter templates with predefined text and variable information taken relating to specific cases, facilitating the creation of form letters when handling a dispute case.

The web interface of each dispute direction is the same except for some functions that are supported only in the issuing or the acquiring directions; for example customer claims registration is only supported for the issuing part of the solution.

Customer claims registration

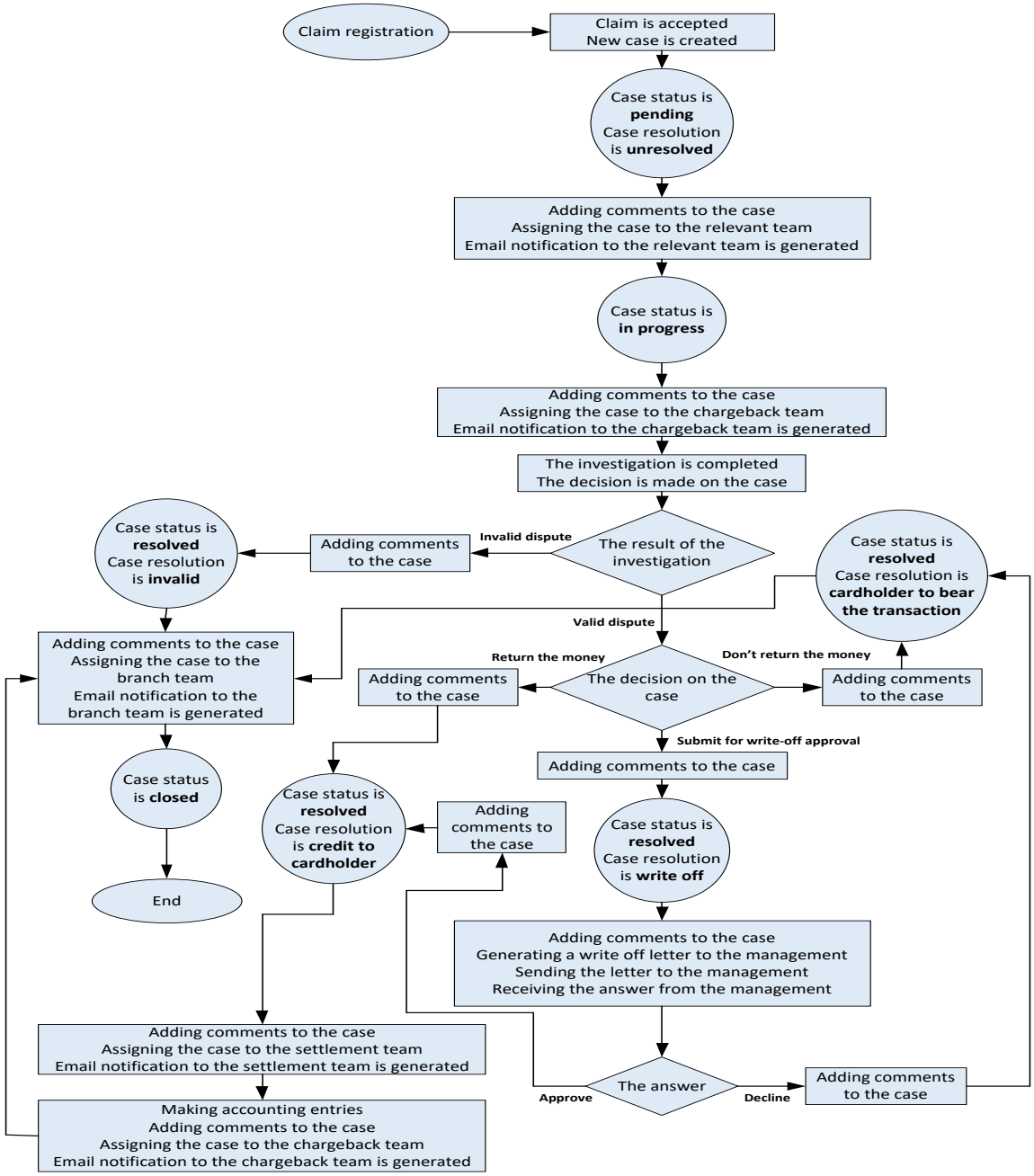
This functionality is used for the initial acceptance of customers' dispute claims and creation of dispute cases. A customer can fill out a dispute form or submit a claim through a variety of alternative channels (for example, email, phone, mobile app, feedback on the website, etc.). The process of registering a customer claim consists of two stages: creating a new record and checking (approving or rejecting) it.



When registering the claim, the user attaches any supporting documents. After registering the claim, the handling process provides basic functionality for viewing, editing and deleting the claims. When submitting the claim for review, the system generates an automatic email notification, which is sent to the common mailbox of the dispute management team. When checking the claim, the dispute management team user accepts or rejects it. If the claim is rejected, the reason for rejecting it is chosen from a predefined dropdown list or specified additionally. If the claim is accepted, the solution enables a new dispute case to be created immediately on acceptance of the claim.

Case flow

The typical case workflows and how case statuses and resolutions change within each specific flow are depicted in the diagram below:



SmartVista Technology & Security Architecture

SmartVista Integration Platform

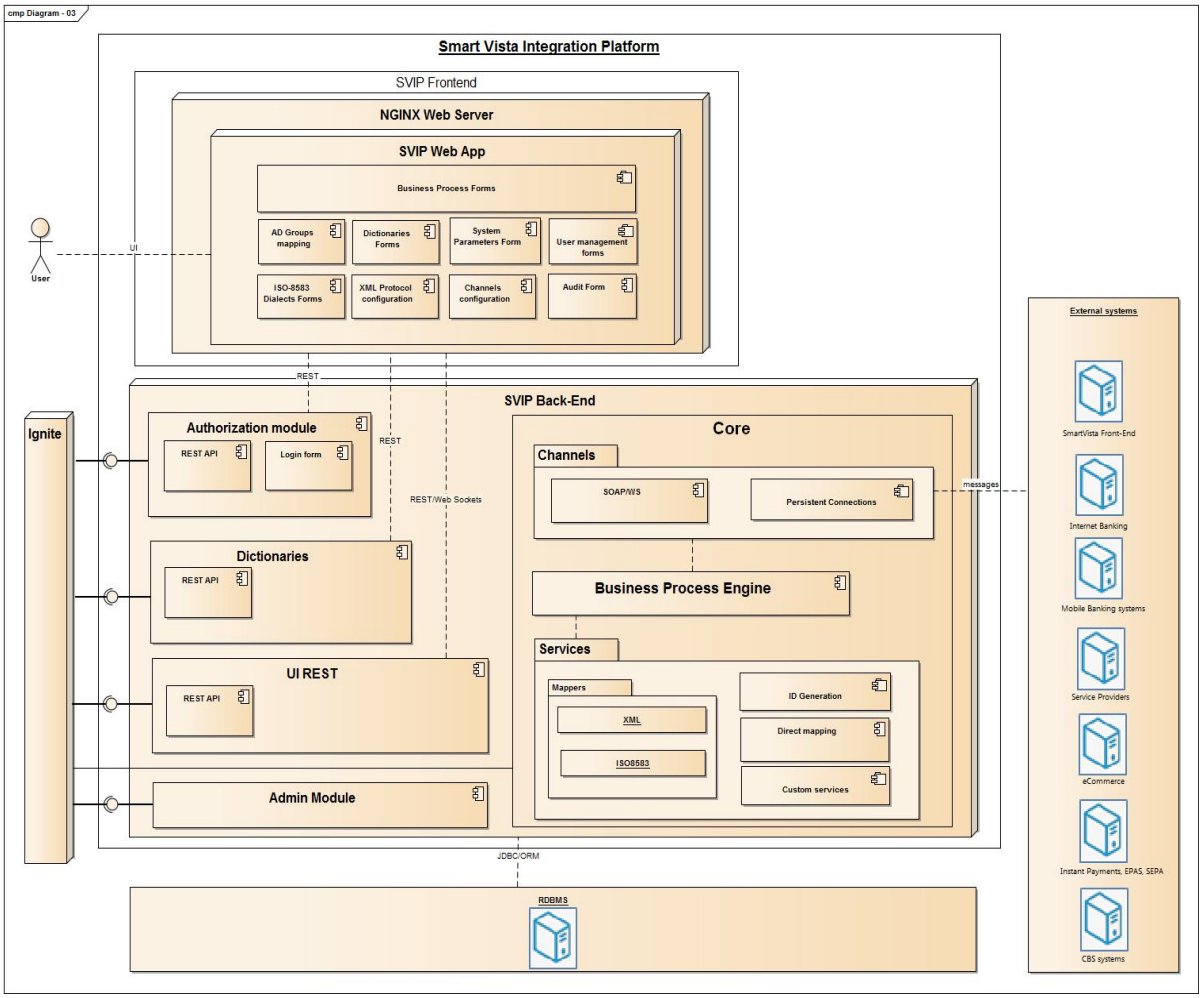
The core of the SVIPS technology is built using the SmartVista Integration Platform. The SmartVista Integration Platform is a technology framework that orchestrates all aspects of payments processing and enables business process modelling, message formatting, channel management through a packaged set of services, tools, and technologies that enable customers to extend the functionality of BPC and third-party solutions. The software solution was designed to perform flexible routing using the Business Process Engine and to transform any data format to any other data format, with the ability to add new services to perform business logic.

The main features and advantages of the SmartVista Integration Platform include:

Feature	Description
New communication protocols and formatters	The SmartVista Integration Platform supports the addition of new communication protocols and formatters using an internal flexible API.
Flexible architecture	The SmartVista Integration Platform can be adapted for any processing solution for example, account to account instant payment processing.
Flexible mapping configuration	The SmartVista Integration Platform provides a flexible mapping configuration from external protocols fields to internal attributes. For example, mapping between internal system formats and ISO-8583 (or XML) fields can be done on the fly (adding blocks, fields, tags, and bit-masks with different encoding).
Field mapping	The SmartVista Integration Platform supports composite field mapping, for example, splitting ISO-20022 fields and tags into subfields and mapping them to internal context attributes. Complex field mapping is also supported, enabling one group of fields to be mapped to another.
Configuration import and export	The SmartVista Integration Platform supports system configuration import\export.
Batch processing	The SmartVista Integration Platform supports batch processing, i.e. processing of files contained many transactions.
User tasks	The SmartVista Integration Platform supports user tasks, which are used to model work that needs to be done by an operator.
Collection of metrics	The SmartVista Integration Platform enables different metrics (for example TPS, availability,

	used thread count, and so on) to be collected and analyzed.
SOA	The SmartVista Integration Platform is built on a highly scalable, service-oriented architecture.
Clustering	The SmartVista Integration Platform supports clustering. This enables multiple core instances to be run in parallel.
Modularity	SmartVista Integration Platform's modularity enables all services to operate independently from each other. It is possible to develop and add new services to the application. The code can be reused.

The SmartVista Integration Platform consists of several major software components, whose functionality is outlined below.



At the highest level, the architecture consists of three separate components:

Back-end component
Front-end component (or user interface)
Database storage

The components are described in detail below.

Back-end component

The back-end component is the central component of the SmartVista Integration Platform. It provides the following functionality:

Data format conversion
Flexible workflow routing using the Business Process Engine
Execution of preconfigured business logic
Interaction with external systems.

The back-end component consists of the following modules:

Core module
Channels
Business Process Engine
Services
Authorization module
Dictionaries module
UI Rest module
Admin Module

Core module

The Core module is the main part of the back-end component. It includes channels, the Business Process Engine, and services.

Channels

Channels are special services that implement communication protocols and are responsible for the interaction with external systems such as core banking systems (CBSs), CRMs, service providers, channels, Internet and mobile solutions, switches, and so on. Currently, the SmartVista Integration Platform supports a protocol for interaction with SmartVista Front End using a permanent connection, as well as a web service SOAP protocol for communication in both client and server modes.

A *channel* is an entry and an exit point of a business process (for both online and offline processes). A channel receives requests from external systems and calls the Business Process Engine. Depending on the connection used (for example, a web service or an ISO 8583 service), the Business Process Engine finds the relevant business process and starts orchestration. The

Business Process Engine executes the process and calls the custom services that are required for orchestration.

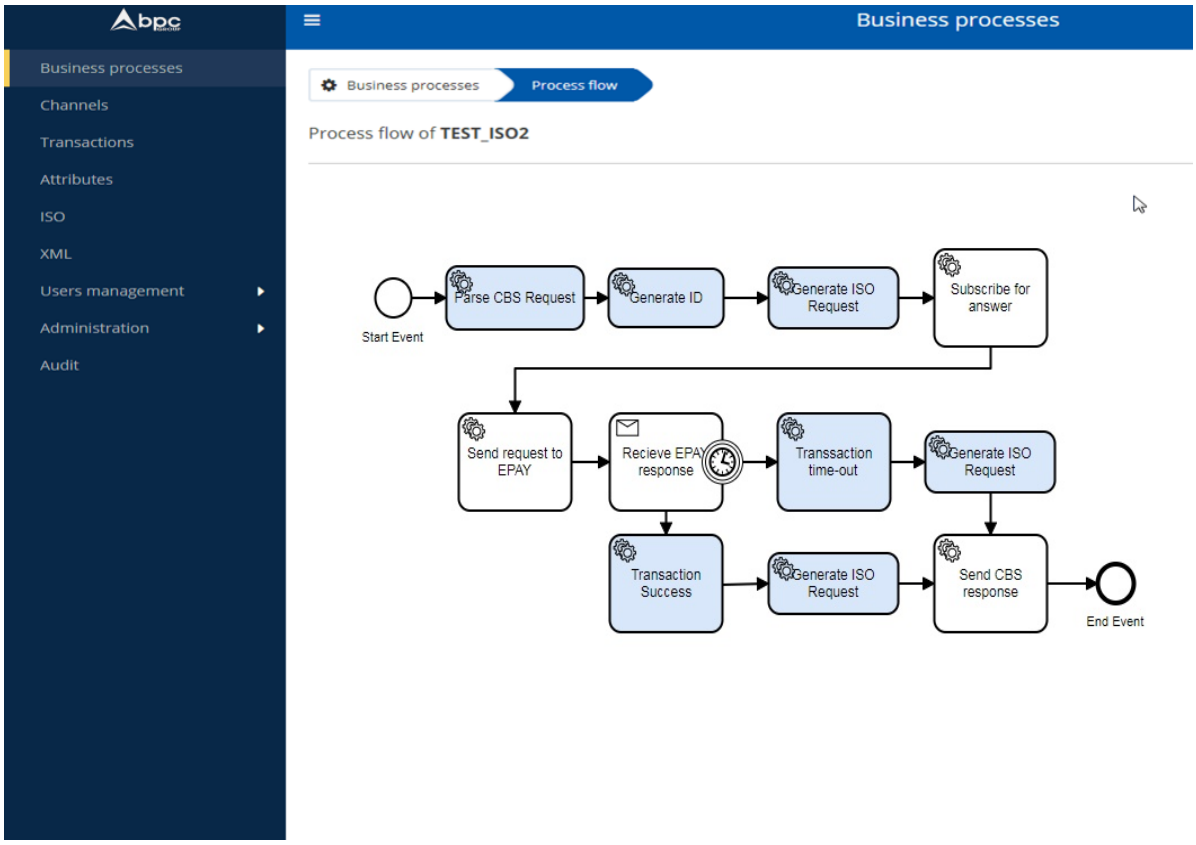
A channel can include only one workflow. A channel can also be used to send response messages and files. Templates for the following connection services are provided in the initial configuration:

Web service supporting interoperable machine-to-machine interaction over a network
REST (Representational State Transfer) — communication between the front-end (user interface) and back-end components
HTTP protocol enables communications between clients and servers
Persistent connection service providing a connection with the SmartVista Front End (SVFE) system

Business Process Engine

The Business Process Engine enables complex message flows and any associated checks to be configured. It provides flexible routing, and enables new workflow entry points to be added on the fly.

A *BPM workflow* is the business logic defined using a BPMN (Business Process Management Notation) editor (it is possible to use the built-in editor or a third-party BPMN editor). A workflow controls the steps and message flows of a business process, and it can include communications with multiple services. The below screen shot shows how workflow is constructed in BPMN editor of SmartVista Integration Platform:



An example of a basic online flow is provided below:

An external system sends an incoming online message.
The SmartVista Integration Platform identifies a workflow assigned to the online channel.
Based on a workflow specified in the business process, the SmartVista Integration Platform performs the following actions:
Parses the incoming message.
Converts the message from an external to the internal format using the internal attributes.
Creates or modifies message fields or data elements according to requirements.
Initiates a call to a service (internal or external).
Processes a response from the service.

Steps 3d to 3e are repeated based on the number of services involved in a workflow and their order, and the business logic defined in the business process.

The SmartVista Integration Platform sends a response message to the transaction initiator.

Services

Services are part of the SmartVista Integration Platform and represent a business activity with a specified outcome. Every service is independent from every other. It is possible to develop and add new service to the application. Source code can be reused.

Services contain a flexible mechanism to transform the formats employed by external systems into internal attributes, and vice versa. The SmartVista Integration Platform implements the following services:

XML constructor (parser or mapper) — defines the XML protocol structure, and converts XML data messages to internal context attributes and vice versa

XML Splitter Service – consumes input stream of the batch XML data and produces split subdocuments

XML Batch Writer Service – writes batch data to file

XML Aggregator Service – consumes subdocuments and accumulate them for preparing batch data

ISO constructor (parser or mapper) — defines the ISO 20022 structure, and converts binary ISO 20022 messages to internal context attributes and vice versa in accordance with the requirements of the ISO 20022 standard

SWIFT MT constructor (parser or mapper) — defines the Swift MT protocol structure, and converts Swift MT messages to internal context attributes and vice versa in accordance with the requirements of the Swift MT standard

Direct Mapping service — sets up of attribute values depending on conditions

ID Generation service — generates the ID of the transaction based on user-defined rules

Subscription services — receives and matches messages in an asynchronous interaction

Update Transaction Status Service — updates the transaction status (for example, setting a transaction status to Success)

Load Balancer Response Service — calculates metric values and builds a response message based on the WatchDog API (interaction with the SmartVista Load Balancer)

Stand-in and Stand-alone module

SVIP module supports stand-in and stand-alone operations modes. Stand-in parameters are defined per each connection. Stand-in mode supports offline authorizations in four different algorithms:

preliminary authorization - the parameter is checked if the IPS is connected to the participant and transaction parameters allow the transaction to be sent to the participant for authorization.

stand-in authorization - stand-in authorization is performed when a transaction was sent to the participant, but the connection to the participant was lost.

preliminary stand-in (stand-alone) authorization - complete transaction processing is performed in IPS. The participant is either not present or is not used for this transaction.

Authorization - when there is a reply to an authorization from the participant, IPS performs the final update of the data for the transaction.

Authorization module

The Authorization module provides the authorization functionality for user interface users. It includes a login page for when users log in for the first time and the ability to configure user privileges. It uses its own REST API.

Dictionaries module

The Dictionaries module enables the configuration of multiple dictionaries, for example, types of transactions, currencies, countries, and so on.

UI Rest module

The UI Rest module is responsible for the communication between the back-end and front-end components. It uses the RESTful API.

Admin module

The Admin module can start, stop, restart, and obtain information about the system components that participate in an Ignite cluster. The module is a dispatch service for system wide Java processes. The module uses Apache Ignite to route requests to the relevant components.

Front-end component (user interface)

A web-based user interface provides easy access to the SmartVista Integration Platform functionality and enables the following tasks to be performed:

- Viewing and adding new business processes
- Editing business processes using the built-in BPMN editor
- Managing business processes (start, stop, and restart)
- Downloading and uploading business processes via files
- Cloning business processes
- Configuring mappings in a business process
- Cloning mappings settings in a business process
- Configuring XML protocols
- Cloning XML protocols
- Viewing the list of transactions with their attributes and logging information (based on the selected debug level)
- Viewing of Batch processing status with details and related transactions
- Adding, modifying, and removing attributes
- Viewing attributes of transactions
- Viewing and managing of User Tasks
- Managing users and roles
- Cloning users
- Configuring Active Directory mappings
- Viewing user sessions

Importing XML protocols
Exporting XML protocols
Configuring Swift MT message structure
Configuring ISO-8583 dialects
Cloning ISO-8583 dialects
Importing ISO-8583 dialects
Exporting ISO-8583 dialects
Adding new channels
Cloning channels
Viewing the status of channels

Auditing user actions
Comparing changes for auditing user actions
Modifying system parameters
Configuring dictionaries
Viewing the status of the Core module
Managing the Core module (start, stop, and apply configuration changes)
Viewing the versions of the SmartVista Integration Platform components and libraries

1.

2.

The front-end component consists of web based pages that are written in JavaScript using the ExtJS framework. The application is deployed on an NGINX web server.

The architecture of a software system is almost never limited to a single architectural style, but is often a combination of architectural styles that make up the entire system.

Architectural style	Description
Component-based architecture	Decomposes application design into reusable functional or logical components that expose well-defined communication interfaces.
Layered architecture	Partitions the concerned application into stacked groups (layers).
Service-Oriented Architecture (SOA)	Refers to applications that expose and consume functionality as a service using contracts and messages.

Component-Based Architectural Style

Component-based architecture describes a software engineering approach to the design and development of the system. It focuses on the decomposition of the design into individual functional or logical components that expose well-defined communication interfaces containing methods, events, and properties. This provides a higher level of abstraction than object-oriented design principles, and does not focus on issues such as communication protocols and shared state.

The key principle of the component-based style is the use of components that are:

- **Reusable -** Components are usually designed to be reused in different scenarios, in different applications. However, some components may be designed for a specific task alone.
- **Replaceable** - Components may be readily substituted with other similar components.
- **Not context specific -** Components are designed to operate in different environments and contexts. Specific information, such as state data, should be passed to the component instead of being included in or accessed by the component.
- **Extensible -** A component can be extended from existing components to provide new behavior.
- **Encapsulated** - Components expose interfaces that allow the caller to use its functionality, and do not reveal details of the internal processes or any internal variables or state.
- **Independent** - Components are designed to have minimal dependencies on other components. Therefore, components can be deployed into any appropriate environment without affecting other components or systems.

The following are the main benefits of the component-based architectural style:

- **Ease of deployment -** As new compatible versions become available, you can replace existing versions with no impact on the other components or the system as a whole.
- **Reduced cost -** The use of third-party components allows you to spread the cost of development and maintenance.
- **Ease of development -** Components implement well-known interfaces to provide defined functionality, allowing development without impacting other parts of the system.
- **Reusable -** The use of reusable components means that they can be used to spread the development and maintenance cost across several applications or systems.
- **Mitigation of technical complexity -** Components mitigates complexity through the use of a component container and its services. Example of component services include component activation, lifetime management, method queuing, event management, and transactions.

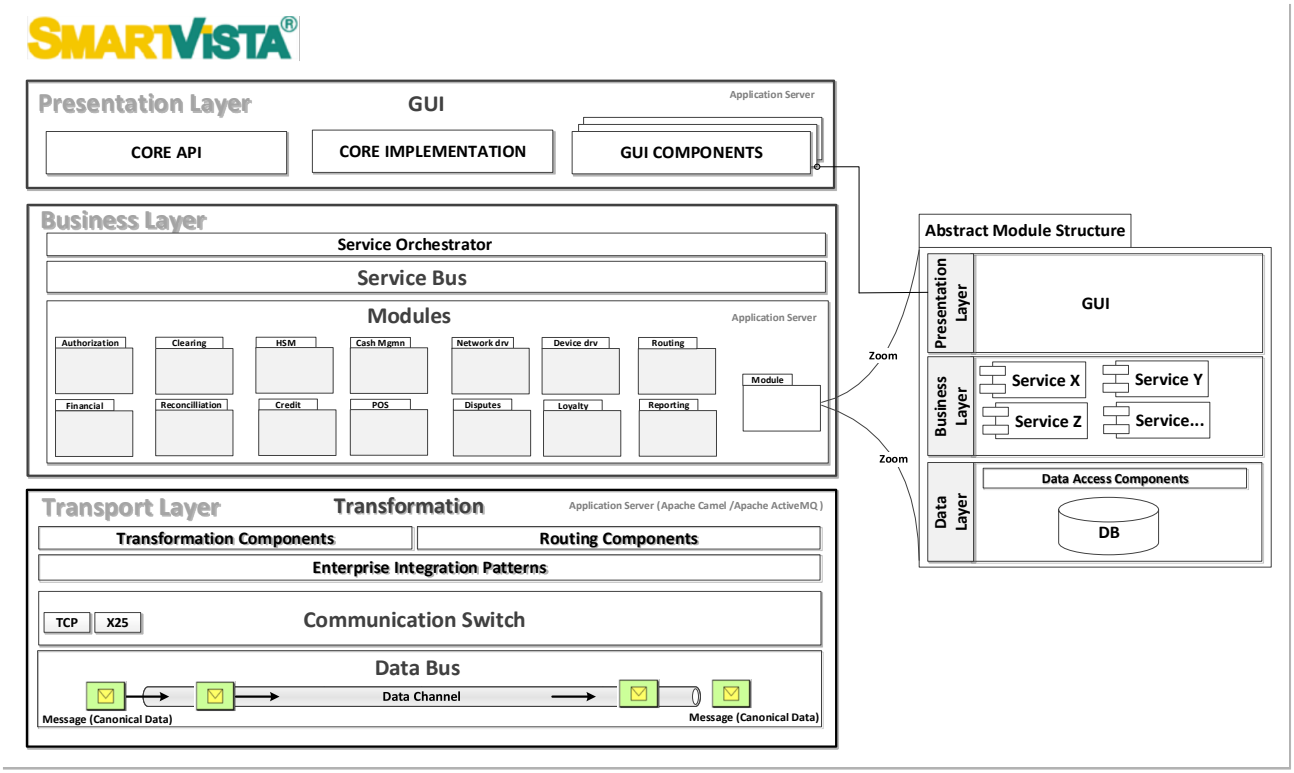
Design patterns such as the Dependency Injection pattern or the Service Locator pattern can be used to manage dependencies between components, and promote loose coupling and reuse. Such patterns are often used to build composite applications that combine and reuse components across multiple applications.

Layered Architectural Style

Layered architecture focuses on the grouping of related functionality within an application into distinct layers that are stacked vertically on top of each other. Functionality within each layer is related by a common role or responsibility. Communication between layers is explicit and loosely coupled. Layering your application appropriately helps to support a strong separation of concerns that, in turn, supports flexibility and maintainability.

SmartVista consists of presentation layer, business layer components and transport layers. SmartVista is an integration component, providing interaction of existing and new modules within SmartVista based automated business processes. SmartVista uses SOA-design composed of services developed using a layered architectural approach and message bus.

Element Name	Description
Presentation Layer	
Core API	Core API consists of a set of services. Services provide GUI components for functional solutions to common and frequently occurring task.
Core Implementation	The service implementation may be part of the core API or provided core implementation, if allowed to use different implementations.
GUI Components	GUI components contain functionality that is available to end-users (operators of the bank). During application startup the core API collects information about installed GUI components: menu items, permissions, configuration parameters.
Business Layer	
Service Orchestrator	Is the engine of business processes (BPE) - a component of the system based on the principles of SOA (see Service-Oriented Architectural Style) that implements the business logic of the system by means of executable business processes.
Service Bus	Abstract entity consists of a pool of services invoked by engine business processes (service orchestrator).
Modules	The module is an abstract element of the system. The module defines an isolated step of processing operations. The module implements calls atomic services.
Transport Layer	
Transformation components	Components are responsible for converting native data format to the canonical data model SmartVista.
Routing components	Components provide transportation data to the data bus.
Enterprise Integration Patterns	Patterns and strategies for enterprise application integration via messaging.
Communication Switch	Communication Switch component to connect online systems.
Data Bus	Data bus used for message transport.
Data Channel	The main element of the data bus (example - MQ queue).
Message	Canonical format data transferred in the form of messages on the data channel.



Service-Oriented Architectural Style

Service-oriented architecture (SOA) enables application functionality to be provided as a set of services, and the creation of applications that make use of software services. Services are loosely coupled because they use standards-based interfaces that can be invoked, published, and discovered. Services in SOA are focused on providing a schema and message-based interaction with an application through interfaces that are application scoped, and not component or object-based. An SOA service should not be treated as a component-based service provider. The SOA style can package business processes into interoperable services, using a range of protocols and data formats to communicate information. Clients and other services can access local services running on the same tier, or access remote services over a connecting network.

The key principles of the SOA architectural style are:

- **Services are autonomous.** Each service is maintained, developed, deployed, and versioned independently.
- **Services are distributable.** Services can be located anywhere on a network, locally or remotely, as long as the network supports the required communication protocols.
- **Services are loosely coupled**. Each service is independent of others, and can be replaced or updated without breaking applications that use it as long as the interface is still compatible.
- **Services share schema and contract, not class.** Services share contracts and schemas when they communicate, not internal classes.

- **Compatibility is based on policy.** Policy in this case means definition of features such as transport, protocol, and security.

Common examples of service-oriented applications include sharing information, exposing industry specific data or services over an extranet, and creating mash-ups that combine information from multiple sources.

The main benefits of the SOA architectural style are:

- **Domain alignment.** Reuse of common services with standard interfaces increases business and technology opportunities and reduces cost.
- **Abstraction.** Services are autonomous and accessed through a formal contract, which provides loose coupling and abstraction.
- **Discoverability.** Services can expose descriptions that allow other applications and services to locate them and automatically determine the interface.
- **Interoperability.** Because the protocols and data formats are based on industry standards, the provider and consumer of the service can be built and deployed on different platforms.
- **Rationalization.** Services can be granular in order to provide specific functionality, rather than duplicating the functionality in number of applications, which removes duplication.

Supported Platforms

Platforms	OS	RDBMS	Application Servers	HSM
HP Integrity Nonstop **IBM Power Systems (System p, System i)** **HP ProLiant Systems (ML, DL, BL … all x86)** **HP Integrity rx Systems** **SUN SPARC Systems (M, T ..all x86)** **Stratus ft Server** **VMware EX**	HP Nonstop OS H-, G-, J-Series HP HPUX 11 IBM AIX 5.3, 6.1 RedHat Linux 5 SuSe Linux 11 OEL Linux 5 Sun Solaris 10 IBM I (i5/OS)	HP SQL/MX Oracle 9i, 10gR2, 11gR1, 11gR2 and DB2 9.7 (Cobra)	• Oracle WebLogic • IBM WebSphere • JBoss	Thales 8000/ PayShield 9000, SafeNet EFT Luna, HP Atalla

SmartVista can run on a laptop with a fairly low specification. For normal production operations, however, we would recommend the use of multiple servers, ideally across multiple

sites, with replication between sites. BPC always provides specific sizing recommendations to its clients, based on criteria detailed below.

Reliability, Availability and Scalability

The SmartVista solution can be scaled in both modes:

- Scale Vertically – grow with extra threads and instances on a single server
- Scale Horizontally – grow with extra threads and instances on an additional server

Scale-Up and Scale-Out scenarios available to distribute system processes across multiple CPUs server or across several servers, with multiple instances of similar processes running concurrently, if needed, to boost throughput.

SmartVista has achieved benchmark results of over 7,000 TPS and handled peak transaction volumes in excess of 2,000 TPS, in a live production environment, at one of our existing customers.

Based on the specific setup of the recommended Production, Back-Up and Test environments, SmartVista provides a range of backup and recovery scenarios, from manual to fully automatic, based on SmartVista , UNIX and Oracle (Oracle Recovery Manager) tools and features. With the recommended storage mirroring and automatic failover to the Back-Up system, an average RPO (Recovery Point Objective) of 5 to 10 minutes is realistic, but will depend on the specific configuration.

The Disaster and Recovery server works in standby configuration. Data replication between production storage and DR storage is provided by Oracle replication tools such as Oracle Data Guard (also Golden Gate or any other DB replication tools can be used).

For backup and restore procedures, BPC recommends setting up separate Production, Back-Up and Test SmartVista environments (instances); Production for business operations, Back-Up for emergency failover and Test for testing fixes and modifications before deployment to Production.

The SmartVista solution supports both "Active-Active" and "Active-Passive" architectures, enabling full redundancy and high availability within each site and between the two sites. There are two typical scenarios to use for active-passive and active-active configurations in order to minimize downtime:

Active-Passive Configuration

- Perform switchover to the backup node with downtime of about a couple of minutes
- Shutdown and then upgrade the target node:
    - Update hardware (add more CPUs, memory, etc.) OR

- Update operating system (OS) or RDBMS OR
- Update application

- Perform switch back

Active-Active Configuration

- Perform switchover to the second production node with no downtime
- Shutdown and then upgrade the target node:
  - *Update hardware (add more CPUs, memory, etc.) OR*
  - *Update operating system (OS) or RDBMS OR*
  - *Update application*
  - *Perform switch back*

The procedures that are used by BPC's specialists for backup are the following:

- Full database and binaries backup is performed on a weekly basis to physical or virtual tape library by Oracle Recovery Manager (Oracle RMAN) and HP Data Protector
- Incremental database backup is performed on a daily basis using the same set of tools (Oracle RMAN and HP Data Protector)

For DR site data replication, HP Continuous Access (hardware-level) or Oracle DataGuard (software-level) is recommended.

In fact, there are no special SmartVista requirements, as the system utilizes an industry wide platform base, such as operating system, application server and database. There are no limitations in the use of industry standard backup/recovery best practices for OS, DB and application server. For example, a centralized backup system (e.g. IBM Tivoli, Veritas Backup) with the necessary agents for OS, Database and application server can be used, or application specific tools like Oracle RMAN. Usually these tools don't require downtime.

SmartVista Testing Tool

SmartVista doesn't only offer the ability for any to any message transformation and orchestration, but it also comes with full testing tool to enable bank to run full and complete tests to ensure that the system functions properly after any configuration changes and enhancements have been made to it.

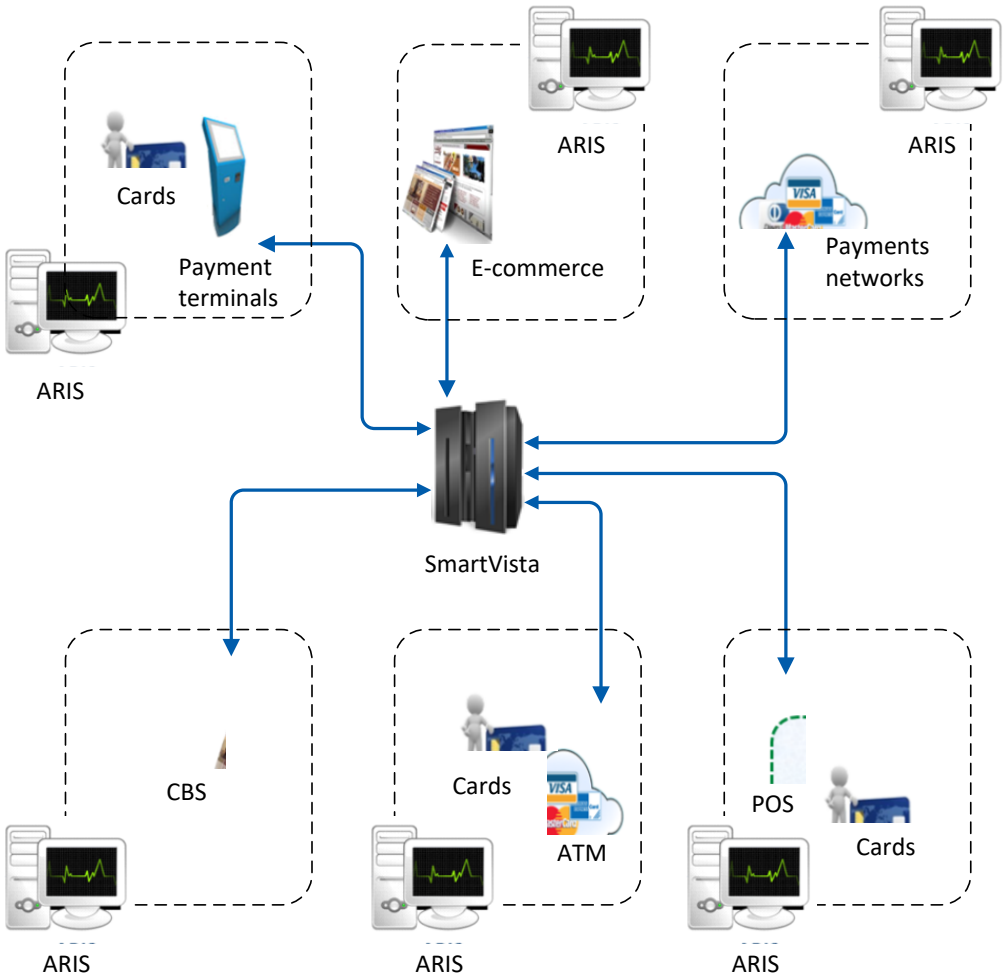
SmartVista's Automated Rapid Integration System (ARIS) solution provides emulation of terminal devices and network entities within one system, and enables test engineers to configure the interactions between them. This makes it possible to create a test environment

and manage the testing process from a single, central point. It can also be used for off-line certification with member banks or for testing with other national switches.

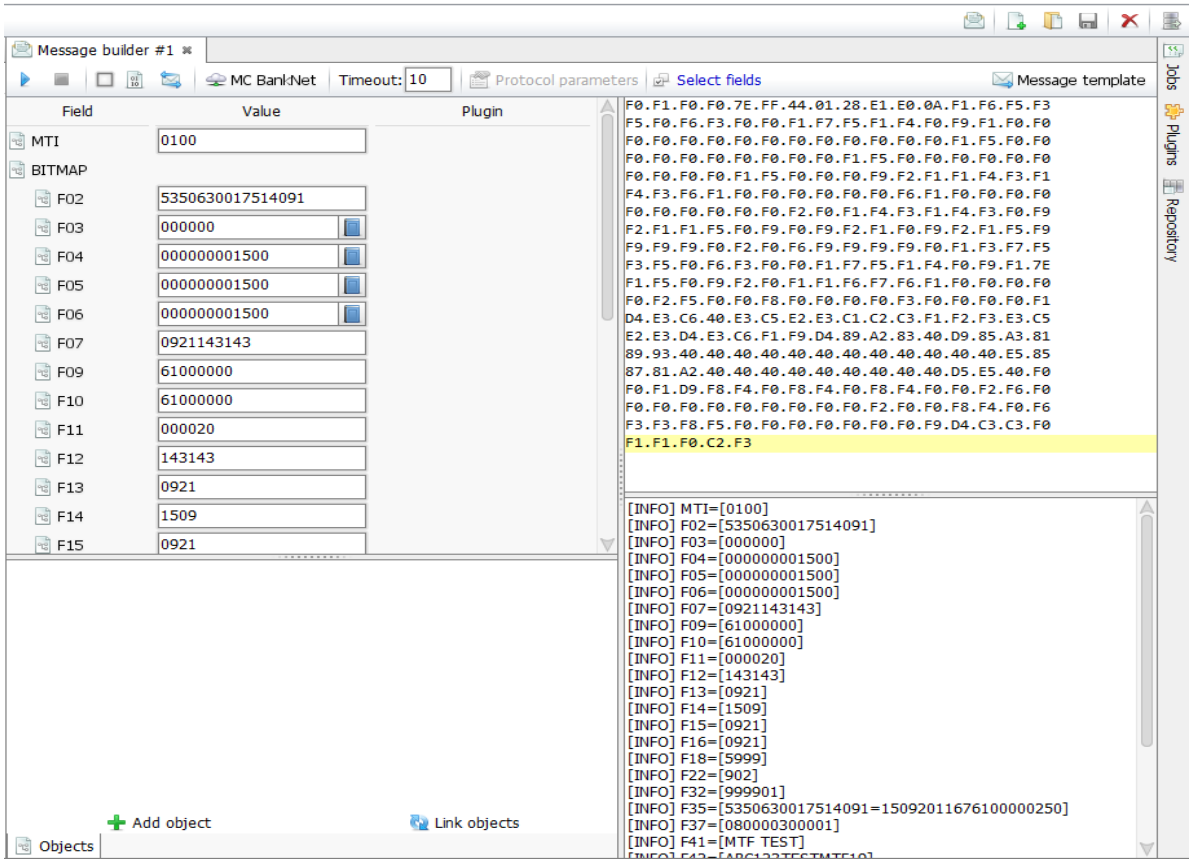
ARIS can emulate the operations and behavior of the following entities:

- Payments systems
- Hosts
- POS
- ATM/kiosk
- HSM

It enables a user to perform testing using different scenarios without the involvement of the real networks and terminal devices. ARIS enables users to configure protocols for various entities, and if necessary, make necessary changes on the fly without any code modifications. Scenarios can be configured and then added to jobs, which can then be scheduled for execution.

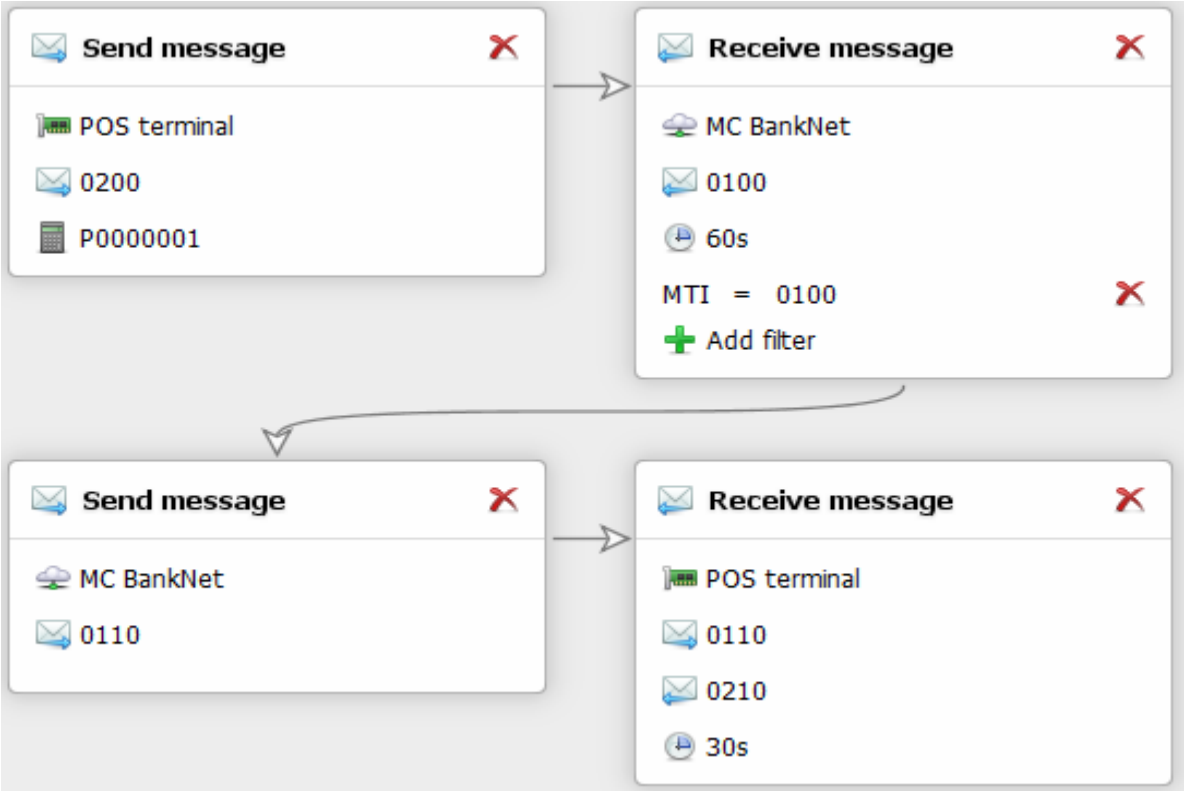


ARIS solution provides a tool called the Message Builder that can send messages and receive responses using preconfigured message templates, which test engineers populate with the relevant values.

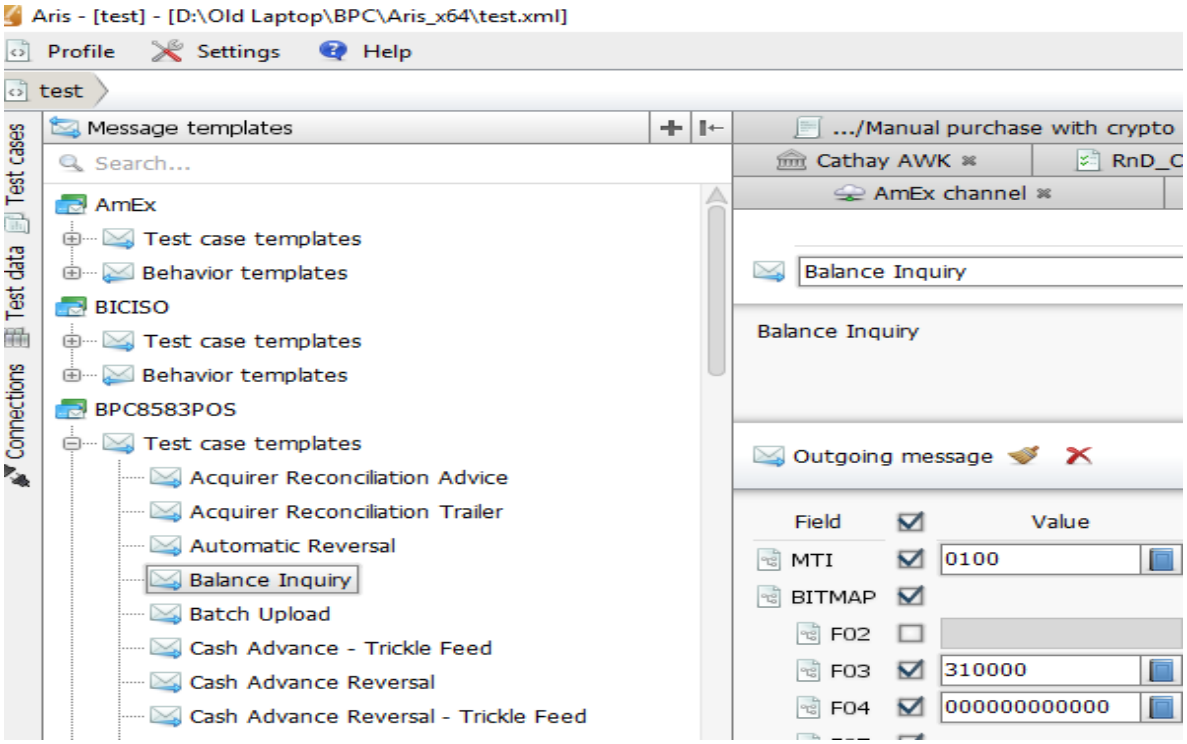


Transaction Scenarios can be used for complex test cases, for example, member bank certification, require a test engineer to test the processing of different message types with different parameters, or to test different routes to ensure that the system is able to receive a specific message from a member bank, and send back a proper response. It is possible to configure different service types representing terminals and networks, and send messages through them as if they were real devices.

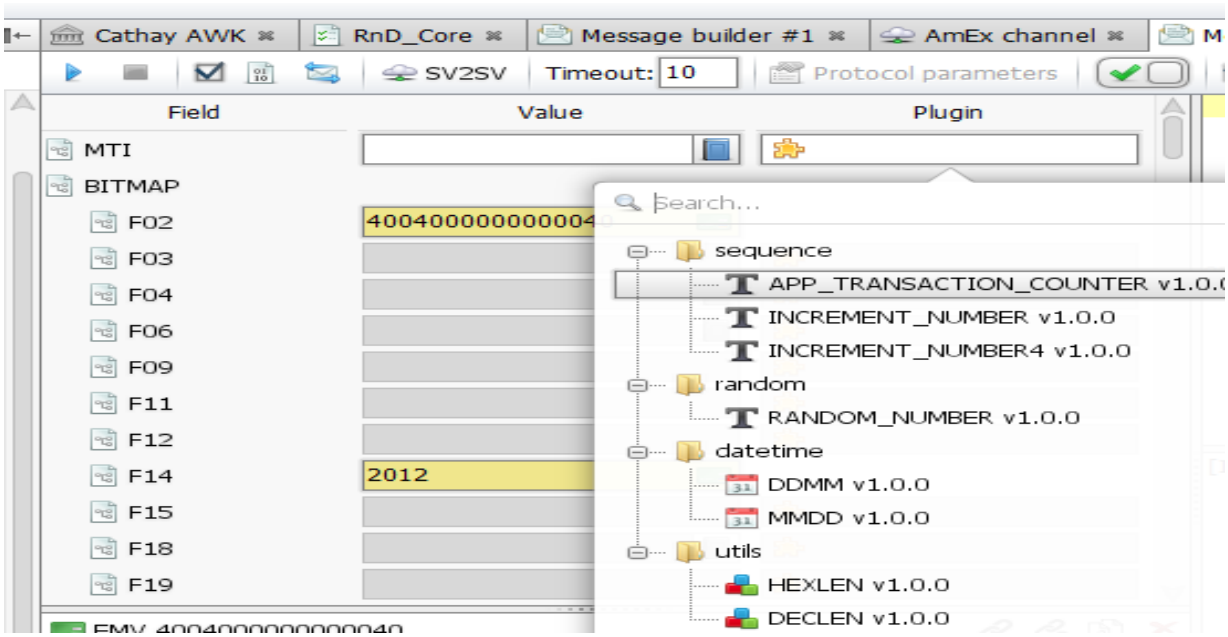
A *scenario* is a set of action blocks linked to each other and executed sequentially. Each action block performs an action, for example, sending a message, receiving the response, matching results, and so on.



The solution comes preconfigured message templates for interfaces such as Visa Base I, ISO 8583, and MC BankNet; UAESwitch and GCCNet specific scenarios can be configured as well.



ARIS also enable the creation of messages from templates and provide plugins which are add-on modules that can be independently compiled by third-party developers to enhance the system functionality. If a field value (such as sequence number, date or time) can be generated automatically, the ARIS solution uses a plugin associated with the field. To automatically populate a field with a value using a plugin, a test engineer activates the value of the corresponding plugin from a list of plugins



Setting up of PKI

Root Certification Authority

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption. It is a collection of hardware, software, and processes that support the use of public key cryptography and the means to verify the authenticity of public keys. PKI enables users and computers to verify the identity of parties they're communicating with, and securely exchange data over private networks as well as public networks such as the Internet. For the NBM RTRP scheme, the use of PKI is to create trust among varied direct and indirect participants and in some cases with their end devices (mobile app) as well.

The entity that will issue digital certificates is called Certificate Authority (CA). NBM will act as a CA once the PKI infrastructure is established with the roll out of the payment system. The infrastructure will composed of Offline Root CA which will be hosted in a physical isolated secure room with its CA server and offline HSM. A key pair of root CA will be generated in HSM certificate. Subsequently the CA certificate will be imported in to the CA server. There will be an Issuing Intermediate Certification Authority setup in NBM, with its own CA server and HSM. A certificate signing request will be issued from Intermediate CA HSM to the Root CA. The Root CA will sign the certificate, which will be imported in to the Issuing CA. From this point onward, any organization that require a certificate will request the Issuer CA to issue it. The payment application will generate key pair in its HSM and a Certificate Signing Request will be submitted to the Issuer CA. The issued certificate generated by the Issuer CA will subsequently be imported in the payment application server.

A typical PKI setup is composed of two tiers. It has following components:

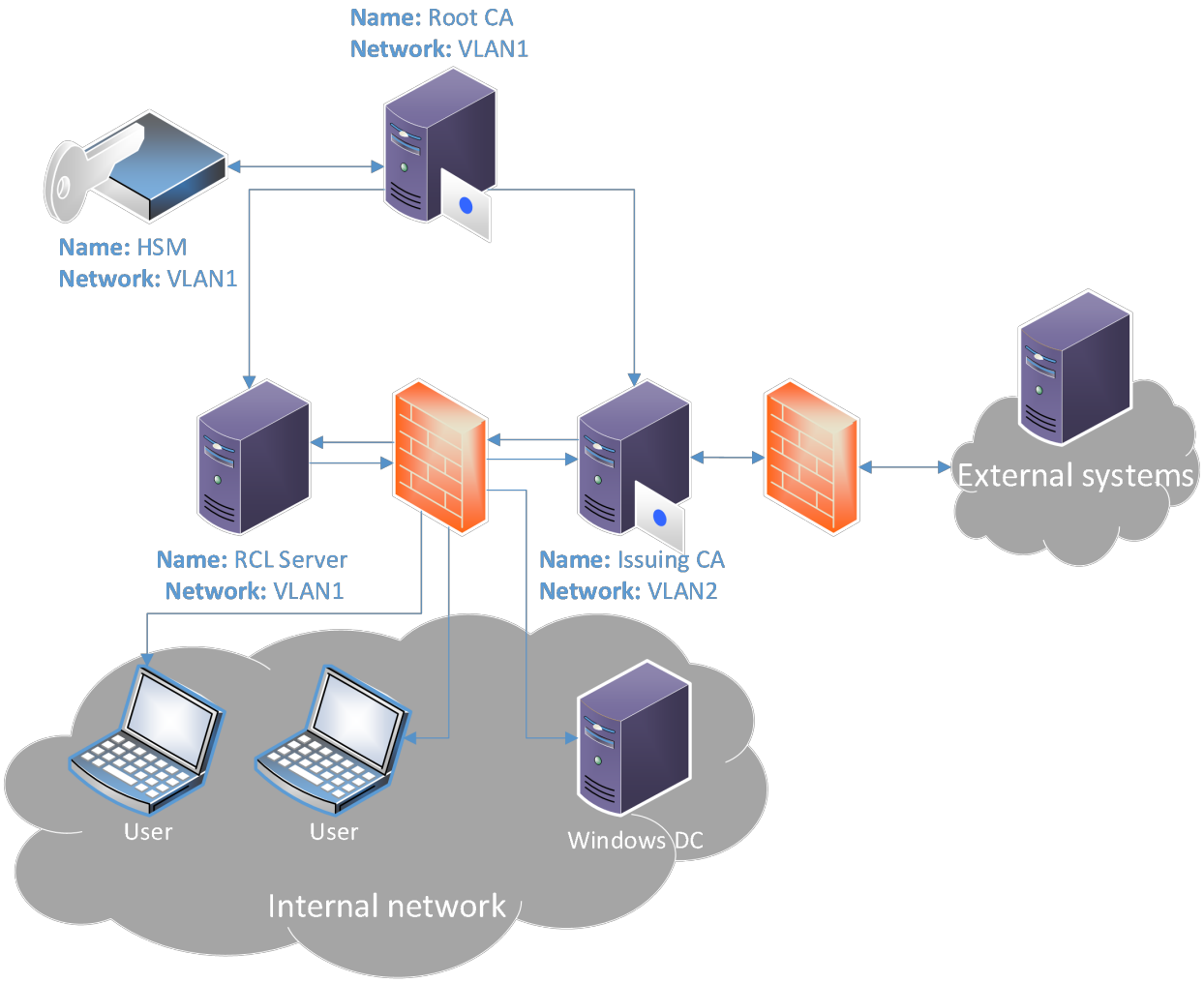
- **Offline Root CA**
  This is the most secure component of the PKI. It is isolated from the existing datacenter environment of a client. It issue the root certificate for the intermediate CA

- **Tier-1 CA**
  This is online CA and that issues certificates to the participants and the central payment system

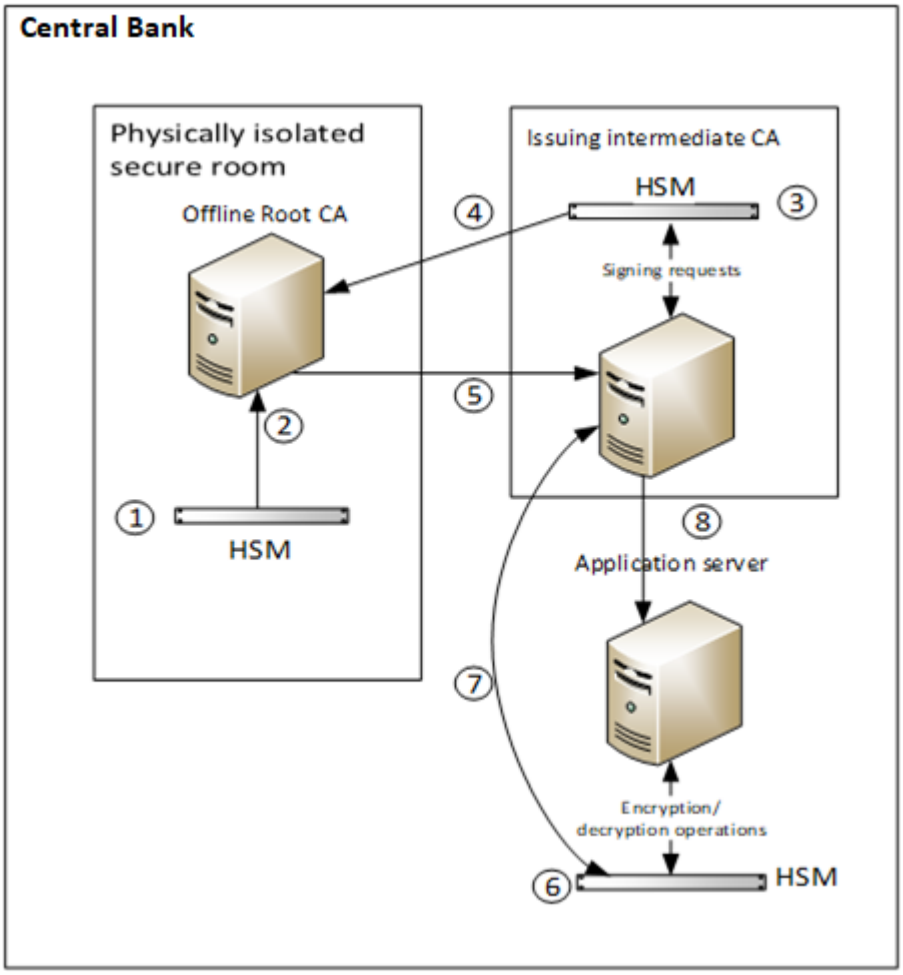
- **CA Enrollment**
  Certificate issuing request from participants are managed from this component

- **Directory Server**
  This is a public server accessible by the participant and it maintains the complete directory of public certificate and certificates revocation list (CRL). This is available usually over a web interface to the participants

BPC uses and has proposed Microsoft Active Directory Certificate Services as a Certificate Authority Server with this proposal.



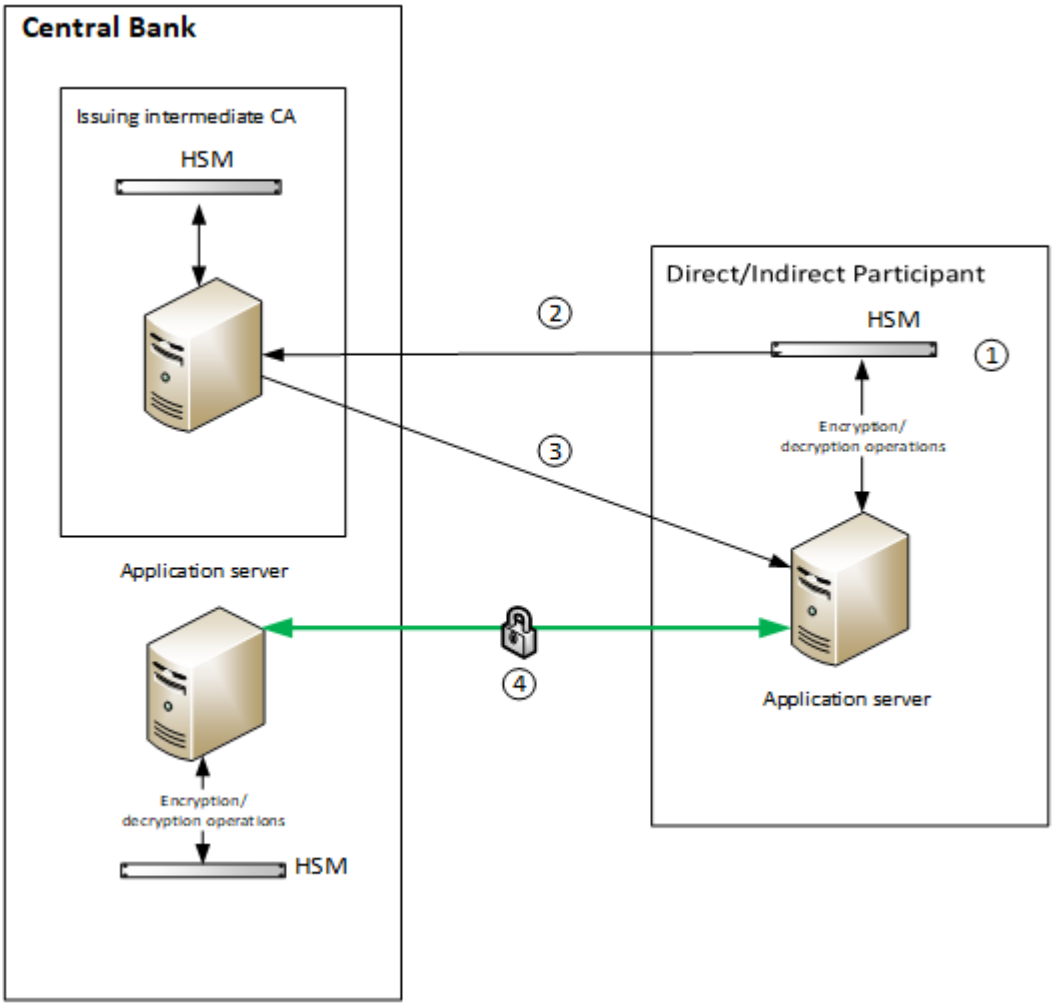
Root Authority Setup



1. Key pair for root CA generated in HSM Certificate
2. CA certificate exported to CA server
3. Key pair for issuing CA generated in HSM
4. Certificate signing request (CSR) transferred to Root CA
5. Signed certificate imported into Issuing CA
6. Key-pair for application server is generated
7. CSR is submitted to issuing CA
8. Issued certificate imported to application server

Participant On-boarding on PKI

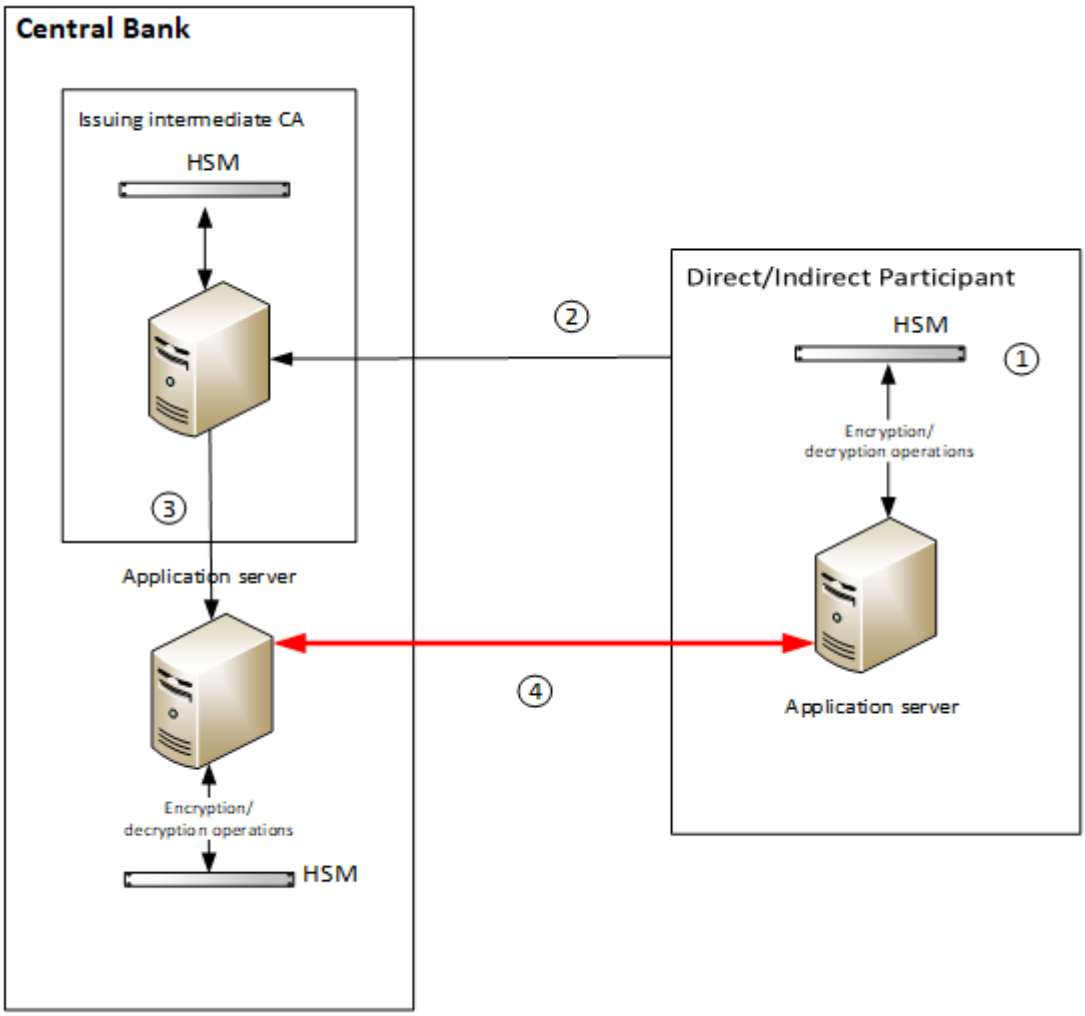
Both direct and in-direct participants can request NBM to issue digital certificates. The steps required to establish certificate trust are explained in the diagram below.



1. Participant generates key-pair in their HSM.
2. Certificate signing request is submitted to NBM issuing CA.
3. NBM CA issues certificate which is then imported to banks' application server.
4. A secure communication channel is now established between NBM and participants with mutual authentication.

Participant Certificate Revocation

Although PKI trust establishment should be a highly secure activity, there is always a chance of certificates being compromised. In such a case, the CA revokes the issued certificate and published a certification revocation list (CRL) that is then shared with all the participants. The following diagram explain the certification revocation steps.



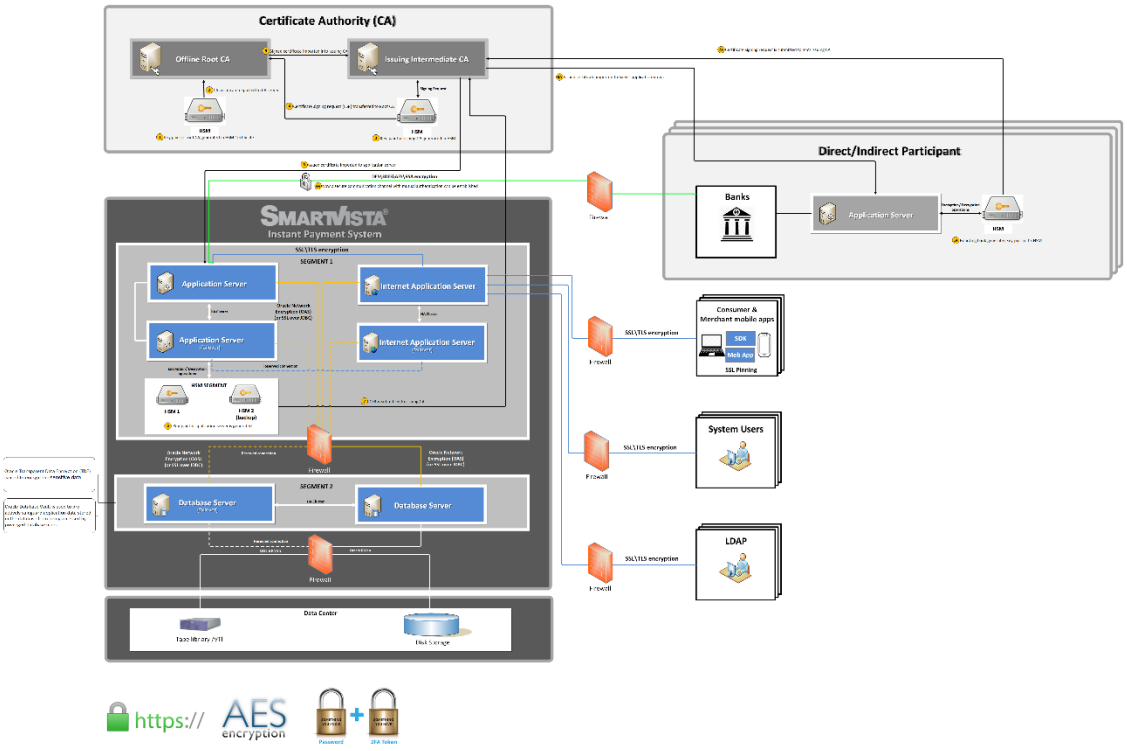
1. A participant certificate is compromises.
2. Particiapant reports incident to NBM
3. NBM issuing CA revokes participant's certificate and publish new certificate revocation list (CRL)
4. Secure channel cannot be established because one certificate is untrusted.

SmartVista Security Architecture

SmartVista provides best in class security practices for secure development, and implementation of Instant payment solution. The SmartVista platform is certified as per Payment Application Data Security Standards (PA-DSS v3.2) which is a global security standards created by major international payment schemes. The purpose of PADSS is for the payment application vendor to develop and deploy secure payment application that offer top of the line protection in all security aspects.

Some of the highlights of SmartVista security architecture are:

- Integration with Public Key Infrastructure that ensure confidentiality, reliability and non-repudiation of transactions exchanged among participants
- Layered protection of both data at rest and data in transit
- Web User interface protected via digital certificates
- Communication among internal and external components is secured via TLS1.2 protocol
- Host Security Module (HSM) support for PKI establishment as well as data encryption of sensitive authentication data like passwords, pins etc.
- Message signatures
- Support for two-factor authentication in web interface for securing sensitive operations
- Fine-grained role based access control



Some of the security policies adopted within SmartVista application are:

Security Policy	BPC Implementation
Security key secure storage	SmartVista uses established mechanisms developed by Oracle to protect the keys that are used to secure cardholder data against disclosure and misuse. Oracle TDE automatically creates encryption keys. A master encryption key is used to protect the data encryption keys. The master key is securely stored outside the database in one of the following ways: • Using Oracle Wallet — the keys are stored in a PKCS#12 formatted file that is password-encrypted. • Keys are stored more securely using Oracle Key Vault (OKV). OKV is Oracle's solution for centrally managing encryption keys, Oracle Wallets, Java Keystores, and credential files. It includes optimizations for managing the Oracle Advanced Security Transparent Data Encryption (TDE) master keys. OKV can be used to make wallet backups and restore those backups. It can also be used in a direct connection mode, in which the master key is removed from the local operating system and is moved to OKV. The database containing the encrypted data asks OKV for the Master encryption when required. OKV supports the new international standard for key management, KMIP (OASIS Key Management Interoperability Protocol). OKV also integrates with an HSM, enabling the HSM to act as a "root of trust" and store a top-level key for the OKV
Use unique ID and secure authentication for administrative access	SmartVista supports unique user IDs. SmartVista uses strong cryptography* to render all payment application passwords unreadable during transmission. SmartVista also uses a strong, one-way cryptographic algorithm, based on approved standards, to render all payment application passwords unreadable during storage. Each password has a unique salt value** that is concatenated with the password before the cryptographic algorithm is applied. All locations in which accounts and passwords are stored by particular SmartVista components are listed in the "Account and password locations" section of the relevant administration guide. * "Strong cryptography" refers to the algorithms and their implementation as recommended by the National Institute of Standards and Technology (NIST), which constitute best practice within the industry. All SmartVista components use SHA-256 or SHA-512 to render all payment application passwords. ** A "salt value" is random data that is used as an additional input to a one-way function that "hashes" a password or passphrase
Automated Audit Trail	The SmartVista payment application provides automated audit trails to enable the following event history to be reconstructed: • All individual user access to cardholder data from the application • All actions that were performed by any individual assigned administrative privileges in the application • Access to application audit trails managed by or within the application • Use of, and changes to the application's identification and authentication

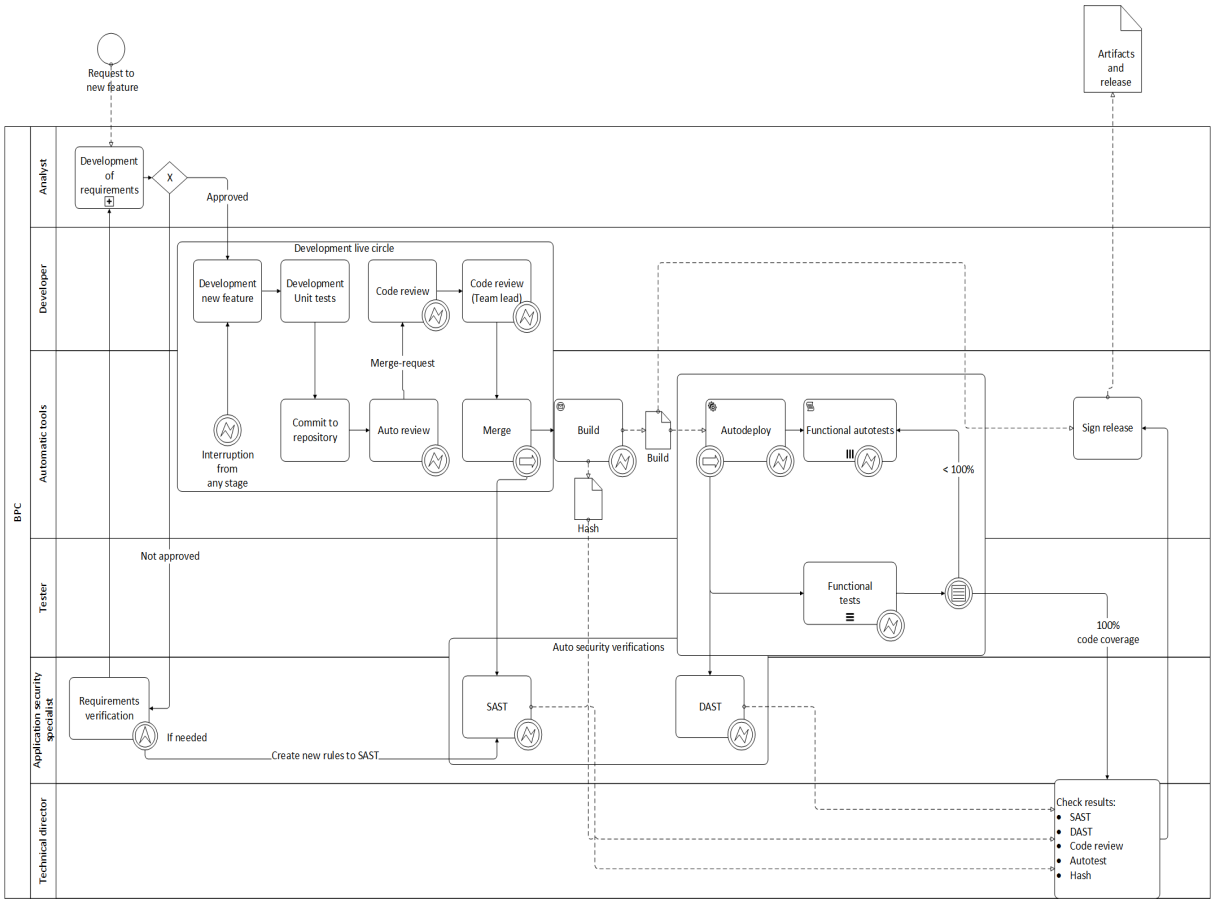
	mechanisms (including but not limited to the creation of new accounts, elevation of privileges, and so on), and all changes, additions, and deletions to application accounts with root or administrative privileges • Initialization, stopping, or pausing of the application audit logs • Creation and deletion of system-level objects within or by the application • The payment application records the following audit trail entries for each event: User identification • Type of event • Date and time • Success or failure indication • Origination of event • Identity or name of affected data, system component, or resource All data is saved to the database.
Facilitate Centralize Logging	Each SmartVista component employs the Syslog protocol for delivering audit trail data.
User secure services, protocols and other components	SmartVista uses only the necessary and secure services, protocols, components, and dependent software and hardware, including those provided by third parties. SmartVista uses HTTPS to access the web interface. The following services and protocols are supported by the SmartVista system: • Oracle SQL*Net • SSH • HTTPS • FTPS • TCP/IP
Implement two-factor authentication for all remote access	SmartVista supports two-factor authentication for all remote access to the payment application that originates from outside the client environment
Secure transmission of data over public network	SmartVista components use secure versions of communication protocols for data exchange. TLS 1.2 is currently used for this purpose. These secure protocols are configured by default during the installation of SmartVista and should not be modified by administrators.
Implementation optimal set-up of SAST/DAST/HAST tools for application security testing	SDLC process of BPC has both SAST and DAST stages. BPC applies varios SAST tools for different programming languages. By default all Java projects is verified by: - Find Security Bugs - PMD - Sonar Analyzer By default all C projects is verified by: - Cppcheck - Clang Static Analyzer - Clang Tidy - RATS

	- SonarCFamily for C/C++ All reports are agregated by SonarQube to view details from different reports. Customer can sign additional agreement to include other SAST tools as Fortify, CheckMarx and etc. Reports from these analyzers can be part of release artifacts.
Application security testing to detect vulnerabilities	Appication security team is involved in developing SmartVista and performs daily verifications of SAST notifications for each merge-request.

SmartVista Secure Application Development

BPC Security Team (BST) is involved in developing SmartVista and uses a centralized tracking to chart the progress of security vulnerabilities identified. This approach combines assessment results so that multiple analysis techniques feed into one reporting and remediation process. Following analysis is performed on the code:

- check of application architecture;
- check of sensitive information data flow;
- static analysis into the code review process to make code review more efficient and more consistent;
- security analysis of Open Source components;
- dynamic analysis security testing of user web-interface;
- several black-box security testing tools as part of the QA process;
- manual verify critical algorithms;
- special attention is paid to documentation, improving documentation is include in the centralized tracking.



The BST has the information that is required by the information security auditors. A combination of written policy, controls documentation, and artifacts gathered through the Secure Software Development Lifecycle (SSDL) gives the BST the ability to demonstrate the organization's compliance story without a fire drill for every audit.

Verification of application architecture

BPC Security Team annually verify application architecture as per the PA-DSS guidelines. The result is adds to the centralized tracking.

Verification of sensitive information data flow

BST holds a technical workshop with development teams as part of the sensitive information data flow review for next point:

- to make sure sensitive authentication data flow is in compliance with PA-DSS and description in Implementation Guide;
- to raise developers knowledge of security features;
- to approve development roadmap for next year.

Static application security testing (*SAST*)

SAST is part of SSDL of SmartVista. Several utilities for checking various programming languages provide maximum automation of code quality tracking. BST classify vulnerability and configure SAST utilities with best practice. For web interface it uses classification OWASP Top 10, SANS Top 25.

Security analysis of Open Source components

For this verification, SAST is used and manual searching vulnerabilities in public networks.

Dynamic analysis security testing (DAST)

DAST is part of SSDL, too and QA use DAST utilities before public release. BST develop guides for QA and check DAST report for each release. Each utility check vulnerability according OWASP Top 10, SANS Top 25, PCI-DSS Compliance.

Black-box security testing

This testing procedure is perform by BST bi-annually for checking full application stack in test environment. This approach allows to identify obsolete and vulnerability third-party components as WebLogic, OS and others.

Manual verification

Manual verification is uses for critical algorithms working with customer data. So correctness and security of algorithms is achieved.

Document validation

BST is involved in document writing and check PA-DSS compliance for Implementation Guide. Also, BST create security checklist for technical writers and review their output bi-annually.

PA DSS certificate

SmartVista is PA DSS certified, having recently undergone a full validation, in line with the latest Version 3.2 standards. Please refer to PCI Security Council official website for evidence.

https://www.pcisecuritystandards.org/approved_companies_providers/validated_payment_applications.php?agree=true

COMPANY	VALIDATION NOTES	DEPLOYMENT NOTES	REVALIDATION DATE	EXPIRY DATE	VALIDATED BY PA-QSA
BPC Banking Technologies					
SmartVista Suite					
Version #: 2.2.22.Y.Z **App Type:** Payment Middleware **Target Market:** Banks, national payment networks, card associations, processors, payment gateways, E-Government and retailers **Reference #:** 17-02.00203.003 **Tested Platforms/Operating Systems:** Red Hat Enterprise, AIX **Service Pack/Build/Version:** Red Hat Enterprise Linux 7.2 (Maipo), AIX: 7100-04-01-1543 (version 7.1, TL4, SP1, year 2015, week 41)	Validated According to PA-DSS *(PA-DSS v3.2)*	Acceptable for New Deployments	30 Mar 2018	28 Oct 2022	Trustwave Holdings, Inc.

PTS DEVICE DEPENDENCIES	EXPIRY DATE
Thales E-Security, payShield 9000 (4-40069)	30 Apr 2019

OTHER DEPENDENCIES
Thales E-Security payShield 8000

ISO 9001:2015 certificate

Certificate

Standard **ISO 9001:2015**

Certificate Registr. No. **01 100 1319423**

Certificate Holder: **BPC AG, doing business as BPC Banking Technologies**
Neuhofstrasse 5a
6340 Baar
Switzerland

Scope: Design, development, implementation, support and maintenance of software; procurement and supply of hardware.

Proof has been furnished by means of an audit that the requirements of ISO 9001:2015 are met.

Validity: The certificate is valid from 2019-05-16 until 2022-04-10.
First certification 2014

2019-05-20

TÜV Rheinland Cert GmbH
Am Grauen Stein · 51105 Köln

www.tuv.com

IAF DAkkS Deutsche Akkreditierungsstelle D-ZM-16031-01-00

TÜVRheinland®
Precisely Right.

V. Working hypothesis

As for the project execution and we would always seek to understand the Critical Success Factors and expand on these through detailed discussion during the Initiation Phase of the project (or before).

These will be logged is a RAID Log, Risk Register, or similar and managed throughout the duration of the project.

In the case of risks in particular, whilst there may be “typical” risks, each project is unique and the environment in which they are, delivered will vary (e.g. current Covid-19 situation).

Risks

Some of the more common risks we might encounter and have to manage (non-exhaustive) would include risks, such as the following:

- Scope creep
- Incomplete or inaccurate scope and/or requirements
- Lack of executive support (both at the start and during the project)
- Insufficient budget
- Lack of resources
- Lack of knowledge/training of staff (or inexperienced staff)
- Poor/bad training
- Changing priorities
- Change of (key) staff members on the project
- Conflict between stakeholders, especially senior stakeholders
- Company politics
- Executive-level changes (different vision or priorities)
- Mergers, acquisitions & major organization restructuring
- Inaccurate estimates (effort/cost)
- Failure to identify all dependencies and constraints
- Inability to manage external dependencies and third parties
- Significant change requests (too many to deal with or which cause huge changes to the timeline or cost)
- Major scope change partway through the project
- Lack of proper Change Management
- Poor quality (documents, etc.)
- Insufficient testing
- Cultural or language related misunderstandings
- Making (not checking) assumptions

- High staff turnover
- Incorrectly evaluating the percentage availability of staff
- Resistance to change
- Poor communication within the team
- Wrong expectations
- Staff do not perform as expected
- Negative attitudes within the team
- Personal conflicts within the team
- Low motivation/moral
- Architecture lacks flexibility
- Technology becomes outdated during the project
- Security vulnerability discovered that requires major rework
- Performance issue discovered that requires major rework
- Lack of documentation for the legacy system (and its interfaces)
- Delays caused by third parties
- Change is company strategy impacts the project approach
- Software fails compliance tests
- Ineffective, poor or slow decision making
- Legal or commercial issues impacting the project
- Approval process is too slow
- Staff must be recruited and are not available on time
- Staff must complete a previous project, which overruns and causes delay to this project
- Clash of organizational cultures
- Legal or Regulatory Change (unexpected)
- Force Majeure
- Market forces
- Methodology, processes and/or procedures not correctly followed and applied
- Poor control and governance of the project
- Security access issues
- Project need is not important enough or poorly understood/defined
- Unplanned work that must be accommodated
- Business case becomes obsolete
- Slow responses to questions and clarifications

- Inadequate or no working space/area for BPC staff when on-site
- Unavailability of experts (SME's) at critical points in the project
- Difficulties accessing environments that BPC is required to support
- Availability of quality production-like data
- Stability of external systems
- Problems integrating with external systems
- Connectivity issues impacting remote support
- Travel issues impacting the ability to get resources on-site quickly

In terms of general assumptions are noted:

- The Project has sufficient priority and importance within the organization
- The Project Scope is sufficiently clear and fixed
- The Project Budget has sufficient contingency capacity to support any likely Change Management
- Project resources have the required knowledge, skills and experience
- Project resources have sufficient availability for the assigned project tasks
- The Project Sponsor has sufficient seniority within the organization
- The client will manage any third parties under their control to ensure dependencies do not cause project delays

VI. Project Management; Approach, Deliverables & Tools

Description of Working Principles

Orientation to objectives

The implementation team, the tasks and the implementation services and deliverables to be performed under this tender, shall demonstrate a consistent orientation towards the achievement of primary objectives of IPS project indicated on item 3.2. and achievement of specific objectives of the project, stated in the same item. Within the technical tender, the Tenderer shall prove on all possible dimensions that the actions planned under the tender will ensure the successful achievement of the primary objective and specific objectives.

From the Project Kick-off and subsequently created Project Management Plan, we seek to gain and document a shared understanding of the objectives of the project and any relative priorities within these objectives.

Though we are a technology company, we never lose sight of the fact that our customers are businesses that have customers of their own, shareholders to please, revenues to generate and ultimately profits to make.

We are a customer-centric organization that puts its customers and their needs first – going "above and beyond" to deliver against the objectives of the project. Sometimes even having to remind our customers of their own objectives – when scope changes, politics and great ideas (for another time) sometimes get in the way.

We share your objectives and want to share in the success from achieving them.

Commitment and Responsibility

The Tenderer shall assume full commitment and responsibility for the success of the project, up to his obligations.

This is fully understood and agreed. We are not a company that seeks to play politics and which plays "the blame game".

We know what our roles and responsibilities are – and we will confidently stand by them.

An ethos you will find at BPC – right to the very top of our organization.

We will also push our customers hard in the same way, working as partners, rather than considering ourselves as simply a "supplier".

Professionalism and Competence

The Tenderer shall prove a high level of professionalism, competence and experience in the field. In order to support the required level of professionalism and competence in accordance with the requirements, the Tenderer should have permanent allocation capacity within the project of highly qualified specialists, as required, and if necessary, to attract specialists from different fields to cover any skills needed in achieving their objectives.

BPC has some of the best talent in the industry today and pays well above the industry average in order to secure and retain such resources.

We seek experienced, hard-working resources that always strive “to be the best” and who will not rest until a successful project has been delivered and customer satisfaction has been achieved.

We ensure our staff are properly trained, coached and monitored to confirm they continue to perform at the highest level, as expected of them.

Where resource or knowledge gaps are identified, we move quickly and with limited bureaucracy in order to close these gaps.

Quality

The term quality should be treated at its absolute value and responsibility. In this context, the Tenderer will follow within the technical tender to express upon their vision on the quality of each deliverable in part, as well as on implementation process as a whole.

BPC believes strongly in the importance of quality in every aspect of delivery.

Following our ISO 9001 and PMP-based Project Methodology – we seek to ensure quality at every step in the process – applying best practices at each stage.

This starts with gaining a clear understanding of the project objectives and agreeing the delivery approach. Then gaining knowledge of the detailed requirements, documenting these and verifying them.

Later, during the testing phases – we seek to ensure the end solution is as well tested as possible, involving our customers in this process as much as possible. Guiding, but also being guided.

Know-how

The Tenderer shall prove sufficient know-how to ensure successful achievement of objectives. Thus, the technical tender should include detailed descriptions of the principle approach in this project, to be described all the methodologies, techniques and tools used in performing the tasks set. The Tenderer should as well take into account and explain how it shall ensure the transfer of one part of this necessary know-how to the Beneficiary to understand and implement the set objectives.

BPC understand our markets, our customers and our products very well – though also understand there is a constant evolution and we continue to ensure our knowledge of all of these - remains recent.

We also understand that, much like a car, it is not enough to simply sell our customers a new car. We must provide the handbooks, adequate servicing and maintenance – and most importantly, ensure you gain the experience and expertise in driving the vehicle, to ensure you get the most benefit and satisfaction from the experience.

We work with our customers to develop unique knowledge transfer and/or training plans – coupled with a testing and certification option.

We also seek to remain “engaged” with our clients to ensure any on-going educational and consultancy needs are also covered.

Please refer elsewhere in this document for additional details.

Efficiency and Effectiveness

The Tenderer shall demonstrate a high level of efficiency and effectiveness of implementation services which is to be provided. Within the technical tender, the Tenderer shall submit the

details of his vision related to the proving of the level of efficiency and effectiveness of rendered services, which will also refer to clearly established quantitative and qualitative indicators.

As a smaller organization than many of our competitors, we have no option other than to be efficient and effective. We do not support a huge staff base or many layers of management.

Everyone must work and deliver – or they don't remain long in the company.

We make use of standards, templates, best practices, as well as tried-and-tested tools and scripts.

We follow our methodology, but also remain pragmatic with an overall sense that we "must get the job done". Fast and efficient – but not surrendering quality in the process.

Flexibility

Given the complex nature of the project, the Tenderer shall explain the degree of flexibility in allocating additional resources if necessary, which it can possibly take in an eventual contract.

We will seek to understand constraints, deadlines and timelines from the outset.

Whilst we will apply the agreed change management, we understand that projects can change over time. This is the nature of a project. It has a start and an end – but is a "living thing".

Understanding this, we must be – and are – flexible on how we handle our projects.

This can imply, adding, removing or changing resources during a project. We, of course, accept this and will always be as flexible as possible in handling any such situations.

Implementation strategy

The implementation strategy for NBM will be composed of following phases:

- **Planning Phase**: The project will be kicked off with an introduction meeting where BPC re-iterate the scope of work and help NBM with the stakeholder identification. During this activity as per the project governance framework the steering committee members will be identified and will be introduced to each other with the agreement on their expected role. After stakeholder identification the use case prioritization will be carried out. BPC will layout the responsibilities of itself and NBM and there will complete agreement on the expectation of the role of each party. A detailed project plan will be worked out listing tasks of both BPC and NBM related to the pre-requisite arrangement, development, test and rollout timelines. It is expected that this phase will take 2 months of execution time.

- **Build and Deploy Phase:** The project plan agreed in Planning Phase will be executed and the prioritized use cases would be developed, tested and deployed on-site for certification testing, SIT, UAT and production rollout. The scheme message specifications and processing guidelines will be created and published to the shortlisted participants for the first use case rollout. The certification testing of the participants will be carried out by BPC resources in full coordination with NBM team members. BPC will keep a strong communication plan and will continue its follow up with NBM and other stakeholders identified during the Planning Phase, to adhere to their part of

delivery in terms of Hardware acquiring, deployment, commissioning, ancillary software acquisition and deployment in the test, pre-production, UAT and production environment. Benchmark testing, performance and security vulnerability testing will be carried out and approved by NBM. The training of product and operations will be carried out for select users of NBM before the pilot launch is performed - on selected participants. It is expected that this stage will take 6 months to complete.

- **Support and Rollout:** The execution will focus on enabling the rest of the use cases as per the scope of work of the project and in parallel the entire fleet of participants being on-boarded as part of the participant on-boarding plan. BPC will carry out the operational task as per the agreed schedule and will take this opportunity to train NBM staff on-the-job for full exposure of all possible operational tasks including settlement & reconciliation, dispute management, participant on–boarding, fraud monitoring, system monitoring, security infrastructure (PKI) management, housekeeping of applications, database, hardware and ancillary software. The scheme rule guidelines will be further tuned as per the outcome of this phase. Altogether this stage may take 8 months to conclude.

- **Implementation Project Closure/Final Acceptance:** This phase will commence after all the use cases as well as operational training are successfully concluded. The phase will include the handover of all the project artifacts (scheme rulebook, standard operating procedure, maintenance procedures, user guides), product licenses and support guidelines. This is estimated to be a 2 month activity.

Project Organisational Chart

BPC Team Structure, Roles & Responsibilities

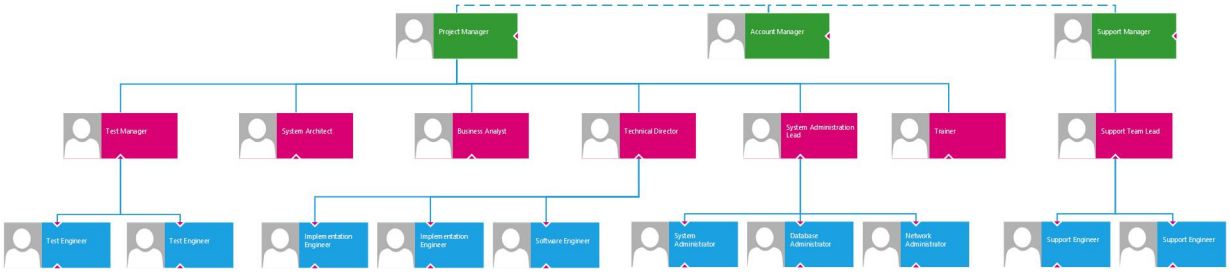
Whilst there are many similarities between projects, each customer and each project is different. We understand this. Our goal is always to bring our experience and best practices whilst at the same time having the flexibility and adaptability to suit individual customer needs.

Given this, team members and team structures will vary from project to project – but the “core” team members tend to remain the same. These will include the Project Manager, Business Analyst and Test Manager.

In cases, one person may play multiple roles and in other cases, a role may be, shared amongst several team members. This depends on the size and complexity of the project, as well as the number of phases and delivery timelines.

In our estimation, the NBM delivery would be somewhere between small/medium and medium, depending on the approach taken and the specifics of the requirements.

Given this and accounting for the specific requirements of NBM, the initial thought on the Project Team Structure would be as shown in the diagram below.



At the top level (shown in green) would be the Project Manager, Account Manager and Support Manager.

These are key roles in the delivery of the project as well as the on-going support of JCC once production go-live has been performed.

Reporting to the Project Manager would be a Test Manager, System (or Solutions) Architect, Business Analyst, Technical Director, System Administration Lead and Trainer.

Below these would sit Test Engineers, Implementation Engineers, Software Engineers (Developers), System Administrator, Database Administrator and Network Administrator.

Reporting to the Support Manager is a Support Team Lead (typically regional) with Support Engineers below them.

The table below describes these roles in further detail.

Role	Duties & Responsibilities
Project Manager	The person within BPC who is overall responsible for the delivery of the project, in line with the agreed delivery approach and project methodology Responsible for planning, directing, tracking and controlling the project ensuring adherence to the project schedule whilst safeguarding the delivery quality in line with the available budget Responsible for ensuring proper communication and reporting to all stakeholders and within the tem Responsible for managing risks, assumptions, issues and dependencies Responsible for managing action items Responsible for managing the project scope and change management Responsible for working cooperatively with the client project manager and project sponsor A key participant in Change Control Boards (CCB's) and Project Steering Committee Meetings
Support Manager	Responsible for ensuring there is a proper strategy and robust approach and processes for client support Responsible for ensuring the Support Team is adequately resources and that they have the skills, training and supervision required Responsible for ensuring the quality of the support provided and that SLA's are achieved or ideally exceeded Responsible for managing all support resources

Account Manager	Responsible for the on-going relationship with the client Responsible for ensuring customer satisfaction Responsible for regular meetings with the client to review SLA targets, business growth (and any related infrastructure impacts) and business planning Responsible for ensuring that clients gain the maximum benefit from BPC products and services Responsible for advising the client about new releases, product enhancements and company news Responsible for acting as a key advisor within the industry in support of client success Help support the growth and success of the client via any additional products and services that may be beneficial to their business
Test Manager	Responsible for analyzing the client scope and requirements and producing a test strategy/plan in line with this Responsible for controlling and assuring the software and systems quality Responsible for managing Test Engineers assigned to the project Responsible for producing a Test Report and the delivery of all test artefacts to the client
Trainer	Evaluates requirements to define the training plan Creates a training program and materials Conducts training and any subsequent test or evaluation

System Architect	Responsible for analyzing the client scope and requirements (including integration aspects) and producing a solutions architecture and design in line with this Responsible for coordinating with the client on architectural and integration aspects Responsible for ensuring that the overall system has the coherence and integrity needed to provide the end-to-end quality, resilience, performance, security, scalability and maintainability required Responsible for guiding IT resources in line with the architectural vision
Business Analyst	Business and technical requirements gathering System integration reviews (SIR) Functional specifications documents (FSD) creation Discovers/elicits business actors and business use-cases Develops business processes description Offers level 1 requirements clarification
Technical Director	Leads the implementation team Defines work packages and assigns tasks to the team Provides senior technical support and guidance Provides effort estimates for IT project tasks Ensures adherence to company IT procedures and standards
System Administration Lead	Coordinates the system administration activities of the project Assigns individual administration tasks to the team Provides team guidance and acts as an escalation point for any infrastructure issues Coordinates and system sizing efforts

Test Engineer	Creates test scenarios and cases in line with the test plan Creates test data Executes testing in line with the test plan Gathers test logs Reports to the Test Manager
Implementation Engineer	Responsible for the application software installation Responsible for setup and configuration of the solution Responsible for integration activities Responsible for unit testing and support of other testing activities Responsible for supporting implementation and migration activities Responsible for aspects of any required warranty support Reports to the Technical Director
Software Engineer	Responsible for non-configuration related software customization Responsible for unit testing and support of other testing activities Responsible for supporting implementation and migration activities Responsible for aspects of any required warranty support Reports to the Technical Director
System Administrator	Responsible for general system administration tasks such as maintaining roles and users Responsible for aspects of system/infrastructure sizing

Database Administrator	Responsible for database administration tasks such as database tuning and supporting aspects of data migration Responsible for aspects of system/infrastructure sizing
Network Administrator	Responsible for network administration tasks such as firewall management and setting up VPN's
Support Team Lead	Responsible for managing and supervising regional support Escalation point for production incidents First level responsibility for SLA adherence Responsible for accepting handover from implementation team
Support Engineer	Responsible for responding to production incidents and seeking resolutions as quickly as possible Responsible for ensuring escalation and senior support as may be needed Responsible for coordinating with clients to seek any additional details on incidents Responsible for testing any hot fixes that may be required

Customer Team Structure, Roles & Responsibilities

Project Manager: It is proposed that the Customer will nominate a Project Manager for interaction with BPC. The Customer's Project Manager is the primary interaction channel with BPC. Standard responsibilities are as follows:

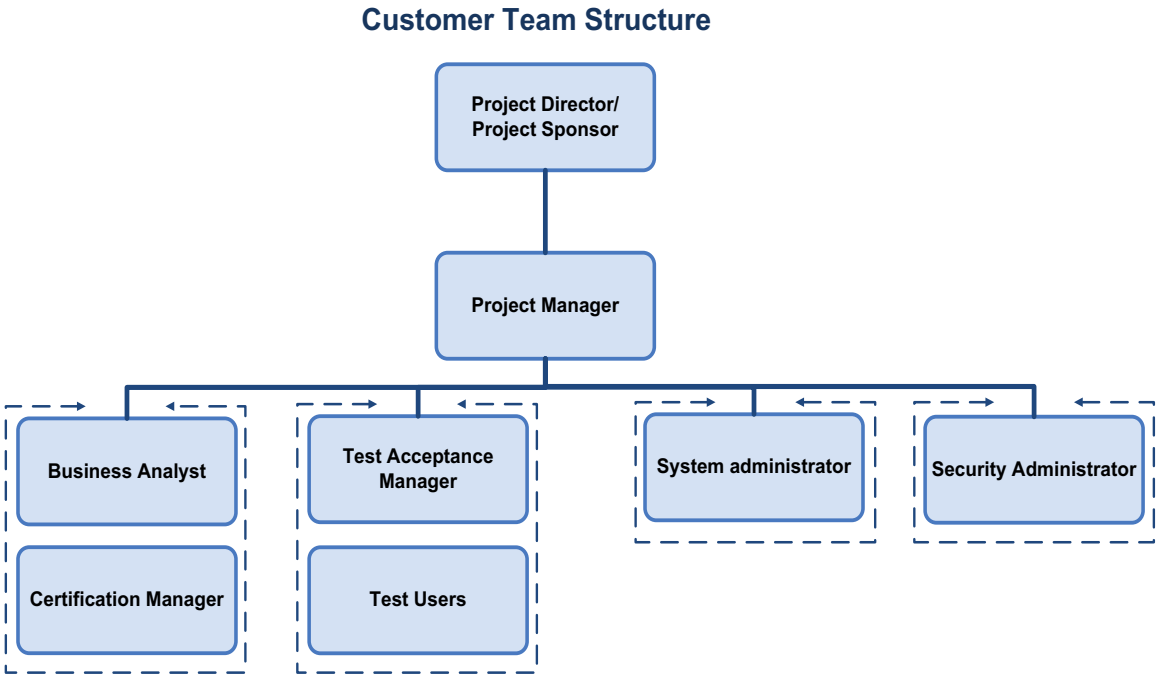
- Preparing the Customer's Schedules.
- Obtaining the Approval of the Project documents from Customer's Authorized Representatives.
- Periodic reports to the Customer's Management.
- Ensure that the premises, personnel, etc. are ready and available for the Project within the scheduled defined in the Project Plan.
- Ensure the qualification of the end users.
- Establish an Acceptance Group.
- Report all the non-settled issues for the consideration of the Project Council.

End User Representatives: These will be customer's end-user who will define the acceptance criteria of the project. Their responsibilities will be:

- Define Acceptance criteria.
- Participate in defining the users' and operational procedures.
- Participate in nominating and training for the personnel.
- Participate the training sessions.
- System usage after Live Operation

Acceptance Group: The Acceptance Group will be responsible for the acceptance of the solution. Its responsibilities will be:

- Approve the User Acceptance Tests
- Provide the necessary data
- Undertake all the scheduled tests
- Record all the deviations during the tests
- Solution acceptance



The following table summarizes basic responsibilities of Client's team members:

Role	Profile	Responsibility
Project director	Responsible for management of the project at a strategic level	• Has full project authority, within the limits of the Client's operating policies, to manage and direct assigned project resources and make decisions regarding the project direction • Establishes the project resource assignments and ensures that the project is properly managed and staffed • Participates in steering committee meetings and decisions
Project manager	Responsible for overall project management and success of the project on Client's side	• Plans, organizes, directs, and manages the daily activities of a project • Communicates with the BPC's project manager • Prepares the project reviews and presents them to the project steering committee
System administrator/ infrastructure engineer	Responsible for connection of external system and devices to the proposed solution	• OS, Cluster Configuration, back-up/archiving, RDBMS and application server maintenance
Business analyst/3rd party system expert	Responsible for preparation of data that has to be migrated from the legacy system	• Responsible for extraction of information/data that was requested by BPC from the legacy systems and providing to BPC team in raw text format. • Takes part & provides inputs in data mapping by assisting BPC in reading/explaining legacy system raw data extract • Takes management/business decision on the data that can't be extracted from legacy system. • Migration Data verification criteria are to be defined by customer. Data validation will be done by customer via reports, random checks. The source systems reports will be provided by customer whereas the destination reports will be provided by BPC. BPC will contribute to migrated data validation by doing SmartVista generic checks without

		checking particular actions or business processes.
Security administrator	Responsible for users' registration, access restriction configuration, and cryptographic keys registration	• Creates user profiles during data migration testing • Configures access restriction policies during data migration testing • Creates user profiles during production data migration and solution implementation • Configures access restriction policies during production data migration and solution implementation • Register cryptographic keys during migration testing, production data migration and solution implementation
Test User/Test Acceptance Manager	Solution testing, data input	• Enter data during test data migration and proposed solution implementation • Verify results of data entry during test data migration and proposed solution implementation • Enter data during production data migration and proposed solution implementation • Verify results of data entry during production data migration and proposed solution implementation
Certification Manager	Payment Networks certification	• Responsible for Payment Networks certification handling • Communicates with Payment Networks during certification scheduling and conducting

Project management plan

Purpose

Project management plans are, used to do the following things:

1. **Plan the project.** The project manager must figure out who, the project team is, how they will be, organized and what the project completion date will be, among other things.
2. **Guide the project manager's decisions.** When project issues arise, your first action should be to consult the project management plan. If there is no guidance there for that particular issue – then it is something to consider putting into the next one for the next project.

3. **Enlighten the project sponsor.** This is one of the most important benefits when writing a project management plan. The project sponsor, who is normally the project manager's boss in one form or another (whether in a different organization or within the same one, physically above the reporting structure or not) is informed about how the project will be managed.

The data in this document represents a mutual acknowledgment of the target parameters of the project, and a commitment to achieving those parameters.

Further to this, it allows all of the following:

- To define the scope and implementation approach
- To define entry, exit and acceptance criteria for the project scope
- To define project communication strategy, change management and responsibilities
- To define the handling of project issues and risks
- To define service level agreements during project testing phase
- To obtain consensus from the project stakeholders on all of the above

It is, documented, as a collection of plans that describes the work to be performed - as well as how the project will be, operated; procedures, which direct project management activities to ensure that key tasks are performed in a systematic and visible manner; and the records that help effectively manage all the project activities.

Depending on the size, complexity and level of governance required, the Project Management Plan can cover all of the following areas listed below, with some or all of the "Project Documents" show. This may differ at the discretion of the Project Manager and as may be agreed.

Project Management Plan	Project Documents	
1. Scope management plan	1. Activity attributes	19. Quality control measurements
2. Requirements management plan	2. Activity list	20. Quality metrics
3. Schedule management plan	3. Assumption log	21. Quality report
4. Cost management plan	4. Basis of estimates	22. Requirements documentation
5. Quality management plan	5. Change log	23. Requirements traceability matrix
6. Resource management plan	6. Cost estimates	24. Resource breakdown structure
7. Communications management plan	7. Cost forecasts	25. Resource calendars
8. Risk management plan	8. Duration estimates	26. Resource requirements
9. Procurement management plan	9. Issue log	27. Risk register
10. Stakeholder engagement plan	10. Lessons learned register	28. Risk report
11. Change management plan	11. Milestone list	29. Schedule data
12. Configuration management plan	12. Physical resource assignments	30. Schedule forecasts
13. Scope baseline	13. Project calendars	31. Stakeholder register
14. Schedule baseline	14. Project communications	32. Team charter
15. Cost baseline	15. Project schedule	33. Test and evaluation documents
16. Performance measurement baseline	16. Project schedule network diagram	
17. Project life cycle description	17. Project scope statement	
18. Development approach	18. Project team assignments	

Project Overview

The project is, expected to provide a system capable of delivering Instant Payments for **National Bank of Moldova**, to be, operated by **National Bank of Molsova**.

Project Scope

The scope is, detailed later in this document, but is generally as follows [subject to change]:

- Instant Payment Platform Core Services
  - Credit Transfer
  - Bulk Payment Flow
  - Payment Exception Flow
  - Payment Return/Refund
  - Direct Debit (optional)
- Instant Payment Platform Overlay Services
  - Request-to-Pay
  - Addressing Service
  - e-Mandate Management (optional)
- Instant Payment Platform Value-Added Services
  - Fraud and Risk Management (optional)
  - Reports and Analytics
  - Billing and Statements
  - Participant Portal
- Disputes Management
- PKI Setup

To be provided, as part of this delivery, will be a system capable of supporting the scope and requirements of the client, which is fully integrated with the clients' business operations and has undergone the required testing and certification to ensure its quality. In addition to this, relevant training and documentation will be, provided - as well as Project Artifacts.

Project Phases

The project is expected to be, delivered over only one project phase (to be confirmed).

Critical Success Factors

The critical success factors as presented on RFP and proposed on section "Understanding of scope"
Note: This may include aspects such as achieving specific deadlines, staying within budget, achieving certain quality levels, etc.

Project Management Approach

This section of the Project Plan is where the overall management approach for the project is, outlined. This section describes, in general terms, the roles and authority of project team members. It also includes which organizations will provide resources for the project and any resource constraints or limitations. If there are any decisions, which are to be, made by specific individuals—for example authorizing additional funding by the project sponsor—this will be, stated here. In effect, this is an Executive Summary for the Project Management Plan.

A project management process (approach) is the management process of planning and controlling the performance or execution of a project. According to the Project Management Institute (PMI), the processes are guided through five stages: initiation, planning, executing, controlling, and closing. Project management, typically, consists of the following processes:

- Define and agree on scope of the project
- Plan the project - time, team, activities, resources, and financials
- Communicate the project plan to the project team
- Agree and delegate project actions
- Manage, motivate, inform, encourage, and enable the project team
- Check, measure, review project progress; adjust project plans, and inform the project team and others
- Review and report on project performance
- Complete project and document lessons learned

BPC makes use of a Project Methodolgy (Approach) based on the one of the most widely used methodologies used globally; PMI (Project Management Institute).

Our methodology seeks to apply best practice processes, based around the PMBOK 6th Edition, whilst seeking to maintain a pragmatic and customer-centric approach which takes account of the project complexity (and related risks), the size of the delivery including the number of resources and third parties involved, how compressed the schedule must be, the available budget and other factors.

Where a task or deliverable does not provide “added value” or real benefit to the project, it will often be, omitted in order to save time and reduce costs.

This is more commonly the case where BPC provides processing and managed services, as the delivery will be closer to out-of-the-box or existing functionality that may already be in live production running. In such bases, some project artifacts may add only limited value and unduly increase costs and schedule.

The table shown below shows the standard PMI Project Management Process Groups, as well as the “Knowledge Areas” – all of which will be covered within this Project Management Plan.

Knowledge Areas	Project Management Process Groups				
	Initiating	Planning	Executing	Controlling	Closing
Project Integration Management	Develop Project Charter	Develop Project Management Plan	Direct and Manage Project Work Manage Project Knowledge	Monitor and Control Project Work Perform Integrated Change Control	Close Project or Phase
Project Scope Management		Plan Scope Management Collect Requirements Define Scope Create WBS		Validate Scope Control Scope	
Project Schedule Management		Plan Schedule Management Define Activities Sequence Activities Estimate Activity Durations Develop Schedule		Control Schedule	
Project Cost Management		Plan Cost Management Estimate Costs Determine Budget		Control Costs	
Project Quality Management		Plan Quality Management	Manage Quality	Control Quality	
Project Resource Management		Plan Resource Management	Acquire Resources	Control Resources	

		Estimate Activity Resources	Develop Team Manage Team		
Project Communication Management		Plan Communications Management	Manage Communications	Monitor Communications	
Project Risk Management		Plan Risk Management Identify Risks Perform Qualitative Risk Analysis Perform Quantitative Risk Analysis Plan Risk Responses	Implement Risk Responses	Monitor Risks	
Project Procurement Management		Plan Procurement Management	Conduct Procurements	Control Procurements	
Project Stakeholder Management	Identify Stakeholders	Plan Stakeholder Engagement	Manage Stakeholder Engagement	Monitor Stakeholder Engagement	

BPC can deliver projects in using waterfall, agile or hybrid mechanisms.

In this case, we would advise something of a hybrid approach – as this would appear to best suit the type of delivery planned.

The project is likely to require multiple phases (or sub-phases), with analysis tasks are the start of each. This allows early “quick wins” to be achieved and allows testing of parts of the solution sooner – allowing misunderstandings (if they exist), architectural issues, infrastructure issues and integration challenges to be identified and addressed sooner – helping to avoid any significant impact to the schedule or budget.

In addition to this, a more “agile” approach can be taken in relation to touchpoints and integration points. For example, GUI’s and Reports can be produced and then enhanced and improved over several iterations, with business and operations users able to trial and comment on them sooner.

Opportunities to have effective “quality gates” (see Quality Management below for further details) should also be taken to ensure excellence in delivery quality. These will be particularly imporant for the following:

- Before moving from Analysis to Design/Build
- Before moving from Design/Build to Integration/System Integration Testing
- Before moving from Integration/System Integration Testing to User Acceptance/Certification
- Before proceeding with Production Go Live (Go/No Go)
- Before moving from Pilot to full Production Rollout and Migration

In order to ensure sufficient and proper Project Governance, weekly meetings, project committees and steering committees may be, created. Please see Communications Management below for further details.

Scope Management

This aspect of the Project Management Plan focuses on the processes required to ensure that the project includes all the work required, and only the work required. Defining and controlling what is and is not included in the project.

- PLAN SCOPE MANAGEMENT—the process of creating a scope management plan that documents how the project and product scope will be, defined, validated, and controlled.
- COLLECT REQUIREMENTS—the process of determining, documenting, and managing stakeholder needs and requirements to meet project objectives.
- DEFINE SCOPE—the process of developing a detailed description of the project and product.
- CREATE WBS—the process of subdividing project deliverables and project work into smaller, more manageable components.
- VALIDATE SCOPE—the process of formalizing acceptance of the completed project deliverables.
- CONTROL SCOPE—the process of monitoring the status of the project and product scope and managing changes to the scope baseline.

It is important that the approach to managing the projects’ scope - be clearly defined and documented in detail. Failure to clearly establish and communicate project scope can result in delays, unnecessary work or failure to achieve deliverables, cost overruns, or other unintended consequences. This section of the project management plan provides a summary of the Scope Management Plan in which it addresses the following:

- Who has authority and responsibility for scope management
- How the scope is defined (i.e. Scope Statement, WBS, WBS Dictionary, Statement of Work, etc.)
- How the scope is measured and verified (i.e. Quality Checklists, Scope Baseline, Work Performance Measurements, etc.)

- The scope change process (who initiates, who authorizes, etc.)
- Who is responsible for accepting the final project deliverable and approves acceptance of project scope

Project Scope Management includes the processes required to ensure that the project includes all the work required, and only the work required, to complete the project successfully. Project scope management is primarily concerned with defining, documenting, and controlling what is and is not included in the project.

The components of a scope management plan include:

- A process to prepare a detailed project scope statement (i.e., requirements) based upon the preliminary project scope statement provided in Charter and/or Project Summary
- A process that specifies how formal verification and acceptance of the completed project deliverables will be obtained
- A process to control how requests for changes to the detailed project scope statement will be, processed.

Project Scope

In this section of the Project Management Plan, the scope of the project is stated. The scope statement from the project charter (if previously created) is the basis for this. That said - the project plan includes a much more detailed scope than the charter. This detail includes what the project does and does not include. The more detail included (in this section), the better the product. This also helps to clarify what is included in the project and help to avoid any confusion from project team members and stakeholders.

Item	Components Needed
Credit Transfer	Integration Platform
Bulk Payment Flow	Integration Platform
Payment Exception Flow	Integration Platform
Payment Return/Refund	Integration Platform
Direct Debit (optional)	Integration Platform
Request-to-Pay	Integration Platform
Addressing Service	Addressing Service

e-Mandate Management (optional)	Addressing Service
Fraud and Risk Management (optional)	Fraud Management
Reports and Analytics	Back-Office
Billing and Statements	Back-Office
Participant Portal	Participant Portal
Disputes Management	Back-Office
PKI Setup	Integration Platform

If any item is, not listed above - it is considered, as being **Out of Scope**.

In all cases, unless specifically documented within an agreed and approved requirements specification, standard out-of-the-box SmartVista functionality, standard configuration settings, and interface specifications will, be assumed. Any deviation from this would be considered as a Change Request – whether treated formally (extra effort/cost and potential schedule impact) or informally ("absorbed" as part of normal project delivery). See Scope Management below.

As a Processing delivery (SaaS or similar), the focus will be primarily on integration and configuration of standard product functionality. The general functionality and related workflows will follow standard functionality in all cases, unless they are, explicitly documented elsewhere. This includes detailing within the existing Contractual Agreement or Statement/Scope of Work documents.

In terms of general project activities, as a Processing project, the focus will be primarily on integration and configuration, with agreed services, expected to have been, defined, within the Contractual Agreement document(s).

As part of the Analysis Phase of the project, Interface Specifications will need to be agreed – taking SmartVista standard interfaces and integrations as a starting point. Additionally, custom configurations will also need to be defined – again taking standard (default) configuration settings as a starting point.

In addition to analyzing, defining and set up (including configuration) of the target system, tasks will also include:

- Project Management
- Testing

- User Acceptance Testing Support
- Certification (with schemes and networks)
- Live Production Implementation
- Pilot and Migration Support
- Handover to Operations

A full Work Breakdown Structure (WBS) and related milestones and deliverables is, found within this document.

Requirements Management

In this section, we document the planned approach for baselining and then managing changes in requirements.

For this delivery, the project team will create the requirements documents and baseline those as follows:

- High-level Business Requirements were initially captured as part of the Scope of Work (SoW) that will have taken place ahead of commencing the project
- Detailed Functional and Non-Functional Requirements (particularly where they differ from standard functionality) are then documented within a Functional Specifications Document (FSD) or similar

Any changes to existing requirements, removal of a requirement or addition of new requirements uses the Change Control Process explained in Section 14 below.

Requirements Development and Documentation Plan

Requirements are to be gathered using a series of **System Integration Review** (SIR) sessions. This can be performed on-site (preferred) or remotely. Depending on the scope, these can be over several days, several weeks or even several months.

These sessions are, planned in advance, and wherever possible, an agenda and even a questionnaire are, supplied in advance, in support of this.

In parallel to this, the production of an associated **Functional Specifications Document** (FSD) takes place. An initial draft version is often be created using the Scope of Work document.

The FSD is a very important document and it will undergo a series of internal (BPC) and external reviews in an iterative way. This ensures a, collaborate and quality based approach.

If there are multiple project phases, it is good practice to have separate FSD's for each – as this allows the solution build and testing to progress on a phase whilst the FSD for the next phase is progressed in parallel. This is a more "agile" approach to delivery.

The Project Sponsor, as well as both Project Managers, at a minimum, must approve the FSD.

This approved FSD then forms the baseline set of requirements against which delivery is, made and change control is, performed.

In addition to this, a **Clarifications Register** may be used. This allows any clarification of requirements to be logged – not only for clear understanding and future reference – but also very valuable in the case of discussions over the appropriate meaning of any given requirement.

Integration Management

This section of the Project Management Plan includes processes that are, performed, to make sure that various elements of the projects are properly coordinated.

PROJECT INTEGRATION MANAGEMENT includes the processes and activities to identify, define, combine, unify, and coordinate the various processes and project management activities within the Project Management Process Groups.

The Project Integration Management processes are:

- DEVELOP PROJECT CHARTER: the process of developing a document that formally authorizes the existence of a project and provides the project manager with the authority to apply organizational resources to project activities.
- DEVELOP PROJECT MANAGEMENT PLAN: the process of defining, preparing, and coordinating all plan components and consolidating them into an integrated project management plan.
- DIRECT AND MANAGE PROJECT WORK: the process of leading and performing the work defined in the project management plan and implementing approved changes to achieve the project's objectives.
- MANAGE PROJECT KNOWLEDGE: the process of using existing knowledge and creating new knowledge to achieve the project's objectives and contribute to organizational learning.
- MONITOR AND CONTROL PROJECT WORK: the process of tracking, reviewing, and reporting overall progress to meet the performance objectives defined in the project management plan.
- PERFORM INTEGRATED CHANGE CONTROL: the process of reviewing all change requests; approving changes and managing changes to deliverables, organizational process assets, project documents, and the project management plan; and communicating the decisions.
- CLOSE PROJECT OR PHASE: the process of finalizing all activities for the project, phase, or contract.

In relation to the delivery of this project, primarily we will apply the following in order to deliver and "integrated management" of the project:

- Handover session between sales/pre-sales along with all relevant materials
- Creation of a Project Management Plan (this document)

- Define, track and manage project work/tasks/deliverables based on the Project Management Plan and Detailed Project Schedule (MS Project) – inclusive of a WBS, deliverables and milestones
- Monitoring and Control of project activities, including via Weekly Meetings and Weekly Reporting, as well as via use of a Project Change Board and Project Steering Committee
- Apply a strict Change Control Process, to manage any change of scope, requirements, resources or priorities
- Ensure that the Project and every Phase of the Project undertaken a Project Closure & Lessons Learned – in order to review work performed and determine any ways of improving future deliveries

Schedule Management

Project Schedule Management includes the processes required to manage the timely completion of the project. The Project Schedule Management processes are:

- PLAN SCHEDULE MANAGEMENT—the process of establishing the policies, procedures, and documentation for planning, developing, managing, executing, and controlling the project schedule.
- DEFINE ACTIVITIES—the process of identifying and documenting the specific actions to be performed to produce the project deliverables.
- SEQUENCE ACTIVITIES—the process of identifying and documenting relationships among the project activities.
- ESTIMATE ACTIVITY DURATIONS—the process of estimating the number of work periods needed to complete individual activities with the estimated resources.
- DEVELOP SCHEDULE—the process of analyzing activity sequences, durations, resource requirements, and schedule constraints to create the project schedule model for project execution and monitoring and controlling.
- CONTROL SCHEDULE—the process of monitoring the status of the project to update the project schedule and manage changes to the schedule baseline.

This section of the Project Plan provides a general framework for the approach, which will be, taken to create the project schedule. Effective schedule management is necessary for ensuring tasks, are completed on time, resources are allocated appropriately, and to help measure project performance. This section of the Project Plan includes discussion of the scheduling tool/format, schedule milestones, and schedule development roles and responsibilities.

The project schedule is, managed by determining whether the project deliverables and milestones are, completed on time.

Project Schedule

The initial draft Project Schedule (and WBS) are, created through accounting for the following:

- The Project Scope (as contractually agreed)
- The High-Level Requirements (found in the Scope of Work)

- Example Project Plans and Work Breakdown Structures
- Project Tasks and Deliverables required for delivery
- Peer Review

At this stage, first thought effort estimates may be, provided – but cannot be validated until the Functional Specifications Document has been completed and approved.

Once the FSD is, approved the Development Team Lead will perform a GAP Analysis and Effort Estimation of the Solution Build. The Test Manager will also reconfirm the effort required for any testing and certification. The schedule can then be updated and baselined.

This baseline schedule is then, used for schedule management including project tracking and ensuring that work progresses according the plan.

The Project Manager can also adjust the planning as required in order to ensure that the schedule is, maintained.

Project Deliverables

Deliverable	Company	Responsible	Role
Kick-off Session Presentation	BPC		Project Manager
Work Breakdown Structure (WBS)	BPC		Project Manager
Project Management Plan (PMP)	BPC		Project Manager
Detailed Project Schedule (MPP)	BPC		Project Manager
Solutions Architecture	BPC		Solutions Architect
SIR Questionnaire(s)	BPC		Business Analyst
Functional Specification Document (FSD)	BPC		Business Analyst
Implementation & Migration Strategy	BPC		Project Manager
Implementation & Migration Plan	BPC		Project Manager
RAID Log (Risk Register)	BPC		Project Manager
Training Plan	BPC		Training Manager

Solution Architecture & Design	BPC		Technical Director
Services & Operation Plan	BPC		Operations Director
Test Plan	BPC		Test Manager
User Acceptance Test Plan	Client		Test Manager
Software Release Notes	BPC		Implementation Engineer
Handover Plan	BPC		Project Manager
Project Closure Report	BPC		Project Manager

Project Milestones

Milestone
Contract Agreed
Project Kick-off Completed
SIR Completed
Functional Specification Document (FSD) Approved
Training Plan Approved
Software Release
Training Completed
Test Plan Approved
Integration Testing Completed
System Integration Testing Completed
Certification Completed
User Acceptance Testing Completed

Deployment Testing Completed
Processing Centre Staff – Ready
GO / NO GO - DECISION
Production Go Live Completed
Pilot Completed
Migration Complete
Project (Phase) Closed

Cost Management

Project Cost Management includes the processes involved in planning, estimating, budgeting, financing, funding, managing, and controlling costs so that the project completes within the approved budget.

The Project Cost Management processes are:

- PLAN COST MANAGEMENT—the process of defining how the project costs will be estimated, budgeted, managed, monitored, and controlled.
- ESTIMATE COSTS—the process of developing an approximation of the monetary resources needed to complete project work.
- DETERMINE BUDGET—the process of aggregating the estimated costs of individual activities or work packages to establish an authorized cost baseline.
- CONTROL COSTS—the process of monitoring the status of the project to update the project costs and manage changes to the cost baseline.
- The ability to influence cost is greatest at the early stages of the project, making early scope definition critical.

The Cost Management Plan clearly defines how the costs on a project, will be managed, throughout the project's lifecycle. It sets the format and standards, by which the project costs, are, measured, reported and controlled. Working within the cost management guidelines is imperative for all project team members to ensure successful completion of the project. These guidelines may include which level of the WBS cost accounts, will be created in and the establishment of acceptable variances. The Cost Management Plan:

- Identifies who is responsible for managing costs
- Identifies who has the authority to approve changes to the project or its budget
- How cost performance is quantitatively measured and reported upon
- Report formats, frequency and to whom they are presented

In terms of BPC, initial effort and cost estimates, are, made by the Head of Project Delivery and Technical Director. Later the Development Lead and Test Lead will refine these cost estimates.

It is then the responsibility of the Project Manager to deliver the project in line with the available budget, as determined by the FIXED PRICE stated in the Contractual Agreement.

If costs are likely to exceed the budget due to internal reasons, the Operations Director must approve these.

If Change Requests are, issued by the client, which have cost implications these must be approved, by, the Change Control Board unless delegated elsewhere.

Quality Management

The Project Quality Management processes are:

- PLAN QUALITY MANAGEMENT—the process of identifying quality requirements and/or standards for the project and its deliverables, and documenting how the project will demonstrate compliance with quality requirements and/or standards.
- MANAGE QUALITY—the process of translating the quality management plan into executable quality activities that incorporate the organization's quality policies into the project.
- CONTROL QUALITY—the process of monitoring and recording the results of executing the quality management activities to assess performance and ensure the project outputs are complete, correct, and meet customer expectations.
    - Quality as a delivered performance or result.
    - Grade it is a category assigned to deliverables having the same functional use but different technical characteristics.
    - The cost of preventing mistakes is generally much less than the cost of correcting mistakes when they are, found by inspection or during usage.
    - Prevention (keeping errors out of the process) and inspection (keeping errors out of the hands of the customer).
    - THE COST OF QUALITY (COQ) includes all costs incurred over the life of the product by investment in preventing nonconformance to requirements, appraising the product or service for conformance to requirements, and failing to meet requirements (rework). Failure costs are, often categorized, into internal (found by the project team) and external (found by the customer). Failure costs are, also called the cost of poor quality. Organizations choose to invest in defect prevention because of the benefits over the life of the product. Because projects are temporary, decisions about the COQ over a product's life cycle are often the concern of program management, portfolio management, the PMO, or operations.

This portion of the Project Management Plan discusses how quality management, will be used to ensure that the deliverables for the project meet a formally established standard of acceptance. All project deliverables should be, defined, in order to provide a foundation and understanding of the tasks, at hand and what work must be, planned. Quality management is the process by which the organization not only completes the work but also completes the work to an acceptable standard. Without a thorough Quality Management Plan, work may be, completed in a substandard or unacceptable manner. This section includes quality roles and responsibilities, quality control, quality assurance, and quality monitoring.

The quality success criteria of each phase of the project are, identified and specified to ensure compliance during project execution. ISO-9001 standards will be, applied as appropriate.

Document Deliverables

All documentation deliverables will apply the following approach to ensure their quality:

- Initial drafts will make use of standard “best practice” templates wherever possible
- Drafts will undergo internal review by supervisors/managers and peers before being shared with the client
- Clients will be given ample opportunity to provide input into the deliverable and review/comment on drafts
- Clients must approve all documentation deliverables
- Any changes to documentation deliverables will have Change Control applied to them, in relation to the original approved version

Software Quality

All software deliverables will apply the following approach to ensure their quality:

- The latest, tested, certified version of products will be used as a starting point in all cases
- Any software coding changes will undergo a code review
- Any functionality, interface or configuration changes made will be specifically tested to ensure their appropriate functioning
- Regression testing will be performed to ensure changes have not affected original processing
- Test Plans will be reviewed and must be approved by the client (see “Documentation Deliverables” above)
- A full set of software testing will take place, including:
    - Unit Testing
    - Integration Testing
    - System Integration Testing
    - Deployment Testing (Operational Acceptance Testing)
- User Acceptance Testing will be performed to ensure client satisfaction
- Certification Testing will be performed to ensure any necessary certifications are achieved

- A Quality Manager and/or Test Manager will oversee the entire “Quality Assurance”, with oversight by the Project Manager

Services Quality

Whilst standard existing services are the starting point of this delivery, should there be any new or modified services required as a result of this delivery – it will be the responsibility of the Operations Director and Technical Director to ensure the appropriate level of service quality in line with Service Level Agreements (SLA’s) and other Key Performance Indicators (KPI’s).

Where additional hardware and network infrastructure is required – they will also be responsible for ensuring their acquisition (see Procurement Management), installation and required testing.

Where additional staff must, be acquired (see Resource Management), it is the responsibility of the Operations Director to work to provision these staff and ensure they are appropriately trained and prepared ahead of starting work on the delivery of any required services.

Resource Management

Project Resource Management includes the processes to identify, acquire, and manage the resources needed for the successful completion of the project.

The Project Resource Management processes are:

- PLAN RESOURCE MANAGEMENT—the process of defining how to estimate, acquire, manage, and utilize physical and team resources.
- ESTIMATE ACTIVITY RESOURCES—the process of estimating team resources and the type and quantities of material, equipment, and supplies necessary to perform project work.
- ACQUIRE RESOURCES—the process of obtaining team members, facilities, equipment, materials, supplies, and other resources necessary to complete project work.
- DEVELOP TEAM—the process of improving competencies, team member interaction, and the overall team environment to enhance project performance.
- MANAGE TEAM—the process of tracking, team member performance, providing feedback, resolving issues, and managing team changes to optimize project performance.
- CONTROL RESOURCES—The process of ensuring that the physical resources assigned and allocated to the project are available as planned, as well as monitoring the planned versus actual use of resources, and performing corrective action as necessary.

BPC makes use of a matrix organization for Project Delivery.

In the first instance, initial engagement is directly with the Head of Project Delivery. The Head of Project Delivery will seek the assignment of a Project Manager and Business Analyst from their respective Resource Managers.

Once assigned, Project Initiation tasks will be progressed including a Project Kick-off and then preparation and execution of a System Integration Review (SIR) – in order to produce the FSD.

Once the FSD has been produced this is the point where full clarity on the scope of delivery is available.

It is then up to the Project Manager to coordinate a GAP Analysis and Delivery Effort Estimation. After this, Work Packages are, created and assigned to the relevant resources. At this point, further clarity on the delivery resources forming the Project Team are, known.

The Project Manager will also engage the Solutions Architect and Test Manager further at this point – in order to prepare test, certification and operational environments. Infrastructure requirements are, also further assessed and if additional infrastructure is required – this will be determined at this point. See Procurement Management for further details on how this is progressed from here.

From the point of contractual agreement and more so from the point the FSD is agreed, the Head of Project Delivery has visibility on the Professional Services to be, delivered. If additional staffing requirements are, needed, it is their responsibility to work with the Head of Human Resources and other Resource Managers to recruit and train staff appropriately before being assigned project tasks.

In cases where services can be delivered by existing staff, but require training, in is the responsibility of the Head of Project Delivery to work with the Training Manager and Resource Managers to ensure this training is planned, prepared and executed ahead of being assigned related project tasks.

Whilst Project Team resources continue to report to their Resource (Line) Managers, they must also report to the Project Manager on a regular (at least weekly) basis and are accountable for the on-time delivery of tasks assigned to them, and the quality delivered.

Where Team Leads are engaged, they too must oversee and track delivery and delivery quality to avoid the need for micro-management of all project resources by the Project Manager.

It is vital that as part of resource assignment, that sufficient availability of resources is ensured by the Resource Manager, in order that timely delivery is not placed at risk. If this appears to be the case, the Project Manager will escalate this immediately to ensure improved availability or assignment of a replacement resource with greater availability.

If there appears to be a knowledge problem with any assigned resources – the Project Manager will escalate this to the Resource Manager to ensure they are, either trained, coached, supervised or replaced as may be required.

Please refer to ‘F3.10 List of key experts.docx’.

Basic responsibilities of BPC’s team members

Role	Profile	Responsibility

Project manager	Responsible for overall project management and success of the project on BPC's side	Plans, organizes, directs, and manages the daily activities of a project, creates risk management plan, and monitors risk during the project Communicates with the project stakeholders, reaches, and maintains commitments Controls project scope, when necessary involves change management procedures to handle change requests Conducts measurements in a course of the project and controls the compliance with the project quality goals Communicates with the clients project manager Prepares the project reviews and presents them to the project steering committee
Business analyst	Responsible for business processes analysis and modeling	Performs target organization assessment Discovers/elicits business actors and business use-cases Develops business processes description
Developers	Responsible for development of the clients Processing Solution modules that require development and/or customization	Develops software components that require development and/or customization Performs unit testing of developed/customized software components Supports system integration testing, user acceptance testing, production implementation, and post go-live support
Test manager	Responsible for planning, organizing, and managing overall testing activities, including test design, test preparation, test execution, and evaluation of testing	Works with BPC's project manager to develop the test strategy Assigns tasks to test engineer Works with developers to review and analyze defects

		Provides test reports to BPC's project manager Evaluates test coverage, results, and effectiveness Leads the project test team
Test engineer	Responsible for activities associated with test execution and test results analysis	Evaluates requirements for testability Develops/updates test cases and test procedures Selects appropriate test techniques Designs/prepares test data Creates/debugs test scripts Monitors test coverage Sets up and executes testing Analyzes and recovers from execution errors Logs detected defects and verifies fixes Participates in reviewing of defects
Implementation engineer	Responsible for installation, configuration, and maintenance of the clients Processing Solution	Participates in defining overall system architecture Installs the solution Configures the solution including performance optimization
Trainer	Responsible for preparation of training materials and conducting of user training	Evaluates requirements to define the training program Creates training program and materials Conducts training

Communications Management

Project Communications Management ROJECT COMMUNICATIONS MANAGEMENT consists of two parts. The first part is developing a strategy to ensure communication is effective for stakeholders.

The second part is carrying out the activities necessary to implement the communication strategy.

The Project Communications Management processes are:

- PLAN COMMUNICATIONS MANAGEMENT—The process of developing an appropriate approach and plan for project communication activities based on the information needs of each stakeholder or group, available organizational assets, and the needs of the project.
- MANAGE COMMUNICATIONS—the process of ensuring timely and appropriate collection, creation, distribution, storage, retrieval, management, monitoring, and the ultimate disposition of project information.
- MONITOR COMMUNICATIONS—the process of ensuring the information needs of the project and its stakeholders are being met.

Communication is the exchange of information. The mechanisms by which information is, exchanged can be in:

- WRITTEN FORM. Either physical or electronic.
- SPOKEN. Either face-to-face or remote.
- FORMAL OR INFORMAL (as in formal papers or social media)
- THROUGH GESTURES. Tone of voice and facial expressions
- THROUGH MEDIA. Pictures, actions, or even just the choice of words.
- CHOICE OF WORDS. There is often more than one word to express an idea; there can be subtle differences in the meaning of each of these words and phrases.

COMMUNICATION ACTIVITIES have many dimensions, including but not limited to:

- INTERNAL. Focus on stakeholders within the project and within the organization.
- EXTERNAL. Focus on external stakeholders such as customers, vendors, other projects, organizations, government, and the public, as well as environmental advocates.
- FORMAL. Reports, formal meetings (both regular and ad hoc), meeting agendas and minutes, stakeholder briefings, and presentations.
- INFORMAL. General communications activities using emails, social media, websites, and informal ad hoc discussions.
- HIERARCHICAL FOCUS. The position of the stakeholder or group with respect to the project team will affect the format and content of the message, in the following ways:
    - UPWARD. Senior management stakeholders.
    - DOWNWARD. The team and others who will contribute to the work of the project.
    - HORIZONTAL. Peers of the project manager or team.
- OFFICIAL. Annual reports; reports to regulators or government bodies.

- UNOFFICIAL. Communications that focus on establishing and maintaining the profile and recognition of the project and building strong relationships between the project team and its stakeholders using flexible and often informal means.
- WRITTEN AND ORAL. Verbal (words and voice inflections) and nonverbal (body language and actions), social media and websites, media releases

The purpose of the Communications Management Plan is to define the communication requirements for the project and how information, will be, distributed in order to ensure project success. By having a solid communications management approach, many project management problems can be, avoided. In this section, an overview of your communications management approach is given. Generally, the Communications Management Plan defines the following:

- Communication requirements based on roles
- What information will be communicated
- How the information will be communicated
- When will information be distributed
- Who does the communication
- Who receives the communication
- Communications conduct

Project communications are a two-way street. Much like project planning, expectations must be set and both the project team and client stakeholders have to carry out their responsibilities in order for communication to go smoothly.

While a project would not start without a project plan in place, a project communication plan is, not as, readily discussed, but it should be.

A Project Management Communication Plan defines how critical information is, delivered throughout the project, by who, and at what frequency. Throughout a project, successful communication about alignment on goals and milestones, and subsequent re-alignment on these as projects change are crucial to stakeholder buy-in and transparency into a project's status throughout the entire project timeline. Communication is critical to keeping a good relationship with the client, and a project communication plan helps in upfront planning, as well as in keeping up that shared understanding of what is, happening and what should be happening throughout the project.

Not all projects are, created equal, and because of that, a project communication plan is unique to a project—which is why it is just as important to think about this at the same time as creating a project plan after kickoff. Large projects have different communication needs from small projects, and the same goes for projects with teams of stakeholders versus a single project contact. Projects with differing goals, budgets, timelines, and even deliverables all require communication tailored to those needs.

Poor communication can contribute to project failure, and therefore, it could spell massive financial loss to the company. At the opposite end of the spectrum, high-performing businesses communicate more frequently and do so more effectively than their low-performing counterparts do.

A Project Management Communication Plan will keep a project on track because it:

- Creates written documentation that the team can reference
- Sets expectations of when stakeholders will receive updates
- Increases stakeholders' visibility into the project and its status
- Provides the opportunity for stakeholders to give feedback, which can help the team detect issues early on and decrease wasted work
- Increases productivity during meetings or eliminates them altogether

To have a project completed - successfully and on time, it is critical to create an effective communication plan.

A Project Management Communication Plan identifies how important information will, be communicated to stakeholders throughout the project. It also determines who will be receiving the communication, how those people will receive it, when they will receive it, and how often they should expect to receive that information.

The project communication plan should include:

- The purpose or goals of the communication plan
- Information about stakeholders and their roles
- The types of information that needed to be shared with stakeholders
- The methods used to communicate
- The frequency that each stakeholder would like to receive information

Stakeholders

Company	Project Role
Client	Project Sponsor
Client	Project Manager
Client	Technical Manager
Client	Test Manager/Lead
BPC	Project Manager

BPC	Delivery Manager
BPC	Business Analyst
BPC	Solutions Architect
BPC	Test Manager/Lead

Communications Matrix

Type	Purpose	Medium	Frequency	Audience
Kick-off Meeting	Introduce the Project Clarify scope & objectives Introduce key team members Review High-level Planning	Conference Call	Once	Project Sponsor Executive Stakeholders Senior Stakeholders Project Managers
Lessons Learned Meeting	Review of the Overall Project Outcome versus plan What went well? What went badly? What actions must, be taken to improve future deliveries?	Conference Call	Once	Project Sponsor Executive Stakeholders Senior Stakeholders Project Managers

Project Status Meetings	Review schedule versus plan Review important RAID items Action Log review Review Priorities Discuss any Change Requests Discuss any Escalations Plans for next period	Conference Call	Weekly **Timing** - Day: - Time:	Project Managers Project Teams
Project Committee Meetings	Discuss major Change Requests Discuss major Escalations RAID Log Review Discuss Resource Issues	Conference Call	Monthly	Project Sponsor Project Managers Senior Stakeholders
Project Steering Meetings	Review Project Schedule Review Project Budget Review Project Scope Review Project Quality	In person meeting (Ideally) Conference Call if not possible	Quarterly	Project Sponsor Project Managers Executive Stakeholder
Project Status Reporting	Communicate Project Status Schedule/Progress RAID Log/Items Action Log Update Plans for next period	E-mail (with attached WSR)	Weekly **Timing** - Day:	Project Sponsor Project Managers Senior Stakeholders Project Teams

System Integration Review (SIR)	Requirements Gathering Functional Non-Functional Additionally: Agree Phases Discuss Schedule Discuss Testing Discuss Training Discuss Implementation & Migration Discuss Communication	In person meeting (Ideally) Conference Calls if not possible	Once (over a prolonged period)	Project Managers Business Analyst (BPC) Business Users Operations Users IT / Development Security Analyst Other SME's
UX/UI Review	Review of the User Screens Review of Screen Flows Review of Report Layouts	Conference Call (with remote demo)	Ad Hoc (based on Sprints)	Project Manager (Delivery) Technical Lead (BPC) Business Users Operations Users
Project Closure (Lessons Learned) Report	Summary of the Project Review of the Overall Project Outcome versus plan What went well? What went badly? Action Items needed to improve future deliveries Conclusion	E-mail (with attached report)	Once	Project Sponsor Project Managers Executive Stakeholder Senior Stakeholders
Training	Training Course Modules	In person meeting (Ideally) Conference Calls if not possible	Ahead of UAT and Ahead of Go Live	Business Users Operational Staff IT / Development

Test Report	Test Results Summary Test Results Details	E-mail (with attached report)	Per Test Phase	Project Manager (Client)
Ad Hoc Meetings	Various	Conference Call	As Required	Varies
Informal Communications	Various	E-mail, Zoom, Skype, Whatsapp, Slack	As Required	Varies

Risk Management

Project Risk Management includes the processes of conducting risk management planning, identification, analysis, response planning, response implementation, and monitoring risk on a project. The objectives of project risk management are to increase the probability and/or impact of positive risks and to decrease the probability and/or impact of negative risks, in order to optimize the chances of project success.

The Project Risk Management processes are:

- PLAN RISK MANAGEMENT—the process of defining how to conduct risk management activities for a project.
- IDENTIFY RISKS—the process of identifying individual project risks as well as sources of overall project risk, and documenting their characteristics.
- PERFORM QUALITATIVE RISK ANALYSIS—the process of prioritizing individual project risks for further analysis or action by assessing their probability of occurrence and impact as well as other characteristics.
- PERFORM QUANTITATIVE RISK ANALYSIS—the process of numerically analyzing the combined effect of identified individual project risks and other sources of uncertainty on overall project objectives.
- PLAN RISK RESPONSES—the process of developing options, selecting strategies, and agreeing on actions to address overall project risk exposure, as well as to treat individual project risks.
- IMPLEMENT RISK RESPONSES—the process of implementing agreed-upon risk response plans.
- MONITOR RISKS—the process of monitoring the implementation of agreed-upon risk response plans, tracking identified risks, identifying and analyzing new risks, and evaluating risk process effectiveness throughout the project.

This part of the Project Plan provides a general description for the approach taken to identify and manage the risks associated with the project.

This is the place to identify and prioritize the risks to a successful project. The plan should list, in table form (or similar) each risk, the mitigation strategy, and the plan of action should that risk

occur. Optionally each risk can also be prioritized and ranked for probability and severity (Risk = Probability x Severity).

Project risk is the risk that the project team may not be able to meet the project goal in the stated timeframe.

Risks must be analyzed on an ongoing basis to accommodate changing conditions and priorities on the project. As new risks are identified, strategies and plans to deal with them must be developed.

The risk factors identified and managed for the project will be accumulated in a **Risk Log** (part of the **RAID Log**), which is attached to this document.

Activities

Activity	Tasks	Participants
Risk identification	The risk assessment workshop will be organized at the beginning of each phase of the project	BPC project manager
Risk analysis and prioritization	Risk factor will be assigned to a member(s) of project team	BPC project manager
	Member(s) of project team will estimate the probability the risk could become a problem and the impact if it does	Assigned member of project team
	The individual analyzed risk factors, will be, collected, reviewed, and adjusted if necessary. The list of risk factors will be sorted by descending risk exposure	BPC project manager

Risk management planning	The top ten risks, or those risk factors having a high estimated exposure will be assigned to individual project members for development and execution of a risk mitigation plan	BPC project manager
	For each assigned risk factor, the recommend actions will be, created, that will reduce either the probability of the risk materializing into a problem, or the severity of the exposure if it does. The mitigation plan will be returned to the project manager	Members of project team
	The mitigation plans for assigned risk items will be, collated into a single list. The completed top ten risk list will be created and made available to the project team	BPC project manager
Risk resolution	Members of project team, who is responsible for executing a risk mitigation plan carries out the mitigation activities	Members of project team
Risk Monitoring	The status and effectiveness of each mitigation action will be reported to the project manager every two weeks	Members of project team
	The probability and impact for each risk item will be re-evaluated and modified if appropriate	BPC project manager

	If any new risk items have been identified, they will be analyzed as were the items on the original risk log and added to the risk log	BPC project manager
	The top ten risk list will be regenerated based on the updated probability and impact for each remaining risk	BPC project manager
	Any risk factors for which mitigation actions are not being effectively carried out, or whose risk exposure is rising, may be escalated to an appropriate level of management for visibility and action	BPC project manager

Schedule for Risk Management Activities

Activity	Schedule
Risk Identification	A risk assessment workshop will be held at the beginning of each phase of the project
Risk Log	The prioritized risk log will be completed and made available to the project team by the end of project initiation phase
Risk Review	The risk log will be reviewed and approved by BPC and OJB project managers on biweekly bases
Risk Management Plan	The risk management plan, with mitigation, avoidance, or prevention strategies for the top ten risk items, will be completed during five working days from the day of risk log acceptance
Risk Tracking	The status of risk management activities and mitigation success will be, revisited as part of the gate exit criteria for each phase of the project. The risk management plan will be updated at that time

Procurement Management

Includes the processes necessary to purchase or acquire products, services, or results needed from outside the project team.

Project Procurement Management includes the management and control processes required to develop and administer agreements such as contracts, purchase orders, memoranda of agreements (MOAs), or internal service level agreements (SLAs). The personnel authorized to procure the goods and/or services required for the project may be members of the project team, management, or part of the organizations purchasing department if applicable.

Project Procurement Management processes include the following:

- PLAN PROCUREMENT MANAGEMENT—the process of documenting project procurement decisions, specifying the approach, and identifying potential sellers.
- CONDUCT PROCUREMENTS—the process of obtaining seller responses, selecting a seller, and awarding a contract.
- CONTROL PROCUREMENTS—the process of managing procurement relationships, monitoring contract performance, making changes and corrections as appropriate, and closing out contracts.

The project manager should be familiar enough with the procurement process to make intelligent decisions regarding contracts and contractual relationships.

The project manager is typically not authorized to sign legal agreements binding the organization.

The Project Procurement Management Processes involve agreements that describe the relationship between two parties—a buyer and a seller

- THE SELLER may be identified as a contractor, vendor, service provider, or supplier. The seller is assumed to be providing services and/or materials to the project and is usually outside the performing organization. For larger, more complex projects the seller may become part of an integrated project team after the contract is awarded.
- THE BUYER may be the owner of the final product, a subcontractor, the acquiring organization, a service requestor, or the purchaser. The seller can be viewed during the contract life cycle first as a bidder, then as the selected source, and then as the contracted supplier or vendor.

The buyer of an item for the project is assigned to the project team and/or is part of the larger organization.

The Procurement Management Plan defines enough to, clearly identify, the necessary steps and responsibilities for procurement from the beginning to the end of a project. The project manager is responsible for ensuring that the plan facilitates the successful completion of the project and does not become an overwhelming task in itself to manage. The project manager will work with the project team, contracts/purchasing department, and other key players to manage the procurement activities.

Many projects have sub-consultants, sub-contractors, and suppliers. The project management plan should identify at the outset what outside products and services are required, how they will be procured, and how their progress and quality will be monitored.

It includes the processes required to acquire goods and services, to attain project scope, from outside the performing organization.

For the purposes of this project, the following staff are involved in the "procurement" of external services and materials (including IT infrastructure):

- xxxxxx CEO, BPC Payment Services

They are responsible for the end-to-end procurement process, from the point that a "need" for external resources has been identified.

It is the responsibility of the Project Manager to assign procurement tasks and to track their timely delivery.

Stakeholder Management

The processes support the work of the project team to analyze stakeholder expectations, assess the degree to which they impact or are impacted by the project, and develop strategies to effectively engage stakeholders in support of project decisions and the planning and execution of the work of the project.

The Project Stakeholder Management processes are:

- IDENTIFY STAKEHOLDERS—The process of identifying project stakeholders regularly and analyzing and documenting relevant information regarding their interests, involvement, interdependencies, influence, and potential impact on project success.
- PLAN STAKEHOLDER ENGAGEMENT—the process of developing approaches to involve project stakeholders based on their needs, expectation, interests, and potential impact on the project.
- MANAGE STAKEHOLDER ENGAGEMENT—the process of communicating and working with stakeholders to meet their needs and expectations, address issues, and foster appropriate stakeholder engagement involvement.
- MONITOR STAKEHOLDER ENGAGEMENT—the process of monitoring project stakeholder relationships and tailoring strategies for engaging stakeholders through the modification of engagement strategies and plans.

Initial engagement with stakeholders will take place during the initiation phase of the project, where expectations will be discussed and wherever possible documented. This includes within this document as well as within the Functional Specification Document.

Senior/executive stakeholder will continue to be, engaged through the Steering Committee Meetings, as well as receiving regular reports, as well as ad hoc upon request or need.

Other stakeholders will be kept advised regarding the project status, required actions, resource planning, etc. – as needed and in line with their respective roles. A number of them may also be involved in the Change Control Board, Project Committee (if there is one) and Project Weekly Meetings.

Due to the general size of the delivery, no other formal stakeholder management is, planned for this project.

Change Management

Change to contracted deliverables and adjustments to scope of work are identified, assessed, assigned and managed to completion by the Implementation Team as defined in the Roles and Responsibilities below.

The Change Management process should be, established at the highest level of authority in an Implementation. That is, at the project level for single project Implementations, or at the program level for Implementations with multiple constituent projects. Changes to key planning documents are to be approved. Documents that are managed and controlled in this manner, and their approvers, are listed in this Change Management Plan.

Change Request

The purpose of a Change Request is to document, track, and control any changes to the contract or adjustments to the agreed-upon scope of work for the implementation. A change may or may not impact the cost or schedule of the project. The Change Request process provides a documented trail of changes as well as information for the assessment of time, resource availability, cost impact of the change (if any) and delivery date of the change.

Two types of Change Requests could be used to document the change:

- Technical Change Request - intended to cover functionality related requirements such as:
  - Additional features and reports requested by Customer;
  - Additional integration with third-party solutions requested by Customer.
- Administrative Change Request - intended to cover changes in the following areas:
  - Change in the scope of work;
  - Change in the project schedule (Delivery date, Go-live date, UAT date, etc.);
  - Additional resources requested by Customer.

Change Process Roles and Responsibilities

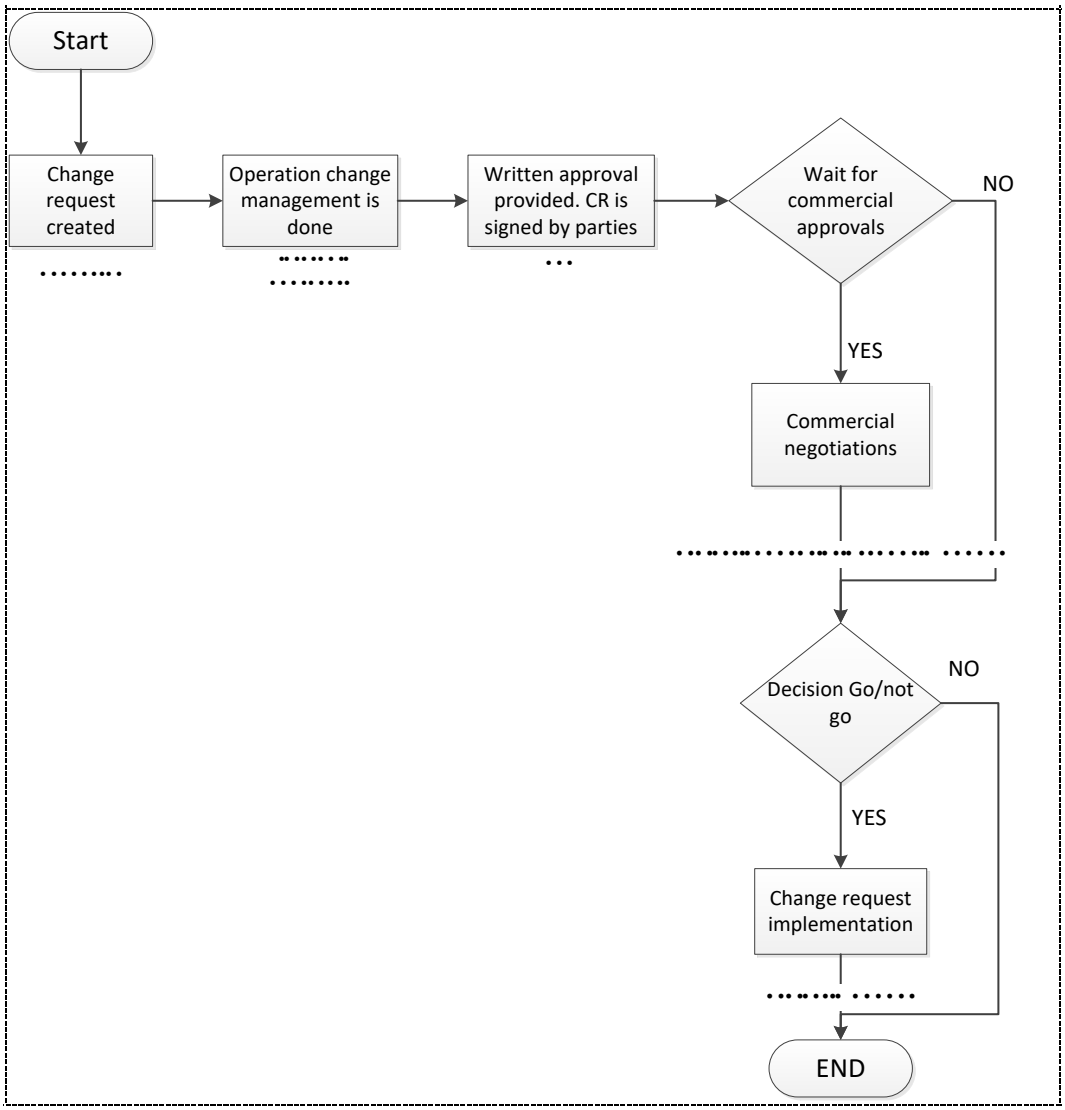
The following table describes the roles and responsibilities of those involves in the change process.

Role(s)	Action(s)
Requestor	Creates and submits the Change Request using the template including all required information, such as financial impact, resource requirements, etc. Any implementation team member may use this process to request a change.

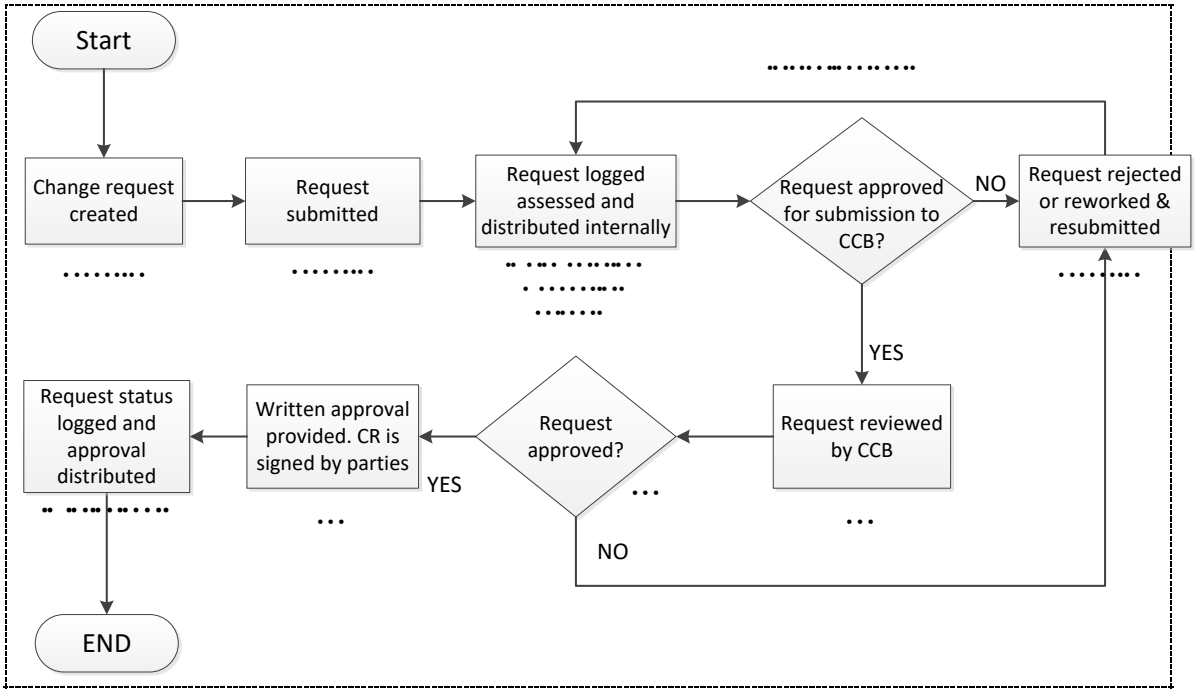
Implementation (Delivery) Manager or delegate (Project Manager)	Receives and enters the request into the request log. Assesses content, evaluates required resources, calculates List of Efforts (LOE) in man/days, defines delivery date and distributes to required internal approvers. Maintains status of the request log and informs interested parties of latest status. Project Manager is not obligated to discuss any price related questions. All price related negotiations must be, done between Commercial Approvers.
Internal Approvers	Typically consists of Technical Director, Delivery Manager and COO International Region. Internal Approvers either approve the request for submission to CCB (including LOE and delivery date), or reject and return to the requestor – possibly for rework and resubmission.
Change Control Board (CCB)	The membership of the CCB may be, defined in the contract. Typically, the CCB involves client representative(s) and BPC representatives(s). The CCB will either approve a request, or reject it and return it to the requestor – possibly for rework and resubmission.
Project Sponsor	Project Sponsorship is the ownership of projects on behalf of the client organization. Project Sponsor has to approve all commercial decision and provide decision go or not go with the provided Change Request. Even implementation project team will approve change request with the customer, Project Sponsor can cancel implementation activities based on agreements with the customer.
Account Manager	An account manager (Sales) is a person in a business who is responsible for the management of the sales and relationship with particular customers. Account manager can act as a Project Sponsor in case Project Sponsor is not available.
Commercial Approvers	Project Sponsor or Account Manager who are responsible for price and other legal tasks negotiations. Commercials Approvers make a decision GO or NOT GO with implementation activities. Project Manager cannot start any actions without approvals from Commercial Approvers.

Overall Change Management process

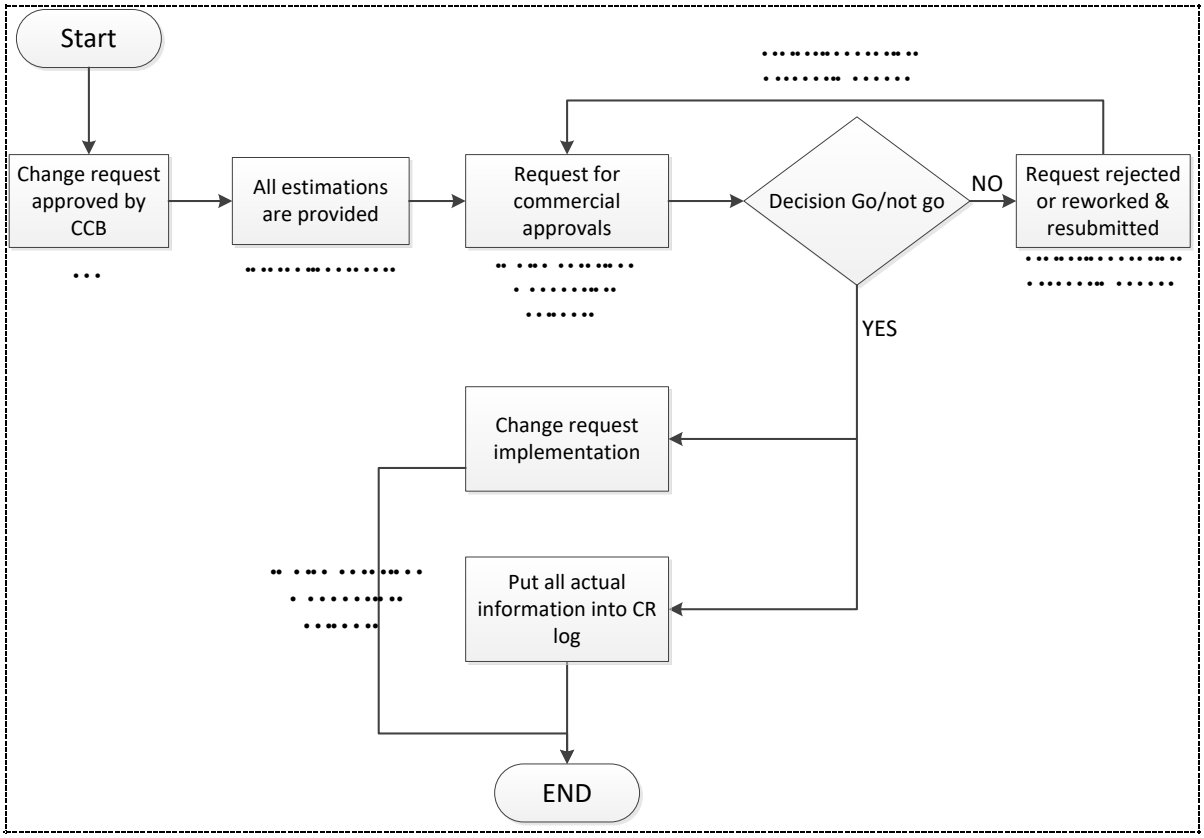
Schematically:



Operational Change Management Process



Commercial change management process



Travel Logistics

Visa and Border Formalities

BPC will make reasonable effort to maintain valid visas for its key staff. In particular, if a person is, expected to travel, effort to obtain a visa will be, made as early as possible. In this case, the client may be, requested to provide a confirmation letter to present at the relevant embassy.

BPC has symmetric expectations and can provide symmetric support for the clients' employees traveling to the BPC headquarters.

Note: Current Covid-19 travel requirements and restrictions must be accounted for.

Working Environment

During on-site sessions, BPC specialists will need:

1) Access to appropriate office facilities
2) Workstation including a desk, a telephone, an access to Internet and a local printer
3) Access to project related documentation, stakeholders and data

Meeting Environment

BPC expects that on-site meetings will be, conducted in adequately equipped rooms. Necessary equipment may include projector, white board, flip-charts, equipment for conference calls, outlets for power and network access, etc.

BPC provides such equipment for meetings at its offices.

Approach, Deliverables & Tools

BPC makes use of a Project Methodology (Approach) based on the one of the most widely used methodologies globally; PMI (Project Management Institute).

Our methodology seeks to apply best practice processes, based around the **PMBOK 6th Edition**, whilst seeking to maintain a pragmatic and customer-centric approach which takes account of the project complexity (and related risks), the size of the delivery including the number of resources and third parties involved, how compressed the schedule must be, the available budget and other factors.

Where a task or deliverable does not provide "added value" or real benefit to the project, it will often be, omitted in order to save time and reduce costs.

This is more commonly the case where BPC provides processing and managed services, as the delivery will be closer to out-of-the-box or existing functionality that may already be in live production running. In such bases, some project artifacts may add only limited value and unduly increase costs and schedule.

The table shown below shows the standard PMI Project Management Process Groups, as well as the "Knowledge Areas" – all of which will be covered within our Project Management Methodology.

Knowledge Areas	Project Management Process Groups				
	Initiating	Planning	Executing	Controlling	Closing
Project Integration Management	Develop Project Charter	Develop Project Management Plan	Direct and Manage Project Work Manage Project Knowledge	Monitor and Control Project Work Perform Integrated Change Control	Close Project or Phase
Project Scope Management		Plan Scope Management Collect Requirements Define Scope Create WBS		Validate Scope Control Scope	
Project Schedule Management		Plan Schedule Management Define Activities Sequence Activities Estimate Activity Durations Develop Schedule		Control Schedule	
Project Cost Management		Plan Cost Management Estimate Costs Determine Budget		Control Costs	
Project Quality Management		Plan Quality Management	Manage Quality	Control Quality	

Project Resource Management		Plan Resource Management Estimate Activity Resources	Acquire Resources Develop Team Manage Team	Control Resources	
Project Communication Management		Plan Communications Management	Manage Communications	Monitor Communications	
Project Risk Management		Plan Risk Management Identify Risks Perform Qualitative Risk Analysis Perform Quantitative Risk Analysis Plan Risk Responses	Implement Risk Responses	Monitor Risks	
Project Procurement Management		Plan Procurement Management	Conduct Procurements	Control Procurements	
Project Stakeholder Management	Identify Stakeholders	Plan Stakeholder Engagement	Manage Stakeholder Engagement	Monitor Stakeholder Engagement	

BPC can deliver projects using waterfall, agile or hybrid mechanisms.

In this case, we would advise something of a hybrid approach – as this would appear to best suit the type of delivery planned.

The project is likely to require multiple phases (or sub-phases), with analysis tasks at the start of each. This allows early “quick wins” to be achieved and allows testing of parts of the solution sooner – allowing misunderstandings (if they exist), architectural issues, infrastructure issues and integration challenges to be identified and addressed sooner – helping to avoid any significant impact to the schedule or budget.

In addition to this, a more “agile” approach can be, taken in relation to touchpoints and integration points. For example, GUI’s and Reports can be produced and then enhanced and

improved over several iterations, with business and operations users able to trial and comment on them sooner.

Opportunities to have effective "quality gates" should, also be taken to ensure excellence in delivery quality. These will be particularly important for the following:

- Before moving from Analysis to Design/Build
- Before moving from Design/Build to Integration/System Integration Testing
- Before moving from Integration/System Integration Testing to User Acceptance/Certification
- Before proceeding with Production Go Live (Go/No Go)
- Before moving from Pilot to full Production Rollout and Migration

In order to ensure sufficient and proper Project Governance, weekly meetings, change control boards and steering committees are typically the case.

We produce a **Project Management Plan** (PMP), which documents all of the following:

- Scope Management
- Requirements Management
- Integration Management
- Schedule Management
- Cost Management
- Quality Management
- Resource Management
- Communications Management
- Risk Management
- Procurement Management
- Stakeholder Management
- Change Management

Project Planning (Schedule Management) makes use of the **Microsoft Project** (MPP) tool, though often a simple Excel spreadsheet is sufficient for the early planning stage and even the drafting of the initial Work Breakdown Structure (WBS). For those without Microsoft Project – the plan is, converted to PDF before it is, shared.

Internally we also make significant use of the **JIRA** tool for creating and managing work packages, as well as linking various work packages together for reference and tracking purposes.

Project Governance and Control, as indicated earlier is, achieved in a number of ways, including the following (in line with the PMP):

- Regular weekly project team meetings (as well as ad hoc ones) where:
    - Progress versus the plan is discussed and tracked
        - Tasks
        - Milestones
        - Deliverables
    - Risks, Assumptions, Issues and Dependencies (RAID) are reviewed
    - Action List/Register items are discussed and updated
- Weekly Reporting
- Change Control Board (CCB) Meetings

- Steering Committee Meetings
- Quality Assurance and Control Measures
- Management Oversight (of Projects and Project Managers)
- Robust Risk Management
- Robust Change Management (Scope, Requirements, other)

In terms of Change Management, a Change Request Form must be completed and submitted. This will have an initial review and assessment before being, presented to the Change Control Board for discussion and approval. Where changes are, requested ahead of any delivery and where their impact is, deemed to be, zero or negligible, where both Project Managers agree – these may not need to be, presented to the CCB – but must still be, logged and approved.

Additional details can, be found in our template Project Management Plan (PMP), which can be provided on request. Note – this also includes information on the project teams and organization.

In terms of how we typically deliver a project (and we are happy to discuss and adapt this if Postbank has different views on this), we would typically have the following phases, as per our PMI-based Project Methodology:

- Initiation Phase
- Planning Phase (Discovery)
- Execution Phase
  - Analysis
  - Design
  - Development (Build)
  - Test
  - Deployment
  - Migration
- Closure Phase

Deliverables

The table below lists the expected Project Deliverables, along with a general description of them.

Deliverable	Responsible	Description
Project Management Plan (PMP)	BPC	A Project Management Plan (PMP) is similar to a PID, but goes into even further detail. It is typically a document produced applying the **PMI** (Project Management Institute) approach. It contains information covering all of the following areas: • Scope Management • Requirements Management • Integration Management • Schedule Management • Cost Management • Quality Management • Resource Management • Communications Management • Risk Management • Procurement Management • Stakeholder Management • Change Management In addition, it contains general information on the Project Management Approach.

Weekly (Progress) Report	BPC	The Weekly (Progress) Report provides information on the project status (progress) and related information, including all of the following:
		• Progress versus the plan
		  ○ Tasks
		  ○ Milestones
		  ○ Deliverables
		• Key/New: Risks, Assumptions, Issues and Dependencies (RAID)
		• Key/New: Action items

Project Plan (Schedule) [MPP]	BPC	A Microsoft Project Plan (MPP) reflecting the Work Breakdown Structure (WBS) and showing all: • Tasks • Resource Assignments • Milestones • Deliverables • Dependencies This plan is, updated and maintained on a regular basis and shared with the client.

Functional Specification Document (FSD) [Discovery Phase]	BPC	A document that captures the Functional and Non-Functional Requirements, as well as detailing the specifics of any interfaces between the solution/system and existing client ecosystem or required third party systems.

Test Plan (and related artefacts)	BPC	A document that details the test scenarios and test cases to be performed, covering all aspects of required testing, including:
		• Integration Testing
		• System Integration Testing
		• Certification Testing (if performed by BPC)
		• Operational Acceptance Testing
		  ○ Implementation
		  ○ Migration / Rollback
		  ○ Penetration
		  ○ Performance
		  ○ Failover/Recovery

User Acceptance Test Plan	Client	A document that details the test scenarios and test cases to be, performed, with a focus on the users and operators of the system and the use cases and usability of the system.
System Documentation (Guides)	BPC	Product documents such as: • User Guide • Administration Guide • Configuration Guide • Developers Guide
Migration Plan	BPC	A document that explains the migration approach and then goes on to detail aspects of the migration such as the migration (and rollback) steps, timings, resources involved, escalation process in case of issues, etc.
Training Plan (and related artefacts)	BPC	A document that details the plan for training and knowledge transfer, including training dates, attendees/audience, modules, tests, prerequisites, etc.
Procedure of production issue investigation	BPC (& Client)	An Incident Management document that explains the general approach to incident handling including raising an incident, responding to one, analysis of incidents and ultimately the resolution of incidents (hot fix/patch and final resolution), tools, escalation procedures, etc. in terms of how any production issue/incident is handled.

Business continuity and disaster recovery plan	BPC (& Client)	A document the outlines the process/procedures and responsible persons involved in handling recovery from a disaster (e.g. Data Centre fire) and more broadly how, as a business, work is able to continue in the face of any form of problem – such as civil unrest or strike action.

The final list of deliverables will, typically be, agreed when producing a Scope of Work (SoW) document – which is then, referenced in the contractual agreement. Certainly, the deliverables list must be, fixed ahead of contractual agreement – with change control applied from that point on.

Approach, Deliverables and Tools used for Analysis phase

Please refer to 'Requirements Management' section.

Approach, Deliverables and Tools used for Design Phase

SmartVista-based solutions are made up of the products and components provided by the SmartVista Suite.

The SmartVista Suite delivers a highly flexible and configurable solution set that focuses on time-to-market, ease of maintenance and reduced total cost of ownership.

We also make use of modern and best practice frameworks and architecture approaches to simplify long-term evolution of the products and solutions, as well as ensure fast and simple integration within an existing ecosystem.

This results in a project implementation **design phase** typically being very limited.

The vast majority of implementations focus on the areas of integration and setup/configuration.

A proposed Solution Architecture is created by an architect, often using Enterprise Architect or Visio.

This identifies the integration points and their interactions.

The Functional Specifications Document details these interfaces, as well as describing their flows in detail – doubling as a form of Technical Specifications Document, when accompanied by any related Appendices and Questionnaires. These also support the later, initial setup and configuration.

This also includes the definition of required BPMN workflows, as required by some products/components – such as the Integration Platform, used by our Instant Payments solution, amongst others.

Technical Business Analysts drive this process, working with the Architect and/or Technical Lead, as well as with Product Manager and other technical SME's.

Where development gaps are identified within a product or component, the Project Manager will coordinate with the Development Department, as well as Product Managers and the Release Manager to ensure the delivery of updates/enhancements at the earliest possible opportunity.

It is the responsibility of the development team leads to manage the individual product/component design, in alignment with our architectural principles and development methodology.

Tools used can vary by product and development team, but include Eclipse, Apache Maven, GitHub, AngularJS, Docker and more.

Approach, Deliverables and Tools used for Implementation / Build phase

Implementation Plan

This section gives further information on the activities and deliverables, however, here we look at the general breakdown of the scope and the kind of activities required in order to, support the implementation.

1. Project Management
    a. Project Kick-off Presentation
    b. Project Management Plan (PMP)
    c. Progress (Status) Reports
    d. Detailed Project Plan (Schedule)
2. Development (Analysis)
    a. System Specifications/Requirements (FSD)– delivered as part of a Discovery
    b. Interfaces Definition (FSD)
    c. User roles and access rights definition (FSD)
    d. Business Rules and Restrictions definition (FSD)
    e. Requirements relevant to the configuration of the system (FSD questionnaires)
    f. User Interfaces (FSD)
    g. Interoperability Requirements (FSD)
    h. Preliminary Data Migration and Test Plan
    i. Definition of the physical and logical architecture design
    j. System sizing support
3. Deployment to development and test environments
4. Deployment of required infrastructure components (client)
5. Development and implementation of the solution
    a. Implementation
    b. Configuration and Parameterization
    c. Implementation of interfaces
6. Planning and implementation of data migration (if applicable)
7. Execution of training activities
    a. Training Plan
    b. Prepare Training Materials
    c. Conduct Training
8. Performance of acceptance test procedures
    a. Test Plan
    b. Test Preparation
    c. Test Execution
    d. Test Reporting
9. Release of production environment to end users

   a. Implementation & Migration Plan
   b. Production Live Implementation
   c. Pilot
   d. Migration (if applicable)
10. Provision of post deployment services (depending on the service delivery model to be selected)
   a. Operational Planning
   b. Hand-over to Support/Operations

In terms of how we typically deliver a project (and we are happy to discuss and adapt this if NBM has different views on this), we would typically have the following phases, as per our PMI-based Project Methodology:

- Initiation Phase
- Planning Phase (Discovery)
- Execution Phase
  - Analysis
  - Design
  - Development (Build)
  - Test
  - Deployment
  - Migration
- Closure Phase

Initiation, Planning and Analysis can largely be taken together and focus on understanding the requirements of NBM and your (new) operating model. There is also a focus on planning for the rest of the project, so this is a time when many management, planning and strategy documents, are produced.

It is, expected that much of these will at least be started during a 2 – 3 week kick-off and **discovery workshop**. All of the referenced NBM staff/team below are likely to be involved and specifically we would seek the following roles to be, represented:

- Project/Business Sponsor
- Project Manager
- Business Analyst
- Test Manager
- Security Analyst
- Business SME's
- Technical SME's
- Operations SME's

It is expected that for the 2 – 3 weeks workshop that the Project Manager and Business Analyst will be in full-time attendance, that the Project/Business Sponsor is there only for the first session and that others will be needed for particular topic areas, depending on a previously agreed agenda.

Following the workshop, for the remainder of this phase, the Project Manager would remain full-time and engage with others internally for any required additional materials, follow up actions and clarifications.

Many of this team will also be required as reviewers of documents produced during this phase.

Note that during this period, we will also seek to determine the optimum operational model, processes, procedures – as well as opportunities to simplify, rationalize, improve and automate.

This "Discovery Phase" is sometimes treated under a separate contract, as its outputs provide a much clearer and more detailed view of how the project will be delivered, the requirements, timeline and costs. Some organizations prefer to have this clarity before proceeding to the next step, as differences in scope, timeline and budget can have a major influence on the business case associated with the project.

As we move, further into the Execution Phase (Design, Development/Build, Test and Deployment) the majority of this will take place within BPC with only a limited amount of involvement required from NBM (unless a more agile approach is agreed).

This said we would seek active involvement from NBM for User Acceptance Testing, Certification and Networking/Connectivity (related to Deployment).

Specific resources needed during this time would be:

- Project Manager
- Test Manager
- Testers (from Business/Operations)
- Network Administrator

Note also, at an agreed point, during this period – we would seek to undertake formal classroom Training for all resources who may be involved in working with the final SmartVista-based system.

As we move to the Migration Phase, the following resources will be, needed:

- Project Manager
- Test Manager
- Testers (including for "friends and family" pilot testing)
- Network Administrator
- Security Analyst (for any required security key migration)

Once all steps have been, completed, we will move into Closure Phase and seek to perform a "lessons learned" on the project – in order to understand what went well and what did not. This will help in ensuring that any future projects and on-going production operations are improved.

All key project team members as well as the Project/Business Sponsor would be, expected to participate in this session, as well as ensure that any follow up actions are, carried out to ensure any required improvements are, made.

Whilst there may be opportunities for less experienced resources to be involved from the NBM side, we generally assume a “strong team” to be in place from NBM, with all key roles being, performed by experienced (10+ years), skilled and knowledgeable resources for the various areas being represented.

The Project/Business Sponsor and Project Manager needs to not only be experienced and skilled, but also have sufficient seniority and authority to ensure that any issues or decisions are handled quickly and not allowed to, cause delay, to the project.

Given the scope, it is certainly **very achievable to deliver the project in 20 months or less**, following project kick-off, on the basis that both companies work collaboratively to achieve this. This means a clear and shared set of objectives, proper staffing (including sufficient resource availability), proper management of risks and changes and seeking opportunities to deliver items in a more agile manor.
Please also refer to the Project Management Plan for further details of deliverables produced during this phase.

Approach, Deliverables and Tools used for Testing phase

Acceptance Testing Plan

All testing will begin with the planning and definition of all the tests to be carried out. The test material will be prepared from the following sources:

- *Unit Testing*: program logic specifications/detailed design, code listing, Project Documents;
- *Vendor Solution System Testing*: context diagrams, process maps, design documents, system use cases, Project Documents;
- *System Testing:* context diagrams, process maps, design documents, system use cases, Project Documents;
- *Integration Testing (SIT)*; (including data migration testing) context diagrams, process maps, design, documents, data migration maps, system use cases, Project Documents;
- *Systems Assurance Testing (SAT)*: design documents, process maps, system use cases, Project Documents;
- *User Acceptance Testing (UAT)*; process maps, system use cases, Documentation, Project Documents.

The Project Team develops a user acceptance test scenario that will verify the system satisfies the business requirements. User acceptance focuses on:

- Operational testing (e.g., ease of use, system availability, input and output data volumes, and frequency of access);
- Functionality testing against business and internal controls requirements;
- Operational testing of interface with other systems;
- Disaster Recovery testing.

The user acceptance test plan package includes:

- Test scenarios;
- Test data;
- Test procedures, scripts, and internal controls;
- Test software specifications;
- Identification of special test hardware;
- Predicted test results.

The user acceptance test is conducted by the Project Team and selected user personnel to ensure the approved business requirements are met. The roles of the Business Users are to support the user acceptance test; asses the readiness of the system for pilot site operations; and provide confirmation, concerns, and issues to the Project Manager.

The test team evaluates the system by executing the user acceptance test plan. Upon completion of the user acceptance test, a report is written that documents results of the test, system issues and their disposition; and identifies corrections and modifications made to the system, user documentation, training program, and courseware.

The benefits of this approach are:

- Testing is focused on what was actually requested
- Testers start from the same documented baseline
- Informs management for prevention of “scope creep”

Procedure for Performing System Integration Testing with Participants

Planning of the certification testing starts at the moment when the Participant is notified about the approval of connection questionnaire sent to them.

To plan the test on the Participant’s side, a project manager (PM) must be assigned to start the activities. This PM:

- Approves on the testing schedule;
- Co-ordinates the timely implementation of all necessary works on the Participant’s side.

Within the certification testing procedure, from the point of view of the Participant, there are the stages specified in Table 1.

Table 1 - Main stages of certification testing

Stage	Description
Preparation for the testing	The Participant performs preparatory actions
Connection	The Participant performs the actions necessary for the connection to IPS

Testing	The Participant performs the necessary tests Based on the results of the certification testing performed, both parties fill in a document of completing the testing.

Two main time slots are allocated for the Participant to conduct the testing procedure (see Table 2).
The reserved test slots are allocated to the Participant if necessary (in case of main certification slot expires due to an unsuccessful result).

Table 2 - Time slots to conduct testing

Time slot	Deadlines	Comment
The main time slot for testing	5 working days	The criteria of success is passing all the approved test scenarios.
Time to correct errors	The deadline is agreed with the Participant	The participant corrects errors in the agreed interval.
The reserve time slot for testing	5 working days	Repeated testing. The criteria of success is passing all the approved test scenarios.

In case of a failed testing by the Participant, the BPC representative notifies the representative of the client. In case of presence of errors after conducting the testing within the main and reserve time slots (see Table 2), the Participant agrees with the PM, a separate plan for repeating the tests.

Preparation for the Testing
The Participant is provided with the guidelines for connecting to the IPS (Instant Payment System) prototype that describes the scheme and procedure for connecting the Participants to the prototype of the Instant Payment System. Based on the received connection parameters (the IP-address and port), the Participant must set up these parameters in their processing systems to connect in accordance with the provided document.

After receiving a confirmation from the IPS support service of the completion of the Participant's settings in IPS, the Participant performs a physical testing of the connection from the Participant's infrastructure to IPS, according to the above mentioned instructions. Within the allocated time slot the IPS support service consults the Participant's staff if necessary. After a successful completion of the connection test, the Participant can start testing the business functions of the IPS prototype according to the current version of the ISO20022 API Specification.

Execution of Testing

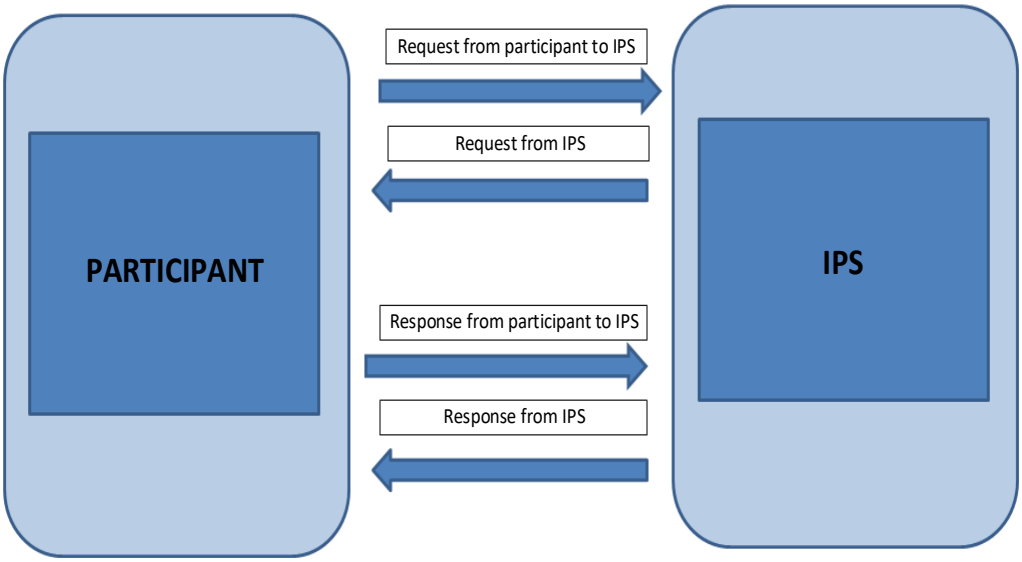
On the agreed date the Participant must be prepared to start testing. All the necessary settings must be implemented in the testing environment of the Participant and IPS, and the availability of all access permissions must be checked. During the testing, the Participant must carry out the tests specified in the test plan. During the period allotted for the testing, the Participant must achieve the successful execution of all test scenarios.

Testing Procedure

The testing of Participants is composed of four stages (the description of each stage is given in the sections below):

- independent testing by the Participant of the structure of generated XML requests (in the off-line mode, without connection to IPS) - the XML Validation; Before starting the online certification, the Participant must conduct an independent testing to ensure that his system is prepared for sending and processing messages in the correct format. The validation is required to make sure that the structure of XML messages comply with the IPS API specification. The Participant can perform the validation of XML messages independently (XSDs are provided separately) or in the way recommended by the IPS support service

- testing by the Participant of requests with connection to IPS, including sending requests to the Participant itself for analyzing the results and adjustment; The scheme of this stage of testing is presented in the diagram (Figure 1):



For this stage the participant needs to connect to the IPS platform. This stage of testing involves such an exchange of messages when the Participant is both the initiator of the request and the recipient. Within this phase, the entire set of tests defined in the plan must be

conducted with the same value specified as the BIC recipient and the BIC sender — it must be the BIC specified by the Participant in the application form on registration.

Testing by the Participant of requests with connection to the IPS, including the service on the IPS side emulating the behaviour of a recipient Participant; This stage is an integral part of the online certification and involves the implementation of tests defined in the plan. Tests of this stage are divided into the following two blocks:

- Block #1 Test scenarios in which the Participant acts as the initiator of a request
- Block #2 Test scenarios in which the Participant acts as the recipient of a request

The description of all test scenarios is presented in the form of tables and as a textual description with recommendations for the implementation. When conducting tests, the participant needs to have the following documents:

- The set of ISO 20022 IPS API specifications.
- The specification ISO 20022_different use cases (Transfers, Inquiries, Validation request)
- The specification of_Customized_Users_Registration
- The guidelines to the set of specifications
- The guidelines on how to connect to the prototype

The interbank testing including sending and exchanging messages between two or more Participants. This stage is final in conducting the certification testing. Information on conducting the testing at this stage, as well as the list of necessary test data are provided separately.

The above procedure and the proposed test script for Payment system is sent as a separate document as part of Technical Proposal submission. Kindly refer to Sample Test Scripts accompanying.

SmartVista Testing Tool
Please refen to 'SmartVista Testing Tool' section.

Approach, Deliverables and Tools used for Go live and Final Acceptance Phases

As a part of the live implementation the following approach is suggested:

Live Implementation
Relevant SmartVista components will be deployed in the live environment adhering to a detailed implementation run book.

Technical Verification Testing
The implementation team consisting of BPC personnel will perform integrity checks ensuring that the live cutover is in accordance with the planned approach. Technical resources from NBM may participate in this verification test alongside BPC resources.

Business Verification Testing
The business verification team from NBM supported by the BPC implementation team will perform business verification testing in adhering to a previously documented test script.

After successful Business Verification Testing, the system is declared successfully implemented in production in accordance with the Go live/Implementation plan.

After this point the business may perform a pilot launch for limited users prior to market launch for customers.

Approach to the Change Management Process

Please refer to 'Change Management' section.

Development policy

Issuing new release includes the following steps:

- **Requirements gathering** – period of collecting all requirements for the new release. As a result, the list of new features and enhancements should be approved.
- **Analysis –** analyzing requirements, preparation of the analytic documents, estimation and schedule commitment
- **Development** – main part of development, all new features and enhancements should be developed during this period.
- **Testing & stabilization** – period of integration testing and bug fixing. All the blocker, critical and major defects should be fixed.
- **Release Management** – Final step of packaging the software for delivery. This includes documentation, training preparation and other necessary steps specific to release.

The plan for new release includes the following milestones. Period of time between the milestones may vary depending on SV product and volume of the release, but aim is to release as frequently as possible within constraints.

- Requirements freeze – final date of requirements gathering
- Resource sign-off – finalized resource allocation plan for the release
- Design Sign-Off – all analytical documents on new functions have been prepared
- Development freeze – development is complete, the release is ready to start testing
- Delivery – testing is complete, the release is placed to the repository for deployment

The above steps are illustrated in the diagram below, categorized into four sections, a) Planning b) Analysis and development c) Testing d) Packaging

Three main areas of responsibilities are

1) R&D – Analysis and Development team

2) R&D – Testing team
3) Implementation Groups

Quality Assurance

Our Quality Management Program, which is an integral part of BPC's International Quality Standard ISO 9001:2015 accreditation, provides the framework for ensuring that quality objectives are set and both customer and regulatory requirements are met.

BPC senior management team is committed to ensuring that we achieve the highest levels of service delivery and customer satisfaction by continuously improving our people and processes and regularly reviewing the effectiveness of the Quality Management System.

The overriding purpose is to ensure that:

- Quality standards are set up front and are clearly articulated and understood by all people engaged on the program
- All delivery processes and mechanisms are clearly articulated and understood and have defined outputs and quality checks designed into them
- All program team members are capable and competent to meet the defined quality requirements
- Rigor and challenge are key facets in ensuring quality outputs are achieved
- A high quality, flexible solution is developed

For this process to be effective, it is important that this is a process that includes Client and BPC to work closely together to deliver a single integrated quality assurance process.

Version Management

BPC follows an ISO 9001 certified software development process. PMI methodology is used for project management. The version control system manages source code and executables. Automated testing procedures are run, and builds are produced regularly.

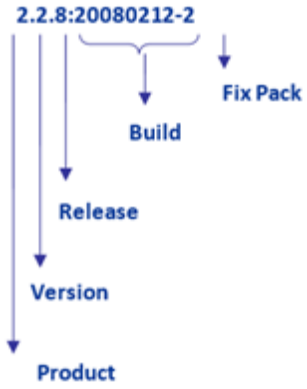
SmartVista contains an intelligent installer, which has a database of releases, files, and checksums. During installation of newer versions, releases, and patches, this installer checks for installed database, executables and compares them with the targets for compatibility and correctness. This installer then automatically copies the relevant files and makes necessary database changes. SmartVista numbering scheme has following hierarchy- Product, Version, Release, Patch Set. Product is the main module name. Version is the major release, which is changed approximately once a year. Release containing major accumulated changes requiring a change in database structure and Payment Network mandatory changes is usually updated once every quarter.

Patch Set is bug fixes and incremental changes not requiring a change in database structure and is released when needed.

Types of Releases

BPC support various mechanisms, such as:

- New releases of the system. New releases of system leave with periodicity about time in some months. These releases are planned and can include correction of errors, additional configuration options and new functionality. This type of releases can be issued 3-4 times a year.
- Payment system updates. We let out the updates connected with periodic releases of payment systems. Such updates leave approximately one month prior to an output of release of corresponding payment system and contain updating system on new functionality entered corresponding payment system. Releases of this type usually are issued two times a year.
- Our system is flexibly set up therefore often-new products are registered by additional configuring system, which our clients make independently, under our management, or in view of our recommendations. In case of if it is necessary to develop additional functionality for the client, and install it not waiting an output of planned release the given functionality are installed in the form of the update prepared for the concrete client, in view of the version of system installed at present at this client.



VII. Answers to section F4.4

FUNCTIONAL REQUIREMENTS

7.1. General functional Requirements

Requirement ID	Requirements	Classification
7.1.1. General requirements		
FR.1	The offered application should be an end-to-end solution that fully supports the entire lifecycle of instant payments processes, according with the best practices in the industry.	Mandatory
Reply	The SmartVista Instant Payment system offers a complete end-to-end solution that supports the entire lifecycle of instant payment process from participant on boarding to clearing and dispute management and to the final settlement. Please refer to 'SmartVista Instant Payments Overview' for more details in the Techincal Proposal.	
FR.2	IPS uses messages in line with the ISO20022 standard. *IPS uses the ISO20022 standard version which can be improved in the course of implementation. All the messages in the system will be in line with that standard, when possible. All the messages in the system are xml messages.*	Mandatory
Reply	SmartVista Instant Payment system natively supports ISO 20022 message interface over xml as well as JSON construct. Please refer to section 'ISO 20022 Messaging Standard' in the Technical Proposal for details.	
FR.3	IPS will carry out the technical validation of every received message, which must include at least: validation of existence of mandatory fields defined in the message format, and of optional fields used in one of the processes. *Additional business validation of messages has been established for every process.*	Mandatory
Reply	The SmartVista Instant Payment system performs message validation based on the configurable business rules defined against a message interface format. The validation on XML schema or other message type like ISO20022 is performed on an incoming message, which is checked for both the	

	format of the field as well as the content. The presence/absence of the field and data format checks are performed and the business logic executes the next step based on the results of these validations. Please refer to section 'Instant Payment Platform Core Services' for details on how the messages are processed and managed.	
FR.4	IPS will terminate the technical validation of a message as soon as the first validation error is encountered and send an appropriate rejection message to the Sender. *As the first validation error is encountered, IPS stops the processing and notifies the Sender thereof with a message. The message contains the code indicating the reason for rejection.*	Mandatory
Reply	This is the default behavior of SmartVista core processing platform. If validation checks fail because of any reason the business logic can be configured to reject a message with appropriate reject code indicating the reason of failure. Please refer to section 'Instant Payment Platform Core Services' where the business process steps are defined and explain the flow when the validation failure occurs.	
FR.5	IPS will receive only those messages from the Sender that have a digital signature. Only the messages specified as such in the technical documentation depart from this rule. *ACK and NACK messages are not considered messages in terms of this rule.*	Mandatory
Reply	SmartVista Payment system will establish PKI using Microsoft Active Directory Certification service. The Certificate Authority (CA) will issue the digital certificates to the participants who will then use it to sign the message and send it to the payment system. The messages received at payment system will be verified after the signature is verified using the private key.	
FR.6	IPS enables A2A interface to users. *IPS enables sending messages in A2A mode to users.*	Mandatory

Reply	SmartVista Instant Payment system supports A2A by default by exposing APIs from the core platform that enable participants to send and receive messages over ISO 20022 message format.	
FR.7	IPS enables users to use web interface. *IPS allows users to perform monitoring and reconciliation of payments via web interface.*	Mandatory
Reply	SmartVista Instant Payment system offers Participant Portal that aides participant user to access the system and perform operations, monitor transactions and initiate liquidity management tasks. Please refer to 'Participant Portal' section in the Technical proposal for more details of the functionality.	
7.1.2. Liquidity		
f FR.8	Every Participant in the system has at least one IPS account *At least one IPS account is opened for every Participant in IPS regardless of whether they are a direct or an indirect participant. If a Participant has more than one account, the account is explicitly stated in the message, otherwise IPS will use the default account. If no default account has been defined, and a Participant has more than one IPS account, IPS will reject the transfer order by sending an appropriate error message.*	Mandatory
Reply	SmartVista Instant Payment system provides highly configurable and sophisticated two-level participant account hierarchy. This hierarchy provides a lot of flexibility to manage any type of participant account and liquidity management, supported by the scheme. The accounting system support one IPS account per participant. This IPS account is referred to as Participant Working Account (in case of direct participant) or PSP Working Account (in case of indirect participant) in the Technical Proposal Section 'Participant Type and Account Management'. Please refer to that section for the accouting detail.	
FR.9	Every IPS account has an account structure, established by operating rules.	Mandatory

Reply	Yes supported by default. Every IPS account holds multiple balances. For example Starting Limit, Remaining Limit and Net position. Please refer to 'Participant Type and Account Management' section for more details.	
FR.10	Every IPS account can be uniquely identified by means of a BIC. IPS system uses 11-character BIC registered in SWIFT or a pseudo BIC assigned by the NBM in this format. *The BIC (or other unique identifier of a Participant similar to the BIC – pseudo BIC) attached to an account is unique in the IPS system.*	Mandatory
Reply	In SmartVista the institution hierarchy includes the following model: Institution -> Account -> Payment Instrument. The BIC is assigned at the Institution level. There can be direct participant institute and an Indirect participant institute. The Indirect participant institute falls under the hierarchy of the direct participant institute. The BIC is unique to the whole platform and cannot be assigned to more than one institute.	
FR.11	Every Direct Participant in the system has a special account opened in the NBM's RTGS system. *A special account is opened for every Direct Participant in the RTGS system which is used for the execution of transfer orders in IPS or for liquidity transfer to/from RTGS, through integration with IPS.*	Mandatory
Reply	SmartVista supports the account hierarchy explained in this requirement. Every direct participant of the Instant payment system will be required to open a special account which we call IPS Pool Account in the NBM RTGS system. This is the pool account that will fund the liquidity of a participant to the IPS. Please refer to the section 'Participant Type and Account Management' for details.	
FR.12	Every Indirect Participant in IPS has an open IPS account connected to exactly one RTGS account of the Direct Participant (settlement bank).	Mandatory

Reply	This is supported by default. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details.	
FR.13	Every IPS account is connected to exactly one RTGS account. An RTGS account may be connected to several IPS accounts *A Direct Participant's IPS account is connected to its RTGS account, an Indirect Participant's IPS account is connected to the Direct Participant's RTGS account*.	Mandatory
Reply	This is the default structure of SmartVista Participant account hierarchy structure. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details.	
FR.14	A participant's IPS account limit is set by the Direct Participant to whose RTGS account that IPS account is connected. *The Direct Participant sets the limit for all IPS accounts connected to its RTGS account.*	Mandatory
Reply	Using both the participant portal (U2A) as well as ISO 20022 APIs (A2A) a direct participant can set IPS account limit for all the participants registered under the direct participant hierarchy. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details.	
FR.15	IPS account limit setting is done by sending an appropriate message in the IPS system. *The Direct Participant sets the IPS account limit by sending an appropriate message, whose technical and business validity are checked by IPS*.	Mandatory
Reply	IPS account limit setting can be done by sending ISO 20022 camt.011 (Modify limit) message to the IPS from the participant system. The IPS perform the required validation and then proceed with the instruction as per the business process configured. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details.	

FR.16	IPS will perform business validation of the limit setting message sent by a direct participant. Message processing will be disrupted and it will be rejected at the encounter of the first error. *IPS validates the inbound message and informs the direct participant of any errors that occurred in the course of business validation. Validations carried out are specified in more detail below. In addition to these validations, technical validations are also carried out.*	Mandatory
Reply	This is supported by default. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details where the business flow of limit setting message is explained.	
FR.17	IPS will validate the authorisation of a direct participant to set the IPS account limit. The Direct Participant whose RTGS account is connected to the IPS account to which the limit is being set is the only one with the limit setting authorisation. *IPS validates the direct participant-sender's BIC and checks if the RTGS account connected to the IPS account to which the limit is being set, corresponds to that BIC.*	Mandatory
Reply	This business logic check is part and parcel of liquidity limit setup in SmartVista Instant payment system. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details.	
FR.18	IPS will check whether the new limit amount pushes the IPS account balance to below zero and will reject the limit setting message with an error message. *IPS will set a new limit amount on the IPS account only if the IPS account balance is not below zero.*	Mandatory
Reply	This is supported by default. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details.	
FR.19	A Direct Participant may set limits to IPS accounts to which its RTGS account is connected without making sure to have coverage on the RTGS account for all defined limits.	Mandatory

	IPS allows for the sum of limits on IPS accounts connected to the RTGS account to be higher than the amount of funds on that account since it is not possible to have a lack of liquid funds, as the RTGS account balance in IPS is also checked in the course of transfer order execution (see FR.65).	
Reply	This is the default behavior as the sum of all IPS working account may be greater than the balance available in the IPS RTGS account (also known as Participant Reflection Account). However over limit is not possible because the balance of both IPS as well as Reflection account is validated before transaction is allowed to proceed. Please refer to section 'Participant Type and Account Management' in the Technical Proposal for more details.	
FR.20	IPS will notify the IPS account holder when the IPS account position reaches the configured parameter in the system (for example 90%) relative to the set limit. *IPS will also notify the Direct Participant whose RTGS account is connected to that IPS account of limit utilization.*	Mandatory
Reply	SmartVista Instant payment system allow setting up of high liquidity threshold as well as low liquidity threshold. In both of these case the appropriate notification is issued to the participant informing them of the account position and next action to take. For example on reaching low liquidity the participant will be asked to topup their limit from the portal or via direct messaging. In case of reaching high liquidity the participant may be asked to defund their liquidity back to RTGS.	
FR.21	IPS will notify the Direct Participant when the RTGS account balance in IPS reaches the configured parameter (for example 80%). *IPS will notify the Direct Participant that the RTGS account balance in IPS has reached the configured parameter relative to the RTGS account balance in the RTGS system (for example 80%).*	Mandatory

Reply	SmartVista Instant payment system allow setting up of high liquidity threshold as well as low liquidity threshold. In both of these case the appropriate notification is issued to the participant informing them of the account position and next action to take. For example on reaching low liquidity the participant will be asked to topup their limit from the portal or via direct messaging. In case of reaching high liquidity the participant may be asked to defund their liquidity back to RTGS	
FR.22	A direct participant transfers funds to/from its RTGS account during a business day and operating hours of the RTGS system with a conditional message MT202 (MX message after SAPI modernization). *A direct participant must not breach the IPS operating rules regarding the RTGS account balance in IPS, when changing its RTGS account balance in the RTGS system. The message which breaches the IPS operating rules will be rejected in the RTGS system*.	Mandatory
Reply	This is supported by default. All business validation on the IPS and RTGS account in IPS are maintainted and configured in the SmartVista Instant payment core processing system. All business logic rules are configured based on the defined IPS operating rules.	
FR.23	IPS will update the RTGS account balance in the RTGS system several times during a business day and operating hours of the RTGS system, in predefined periods, so that it corresponds to the RTGS account balance in the IPS system at the moment of update. Update is mandatory at the beginning of an RTGS system business day (immediately following load balances – reading RTGS account balances from the previous business day of the system), and before the period determined for issuing statements of account at the end of the RTGS system business day. *The process may also be initiated by the operator upon request (for example in case of direct/indirect participant's inability to settle their liabilities).*	Mandatory
Reply	The IPS update to RTGS balance is supported as a basic features. Both topup (from RTGS to IPS) and defund (from IPS to RTGS) is supported at predetermined period of a day or at regular interval. This depends on the business use case and requirement of the bank. Likewise the IPS update of the RTGS balance is also possible on demand from the participant both	

	from the Participant portal as well as via ISO 20022 messages. IPS operator which will be NBM can also initiate this request from the participant portal.	
7.1.3 Reporting		
FR.24	IPS must enable Participants to view the balance of IPS accounts in A2A and U2A modes. *U2A and A2A (A Participant may check the balance in the IPS account on the screen or by an appropriate message)*.	Mandatory
Reply	The balance checking is available both via Participant Portal (U2A) as well as via ISO 20022 message (A2A) APIs balance inquiry message.	
FR.25	IPS must enable Direct Participants to view the balance of the RTGS account in IPS. *U2A and A2A*	Mandatory
Reply	This is supported by default. Please check 'Participant Portal' section for more details.	
FR.26	IPS must provide all the queries necessary for monitoring the work in the system to Participants. *A2A*.	Mandatory
Reply	SmartVisa Instant Payment system support a large set of APIs through which participant can monitor their transactions, liquidity, Central addressing scheme, limits and reports.	
FR.27	IPS will initiate report generation at the end of the RTGS system day or at the moment defined under the IPS operating rules or in line with the schedule previously requested by the Participant.	Mandatory

	Statement of account turnover and Statement of account for all Participant accounts.	
Reply	SmartVista Instant Payment system supports business report generation at the end of a cycle via camt.052 ISO 20022 message. The message is sent to the respective participant at any moment defined by the IPS with details of transaction peformed during the period.	
FR.28	IPS should provide generation of reports that contain data available since the last report up to the present moment.	Mandatory
Reply	Supported by default.	
FR.29	IPS will validate the authorisation of Participants to perform certain queries in line with account ownership in IPS. *The NBM has query authorisation for all accounts and all transactions in the system. A Direct Participant has query authorisation for all IPS accounts connected to its RTGS account.*	Mandatory
Reply	The participant permission set is maintained in the SmartVista Instant Payment system and is enforced both in A2A as well as U2A mode. For example direct participant can view and perform liquidity management funcitons on all IPS account under its hierarchy. Indirect participant can view its account and may initiate request for liquidity topup and defund to the direct participant.	
7.1.4. Administrative functions		
FR.30	IPS is required to enable the NBM to connect direct and indirect participants in the system.	Mandatory

Reply	This is default feature and supported. Please refer to 'Instant Payment Platform Core Services' section in the Technical Proposal for more details.	
FR.31	IPS enables the NBM to block/unblock a Participant's IPS account. *Separate blocking of credit and debit functions of an IPS account is required.*	Mandatory
Reply	The participant account permission are maintained within SmartVista Instant payment system. Please refer to 'Participant Type and Account Management' section in the Technical Proposal for more details.	
FR.32	IPS provides predefined tests for checking participants' operation to the NBM. *Functionality needs to be provided that will enable validation of participants' compliance with the requirements defined in SLA (originating from the operating rules).*	Mandatory
Reply	BPC will provide the required support and expert advice to NBM to define the technical standards as well as standard operating procedures. The scheme rules determine by the bank will be based in the input from BPC to ensure smooth operations for all participants.	
FR.33	IPS should provide an appropriate graphic interface which will enable the NBM staff to configure IPS system parameters as a whole and individually.	Mandatory
Reply	SmartVista provide easy to use Participant Portal as well as Operator portal for the NBM staff to use the system and set configuration to run the IPS operations effectively. Please refer to 'Instant Payment System Value-Added Services' section for more details.	
FR.34	Change of direct participant for a given indirect participant. *The purpose of the change is to ensure business continuity for the indirect participant in the system in case it decides to change the direct participant.*	Mandatory

Reply	The participant hierarchy can be changed by the NBM operator on demand from participant. This is possible from the operator portal user interface.	
FR.35	IPS is required to enable the NBM to create and delete direct and indirect participants in the system. *Only system participants with zero balance on the IPS account may be deleted from the system.*	Mandatory
Reply	SmartVista Instant Payment System allow participant to be deactivated temporarily or permenantly based on business requirements. The zero balance business rule can be configured before allowing participant to be permenantly disabled in the IPS.	
FR.36	An appropriate software solution (A2A) needs to be provided for the NBM as a system participant.	Mandatory
Reply	SmartVista Instant Payment system offers both message based (A2A) as well as user interface based (U2A) connection to both NBM operator as well as participants. With easy to use user portals all operations can be carried out from the user interface. At the same time a large number of APIs are available for participant to use to integrate in their channels.	
Reply	SmartVista will support this requirement and will operate as per the data retention policy of the NBM.	

7.2. Transfer Order

List of messages in processing of transfer orders:

Message	**Description**	**Message**
Transfer order	Message for initiating the transfer of funds in IPS	pacs.008 (DS-02 SCT Inst)
Rejection of transfer orders	Message IPS sends to the Payer in case of failure to process a transfer order due to validation error, rejection of a transfer order by the Payee, insufficient funds or timeout.	pacs.008 (DS-03 SCT Inst)
Payee's response	Message sent by the Payee to IPS on acceptance/rejection of a transfer order	pacs.002
Error message to the Payee	Message notifying the Payee that the response has not arrived in due time or that the Payee's response failed the validity check	pacs.002

Confirmation of transfer order execution	Message sent by IPS to the Payer and Payee on transfer order execution (positive confirmation)	pacs.002

List of processes related to execution of transfer orders

Process code	Description
IPS.PMNT.01	General conditions
IPS.PMNT.02	Business and technical validation of transfer orders; the transfer order has been rejected and the Payer informed thereof at the occurrence of the first error in the course of validation.
IPS.PMNT.03	Reservation of funds in the Payer's account; if reservation is not possible, the transfer order is rejected and the Payer informed thereof with a rejection message.
IPS.PMNT.04	Forwarding a transfer order to the Payee
IPS.PMNT.05	Waiting for a reply by the Payee until a timeout occurs
IPS.PMNT.06	Technical and business validation of the Payee's response; Payee's response has been rejected and the Payee informed thereof at the occurrence of the first error in the course of validation; the decision whether the transfer order has been accepted or rejected.
IPS.PMNT.07	Un-reservation of funds in case of transfer order rejection
IPS.PMNT.08	Execution. Change of credit and debit account balance and informing Participants

7.2.1. ***General conditions (*IPS.PMNT.01)**		
FR.37	IPS processes transfer orders following the principle "first-in-first-out" without prioritisation or reordering of received orders. *Participants are not able to influence IPS in order to process a specific transfer order by assigning a higher priority to it. However, bearing in mind the payment authorisation process, distributed architecture of the system solution, network responsiveness, which affect the processing of incoming transfer orders, participants cannot rely on those orders being processed in the same order they were sent in.*	Mandatory
Reply	The SmartVista Instant Payment core platform by default offers asynchoronous message processing where the order of the message sent and receive are not determined and all participant in the system may send or receive message in any order and process the accordingly. A message is identified via a message identifier which is generated by the Instant	

	payment system to facilitate the participant for message processing and reconciliation.	
FR.38	IPS will execute a transfer order immediately and will not queue or hold a transfer order for later processing. A transfer order with the execution date and time later than the reception date and time and standing order are an exception to this rule. *IPS does not queue a transfer order, but executes it immediately, transfer order is not held for later execution in case of insufficient funds or for some other reason. A transfer order with the execution date and time later than the reception date and time and standing order described in another customer request and configured at the system level are an exception to this rule.*	Mandatory
Reply	SmartVista Instant Payment system is completely compliant to this requirement. This principle holds true for online real-time messaging. However in case of bulk batch processing via file based mechanism the execution time will come later than the reception time.	
FR.39	IPS will reserve funds from a transfer order in the Payer's IPS account in order to ensure order execution. *Upon receipt of a transfer order from the Payer, IPS reserves funds on the Payer's IPS account and debits or unreserves funds depending on whether the transfer order has been executed or rejected by the Payee or for some other reason (timeout). The procedure is necessary to ensure the execution of transfer orders.*	Mandatory
Reply	SmartVista Instant Payement system offers business process management using Business Process Model and Notation tool that enable defintion of an end to end business and transaction flow without any need for scripting or development. The business process of placing a hold on a payer account before sending it to payee or debiting it in response is a pure configuration job. Hence SmartVista can fully meet this requirement.	
FR.40	The Payer will specify the data source in the field (xx) of the transfer order created based on the data in the CAS. *The transfer order contains fields (flags) that serve to specify the data source for the payer and/or payee from the CAS.*	Mandatory

Reply	SmartVista Instant payment system will support the requirement to carry the required data indicating the usage of CAS in the transfer order. Using the mapping functionality of SmartVista Instant payment system it is just a matter of configuration.	
FR.41	The Payer transfers the required reference data of the received bill in the fields (xx) in the transfer order created based on the data received in the bill – invoice payment process (BP). *The transfer order contains fields (flags) that serve to specify the data source for the payer and/or payee from the CAS.*	Mandatory
Reply	SmartVista Instant Payment system allow any fields to be configured from sender to receiver. Using the mapping functionality available over a user interface it is a matter of configuring the required field to hold the respective data.	
FR.42	By sending a positive response to a transfer order created based on the data received in the bill – invoice payment process (BP) (which contains the required reference data of the received bill in the fields (xx)), the Payee confirms that transfer order elements (the Payee's BBAN, the Payee's BIC, the amount, ...) are in compliance with the BP request. *Confirmation of elements from the bill – invoice in a transfer order.*	Mandatory
Reply	SmartVista Instant Payment System fully complies to this requirement. The invoice data can be sent as part of the request for the payee request to the payer in the ISO 20022 message format.	
	7.2.2. ***Validation (*IPS.PMNT.02)**	
FR.43	IPS will perform business validation of a transfer order sent by the Payer. Transfer order processing will be terminated as soon as the first validation error is encountered and that order will be rejected with an appropriate message. *IPS validates a received transfer order and informs the Payer of any errors that occurred during business validation. More detailed business validations*	Mandatory

	are specified below. In addition to these, technical validations are also carried out.	
Reply	SmartVista by default supports this processing flow. Please refer to section 'Instant Payment Platform Core Services' for details.	
FR.44	IPS validates the authorisation of a Payer to deliver a transfer order based on the sent BIC (field AT-06 in DS-02 SCT Inst). *IPS validates the Payer's transfer order in terms of validation of authorisation to debit the IPS account.*	Mandatory
Reply	SmartVista by default supports this processing flow. Please refer to section 'Instant Payment Platform Core Services' for details.	
FR.45	For each transfer order, IPS will identify the IPS account for debiting and the RTGS account connected to that IPS account. IPS account identification will be derived from the Payer's BIC (field AT-06 in DS-02 SCT Inst) and the currency of the transfer order. *The Payer's BIC from the field AT-06 of dataset DS-02 SCT Inst is uniquely linked to the IPS account connected to exactly one RTGS account.*	Mandatory
Reply	SmartVista fully complies with this requirement. Please refer to 'Instant Payment Platform Core Services' and 'Participant Types and Account Management' section for more details.	
FR.46	For each transfer order, IPS will identify the IPS account that is credited and the RTGS account connected to that IPS account. Account identification will be derived from the Payee's BIC (field AT-23 in DS-02 SCT Inst) and the currency of the transfer order. *The Payee's BIC from the field AT-23 of dataset DS-02 SCT Inst is uniquely linked to the IPS account connected to exactly one RTGS account*.	Mandatory

Reply	SmartVista fully complies with this requirement. Please refer to 'Instant Payment Platform Core Services' and 'Participant Types and Account Management' section for more details.	
FR.47	For each transfer order, IPS checks whether the Payee is a system participant. The Payee's BIC (field AT-23 in DS-02 SCT Inst) will be used for Payee's identification. *IPS will reject every transfer order if it is determined that the Payee is not in the system or cannot be identified based on the transfer order*.	Mandatory
Reply	This is default behavior of SmartVista Instant Payment System. A message originating from a unknown source is rejected.	
FR.48	IPS will validate that the received transfer order was already forwarded, i.e. if it is a duplicate. The validation is conducted based on the Payer's message in the time interval defined at the system level (for example: 30 days). The validation is conducted based on the Payer's BIC (AT-06 in DS-02 SCT Inst) and reference (AT-43 in DS-02 SCT Inst). The time interval relates to the period in which executed transfer orders are kept in the system (for example, 30 days retention period). *The DS-02 dataset of the SCT Inst scheme defines two identification fields, of which the field AT-43 is filled by the Payer, but that identifier does not have to be unique at the system level because different Payers may use the same identifier. For that reason the uniqueness validation of the transfer order uses the combination of the BIC and message reference.* *Rules of unique identification will be described in operational rules. It is assumed that a special field within ISO20022 (dedicated to unique transaction/message identification) will be used for this purpose. The best approach is to have lifetime unique identification of each transaction with incremental increase of this ID for each new transaction.*	Mandatory
Reply	SmartVista support detection of duplicate transactions. The duplication criteria is set by using a composite key in the database and comparing it with the incoming message. For example using BIC, Transaction reference number, and data/time a transaction uniqueness can be ensured and duplication can be captured.	

FR.49	IPS will not debit the blocked IPS account. *IPS will reject the transfer order if the IPS account that should be debited is blocked for debiting.*	Mandatory
Reply	This feature is supported by default.	
FR.50	IPS will not reduce the balance in the blocked IPS account. *IPS will not reduce the balance in the IPS account blocked for debiting. The transfer order will be rejected.*	Mandatory
Reply	This feature is supported by default.	
FR.51	IPS will not debit the IPS account if its RTGS account is blocked for debiting. *IPS will reject the transfer order if the RTGS account, connected to the IPS account that should be debited, is blocked for debiting.*	Mandatory
Reply	This feature is supported by default.	
FR.52	IPS will not credit the IPS account blocked for crediting. *IPS will reject the transfer order if the IPS account that should be credited is blocked for crediting.*	Mandatory
Reply	This feature is supported by default.	
FR.53	IPS will not increase the balance in the IPS account blocked for crediting. *IPS will not increase the balance in the IPS account blocked for crediting. The transfer order will be rejected.*	Mandatory
Reply	This feature is supported by default.	
FR.54	IPS will not credit the IPS account if its RTGS account is blocked for crediting.	Mandatory

	IPS will reject the transfer order if the RTGS account, connected to the IPS account that should be credited, is blocked for crediting.	
Reply	This feature is supported by default.	
FR.55	IPS validates that the timestamp (field AT-50 in DS-02 SCT Inst) is later than the configuration parameter or earlier than another configuration parameter. *IPS has a time configurable window for which it accepts transfer orders in relation to the stated timestamp (AT-50 in DS-02 SCT Inst). For example, not earlier than 0.1 second and no later than 20 seconds, excluding transfer orders with a future date and standing orders (it is in SCT Inst timestamp).* *All timestamps use the IPS system time as the reference time*.	Mandatory
Reply	SmartVista supports this requirement. It can setup a timestamp window with a tolerance criteria beyong which the transaction may be declined if received from sender.	
FR.56	IPS validates that the transfer order currency corresponds to the currency of the debit and credit accounts. *IPS executes the transfer order provided that the debit and credit accounts are in the same currency as the transfer order.*	Mandatory
Reply	SmartVista Instant Payment System support this requirement by default.	
FR.57	IPS will validate dates of opening and closing of IPS debit and credit accounts from the transfer order in relation to the operating day of the system. It is validated that the operating day is later than the opening date and/or earlier than the closing date. *IPS rejects the transfer order if at least one of the accounts does not fulfil the stated requirement. For the purpose of business validation of a transfer order, IPS account is opened on the opening date and closed in the moment it is blocked due to licence revocation, which can happen before the actual closing date due to procedures prescribed by regulations.*	Mandatory

Reply	SmartVista will comply to this requirement to check the opening and closing day of the account when validating the transfer order to process further	
FR.58	IPS will validate dates of opening and closing of RTGS accounts based on data from the transfer order in relation to the system operating day. It is validated that the operating day is later than the opening date and/or earlier than the closing date. *IPS rejects the transfer order if at least one of the RTGS accounts does not fulfil the stated requirement. An RTGS account is opened on the opening date and closed before the closing date, i.e. in the moment it is blocked due to licence revocation.*	Mandatory
Reply	SmartVista will comply to this requirement to check the opening and closing day of the account when validating the transfer order to process further	
FR.59	IPS will validate that the amount from a transfer order is not greater than the configured amount for the currency of the transfer order. *The NBM Decision defines the maximum amount that can be executed in the payment system that is not systemically important. IPS needs to have the possibility to set that parameter at the system level. Besides, IPS could have such configuration that will allow the system participant to define its requests that are not larger than the ones in the system regarding the amount in the transfer order.*	Mandatory
Reply	SmartVista can configure a transfer order limit at a participant level or it can be set at IPS and RTGS account level. Limit hierarchy can be established if required by the bank. Hence it is just a matter of configuration.	
FR.60	IPS will validate that the transfer order has IBAN of the payer and payee – end customers. *Account numbers of the payers and payees – end customers are compulsory fields in the dataset* DS-02 SCT Inst *in the transfer order. IPS will only validate their presence, but not their content..*	Mandatory

Reply	SmartVista will fully comply with the requirement to validate end customer IBAN account in terms of its presence. It will be treated as a mandatory field in the Transfer Order.	
FR.61	IPS will notify the Payer in case the transfer order has an error by sending an order rejection message. *IPS will send the Payer information on the error which occurred during the transfer order validation. The error notification should be localised in terms of language.*	Mandatory
Reply	SmartVista Instant Payment system fully complies with this requirement. Please refer to the 'Instant Payment Platform core Service section in the Technical Proposal for details.	
	7.2.3. ***Reservation of funds (*IPS.PMNT.03)**	
FR.62	IPS will reserve funds in the Payer's IPS account after the validation of the transfer order. Reserved funds are not available for execution or reservation under other orders, return of funds or withdrawal of liquidity from the connected RTGS account. *IPS reserves funds after it has validated the transfer order so as to provide the execution of such order after it receives the Payee's message on accepting the transfer order (the transfer cannot be rejected due to insufficient funds). If the Payee rejects the transfer order, IPS will cancel the reservation and reject the transfer order. Funds are also reserved in the connected RTGS account.*	Mandatory
Reply	SmartVista Instant Payment System supports this requirement. The reservation of the funds can be configured as part of setting up the business process of the Transfer order instruction. Once funds are reserved they wont be accessible unless the payee confirm with the pacs.002 status message that the message has been sucessfully processed. Setting up the fund reservation is possible via BPMN configuration in SmartVista with no coding or scripting.	
FR.63	IPS will reserve funds in a Payer's IPS account and reduce the available funds (balance) in that account. Reserved funds are not available for	Mandatory

	execution or reservation under other orders, return of the funds or withdrawal of liquidity from the connected RTGS account. *IPS reserves funds after a successful validation of the transfer order so as to provide the execution of such order after it receives the Payee's confirmation message (the transfer cannot be rejected due to insufficient funds). That lowers the balance in IPS account, as well as the RTGS account balance in IPS. If the Payee rejects the transfer order, IPS will cancel the reservation and reject the transfer order.*	
Reply	SmartVista will fully comply with this requirement. Setting up of the instruction to reserve the funds of the Payer participant and then lowering the balance while receiving the payment confirmation from payee is all configurable from SmartVista Instant payment system BPMN tool.	
FR.64	IPS will reject the transfer order in case: • available funds in the Payer's IPS account are less than the amount from the transfer order • RTGS account balance in IPS that is connected to the Payer's IPS account is less than the amount from the transfer order. *No transfer orders will be executed if there are no available funds in IPS for the amount in that order. The transfer order can reduce available funds in IPS account to zero.*	Mandatory
Reply	SmartVista supports this requirement by default. Please refer to section 'Participant Type and Account Management' for more details.	
FR.65	IPS will notify the Payer in a message about rejecting the transfer order using a special error code, when it cannot reserve funds in the Payer's IPS account or if there are no available funds in the balance of the connected RTGS account in IPS. *Rejection message should be localised in terms of language*.	Mandatory
Reply	Supported by default.	

	7.2.4. ***Transfer order forwarding (*IPS.PMNT.04)**	
FR.66	IPS will forward a transfer order to the Payee if it was successfully validated and reserved.	Mandatory
Reply	Supported by default.	
	7.2.5. ***Payee's response (*IPS.PMNT.05)**	
FR.67	The processing of a transfer order will continue after receiving a positive or negative response from the Payee or after the time foreseen for such response has expired, which is defined by the operating rules (it is configurable). *The transfer order is in standby mode in IPS until it receives a positive response (accepted order) or a negative one (rejected order) by the Payee or until the time has expired (timeout), which is defined by the operating rules for that response. The Payee sends its response in an appropriate message.*	Mandatory
Reply	This flow is supported by default. Please refer to section 'Instant Payment Platform Core Services' for more details.	
FR.68	IPS will reject a transfer order in case the configured time has expired and the Payee's response was not received. Reference time for calculating timeout is the time set in the transfer order (field AT-50 in DS-02 SCT Inst). *When the time foreseen for the Payee's response has expired, IPS rejects the transfer order. Waiting time is configured on IPS level and forms part of the IPS operating rules. In the SCT Inst scheme, the maximum waiting time is 20 seconds from timestamp from the transfer order.* *The operating rules will clearly stipulate when an end-customer account can be credited by the Beneficiary institution taking into account the legal framework.*	Mandatory
Reply	This flow is supported by default. Please refer to section 'Instant Payment Platform Core Services' for more details.	
FR.69	For some Participants, IPS will credit the Payee's IPS account without waiting for the Payee's response. IPS allows the Operator to configure such	Mandatory

	a Participant in accordance with the operating rules and based on the functionalities described in section 7.9 “Participant unreachable function and pre-autorisation facility”.	
Reply	SmartVista supports stand-in authorization where the system authorizes the transaction on behalf of the payee in several cases. Some of the cases are no availability of payee due to maintenance shutdown, bad network connection between IPS and payee participant, or especial condition of the payee where it has establish an agreement to allow stand-in.	
FR.70	IPS will notify the Payee in an appropriate message in case of response timeout. *Message sent is in the defined format.*	Mandatory
Reply	This flow is supported by default. Please refer to section 'Instant Payment Platform Core Services' for more details.	
FR.71	IPS will notify the Payer in the message on rejecting a transfer order in case of Payee response timeout. *Message sent is in the defined format.*	Mandatory
Reply	This flow is supported by default. Please refer to section 'Instant Payment Platform Core Services' for more details.	

7.2.6. ***Validation of the Payee’s response (*IPS.PMNT.06)**

The Payee’s response is defined by the process of executing the transfer order. The Payee can accept or reject the transfer order

FR.72	IPS will perform business validation of the Payee’s response. When the first error is detected, further processing of the Payee’s response will stop and the response will be rejected in an appropriate message. *IPS validates the Payee’s response and notifies it in case there is an error in business validation. More detailed business validations are specified below. In addition to these, technical validations are also carried out.*	Mandatory

Reply	SmartVista by default supports this flow in terms of validating the payee response to a transfer order request. Please refer to section 'Instant Payment Platform Core Services' for more details.	
FR.73	IPS will validate that the Payee that sent the response is the Payee to which the transfer order was forwarded. *The Payee of the transfer order can be the only sender of the response. Validation is performed according to the BIC of the Payee from the original transfer order.*	Mandatory
Reply	This is default behavior of SmartVista. Every message whether request or response is validated against the source from where it originated from to see if it is the legitimate source allowed to operate on IPS platform.	
FR.74	IPS will pair the response message with pending transfer order using the Payee's BIC (field AT-06 in DS-02 SCT Inst) of the forwarded transfer order and reference of that order (field AT-43 in DS-02 SCT Inst). If it cannot pair the mentioned data with the response, validation is cancelled. *IPS processes the Payee's responses only for transfer orders that are forwarded to that Payee and are pending, i.e. for those transfer orders that did not get final status yet (executed or rejected). Since there are multiple participants in IPS, the Payee's BIC is also used besides the transfer order reference in order to ensure uniqueness of identification of that transfer order.*	Mandatory
Reply	This is default behavior of SmartVista. The response message is validated by BIC and Transaction Identifier generated by the IPS in the request message.	
FR.75	IPS will notify the Payee that sent the response about an existing error in an error message. The message will include the error code and localised error description in terms of language. *Besides notifying the Payee, IPS will notify the Payer that sent the transfer order that the order is rejected in a message about transfer order rejection. This message will be sent after reserved funds are released. The message is localised in terms of language*.	Mandatory

Reply	This is default behavior and transaction flow of the transfer order in SmartVista. Please refer to section 'Instant Payment Platform Core Services' for more details.	
FR.76	After validating the response, IPS will execute the transfer order or reject it depending on the response. *In case the Payee rejected the transfer order, reservation in the Payer's IPS account will be released.*	Mandatory
Reply	This flow is supported by default. Please refer to section 'Instant Payment Platform Core Services' for more details.	
	7.2.7. ***Release of funds (*IPS.PMNT.07)**	
FR.77	IPS will release funds in the Payer's IPS account when it rejects the order that initiated that reservation. IPS will reduce the amount of reserved funds by the transfer order amount for which the reservation was made. The available amount in the IPS account will be increased by the same amount. *During transfer order execution, funds are reserved in the Payer's IPS account as a guarantee that the order will be executed provided that the Payee's response passes the validation and the Payee accepts the transfer order in its response. In case there is no execution (Payee's response does not pass the validation, timeout expires or the Payee's response is negative), the reserved funds should be released for other orders or for liquidity transfer.*	Mandatory
Reply	This is default behavior of SmartVista transfer order funds reservation and release mechanism. The flow is configurable and can be modified as per the scheme rules of the IPS.	
FR.78	In releasing reserved funds in IPS account, IPS will also release funds in the connected RTGS account and increase the RTGS account balance in IPS by the transfer order amount for which the reservation was made *During transfer order execution, reserved funds reduce the RTGS account balance in IPS which guarantees that the order will be executed provided that the Payee's response passes the validation and the Payee accepts the transfer order in its response. In case there is no execution (Payee's response does not pass the validation, timeout expires or the Payee's*	Mandatory

	response is negative), the reserved funds should be released for other orders or for liquidity transfer.	
Reply	This is default behavior of SmartVista transfer order funds reservation and release mechanism. The flow is configurable and can be modified as per the scheme rules of the IPS.	
FR.79	IPS will notify the Payer that sent the transfer order on releasing reserved funds in its IPS account, in a message on rejecting the transfer order. The rejection message should consist of the code that explains the reason for rejecting, or forward the code that the Payee forwarded in its response. *Unsuccessful validation, time expired for the Payee's response or negative response of the Payee (for example, there is no such account of the end customer) can initiate the process of releasing reserved funds in IPS. In case the Payee rejects the order, IPS will forward the code from the negative response.*	
Reply	This is default behavior of SmartVista Instant payment system and is fully supported.	
	***7.2.8. Execution – settlement* (IPS.PMNT.08)**	
FR.80	IPS executes transfer orders individually, without netting, in gross amount. *IPS does not net amounts from the order considering the instant nature of the system.*	Mandatory
Reply	SmartVista Instant Payment system support both gross and net settlement. As per the requirement SmartVista can be configured to to execute transfer order individually in a gross settlement manner.	
FR.81	IPS will execute the transfer order through IPS account. *Execution is done by debiting and crediting appropriate IPS accounts.*	Mandatory
Reply	This is default behavior of SmartVista. Please refer to section 'Participant Type and Account Management' for more details.	

FR.82	Executing a transfer order in IPS is done after successful validation of the Payee's positive response. *The time of execution is written at the moment of execution on the date on which the transfer order was executed in IPS. The time of execution is according to the calendar date.*	Mandatory
Reply	This is default behavior of SmartVista. Please refer to section 'Participant Type and Account Management' for more details.	
FR.83	IPS executes the transfer order in the full amount that was stated in that order. *If it is not possible to execute the transfer order in its full amount, it is rejected, orders are not executed partially*.	Mandatory
Reply	This is default behavior of SmartVista Instant Payment System.	
FR.84	IPS uses reserved funds for the transfer order in IPS account that is debited. *IPS will execute the transfer order using reserved funds in IPS account that is debited for that transfer order and instantly approves those funds in IPS account that is credited (end customer – the payee can use these funds immediately after the Payee's approval).*	Mandatory
Reply	This is default behavior of SmartVista. Please refer to section 'Participant Type and Account Management' for more details.	
FR.85	IPS, by debiting/crediting the Payer's/Payee's IPS account reduces/increases the balance in their IPS accounts.	Mandatory
Reply	This is default behavior of SmartVista. Please refer to section 'Participant Type and Account Management' for more details.	
FR.86	IPS, by debiting/crediting the Payer's/Payee's IPS account reduces/increases the balance in RTGS accounts in IPS connected to those IPS accounts.	Mandatory

Reply	This is default behavior of SmartVista. Please refer to section 'Participant Type and Account Management' for more details.	
FR.87	IPS executes only transfer orders based on credit transfer. A transfer order can have a future date, but it can also be a standing order. *IPS accepts only transfer orders that debit the Payer's IPS accounts. Any functionality that requires funds withdrawal is not a project subject in this phase (for example, transactions initiated by the Payee – direct debit).*	Recommended
Reply	BPC fully understand and completely support this requirment.	
FR.88	IPS will notify the Payer and the Payee on a successfully executed transfer order by confirming the execution of that order. *The message is localized in terms of language.*	Mandatory
Reply	SmartVista will fully support this requirement to notify all the participants involved in the transfer order instruction settlement. Localization as per country language will be supported.	
FR.89	IPS will also notify the direct participant whose RTGS account is connected to the Payer's / Payee's IPS account (indirect participants) on successfully executed transfer order by forwarding copies of the original transfer order.	Mandatory
Reply	SmartVista will fully support this requirement to notify all the participants involved in the transfer order instruction settlement. Localization as per country language will be supported.	

7.3. Recalls

List of messages for processing recalls

Message	**Description**
Recall	Message sent by the Payer requesting a return of funds that were previously settled by the transfer order.
Recall rejection	Notification informing the Payer about an error in the recall message.

Recall response	Response to the recall (accepting or rejecting).
Rejection of a recall response	The message that notifies the response sender (Payee) that the recall response has an error or that it does not have enough funds (it is used only in cases when the payee sends pacs.004 – positive response).
Recall response confirmation	Message that notifies the Payee and the Payer that the recall has been settled successfully.

List of processes for processing recalls

Process code	**Description**
IPS.RECALL.01	Technical and business validation of the recall message
IPS.RECALL.02	Recall forwarding to the Payee
IPS.RECALL.03	Technical and business validation of the recall response message and notification of the Payer in case the recall response is negative.
IPS.RECALL.04	Processing a positive recall response and executing the return of funds.

	7.3.1. ***Validation of recalls (*IPS.RECALL.01)**	
FR.90	IPS will perform the business validation of recalls sent by the Payer. Validation will be cancelled and the recall rejected if IPS finds the first error. *In case the recall is rejected, the sender (Payer) will receive an appropriate message. In addition to these, technical validations are also carried out.*	Mandatory
Reply	SmartVista fully complies and support this requirement.	
FR.91	IPS will validate the authorisation of the Payer to send the recall based on the BIC stated in the message (SCT Inst DS-02 field AT-06) of the transfer order that is part of the recall message (DS-05 SCT Inst). *The sender authorised to send recalls is at the same time the party which sent the original transfer order (Payer). IPS validates data from the original transfer order which is integral to the recall message. IPS validates the authorisation to send responses using reference data in the system*.	Mandatory
Reply	SmartVista fully complies and support this requirement.	
FR.92	IPS will validate that the Recipient of the recall is available. The Recipient of the recall is the Payee from the original transfer order determined based on	Mandatory

	its BIC (dataset DS-02 SCT Inst field AT-23) as a part of the recall message (DS-05 SCT Inst). *IPS uses data from the copy of the original transfer order which is a part of the recall message in order to determine if IPS can reach the Recipient of the recall. IPS does not further validate data from the transfer order which form part of the recall message. For validation, IPS uses reference data in the system*.	
Reply	SmartVista fully complies and support this requirement. The R-Message types are fully supported.	
FR.93	IPS will check if the received transfer order has already been forwarded, that is, whether it is a duplicate. The check is performed based on the return of funds on a recall in the time interval defined at the system level (for example: 30 days). The check is performed based on the BIC of the Payee from the copy of the transfer order which was a part of the response to the executed recall and reference of the recall of the Payer from that response. The time interval relates to the period in which executed transfer orders are kept in the system (for example, 30 days). *Reference of the Payer does not have to be unique at the system level, so the Payee's BIC and the Payer's reference are used for uniqueness validation*.	Mandatory
Reply	SmartVista fully complies and support this requirement.	
FR.94	IPS will reject the recall in case there is an error during validation and will notify the sender (Payer) of the recall in a recall rejection message. *In case that the recall contains an error, the party that sent the recall is notified (Payer).*	Mandatory
Reply	SmartVista fully complies and support this requirement.	
	7.3.2. Forwarding of recalls (IPS.RECALL.02)	
FR.95	IPS will forward a valid recall to the Payee based on the Payee's BIC (field AT-23 in DS-02 SCT Inst) in the recall (dataset DS-05 SCT Inst).	Mandatory

	After the stated validations, IPS does not perform further processing, but only forwards the recall to the Payee.	
Reply	SmartVista fully complies and support this requirement.	
	7.3.3. ***Validation of recall responses (*IPS.RECALL.03)**	
FR.96	IPS will perform the business validation of the recall response sent by the Payee. When the first error is detected, further processing of the recall response will stop and it will be rejected with an appropriate message. *In case the recall response is rejected, the sender (Payee) will get an appropriate message. In addition to these, technical validations are also carried out*.	Mandatory
Reply	SmartVista fully complies and support this requirement.	
FR.97	IPS will validate the sender's (Payee's) authorization to send the recall response. *The party authorized to send recall response is at the same time the party to which IPS has forwarded the recall. IPS uses data from the copy of the original transfer order which forms part of the recall response (if the Sender of the recall response is authorized to send the response). IPS validates the authorization to send responses using reference data in the system.*	Mandatory
Reply	SmartVista fully complies and support this requirement.	
FR.98	IPS will validate that the Payer from the recall response is available. *IPS uses data from the copy of the original transfer order which forms part of the recall response (if the Payer that receives the recall response is available). For validation, IPS uses reference data in the system.*	Mandatory
Reply	SmartVista fully complies and support this requirement.	

FR.99	IPS will validate that the recall response contains data on accepting or rejecting, in accordance with possible codes which are defined for recall responses (dataset DS-06 SCT Inst). *IPS processes accepting of recalls (the following requests in this part). If the recall response is negative (recall rejected), IPS forwards it to the Payer.*	Mandatory
Reply	SmartVista fully complies and support this requirement.	
FR.100	In case the recall response is positive (recall is accepted), IPS will confirm that the response contains the Payer's BIC and the Payee's BIC within the transfer order (dataset DS-02 SCT Inst), which forms part of the message on accepting recall (dataset DS-06 SCT Inst). *Copy of the transfer order (DS-02 SCT Inst) will be a part of the accepted recall (dataset DS-06 SCT Inst).*	Mandatory
Reply	SmartVista fully complies and support this requirement.	
FR.101	In case the recall response is positive, IPS will identify IPS accounts which it will use for executing the recall, based on the Payer's BIC and the Payee's BIC. IPS will also consider the account currency. The Payer's BIC and the Payee's BIC will exchange their roles in order to make a reversed cash flow. *Within the recall response message, there is a copy of the transfer order which contains the Payer's and the Payee's BICs (dataset DS-02 SCT Inst, which forms part of DS-06 SCT Inst). In order to return the funds, it is necessary to exchange the roles of stated participants.*	Mandatory
Reply	SmartVista fully complies and support this requirement. SmartVista also provides a Dispute Portal which is a centralized system that offers the recall and return management via a user interface which can be made accessible to all the participant to manage the complete dispute lifecycle of a transaction. NBM IPS scheme can establish dispute management via the exchange of R-Type messages between participants. Alternatively NBM has an option to rollout dispute portal as a service to the participant as well.	
FR.102	If the recall response is positive, IPS will check whether the credit account is blocked (the IPS account and connected RTGS account).	Mandatory

	The account identified by IPS based on the BIC contained in the copy of the transfer order in a positive recall response may be blocked for crediting in the period between the processing of the original transfer order and processing of the response to the transfer order. *No recall for blocked accounts.*	
Reply	SmartVista would validate the account status when a recall request is initiated by the sender and will reject if in case the account is not ready to process the refund. Also when recall response is received from particpant SmartVista would again check the IPS account status and if it would be ready to receive credit then it would proceed with the recall response. Otherwise the message would be rejected and participant would be informed.	
FR.103	If the recall response is positive, IPS will check whether the debit account is blocked (the IPS account and connected RTGS account). *The account identified by IPS based on the BIC contained in the copy of the transfer order in the positive response to the recall may be blocked for debiting in the period between the processing of the original transfer order and processing of the positive response to the transfer order.* *No recall for blocked accounts.*	Mandatory
Reply	SmartVista would validate the account status when a recall request is initiated by the sender and will reject if in case the account is not ready to process the refund. Also when recall response is received from particpant SmartVista would again check the IPS account status and if it would be ready to receive debit then it would proceed with the recall response. Otherwise the message would be rejected and participant would be informed.	
FR.104	IPS will validate that the amount in the positive response to the recall does not exceed the amount configured for the currency of the transfer order, nor the amount of the original transfer order. *This request is identical to the request relating to the transfer order FR.60 in the retention period (e.g. 30 days).*	Mandatory

Reply	SmartVista will fully comply with the business rules as stated in this requirement.	
FR.105	IPS will validate the dates of opening and closing of the accounts being debited and credited (the IPS account and connected RTGS account) in case of a positive recall response relative to the operating day of the system. It is validated that the operating day is later than the opening date and/or earlier than the closing date. *This request is identical to the requests relating to the transfer order FR.58 and FR.59*	Mandatory
Reply	SmartVista will fully comply to this requirement.	
FR.106	The IPS will reject the recall response in case there is an error during validation and will notify the sender (Payee) by a recall response rejection message. *This message also contains the reason for rejection and is localized in terms of language.*	Mandatory
Reply	SmartVista will fully comply to this requirement.	
FR.107	IPS will send to the Payer the Payee's negative response to the recall that has been successfully validated. *IPS only notifies the Payer in case of a negative recall response. (The positive recall response is processed further).*	Mandatory
Reply	SmartVista will fully comply to this requirement.	
	7.3.4. Processing a positive recall response (IPS.RECALL.04)	
FR.108	IPS will use a positive recall response (accepted) to establish the appropriate elements for the transfer of funds from the Payee to the Payer. *In case of a positive recall response which has been fully validated, IPS automatically transfers the funds from the Payee to the Payer (in the amount stated in the positive response, without getting into the legal*	Mandatory

	relationship between the Payer and the Payee, but not higher than the systemically configured amount for a transfer order).	
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.109	When transferring funds from the Payee to the Payer, IPS will use the recalled amount taken from the positive recall response (field AT-46 of dataset DS-06 SCT Inst). *The recalled amount is found in the mandatory field of the recall response (AT-46 dataset DS-06 SCT Inst). That amount cannot exceed the systemically configured amount for a transfer order).*	Mandatory
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.110	Requests already stated in the section for execution of transfer orders apply accordingly to transfer orders automatically generated by IPS during processing of a positive recall response, except in cases described below. *The recalled amount may differ from the amount in the original transfer order*.	Mandatory
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.111	IPS will reduce/increase the balance in the corresponding accounts (IPS and RTGS accounts) in relation to the recall.	Mandatory
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.112	The IPS will reject positive recall responses due to insufficient funds in the following cases: • the available funds in the Payee's IPS account are lower than the amount of recall	Mandatory

	• the balance in the RTGS account in IPS that is connected to the Payee's IPS account is lower than the amount of recall *A positive recall response may reduce the available funds in accounts to zero.*	
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.113	IPS will notify the Payee and Payer that the recall has been successfully executed by sending a confirmation of execution of that recall.	Mandatory
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.114	IPS will notify the Payee (sender of the recall response) by sending a rejection message in case the execution did not occur (insufficient funds). *This message contains the reason for rejection.*	Mandatory
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.115	The IPS will notify the Direct Participant whose RTGS account is connected to the Payer's/Payee's IPS account (indirect participants) of the successful execution of recall by forwarding a copy of the Payee's positive response to the recall request.	Mandatory
Reply	This is default behavior of SmartVista dispute management and is fully supported.	
FR.116	IPS enables the configuration of the parameter concerning the number of days (e.g. 10) until which recalls may be sent for transfer orders whose date is later than the system date reduced by the configured number of days.	Mandatory

Reply	The time duration to allow recall to be sent is configurable in SmartVista and will be governed by the IPS scheme rules.	

7.4. Transaction status validation (Investigation)

IPS enables the validation of the status of a transaction, which can be initiated by the Payer (the process is also a part of the SCT Inst scheme). Transaction status is the status of the execution of a transfer order.

List of messages for processing transaction status queries

Message	**Description**	**Message**
Query about the status of a transaction (transfer order)	Message sent by the Payer requesting information about the current status of a sent transaction (transfer order).	pacs.028
Rejection of a transaction status query	Message notifying (informing) the Payer about an error in the transaction status query.	pacs.002
Response to a transaction status query	Message notifying the Payer about the status of a transaction containing the current status of that transaction.	pacs.002

List of processes for processing recalls

Process code	**Description**
IPS.IV.01	Technical and business validation of a transaction status query.
IPS.IV.02	Response sent to the Payer.

7.4.1. Validation of a transaction status query

FR.117	The IPS should ensure that the Payer has the ability to validate the status of a previously sent transaction. Status validation will stop and query will be rejected on the occurrence of the first error in the query. *Message informing the Payer about unsuccessful query validation. In addition to these, technical validation is also carried out.*	Mandatory
Reply	SmartVista Instant payement system support Payment Status Request pacs.028 message where it can be initated by both the sender and receiver	

	of the message under certain conditions. Please refer to Section 'Instant payment Core Platform Services' for more details.	
FR.118	The IPS will search for the transaction whose status is queried based on the data in the status enquiry message. If no matching transaction can be found, the status query is considered invalid. *Transaction status query message contains the Payer's reference (field AT-43 of dataset DS-02 SCT Inst) and the timestamp of the transaction, which is used to find the transaction whose status is queried.*	Mandatory
Reply	SmartVista supports this requirement by default.	
FR.119	IPS will ensure the availability of transactions (transfer orders) for status query for a configurable timeframe, which depends on the period for retention of transfer orders in the system. *IPS will provide data for the transaction status query for the period configured by the number of calendar days (e.g. 30), which is directly linked to the period for retention of transfer orders in the system, after which these data become unavailable. The above period may be changed in the operating rules, should the need arise.*	Mandatory
Reply	Based on the operating scheme rules of the IPS, SmartVista can support the retention period of the transfer order and the consequent transaction inquiry for getting the status of the original transaction.	
FR.120	IPS will validate that the sender (Payer) is authorised to send that query based on the BIC from the transfer order whose status is requested. If this is not the case, the query will be rejected. *Only the Payer is authorised to send a transaction status query.*	Mandatory
Reply	SmartVista will allow only those payer to initiate transaction inquiry which initiated the original transfer order.	
FR.121	IPS will notify the sender in case of an error occurring during the validation of the transaction status by sending a transaction status query rejection message.	Mandatory

Reply	The Payment status report pacs.002 would be send to inform the sender of the status of transaction inquiry pacs.028 message.	
	7.4.2. Processing of transaction status query messages (IPS.IV.02)	
FR.122	IPS will respond to a status query by sending a transaction status message. This message will be a copy of the rejection message or a copy of the message on transfer order execution; these messages are sent to the Payer during the execution of a transfer order whose status is queried.	Mandatory
Reply	SmartVista supports this requirement by default.	

7.5. Central alias service (IPS.CAS)

The central alias service (CAS) allows the Payer to obtain information required for creating a transfer order (the account number only, or other data required for identifying end customers of a payment service – customers) by using attributes such as the Biller's ID, card number, mobile phone number, TIN, e-mail, etc.

For information necessary to identify end customers of payment services, the Payer submits a request for customer details in IPS using alias data. IPS will answer to the request by sending the mandatory data necessary for creating a transfer order. Participants in the system submit data on the customers with prior consent of end customers.

List of messages in CAS operation

Message	**Description**
Request for customer details (using alias data)	Message by which the Payer requests the data necessary to execute a transfer order (e.g. payer's/payee's account number).
Message on an error in the request	Message sent by IPS when it encounters a technical/business invalidity in a request for customer details
Customer details (response to the request)	Message sent by IPS with customer details necessary to execute a transfer order
Request for recall of customer details	Message recalling an entry in the CAS. With this message, the customer is deleted from the database and its details can no longer be obtained.

Request for entry of customer details	Message sent by a Participant in the system on behalf of its client, which assigns an alias and its content (key), which can be used to obtain details on that client necessary to create a transfer order. The alias is a symbolic sign of an attribute (for example: mobile phone number, tax identification number, email...). The same message is used to update data for existing CAS entries

List of processes

Process code	Description
IPS.CAS.01	Business and technical validation of a request for customer details
IPS.CAS.02	Sending of customer details (response to the request) or notification that the customer was not found
IPS.CAS.03	Processing of a Participant's request for entry of customer details
IPS.CAS.04	Processing of a recall of customer details
IPS.CAS.05	Sending of a request for entry of customer details using batch files and their processing

	7.5.1. ***Technical and business validation of a request for customer details (IPS.CAS.01)***	
FR.123	IPS will carry out business validation of a request for customer details sent by the Payer. On the occurrence of the first error, processing of a request for customer details will stop and the request will be rejected using the appropriate message. *IPS validates the received request for customer details and notifies the Payer in case of an error in business validation. More detailed business validations are specified below. In addition to these validations, technical validations are also carried out.*	Mandatory
Reply	SmartVista fully complies to this requirement. Please refer to section 'Instant Payment Platform Core Services' for more details.	
FR.124	IPS will validate that the request for customer details contains the alias configured in the IPS system, based on which customer details are requested. *IPS checks whether the alias in the field (??) of the message (??) is an alias configured in IPS. For example, the system can be configured so that an alias is: mobile phone number, tax identification number, email, etc. If the alias from the request for customer details is not configured, IPS will reject the request by sending an error message.*	Mandatory

Reply	SmartVista fully complies to this requirement. Please refer to section 'Instant Payment Platform Core Services' for more details. Addressing services details and features are explained in Section 'Addressing Service'	
FR.125	For every request for customer details, IPS will validate customer existence in the CAS based on the alias and the content of the alias. *Based on the alias and the content of the alias (for example, the alias is the mobile phone number, and the content is 555-100), IPS will send a query to the CAS to validate that there is an entry corresponding to those attributes. If the appropriate entry is not found, the request is rejected by sending an error message.*	Mandatory
Reply	This is default behavior of SmartVista Addressing Service which works in tandem with the SmartVista transaction core system. This requirement is fully supported.	
FR.126	IPS will inform the Payer if an error has been detected during the processing of a request for customer details. *IPS will send to the Payer the notification of the error that occurred during the processing of a request for customer details. The error notification should be localised in terms of language.*	Mandatory
Reply	This is default behavior of SmartVista Addressing service. The notification error will be configured as per local language requirement.	
	7.5.2. ***Sending of customer details (IPS.CAS.02)***	
FR.127	IPS will, at the request for customer details based on an alias and the content of the alias, deliver the elements necessary for creating a transfer order (BBAN, etc.). *IPS will send customer details to the Payer based on the alias and the content of the alias sent in the request. The message will contain the original identifier of the Payer's request for customer details (BIC and message – request reference).*	Mandatory

Reply	SmartVista Addressing service complies with this requirement. This is default behavior of the service.	
	7.5.3. ***Processing of a Participant's request for entry of customer details (IPS.CAS.03)***	
FR.128	IPS will carry out business validation of a request for entry of customer details sent by the Participant. On the occurrence of the first error, processing of the request will stop and the request will be rejected. The Participant is obliged to submit all mandatory fields in line with the message format. *IPS validates the received request for entry of customer details and notifies the sender (Participant) in case of an error occurrence during business validation. Validations carried out are specified in more detail below. In addition to these validations, technical validations are also carried out.* *Additional validations will be established based on the customer's requests during the project.*	Mandatory
Reply	SmartVista Instant Paymetn System offers business process and transation setup and flow definition via BPMN tool which is available through the user interface that enables bank operator to create new business rules and processing flow without any need to code or write a script. With the help of the BPMN tool the bank itself can create the processing flow and the business logic required as per the scheme and operator rules. BPC will fully comply with this requirement and will configure the business validation of customer entry in the Central Alias Scheme as listed.	
FR.129	IPS will validate that the request for entry contains the alias configured in the IPS system, based on which entry of customer details is requested. *IPS checks whether the alias in the field (??) of the message (??) is an alias configured in IPS. For example, the system can be configured so that an alias is: mobile phone number, tax identification number, email, etc. If the alias from the request for entry of customer details is not configured, IPS will reject the request by sending an error message.*	Mandatory
Reply	SmartVista Addressing service fully complies with this requirement.	

FR.130	For each request for entry of customer details, IPS will validate that the details concerning the customer's account are in line with the Sender's authorisation. The Sender may only send a request for entry pertaining to the customers that are its clients. *IPS determines the structure of customer accounts it maintains and validates that it corresponds to the elements of the message (account), based on the Sender's BIC. If there is no correspondence, an error message is sent.*	Mandatory
Reply	SmartVista Addressing service fully complies with this requirement.	
FR.131	IPS will notify the Sender (Participant) in case of an error in the processing of a request for entry of customer details, or that the entry was successfully entered in the CAS. *IPS will send to the Sender (Participant) the notification of the error that occurred during the processing of a request for entry of customer details. The error notification should be localised in terms of language.* *If the entry is successful, IPS notifies the Participant thereof.*	Mandatory
Reply	SmartVista Addressing service fully complies with this requirement.	
	7.5.4. ***Processing of a recall of customer details (IPS.CAS.04)***	
FR.132	IPS validates the received request for recall of customer details and notifies the Sender (Participant) in case of an error during business validation. *IPS validates the received request for recall of customer details and notifies the Sender (Participant) in case of an error during business validation. Validations carried out are specified in more detail below. In addition to these validations, technical validations are also carried out.*	Mandatory
Reply	SmartVista Addressing service fully complies with this requirement.	
FR.133	For each request for recall of customer details, IPS will check whether the details concerning the customer were entered by that Sender. The Sender may recall customer details only if it created them. The system operator	Mandatory

	(administrator) may recall any customer details, regardless of who created them. Recalled customer details are deleted from the base. *IPS must not allow that customer details are changed by Participants that did not enter them, except for the system administrator in cases when the creator is unable to do so, when the creator refuses to do so at the customer's request, and similar.*	
Reply	SmartVista Addressing service fully complies with this requirement. The Participant Portal allows both participants and the scheme operator to perform housekeeping function on the central alias scheme which may include removing inactive aliases, aliases added due to mistake, update of alias with new information etc.	
	7.5.5. ***Data reading by batch processing (IPS.CAS.05)***	
FR.134	IPS supports reading of files in one of the following formats: xml, csv, xls. The sender may send the file with details on customers which will be entered in the CAS. All the controls from the group (IPS.CAS.03) apply to the data in the file. The file must have a digital signature.	Mandatory

7.6. Dispute Management Module (IPS.DM.01)

Reply	SmartVista Addressing service will fully comply with this requirement. Some customization will be needed to support the batch upload feature requested.	
FR.135	IPS has Dispute Management Module which allows Participants to initiate and resolve disputes after processing of transfer orders and recalls. This module should enable: • To initiate a dispute; • To exchange with investigation requests and supporting information between concerned Participants; • To close Dispute when resolved; • To escalate dispute to System administrator in case of resolution is not achieved;	Mandatory

	• To initiate Recall process if agreed between Participants; • To provide Reporting on Disputes.	
Reply		

7.7. Statistics, monitoring, reporting, alerts (IPS.SM.01)

FR.136	IPS has an automated statistical collection during processing of transfer orders and recalls. This module should enable: • The module should perform automatic collection of data • Updating the statistical data during the payment process • The module should perform automatic analysis of data • Reporting based on collected statistical data for the defined template (since a list of records in this report can be very long, filtering restrictions can be applied) • Online matching of Transfer Orders based on collected statistical data • Alert mechanism of the System administrator (via report or User screen) or rejection of payment if this match has been detected.	Mandatory
Reply	BPC has proposed Fraud and Risk Management system which is one of the modules that offer value-added service to the system. The Fraud system has capability to prevent and detect in real-time any potential fraud scenario taking place in the IPS scheme. Transfer order of payments can be rejected in realtime if they match the rules defined. Similary any statistical analysis of the data is possible where the system captures the statistics and use it in the rule engine to make a decision about a transaction.	
FR.137	IPS provides monitoring facilities for Participants for unavailability schedules (announced by all Participants), current unavailability windows opened as well as sudden announcements *See requirements in section 7.9. "Participant "unreachable" function and pre-autorisation facility"*	Mandatory

Reply	Through the operator portal provided by SmartVista, IPS staff and participant can view the connection status of the participant and can monitor the unavailability schedule.	
FR.138	IPS provides monitoring facilities for System Operator for unavailability schedules, current unavailability windows opened as well as sudden announcements	Mandatory
Reply	Through the operator portal provided by SmartVista, IPS staff and participant can view the connection status of the participant and can monitor the unavailability schedule.	
FR.139	IPS provides report for scheduled upcoming unavailability schedule	Mandatory
Reply	SmartVista will fully comply with the unavailabilty schedule requirement.	
FR.140	IPS provides historical report for unavailability start and finish activities (system-wise)	Mandatory
Reply	SmartVista will fully comply with this requirement.	
FR.141	IPS provides historical report for unavailability start and finish activities (Participant-wise)	Mandatory
Reply	SmartVista will fully comply with this requirement.	
FR.142	IPS issues alerts concerned Participants at pre-defined time before planned windows start and finish	Mandatory
Reply	SmartVista will fully comply with this requirement.	
FR.143	IPS issues alerts to Participants when unavailability windows start and finish	Mandatory
Reply	SmartVista will fully comply with this requirement.	

FR.144	IPS issues alerts to System Operator when unavailability windows start and finish	Mandatory
Reply	Using the notification solution provided with the proposal, SmartVista Instant payment system will generate the alert and send it to the respective receipent informing them of the downtime and unavailability window.	

7.8. Request To Pay and Payment Initiation Request (IPS.RTP)

List of messages in Request To Pay (RTP) and Payment Initiation Request (PIR) processing

Message	Description	Message
RTP initiated by Creditor	Message for initiating the RTP by Creditor	Pain.013
Response on RTP	Message for response on RTP initiated by Creditor	Pain.014
PIR by Third Party	Message for initiating the RTP initiated by Third Party	Pain.001
Response on PIR	Message for initiating the RTP initiated by Third Party	Pain.002

List of processes

Process code	Description
IPS.RTP.01	General conditions
IPS.RTP.02	RTP and PIR business process (validations)

7.8.1. General conditions (IPS.RTP.01)

FR.145	IPS processes Request to Pay received from Creditor, registers it and routes for Processing by Payer. *Payer may reject it or issue a transfer with a clear reference to Request to Pay. Payer may issue one transfer per each RTP. Multiple transfers for the same RTP are not allowed*.	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.146	IPS processes Payment initiation Request received from Third Party, registers it and routes for Processing by Payer.	Mandatory

	Payer may reject it or issue a transfer with a clear reference to Payment initiation Request. Payer may issue one transfer per each PIR. Multiple transfers for the same PIR are not allowed.	
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.147	Payer shall issue transfer on RTP or PIR within pre-defined timeout defined by processing rules. *IPS routes RTP or PIR immediately for Payer which shall process it and send transfer or rejection notice back to IPS. If a transfer order arrives after timeout expired it is rejected by the system. The system notifies Creditor that RTP or PIR has not been replied by Payer.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.148	RTP and PIR does not reserve and/or move any funds on Payer account. *Funds are reserved and/or moved only after transfer comes to the system and in case of transfer is successfully validated by the system.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.149	Transfer created on the basis of RTP or PIR must contain unique reference to initiating RTP or PIR. *If RTP or PIR reference is present in the transfer and RTP or PIR is not found then the transfer is rejected. Duplicated transfers created for the same RTP or PIR are rejected as well.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.150	The Payer will specify the data source in the field (xx) of the RTP created based on the data in the CAS.	Mandatory

	The RTP order contains fields (flags) that serve to specify the data source for the payer and/or payee from the CAS.	
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.151	The Payee includes the required reference data of the received bill in the fields (xx) in the RTP created based on the data in the invoice payment process (BP). *RTP contains fields (flags) that serve to specify the data source for the payer and/or payee from the CAS.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.152	By sending a positive response to a transfer order created based on the data received in the RTP or PIR – invoice payment process (which contains the required reference data of the received invoice), the Payee confirms that transfer order elements (the Payee's BBAN, the Payee's BIC, the amount, ...) are in compliance with the BP request.	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
	7.8.2. ***Validation (IPS.RTP.02)***	
FR.153	IPS will perform business validation of a RTP or PIR sent by the Creditor or by Third Party. RTP and PIR processing will be terminated as soon as the first validation error is encountered and that order will be rejected with an appropriate message. *IPS validates a received RTP/PIR and informs the Sender of any errors that occurred during business validation. More detailed business validations are specified below. In addition to these, technical validations are also carried out.*	Mandatory

Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.154	IPS validates the authorisation of a Sender to deliver a transfer order based on the sent BIC. *IPS validates the Creditor or Third Party in terms of validation of authorisation to issue RTP or PIR.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.155	For each transfer order, IPS will identify the IPS account for debiting Party. IPS account identification will be derived from the Payer's BIC and the currency of RTP/PIR. *The Payer's BIC from the RTP/PIR is uniquely linked to the IPS account.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.156	For each transfer order, IPS will identify the IPS account for crediting Party. IPS account identification will be derived from the Payee's BIC and the currency of RTP/PIR. *The Payee's BIC from the RTP/PIR is uniquely linked to the IPS account.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.157	For each transfer order, IPS checks whether the Payer and Payee is a system participant. The Payer's and Payee's BICs will be used for Payer's and Payee's identification. *IPS will reject every transfer order if it is determined that the Payer or Payee is not in the system or cannot be identified based on the RTP/PIR.*	Mandatory

Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.158	IPS validates that the RTP/PIR currency corresponds to the currency of the debit and credit accounts. *IPS routes RTP/PIR to Payer provided that the debit and credit accounts are in the same currency as the transfer order.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.159	IPS will validate that attributes of a transfer order created on the basis of RTP/PIR correspond to RTP/PIR. *IPS will validate that attributes of a transfer order created on the basis of RTP/PIR correspond to RTP/PIR.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.160	IPS will validate that the transfer order has correct syntax of account numbers of the Payer and Payee – end customers. *Account numbers of the payers and payees – end customers are compulsory fields in RTP/PIR. IPS will only validate their presence and syntax, but not their content.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.161	IPS will notify the Sender in case the RTP/PIR has an error by sending an RTP/PIR rejection message. *IPS will send the Sender information on the error which occurred during the RTP/PIR validation.*	Mandatory

Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.162	IPS will notify the Sender in case the RTP/PIR has been rejected by Payer by sending an RTP/PIR rejection message. *IPS will send the Sender information on the rejection of RTP/PIR by Payer.*	Mandatory
Reply	SmartVista fully complies with this requirement . Please refer to section ' Instant Payment Platform Overlay Services' for more details.	
FR.163	For some Participants, IPS will debit the Payer's IPS account without waiting for the Payer's response. IPS allows the Operator to configure such a Participant in accordance with the operating rules and based on functionalities described in section 7.9 "Participant unreachable function and pre-autorisation facility".	Mandatory
Reply	SmartVista offers stand-in processing in case a participant is unavailable to receive a payment request. This requirement will be supported fully.	

7.9. Participant "unreachable" function and pre-autorisation facility

Given the required 360/7/24 availability for the participants in IPS system, a mechanism to deal with planned and unexpected "participant out of reach" situations is needed.

Functionalities described in this section are intended to allow:

i. Scheduled maintenance window (planned "unreachability") management (announce/delete) by Participants;

ii. Scheduled maintenance window (planned "unreachability") management by IPS Operator;

iii. Start/finish management of scheduled and unexpected "unreachability" window by Participants;

iv. Start/finish of scheduled and unexpected "unreachability" window by IPS Operator;

v. To provide monitoring facilities for Participants for "unreachability" schedules (announced by all Participants), current "unreachability" windows opened as well as unexpected announcements via existing monitoring workstations;

vi. To provide monitoring facilities for IPS Operator for “unreachability” schedules, current “unreachability” windows opened as well as unexpected announcements via existing monitoring workstations;

vii. To issue alerts to Participants and IPS Operator when “unreachability” windows start and finish;

viii. To implement automated pre-authorisation service functions to allow pre-authorization of certain payments (on predefined criteria) for some pre-defined types of payments, or during “unreachability” window, or in case of RTP/Transfer order timeout event.

To achieve this goal, the following functions shall be implemented in the IPS system:

i. “unreachability” window registration and management in IPS system

ii. implementation of automated pre-authorisation service as a separate module.

Interconection with other IPS scheme processes:

i. RTP and Transfer order payment processing shall be modified in case of “unreachability”window is opened for concerned Participant;

ii. RTP and Transfer order payment processing shall be modified in case of timeout event occurred during RTP or Transfer oreder payment processing.

List of processes for “unreachability” window

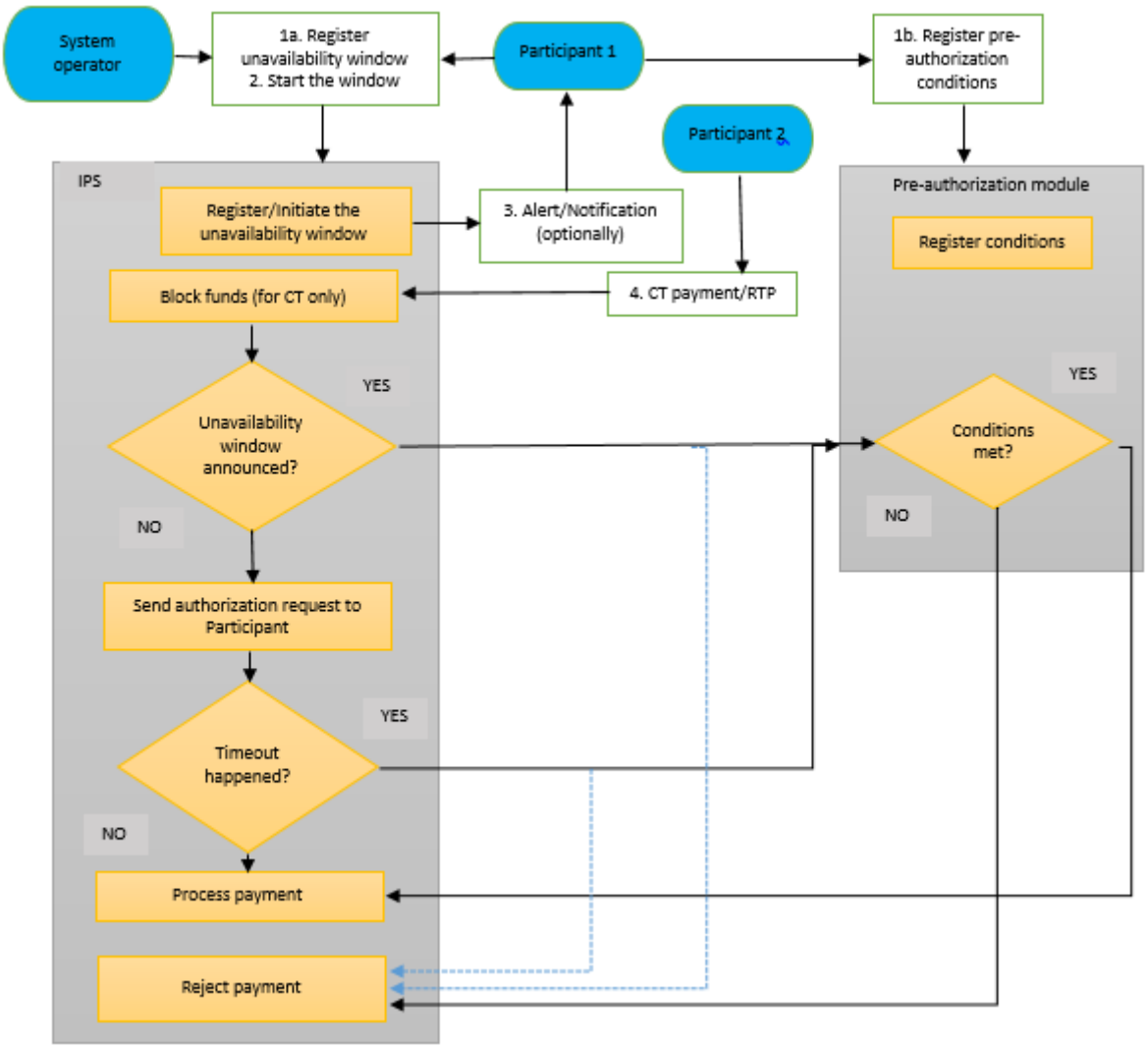
Process code	**Description**
IPS.OUT.01	In case of scheduled unreachabilty, Business process starts from registration of future unreachability event (window) in the IPS
IPS.OUT.02	At predefined time interval before planned time, IPS (optionally) issues a system event notification to “unreachable” Participant that unreachability shall be started soon
IPS.OUT.03	Participant shall initiate (start) unreachability window at time when unreachability starts and finish it at time when unreachability finishes. IPS doesn’t start/finish unreachability window automatically. IPS system records actual window start and finish time in the IPS database. In case Participant requests for “unexpected” unreachabily, IPS system registers unreachability window and immediately starts it. As for IPS system doesn’t finish this window automatically and Participant shall perform this operation. Participant shall announce planned unreachability finish time even for unexpected unreachability windows

IPS.OUT.04	When RTP or Transfer order payments arrives, the system verifies if the unreachability is started for the Participant and process RTP/TO payment accordingly. In case of pre-authorisation module is used, then a request is sent to this module. RTP pre-authorization criteria are applied for Debiting Participants, i.e. the module generates a payment on behalf of Debiting Participant. Transfer order payment pre-authorization criteria are applied for Crediting Participants, i.e. the module generates a payment authorization on behalf of Crediting Participant. In case of module is not used then RTP or payment are simply rejected with an appropriate rejection reason

List of processes for automated pre-authorisation:

Process code	**Description**
IPS.AUTH.01	Business process assumes that Participants register in advance pre-authorization criteria for RTP and Transfer order payments. IPS system consults if payment can processed without authorization by concerned Participant based on these predefined criteria (at any time, or during unavailability window, or in case of RTP/Payment timeout event). These criteria include: - Sender - Receiver - Individual amount - Aggregated amount (daily)

The overall business process is presented at the diagram below:



7.9.1. Unavailability schedule management (*IPS.OUT.01*)		
FR.164	IPS allows Participant to announce scheduled maintenance window ("planned unavailability") *Participant shall be available to do it via API call.* *Planned window contains following attributes (at least):* - *Unavailability type (planned/sudden)* - *Unavailability reason (system dictionary)* - *Planned (scheduled) unavailability start time* - *Planned (scheduled) unavailability finish time*	Mandatory

	- *Narration data with description* - *Audit information* - *Pre-authorization conditions in pre-authorization module.*	
Reply	SmartVista will fully comply with this requirement with some customization.	
FR.165	IPS allows System Operator to announce scheduled maintenance window on behalf of Participant *System Operator shall be available to do it via DBO workstation*	Mandatory
Reply	SmartVista will fully comply with this requirement with some customization.	
FR.166	IPS allows Participant to manage unavailability schedule (delete scheduled maintenance window announced earlier) *Participant shall be available to do it via API call*	Mandatory
Reply	SmartVista will fully comply with this requirement with some customization.	
FR.167	IPS allows System Operator to manage unavailability schedule (delete scheduled maintenance window announced earlier) on behalf of Participant *System Operator shall be available to do it via DBO workstation*	Mandatory
Reply	SmartVista will fully comply with this requirement with some customization.	
7.9.2. Unavailability window start and finish announcement (*IPS.OUT.03)*		
FR.168	Participant initiates unavailability window start for scheduled maintenance window *Participant shall be available to do it via API call*	Mandatory

Reply	SmartVista will support this requirement with some customization.	
FR.169	System Operator initiates on behalf of Participant the unavailability window start for scheduled maintenance window *System Operator shall be available to do it via DBO workstation*	Mandatory
Reply	SmartVista will support this requirement with some customization.	
FR.170	Participant announces and starts unplanned maintenance window and its start in case of sudden technical issues *Participant shall be available to do it via API call*	Mandatory
Reply	SmartVista will support this requirement with some customization.	
FR.171	System Operator announces and starts on behalf of Participant the unplanned maintenance window in case of sudden technical issues *System Operator shall be available to do it via DBO workstation*	Mandatory
Reply	SmartVista will support this requirement with some customization.	
FR.172	Participant finishes unavailability window (announced earlier) *Participant shall be available to do it via API call*	Mandatory
Reply	SmartVista will support this requirement with some customization.	
FR.173	System Operator finishes on behalf of Participant the unavailability window (announced earlier) by Participant *System Operator shall be available to do it via DBO workstation*	Mandatory
Reply	SmartVista will support this requirement with some customization.	

7.9.3. Pre-authorization service (*IPS.AUTH.01)*		
FR.174	To allow Participant to configure (add/modify/suspend/delete) “pre-authorization” profiles for Payments and RTP requests under normal conditions	Mandatory
Reply	SmartVista support stand-in processing on behalf of the authorization participant. The requirement will be supported via some customization.	
FR.175	To allow Participant to configure (add/modify/suspend/delete) “pre-authorization” profiles for Payments and RTP requests during the time when “unavailability window” is opened	Mandatory
Reply	SmartVista support stand-in processing on behalf of the authorization participant. The requirement will be supported via some customization.	
FR.176	To allow Participant to configure (add/modify/suspend/delete) “pre-authorization” profiles for Payments and RTP requests for timeout events (if response for RTP or Payment didn’t come in pre-defined timeout)	Mandatory
Reply	SmartVista support stand-in processing on behalf of the authorization participant. The requirement will be supported via some customization.	
FR.177	To allow System Operator to monitor “pre-authorization” profiles defined by Participants	Mandatory
Reply	SmartVista support stand-in processing on behalf of the authorization participant. The requirement will be supported via some customization.	

7.10. Billing

FR.178	The IPS must contain a framework with possibility to define fees for services provided by the IPS, including but not limited to the following fee types: - transaction fee (by type of transaction) - fee for registration of participants	Mandatory

	- monthly/yearly fee - penalties - possibility to define fees for “unavailability window” management functions (announce/delete/start/finish). - possibility to define fees for pre-authorization services (for timeout / unavailability window)	
Reply	SmartVista comes with a sophesticated billing module. Please refer to 'Billing and Statement' section in the Technical Proposal for more details.	

NON-FUNCTIONAL REQUIREMENTS

8.1. Requirements

Req. ID	Requirements	Classification
1. Requirements for the main characteristics of the solution		
NF. 1	The architecture of the solution shall be aligned to best practices and standards to meet the highest criteria for integrity, compatibility, performance and reliability.	Mandatory
Reply	Please refer to Section ”Reliability, Availability and Scalability”.	
NF. 2	The solution will have an open and modular architecture, which will allow easy implementation and integration with different systems.	Mandatory
Reply	Please refer to Section “Service-Oriented Architectural Style”.	
NF. 3	The technological architecture of the application must have a high level of resistance to failures, and should not contain single points of failure (SPOF).	Mandatory
Reply	Please refer to Section “Service-Oriented Architectural Style”.	
NF. 4	The IPS system must provide native integration capabilities with other systems such as automatic interbank payments systems (AIPS), Participant systems, etc. *NBM expects that Vendor will explain in details how proposed IPS solution:* • *Supports STP approach for interaction with external systems* • *Distribute information to external systems*	Mandatory
Reply	Please refer to Section “SmartVista Integration Platform”.	
NF. 5	Due to high amount of processed data, to ensure increased productivity, the solution shall have native integrated capabilities such as in-memory processing, multi-thread processing, parallel execution of jobs, etc.	Mandatory
Reply	Please refer to Section ”Reliability, Availability and Scalability”.	
NF. 6	The solution shall ensure a high level of stability and operational performance. In this regard, the solution shall have effective mechanisms for handling errors, in order to avoid data loss, system-wide blocking processes, system failure etc.	Mandatory

Reply	Please refer to Section ”Reliability, Availability and Scalability”.	
NF. 7	The application architecture must ensure the integrity and accuracy of the data when data are being accessed and modified simultaneously by multiple entities (users, internal processes, external applications), with notification of user.	Mandatory
NF. 8	The solution shall have the ability to be timely adapted to the new business needs. It is very important that this will be possible only through parameterization and configuration adjustments in the applications (versus changes in code), thus minimizing adjustment costs supported by the IPS.	Mandatory
Reply	Please refer to Sections “Component Based Architectural Style” and “Layered Architectural Style”.	
NF. 9	The solution shall be easy maintainable. In this regard, the solution architecture shall allow implementation of new versions delivered by the software provider without affecting the architecture of existing customizations, components implemented by the NBM and interfaces with other external applications.	Mandatory
Reply	Please refer to Section “Component Based Architectural Style”.	
NF. 10	The solution will be based on web interfaces, shall have user-friendly interfaces, be simple and intuitive in use.	Mandatory
Reply	Please refer to Section “Layered Architectural Style”.	
NF. 11	The solution shall ensure a very high level of security, taking into account the integrity, confidentiality, availability and non-repudiation concerns regarding the data to deal with, so that control measures provided at the system level is proportional to the risks involved. In this regard, the most important objectives security to be achieved are: a. ensure an adequate level of confidentiality, authenticity, integrity and availability of data during its entire lifecycle and ensure non-repudiation of each single transaction in the system; b. ensure an effective control of logical access and prevent any unauthorized access to its data; c. ensure an effective auditing by monitoring and logging user activities at the system level;	Mandatory

	d. prevent loss, modification or misuse of information within the system;	
Reply	Please refer to Section “SmartVista Security Architecture”.	
2. Detailed requirements		
2.1. Architecture requirements		
NF. 12	NBM opts for an open and modular architecture, based on pre-integrated components. These principles must be visible at all levels of the architecture of application that is part of the offered solution.	Mandatory
Reply	Please refer to Sections “Component Based Architectural Style” and “Layered Architectural Style”.	
NF. 13	The architecture of the solution will be service-oriented (SOA).	Mandatory
Reply	Pease refer to Section “Service-Oriented Architectural Style”.	
NF. 14	The architecture of application will be client-server type, organized in at least 3 vertical layers, clearly divided so that each higher level will depend only on its lower level.	Mandatory
Reply	Please refer to Section “Layered Architectural Style”.	
NF. 15	Communication between all application components will be done in a secure manner, using for this purpose of the internal interfaces of the application components.	Mandatory
Reply	Please refer to Section “SmartVista Security Architecture”.	
2.2. Requirements for interoperability		
NF. 16	The IPS must have native integration capabilities which will easily allow the integration with different systems. *In the project scope will be included the integration with the AIPS (RTGS module) system installed at NBM, via online messaging interfaces. There will be also available the option to integrate with other IT systems of the NBM, via web services and XML file formats.*	Mandatory
Reply	Please refer to Section “SmartVista Integration Platform”.	
NF. 17	Interaction based on Web-services must be available as an integration capability in IPS.	Mandatory

	List of interfaces available and integration approach must be specified by Vendor.	
Reply	Please refer to Section “SmartVista Integration Platform” of the Technical proposal Document. This Section describes the available out of the Box Integration Channels and Interfaces including JSON/Restful APIs, SOAP Webservices, ISO 20022, XML, ISO 8583, Swift, XML Formats, MQ and others	
NF. 18	The IPS must be capable to interact with external systems via SWIFT network. *Vendor is requested to:* • *Explain how proposed solution is connected to SWIFT network* • *Provide full list of SWIFT protocols and services supported by proposed solution*	Mandatory
Reply	SmartVista supports Swift MT/MX formats basd on SmartVista Integration Platform.	
NF. 19	The IPS must support SWIFT MX ISO 20022 messages for interaction with external systems.	Mandatory
Reply	SmartVista supports SWIFT MX based on ISO20022 support of SmartVista Integration Platform	
NF. 20	The IPS must be capable to interact with external systems by means of web services via private network.	Mandatory
Reply	Please refer to Section “Setting up of PKI”.	
NF. 21	System must support a set of standard interfaces with Participants and other systems. *Vendor must provide full list of standard interfaces being a part of the proposal.*	Mandatory
Reply	Please refer to Section “SmartVista Integration Platform” of the Technical proposal Document. This Section describes the available out of the Box Integration Channels and Interfaces including JSON/Restful APIs, SOAP Webservices, ISO 20022, XML, ISO 8583, Swift, XML Formats, MQ and others	

2.3. Requirements for flexibility		
NF. 22	The solution shall allow at least the following user configurable operations: a. define/customize business rules; b. define/customize automated actions based on different events, time schedule; c. define new business workflows, or customize the existing ones; d. define new reports, based on customizable templates.	Mandatory
Reply	SmartVista provides all relevant tools to users including Portals and GUIs to define/configure business roles including scheduled actions or event triggered actions. SmartVista Integration Platform includes BPMN Workflow Engine Please refer to Section “SmartVista Integration Platform” for further information. SmartVista includes Reporting and Anayltics tools including Jasper Reports, which allows to configure customized reporting templates by authorized Users. Please refer to Section “Reports and Analytics” for additional informations.	
NF. 23	The application will allow to customize views and user forms. The application will allow to create new user forms for accessing the business logic of the application.	Mandatory
Reply	SmartVista can be accessed via GUI including role based access control, which also allows to only provide relevant views and menu items to users based on their role. Users can then also define themselves their most used forms based on bookmark feature.	
NF. 24	The application will allow customizing existing reports (e.g. adjust data set, formatting).	Mandatory
Reply	Please refer to section “Reports and Analytics”.	
NF. 25	The application will allow the definition and management of normative reference information used within the application. The data source for reference information may be internal or external (e.g. external database, external web service, external file).	Mandatory
Reply	Please refer to Section “SmartVista Integration Platform”.	

NF. 26	The solution must provide friendly GUI interfaces for administrators to allow the customization/configuration activities, where most operations can be performed by click and drag-and-drop.	Mandatory
Reply	SmartVista provides GUIs including additional Portals with Role based access control, which allows easy configurations from the Administrator. Operations can be done manually based on pre defined authorized roles manually via GUIs.	
NF. 27	The application will allow the definition and customization of external interfaces of the application (e.g. setting available business function, setting the format of input/output data, setting communication protocols, access control settings, etc.).	Recommended
Reply	Please refer to Section " SmartVista integration Platform"	
2.4. Requirements for usability		
NF. 28	All business functions available to users of application must be accessible through web interfaces.	Mandatory
Reply	SmartVista includes relevant GUIs and Portals to make all functions available and accessible to authorized users, based on role based access control.	
NF. 29	All user interfaces must be in English language. *It is recommended the user interfaces to be available also in Romanian language*.	Mandatory
Reply	SmartVista supports Multi Language including English and Romanian language.	
NF. 30	Application will have user-friendly interfaces that are intuitive and convenient to use for business users and users with administrative roles.	Mandatory
Reply	SmartVista provides users with relevant GUIs and Portals including configurable Screens based on role based access control mechanism.	
NF. 31	The system shall be intuitively clear for the users so that it will allow the use of the system with a minimal training.	Mandatory
Reply	SmartVista can be configured to show only relevant Functions based on the Role of the User.	

NF. 32	Documentation related to the solution shall contain complete guides, detailed and updated for all groups of users.	Mandatory
Reply	SmartVista comes will all relevant Guides including User Guide, Administration Guide, Configuration Guide, Developers Guide.	
NF. 33	Users shall have access to context-sensitive help.	Recommended
Reply	SmartVista GUIs and Portals include Help Functions including Search function and integrated Guide.	
NF. 34	The solution shall allow saving intermediate work and operations initiated by the user (automatically or at user request).	Recommended
Reply	SmartVista allows the saving of intermediate work eg.: User manually create new Application Form and need additional information's to finalize.	
NF. 35	The solution shall allow users to customize its own workspace (e.g., adding menu items to favorites, displaying the latest hits, save searches, save templates, etc.).	Recommended
Reply	SmartVista GUIs and Portal allows to favorite workspace based on Bookmarks and showing used templates and searches. Also based on pre-defined Role, just all relevant Menu items will be displayed based on the user roe.	
NF. 36	User interfaces shall allow easy navigation through solution forms, by using complementary mechanisms (e.g., mouse and/or keyboard and/or special functions).	Mandatory
Reply	SmartVista GUIs/Portal are build to support the user to easily navigate throught the menu either with Mouse and/or keyboard.	
NF. 37	The application must provide a mechanism for centralized displaying (e.g. dashboard) of all actions that user has to perform within the application.	Recommended
Reply	SmartVista provides Role based access control, which allows to provide users with pre-defined screen showing only the relevant menu items to them.	
2.5. Requirements for security		
2.5.1. Security architecture		
NF. 38	The solution must implement a Multi-layered security approach at the application level and have the ability to integrate into institutional model of	Mandatory

	NBM (further into institutional model of CSD) for information security management (based on ISO 27000 family of standards).	
Reply	Please refer to Section “SmartVista Security Architecture”	
NF. 39	All access credentials used by the application shall be configurable in the administrative interface. Applications shall not contain hardcoded credentials for access.	Mandatory
Reply	SmartVista provides The solution implements the RBAC (Role Based Access Control) approach to user rights and responsibilities. It allows defining roles and assigning roles to users or groups of users. The roles consist of autonomic roles that regulate system functions separately and they can be assigned for any individual user id as complimentary to the role. Administrators can perform user management tasks including: ● Viewing registered users ● Adding and deleting users ● Assigning roles to users ● Changing a user’s password ● Assigning institutions and agents to users ● Changing the user status (blocked or active) ● Changing the user’s type (global administrator, local administrator, or general user) ● Auditing user sessions ● Auditing user actions	
NF. 40	None of the solution components shall contain stored access credentials in open form (in databases, configuration files).	Mandatory
Reply	SmartVista Product Suite is PA DSS validated and makes use of latest best practise of security and cryptography to ensure credentials are not stored in open clear text form. It is also possible to use LDAP server(including MS Active Directory) as a backend storage for credentials. According to modern requirements for authentication subsystem (PA-DSS 3.2, NIST SP800-63-3) we also support digital certificates as a second factor for user authentication. So you can use multi-factor or single-factor cryptographic devices or software (according to NIST SP800-63-3	

	classification) to organize secure and flexible authorization for different user classes.	
NF. 41	All solution related system processes shall run with minimum privileges needed to execute the tasks assigned.	Mandatory
Reply	SmartVista is using Role Based Authentication Control mechanism to ensure all relevant privileged can be assigned to a User of a specific Role by the Administrator.	
NF. 42	All external interfaces of application will be accessed by using secure authentication methods (e.g. X.509 certificate-based authentication).	Mandatory
Reply	The SmartVista application supports PKI and SSL in different layers: 1) GUI layer: • provides secure connections (HTTPS) for web-browsers which work with SV Web-UI; as a result, a secure tunnel is established between user and SV Web-UI; • provides secure communication channels (SSL protection) for existing web-services; as a result, a secure tunnel is established between SV IG application and external clients; • provides secure data sources (SSL protection) to Oracle database; as a result, a secure tunnel is established between SV Web-UI application, SV Payment Gateway application and Oracle database(s); 2) Database client and Database Interface: • provides secure communication channels (SSL protection) between database and program components; as a result, all traffic between database and SV modules/tools is secured; 3) External software components: • provides secure data tunnels (SSL, IPsec or other protection) between SV components; for instance, SV-to-SV communication between two nodes can be organized through SSH tunnel; 4) Additional hardware equipment: • provides secure network tunnels (SSL, IPsec or other protection) between SV components and external systems; for instance, communication with	

	payment networks can be organized through network equipment with ciphering facility.	
NF. 43	The solution will be able to encrypt sensible data stored in the database.	Recommended
Reply	SmartVista has been built to comply to industry standard security requirements and hence is able to mask and encrypt sensitive in the database	
2.5.2. Authentication		
NF. 44	Application will permit registration of users and their profile information (e.g. ID, password, first name, surname, email, etc.).	Mandatory
Reply	SmartVista allows the registration of Users including the secure storage of User data.	
NF. 45	Application should support strong authentication mechanisms, including two factor authentication. *Vendor will describe all supported mechanisms for user authentication.*	Mandatory
Reply	The SmartVista Payment system by default supports authentication certificates and soft tokens. For token validation the system GUI components will integrate with RSA SecureID soft token solution for 2FA authentication. The steps of authentication will be: 1) User logs in to user interface of either application or OS 2) Application performs authorization with password via centralize login system (1st factor authentication) 3) Application calls RSA Authentication Manager for the 2 factor authentication 4) RSA Authentication Manager generates otp and sends it to user mobile phone or desktop notification 5) RSA Authentication Manager calls its agent for prompt of OTP at application UI 6) User enters received OTP into agent prompt 7) Agent sends OTP to RSA Authentication Manager for verificaiton 9) RSA notifies application user interface of the result of authentication and sucessfully logs the user in in case of successful authentication	
NF. 46	User passwords must be protected within the application. The method of protecting passwords must ensure the impossibility of their interception, deduction or retrieval.	Mandatory

Reply	The entire SmartVista Product Suite is PA DSS validated and makes use of the latest, best practice security and cryptography.	
NF. 47	Application will allow: a. Setting password policy requirements for at least: the complexity of password, password change requirement, password lifetime, repeated use of passwords, the number of failed login attempts and dictionary of prohibited passwords. In this case, the application will timely provide the user with information regarding the use of password usage policies (e.g. a message about password expiring in n days). b. Application will allow segregated use of password usage policies for different user groups. c. Application will enable their users to change the password via user interface.	Mandatory
Reply	According to modern requirements for authentication subsystem (PA-DSS 3.2, NIST SP800-63-3) we also support digital certificates as a second factor for user authentication. So you can use multi-factor or single-factor cryptographic devices or software (according to NIST SP800-63-3 classification) to organize secure and flexible authorization for different user classes. For example, you can require to use password protected token with certificate for administrators authentication and allow to use authentication by password only for regular users.	
NF. 48	Application will allow to block, disable or suspend user accounts at the application level.	Mandatory
Reply	SmartVista supports full User Management of SmartVista users.	
NF. 49	Application will allow users to access application only through an authentication procedure.	Mandatory
Reply	SmartVista can only be accessed based on pre authentication using the defined authentication mechanism. (eg.: 2 Factor Authentication)	
NF. 50	Application will allow differentiated use of authentication methods, depending on different categories of users.	Recommended
Reply	See NF. 47	

NF. 51	Application will permit to set the number of simultaneous connections that can be initiated by a user. In case this feature is not supported, the solution will not allow more than one connection per user.	Mandatory
Reply	SmartVista can be configured, that User only allowed one connection based on opened session.	
NF. 52	Application will permit to set user session timeout in case of inactivity.	Mandatory
Reply	SmartVista has a configurable session timeout parameter. If the user was inactive for a period more than the configurable session timeout period she/he will be logged out.	
NF. 53	Application will provide mechanisms to prevent unauthorized take-over of active sessions initiated by legitimate users.	Mandatory
Reply	SmartVista meets all requirements of OWASP Session Management. To protect from session replication are used several levels of security: - secure connection (only HTTPS) - unique random cookies - hijacking protection (one user - one session) - CSRF-token protection	
NF. 54	Application will provide the necessary mechanisms for implementation of Single Sign-On (e.g. Kerberos).	Mandatory
Reply	SmartVista supports LDAP, Active Directory, Kerberos, SSO.	
2.5.3. Authorization		
NF. 55	Authorization method in the application will be based on the principle "everything not expressly permitted is forbidden".	Mandatory
Reply	SmartVista RBAC Mechanism ensures, that User only get granted access to relevant Functions and Menu Items based on his Role privileges and has no access to anything more.	
NF. 56	Application will allow definition of user groups and roles within the application, and association of users of the application with these groups and roles.	Mandatory

Reply	See NF.39	
NF. 57	Application will allow the granting of access rights for user, user groups and user roles. A group can contain multiple subgroups / roles. A user can be assigned to one or more groups or roles, access rights being determined cumulatively.	Mandatory
Reply	See NF.39	
NF. 58	Application will allow temporary delegation of rights held by one user to another user. The delegation will be made with keeping or suspending of rights owned by the user to whom these rights are being delegated.	Mandatory
Reply	SmartVista allows to delegate actions based on defined Roles and groups.	
NF. 59	Application will provide views and reports regarding existing access rights within the application. They can be parameterized by at least the following parameters: user group / role within the applications, user ID, business entity, property related to business entity, permitted operations.	Mandatory
Reply	See NF.39	
NF. 60	The solution must support multi-level authorization framework for verifications and approvals, based on configurable business workflows. At least three levels must be available by default.	Mandatory
Reply	SmartVista supports configurable business workflows (see more in detail in section “SmartVista Integration Platform”) including unlimited authorization level.	
	2.5.4. Input and output validation	
NF. 61	Application will provide appropriate mechanisms to prevent manipulation of the input data (user inputs, inputs from external applications).	Mandatory
Reply	All the critical operations support "maker-checker" pattern in order to avoid for one user to be responsible for sensitive actions. Sensitive data becomes available to the operators only when correct search information is presented to the system (e.g. first name+last name+id or first name+last name+birthdate, etc.)	
	2.5.5. PKI	

NF. 62	IPS infrastructure must ensure the protection of the integrity of messages exchanged between IPS system participants and the operator. *Integrity protection should be ensured using PKI and digital signatures for sender messages as well as the validation of the digital signature by the recipient.*	Mandatory
Reply	Please refer to Section "Setting up of PKI"	
NF. 63	The IPS infrastructure must ensure the protection of confidentiality of data exchanged between IPS system participants and the operator. *Confidentiality protection is provided by using PKI and traffic encryption between system participants and the operator at application level.*	Mandatory
Reply	Please refer to Section "Setting up of PKI"	
NF. 64	Client application modules need to be ensured that enable the integration of participants into the PKI of the IPS system. *Adequate software support should be ensured for each of the proposed methods for connecting participants to the IPS system.*	Mandatory
Reply	Please refer to Section "Setting up of PKI"	
NF. 65	The solution for the electronic signature and PKI will meet the following technical requirements: • Centralized management of public key certificates, based on a widely-adopted protocol (e.g. LDAP), with posibilites for scaling up and integration with other solutions. • Acceptance of third-party certificates as Root of Trust (RoT). • Acceptance of certificates with RSA public key of length up to 4096 bit, SHA-256 as signature/hash algorithm and up to 4 levels of certification path. • Private key and private key's password / PIN will be protected against being tampered with or eavesdropped during the creation of electronic signatures. • Modern and commonly used standards and specifications will be used for creation of signature, such as RSA of minimum 2048 bit for end user keys, SHA-256, AES-256.	Mandatory

	• Possibility for integration with Hardware Secure Modules (HSM) and other electronic signature creation means by using PKCS#11 (v.2.20+) standard. • Addressing the requirements of security standards in the field of digital payment protection, such as PCI SSC, will be considered as an important advantage.	
Reply	Please refer to Section "Setting up of PKI"	
	2.5.6. Auditing and security monitoring	
NF. 66	For auditing and security monitoring, the following requirements are applicable: a. The proposed solution will have audit components that will centrally collect and manage audit records at each component level. b. Audit component shall allow granular configuration of audit policies. c. The proposed solution shall allow determining the specific characteristics of events that must be registered (e.g. products in a certain period, certain events, facts). d. Application shall allow auditing of any event within the application. e. Each audit record shall contain at least: i. Moment in time of the event; ii. Subject of the event (User ID); iii. Categories of affected data/parameters; iv. Event that happened; v. IP address of the source that initiated the event, or any other information permitting to identify the source; f. Audit records will not include confidential business information (eg. inserted passwords at failed attempts) g. The application will allow to fix historical versions of the data, which will be considered extremely sensitive.	Mandatory

	h. The application will be able to automatically generate the notifications to those responsible for the production of certain security events, according to set up configurations. i. Audit component shall use the system clock set to the operating system that runs the audit component. j. The proposed solution shall have secure mechanisms to protect the integrity of audit information recorded.	
Reply	All user activities are monitored and recorded in audit logs. These logs may be viewed by users with the necessary privileges. The audit logs contain details including: ● User's login ● User's privileges ● Address of the user's machine on the computer network used to access the SmartVista system ● Date and time of the user's action (the time displayed is accurate to one microsecond) ● System object type affected by the user's action ● System object identifier affected by the user's action ● Action status (successful or failed) ● Name of the modified database column ● Type and format of modified data ● Previous parameter value if the value was either updated or deleted ● New parameter value if the value was updated and inserted Procedures that perform day-to-day tasks such as incoming file uploads, transaction matching, and clearing file generation, are organized in the proposed system as processes. The information that results from running these processes is stored in logs for use in troubleshooting and auditing. The following criteria can be used to search for processes in the logs: ● Name of the process	

	● Session identifier ● Start and end date of the process ● Status of the process ● User who initiated the process ● Progress of the process (shown as a percentage) Additional information about specific processes can be viewed including: ● General process information, such as process name ● Statistical data relating to the process ● Trace data of the process ● Hierarchical structure of the process ● Parameters used in the process ● List of the processed files that resulted from running the process ● List of the transactions relating to the process Log messages are stored according to the current global logging level. The following logging levels are available: ● Fatal — all events critical for the system health such as startup and shutdown commands, all connection messages (line up, line down, signed on, signed off, and so forth) ● Error — all error messages including sequential timeouts for the HSM, incorrect keys for the HSM or POS terminal, error messages about non-working connections ● Warning — system warning messages such as timeouts. If these messages appear continuously, they need to be investigated further. ● Info — all information messages such as input and output commands ● Debug — the most detailed information is logged at this logging level	

	By default the audit trail captures users, resources (before-and-after) and actions taken. It also captures security violations and provides audit filter over the logged events. The logged events can also be sent to a third-party system for further processing.	
NF. 67	The solution shall have also its own user interfaces for accessing and processing recorded log events, including filtering of audit records by any field owned and their export in the usual format.	Mandatory
Reply	SmartVista comes with includes UI to view and search/filter audit records depending on the User rights (eg.: Administrator is allows to see the Audit Logs)	
NF. 68	Audit component shall be able to be integrated with solutions based on open standards, such as SIEM (Security Incident and Event Management) to take over the audit records produced in the solution by SIEM.	Recommended
Reply	SmartVista comes comes with a dedicated and standalone audit log module which receives data fees from all other components such as user actions, login/logons, parameters changes and others. According to the security standards the log can't be edited but can be extracted as per configured output format. Solution supports a range of SIEM software like HPE Arcsight, Qradar, MCafee.The solution can integrate with SBP current SIEM software.	
NF. 69	The audit component will own a mechanism for historical audit records archiving. The archiving process can also be parameterized by (frequency, data seniority, archiving format, destination, etc.).	Mandatory
Reply	SmartVista Archiving mechanism is based on use of backup and archiving tools.	
2.6. Requirements for Maintainability		
NF. 70	The offered solution should be easily maintainable and meet the following basic characteristics: a. Unified technology platform (a single database management system, a single hardware/software infrastructure); b. A single vendor for software modules that are part of the offered solution;	Mandatory

	c. A minimum number of development environments used for the development of application which is part of the offered solution; d. Effective mechanisms to identify and monitor problems appeared during the exploration of the solution.	
Reply	SmartVista is the fully in-house developed Platform of BPC including all relevant Modules including in the technical proposal document. Please refer to section “Layered Architectural Style” in relation to maintainability.	
NF. 71	For application to be available and accessible to business users at agreed level, they must be continuously monitored and maintained. Application must enable proactive problem identification and prevention by facile going of operational maintenance activities across all application components.	Mandatory
Reply	SmartVista System Monitoring is designed to provide centralized health monitoring of the SmartVista platform infrastructure and components using a single tool. It facilitates the monitoring of the system status itself, observes system components’ health, raises alerts and performs automated actions in the case where critical situations are encountered. In addition, the application gathers important statistics. System Monitoring is a standalone application with its own data storage. The solution is based on Zabbix and implements specific monitors for SmartVista components and the Oracle database. "The application monitors all components of SmartVista and keeps track of the statuses of on-line authorization processes and batch/off-line processes. It also provides the SmartVista infrastructure monitoring in a visual mode, so that users can see the generalized status information about the system as a whole with ability to compare several graphs to identify the root-problem. The monitoring application is used as a centralized point for the collection of data from all core SmartVista components and other related modules, tools and utilities. SmartVista monitors, working in conjunction with Zabbix agents or via JMX, provide the monitoring application with detailed system health information from the various relevant data sources. The design of SV system monitoring extensions provide an opportunity to use them with other external monitoring software (not necessarily Zabbix). In addition to the standard monitoring functions such as CPU, memory, and other widely used monitoring data, SV monitoring extensions (monitors)	

	provide additional data to the monitoring server (system monitoring customization). With the data that is collected from monitoring agents that are busy executing, Zabbix visualization tools are used to visualize overall system health (as well as that of separate system components) and important event history to the monitoring system operators. The Zabbix capabilities related to alerting and notifications are then used to setup the required notifications for system health events that should be sent to the responsible personnel. The monitoring application Web UI (Zabbix PHP-frontend) provides user access to dashboards, statistics, graphs, reports and configuration parameters of the monitoring system. The System monitoring application collects and analyses a variety of data related to the SmartVista system health which is used for: • SmartVista Infrastructure Monitoring o System resource monitoring (CPU, disks, memory, log space, etc.) o Database monitoring (Oracle DB) • Keeping track of SmartVista components connections, including: o Networks and host to host connectivity o Service provider connection (payment gateways, SMS gateways) o CBS connections o HSM connectivity • Monitoring SmartVista processes' states and their UNIX queues load o Reporting important or critical process related events (such as process crash, automatic restart and post-crash recovery, etc.) to the server • Information about transactions authorized by SmartVista o The number of transactions per given behavior (for example by transaction type, issuer institution, acquirer institution, terminal type, response code, etc.) per minute (10 mins, etc.) o Number of TPS - authorizations performance per institution	

	o Authorization rates (approvals, technical faults, etc.), average duration and other specialized metrics over filtered (by issueing/acquiring institutions, etc.) transactions • Monitoring of the batch/off-line SVBO containers and processes states o EOD, Applications processing, posting generation, etc.	
NF. 72	The solution will allow to monitor its own business-related parameters: the processing time for input/output messages, transaction processing time, etc. and generate appropriate notifications when certain parameters exceed critical thresholds.	Recommended
Reply	See NF.72	
2.7. Requirements for performance, continuity and resilience		
NF. 73	The solution must have the ability to process in a timely manner the transactions performed by IPS, according to volumes resulting from its activity. Technology platform architecture proposed by the Tenderer must provide the following minimum performance levels for application: a. IPS must be designed to enable the execution of 5,000,000 transactions (transfer orders) in A2A mode; b. IPS must be designed to enable the execution of about 100 transactions (transfer orders) in A2A mode per second in the peak times; c. IPS will complete the established tasks in the transfer order execution in less than 1 second. The established tasks executed by IPS within the defined deadline entail: Validation of the received message and forwarding it to the Recipient; Validation of the inbound Recipient's response, execution (in case of a transfer order) and forwarding the response (network delays and recipient's response delays are not accounted for this purpose). *The Vendor shall indicate in his offer the guaranteed minimum values of performance characteristics of the application, taking into account the technology platform recommended by Tenderer.*	Mandatory
Reply	Please refer to Section "Supported Platforms"	
NF. 74	IPS must support a configuration to operate on a 24/7 basis.	Mandatory

	IPS must be configured in such a way as to enable operations in 24/7 mode with the availability higher than 99.99% per month. All the system components must function in active-active mode. *Vendor shall describe continuous availability options and proposed technologies for disaster recovery supported by the solution. Recovery times for different options have to be described.*	
Reply	Please refer to Section "Supported Platforms"	
NF. 75	IPS must enable changes to the configuration on-the-fly with near to zero downtime. *IPS should be designed to enable the upgrade process on-the-fly, including changes to the set of messages and processes in the system as well as addition of new functionalities. The system should have the possibility to operate with multiple message versions simultaneously.*	Mandatory
Reply	Please refer to Section "Supported Platforms"	
NF. 76	IPS must ensure that changes to hardware configuration meet the new capacity requirements. *IPS should be designed to enable acceleration of message processing only by adding the hardware.*	Mandatory
Reply	Please refer to Section "Supported Platforms"	
NF. 77	IPS must ensure a RPO (Recovery point objective) value of zero. *In case of a system failure, IPS must not lose a single transaction executed.*	Mandatory
Reply	Recommended Platform Sizing was done based on RPO value of zero. Please refer to Section" Recommended Platform"	
NF. 78	IPS must ensure a RTO (Recovery time objective) not longer than 15 minutes. *In case of a system failure, maximum recovery time must not be longer than 15 minutes.*	Mandatory
Reply	Recommended Platform Sizing was done based on RTO value no longer than 15 minutes. Please refer to Section" Recommended Platform"	
NF. 79	The IPS system will have suitable instruments for executing backup procedures and the management of the historical backup copies.	Mandatory

Reply	Please refer to Section “Supported Platforms”	
NF. 80	The IPS system will have defined operational recovery procedures, to ensure the availability and accessibility of the solution in case of major incidents.	Mandatory
Reply	Please refer to Section “Supported Platforms”	
2.8. Requirements for scalability		
NF. 81	During the use of the IPS system, it is possible that the number of processed transactions to increase or decrease significantly from time to time. To make a rational use of processing resources the solution required by NBM should be easily scalable (up and down).	Mandatory
Reply	Please refer to Section “Supported Platforms”	
NF. 82	Solution will allow to increase the processing capacity without disrupting the business activity. To this end, application will support horizontal expansion of processing capacity (e.g. hardware infrastructure upgrade, adding new servers for application servers and performing load balancing).	Mandatory
Reply	Please refer to Section “Supported Platforms”	
NF. 83	Application can be configured for automatic load distribution and automatic scaling at the level of key components (lag sensitive applications). Scaling of the application will take place both up and down.	Recommended
Reply	Please refer to Section “Supported Platforms”	
2.9. The technological and infrastructure requirements		
NF. 84	The technological and infrastructure architecture represents all software and hardware components necessary to ensure the operating environment in which all solution components shall run. The technological platform includes development platforms, database management systems, operating systems that can run solution components, specific system software required to be installed for correct run of the solution, hardware platform that can run solution components, etc. In order to be scalable, flexible and easily maintainable, it is recommended that all solution components have a minimum level of dependence on the technological platform on which it runs.	Recommended

Reply	Please refer to Section “Component Based Architectural Style”, “Layered Architectural Style” and “Service-Oriented Style”	
NF. 85	Platform technologies presented in the solution architecture shall be open technologies or widely used technologies.	Mandatory
Reply	SmartVista embraces open standards and makes use of all of the following: • Java-related stack; Java/J2EE, Eclipse, Jenkins, Maven, Gradle, FindBugs, PMD, Subversion (svn), JSF, EJB, JPA, CDI, Servlet, PrimeFaces, Spring, SLF4J, Logback, Apache commons, Apache CXF, Woodstox, Jackson & IzPack • C-related stack; ANSI C, Shell scripting, Eclipse / Source Navigator, Autotools, Jenkins, CUnit, splint, valgrind, Subversion (svn), POSIX and X25, cURL (http/https), OpenSSL, LIBXML2 (xml), libevent2 & gSOAP (soap) SQL-related stack; PL/SQL (Oracle), SQL/PL (DB2), ANSI SQL (SQL/MX), PL/SQL Developer, SQL Navigator, Eclipse, Toad, Jenkins, Subversion (svn), Enterprise Other than a hardware platform on which to operate, SmartVista requires a minimal set of third party software in order to operate. These are listed below. It should be noted that SmartVista products do not link in third party libraries. This ensures that in committing to SLA’s, BPC are fully in control and not reliant on support from other parties who may not be able to achieve similarly high SLA standards. Server side software: • Operating System (any POSIX compliant UNIX system such as HP-UX, AIX, Solaris and Linux) • Database (Oracle; versions 9 through to 12 supported) • Java Application Server o Oracle WebLogic Server (preferred) or IBM WebSphere • Java Virtual Machine (JVM) Client side software: • Microsoft Windows • Internet Browser (Firefox is preferred)	
NF. 86	To run the application it will require only standard equipment, available to be purchased by NBM freely on the market.	Mandatory
Reply	Please refer to Section “Supported Platform” and Section “ Recommended Platform”	

NF. 87	The application must support the creation, modification, processing, storage and access for text data in Unicode format.	Mandatory
Reply	Unicode and double-byte encoding is supported by solution design.	
NF. 88	The IPS system must include clearly defined system administration procedures, which should be automated as far as possible.	Mandatory
Reply	SmartVista solutions administration includes System Administration and Business Administration. System Admnistration: User and Role Administration: • User's access to system pages • Actions that the user can perform • Visibility of buttons and other controls • Adding, editing, and deleting roles • Embedding roles in other roles • Viewing registered users • Adding and deleting users • Assigning roles to users • Changing a user's password • Assigning institutions and agents to users • Changing the user status (blocked or active) • Changing the user's type (global administrator, local administrator, or general user) • Auditing user sessions • Auditing user actions Auditing: • The user's login • The user's IP address • Date and time of the user's last logon attempt • Date and time of the user's last logoff attempt • Date and time of the user's action User Privilges: • Address of the user's machine on the computer network used to access the SmartVista system • Date and time of the user's action (the time displayed is accurate to one microsecond) • System object type affected by the user's action • System object identifier affected by the user's action	

	• Action status (successful or failed) • Name of the modified database column • Type and format of modified data • Previous parameter value if the value was either updated or deleted • New parameter value if the value was updated and inserted Logging Levels: • 0 — most detailed information • 1 — low level debugging information • 2 — content of variables, and so on • 3 — information to be used for testing purposes • 4 —production mode messages, such as debugging and error messages. The information is PCI-DSS compliant. • 99 — no messages are logged Process Files: • Identifier of the session when the process was run • Name of the process file • Process that created the log • Date and time when the file was created • Purpose of the file, for example, a posting file • Logged trace message text based on the level of tracing detail (Fatal error, Error, Warning, Info, or Debug) • Information about transactions performed by the process files • Information about the specific reports generated for the processes System Monitoring: • Health of the Switch processes • Switch system queues (queue size for each Switch process) • Transactions per second (approved versus declined for different transaction types)	
NF. 89	The IPS system must include clearly defined system maintenance procedures. *Vendor shall describe required maintenance procedures and periodicity of those procedures.*	Mandatory
Reply	Please refer to 'BPC AG MAINTENANCE AGREEMENT.docx' and 'BPC AG PROFESSIONAL SERVICES AGREEMENT.docx' documents.	

NF. 90	The proposed solution will meet the minimal infrastructure requirements stated in ***Chapter 8.2. Additional information related to non-functional requirements***, ***Table 2*** - ***Minimal infrastructure requirements.*** *Vendor shall include in his offer detailed information on the recommended technology platform, taking into account the needs of NBM defined in this tender specification. If the case of the winning bid, this will be taken as basis for determination of technology platform related to the application.*	Mandatory
Reply	Please refer to section "Recommended Platform"	
2.10.	***Data Retention and Archiving***	
NF. 91	IPS must be able to store all operational data for a minimum of two years, without affecting its performance.	Mandatory
Reply	Please refer to section "Recommended Platform"	
NF. 92	IPS must ensure that the system operator is able to retrieve transaction data and data on participants in the system up to 10 years. *Different access methods should be implemented for "recent" and "old" transactions.*	
Reply	See NF.91	
NF. 93	The IPS system must support the efficient data archiving procedures. *Vendor has to describe archiving approach and automated/manual procedures*	Mandatory
Reply	The archiving mechanism is based on use of backup and archiving tools. We recommend use of external virtual and physical tape librarians and devices to take incremental and full snapshots of the database and the system images.SmartVista supports Oracle partitioning by design as well as partitions for archiving and purging.	
NF. 94	The IPS system must maintain sufficient information for audit purposes for a period of at least seven (7) years.	Mandatory
Reply	SmartVista allows to configure the period	
NF. 95	The IPS system must provide an efficient data archiving solution for data protection based on flexible backup-restore approach	Mandatory

Reply	SmartVista provides a range of backup and recovery scenarios, from manual to fully automatic, based on SmartVista , UNIX and Oracle (Oracle Recovery Manager) tools and features	
2.11. Requirements for environments		
NF. 96	IPS will operate at least the following environments for the tendered solution: - Production – This will be the main environment to deploy the solution for production; - Testing and Developments - IPS will maintain the development and the test environments even after going into production, for development and testing purposes; - Back-up - For resilience and back-up purposes IPS intends to implement an active/ active failover node architecture. In this regard, the Tenderer will consider these facts, when calculating the number of licenses.	Mandatory
Reply	Considered in Sizing. Please refer to Section “Recommended Platform”	
NF. 97	The solution will have in place mechanisms to assure the transfer of data between different environments.	Mandatory
Reply	Please refer to Section “Supported Platform”.	
NF. 98	The solution shall have in place some mechanisms to assure puzzling or depersonalization of the data when copied from production to test environment.	Recommended
Reply	SmartVista also supports encryption/decryption/masking of the data by use of specific Tokenizer module developed in-house by BPC. The module is responsible for protecting the sensitive data to comply with PCI DSS requirements.	
2.12. Source Codes		
NF. 99	The Tenderer undertakes to provide for the application that is part of the offered solution (including third parties) guarantees regarding the transmission of source codes in cases where for some reason the software supplier will not be able to maintain it (eg. liquidation, bankruptcy,	Mandatory

	reorganization etc.). In the event that the source code can not be transmitted, it is necessary to provide an escrow commitment.	
Reply	Please find Software Escrow Agreement template included.	

8.2. Additional information related to non-functional requirements

Table 2: Minimal infrastructure requirements

Client side:	HW requirements	Requirements for HW should be as minimal as possible. It must run on VDI infrastructure of NBM without any visible impact on the performance of the virtual desktop machine.
	Operating environments	Windows 10/ VDI Citrix XenDesktop 7.5 and newer operating systems
	Software type:	Recommended: Thin client running on standard Web browser (IE, Chrome, Mozilla)
Server side:	Supported HW platform	x86 platform
	Supported operating systems	Linux or Windows Server family
	Supported versions for operating systems	OS must be maintained by their manufacturers and to be one of the last two major versions
	Supported database systems	Oracle 19c or MS SQL 2019, or newer versions
	Requirements for virtualization	Must support virtualized infrastructures based on Xen or VMware hypervisors
	The minimal accepted requirements for cryptographic algorithms in NBM	a. AES-256 for encryption of electronic data; b. SHA-2 for message digest; c. RSA 2048bit for end-point private keys.

IMPLEMENTATION REQUIREMENTS

9.1. Project management requirements

Req. ID	Requirements	Classification
1. General project management requirements		
IR.1.	The goal of project management is to provide the necessary skills for project organizing and management to successfully achieve the set objectives. During the project life cycle there should be assured efficient resource planning and allocation, progress control during each stage, quality monitoring and evaluation of the deliverables, etc.	Mandatory
Reply	BPC commits to ensuring sufficient resources, of good quality will be assigned to ensure a quality delivery – in line with our ISO 9001 and PMI-based Project Methodology. Refer to the accompanying draft PMP, as well as information provided regarding our project organization, approach and deliverables.	YES
IR.2.	The Tenderer is responsible for the implementation project management, as well as for execution of activities and project plan mutually agreed with the Beneficiary. The Tenderer is responsible for identifying and mobilizing the adequate resources to execute the project plan activities in his responsibility, at the agreed quality level.	Mandatory
Reply	This is understood and agreed. Roles and responsibilities are documented within the draft PMP and planning will be discussed and agreed, in detail, as part of Project Initiation – or sooner, if sufficient detail is available to allow this.	YES
IR.3.	The Beneficiary is responsible for all procedural and administrative matters relating to the launching, contracting and financial management of the project (including payments) related to project implementation activities.	Mandatory
Reply	All tasks and activities under our control – we will manage any procedural and administrative aspects. Where there is a shared responsibility, we will coordinate with you to ensure timely handling of these matters.	YES
IR.4.	A well-known project management methodology or standards (e.g. PRINCE2, PMBOK etc.), or an internal developed methodology, based on	Mandatory

	these standards or methodologies, shall be used for the implementation project and shall be appointed specifically.	
Reply	Agreed. We make use of a PMI-based methodology, as described in our draft PMP.	YES
IR.5.	In order to organize the project, the Tenderer shall appoint a Project Manager, who will manage the project team.	Mandatory
Reply	Agreed. This is standard practice.	YES
IR.6.	A detailed project organizational chart covering the key roles will be provided as part of the tender. For each role, the Tenderer shall describe the main responsibilities. Members of the Steering Committee, Project Management team, Functional teams, Technical experts, Support team etc. will be clearly identified in the project organizational chart. This chart shall be part of Project Initiation Document (Initial Project Management Plan).	Mandatory
Reply	The Project Organizational Chart is included in our response and confirmed – it is included in our draft PMP.	YES
IR.7.	The Tenderer Project Manager has the authority and responsibility to coordinate project implementation, so as to successfully achieve the project objectives set. The main responsibility of Project Manager is to ensure that all required deliverables are submitted on time and meet the expected quality standards.	Mandatory
Reply	This is understood and confirmed. Refer to the draft PMP for roles as responsibilities, as well as the section on our approach to Project Management.	YES
IR.8.	The Project Manager will ensure a proper management of project risks, quality and progress control of deliverables at every stage of the project. It will also be provided a control of interdependencies between the project components to minimize any risk of project stagnation.	Mandatory
Reply	The project manager will manage all aspects of the project, including risks, quality, scope and more – in line with the draft PMP and PMI (PMBOK) standards.	YES
IR.9.	The Project Manager will ensure an effective communication within the project, through progress reports with a weekly frequency toward project manager of Beneficiary and with a monthly (or when is necessary) frequency toward Steering Committee Group of the Beneficiary, and also phase report for end of each project stage. Simultaneously, the Tenderer	Mandatory

	shall provide an adequate level of transparency in project management through adequate documentation (e.g. minutes of meeting, weekly progress report, etc.) of all project management aspects.	
Reply	Communications Management is part of our PMI-based Methodology and is described in our draft PMP. Exact details will be discussed and agreed during the project kick-off, but can be aligned as suggested.	YES
IR.10.	The Project Manager of the Tenderer has the authority and responsibility to conduct daily project activities.	Mandatory
Reply	Agreed. An assigned project manager must have sufficient authority to perform the required role.	YES
IR.11.	The Project Manager of the Beneficiary has the role to organize the Beneficiary's resources so that they are useful to the project and available as needed to the project plan. The Project Manager of the Beneficiary provides official interface of communication of daily issues and of reporting regarding project progress between the Project Manager of the Tenderer and Beneficiary	Mandatory
Reply	The Project Manager will perform resource management and task allocation/planning – in line with the PMP. The PM will be the primary point of contact during the entire project.	YES
IR.12.	Team leaders may be appointed by the Tenderer, having the role of an intermediary in the communication and control process. The Beneficiary shall appoint one or more members of those teams made by the Tenderer. This will facilitate communication between the parties and will minimize official contact points between the teams. The primary responsibility of a Team Leader is to ensure the achievement of deliverables under the conditions set by the Project Manager of the Tenderer.	Mandatory
Reply	Team Members and Communications lines will be handled efficiently and in line with best practice and agreed protocols.	YES
IR.13.	The Tenderer is required to ensure timely resolution of identified issues related to its direct responsibility and include in its tender a description of the mechanism of escalation / resolution of identified issues.	Mandatory
Reply	The Project Manager will make use of a RAID Log for management of Risks, Assumptions, Issues and Dependencies.	YES

	Our structure is relatively flat and the escalation process and people involved will be made fully clear.	
2. Project management activities and deliverables requirements		
IR.14.	The main Project Management activities: a. Provide the initial project management plan covering at least the following initial items: project plan (stages, phases, milestones, duration, responsibilities, etc.), roles description, quality management plan, risk management plan (including initial identified risks and related remediation measures), resource management plan, change management plan, communication plan, annexes (forms of all project management documentation, e.g. of reports, minutes of meeting, acts, etc.). b. Adjust the project management plan at the project start, based on agreement with NBM. c. Adjust the project management plan on a need base during the project timeframe, based on agreement with NBM. d. Organize the kick off meeting and the project meetings (ex. Steering Committee meetings etc.) together with NBM. e. Execute and monitor the project and provide weekly and monthly/or as needed recurrent project reporting, end of phase reporting in a format agreed by parties. f. Close the major project phases and provide the draft of the acceptance documents to NBM prior to formal acceptance. g. Preparation and presentation the end of phase report. h. Preparation and presentation of the progress report on a monthly basis (or when is necessary) to the Steering Committee Group	Mandatory
Reply	The PMP and Detailed Project Plan (Schedule) can be handled in the way described, remaining in line with our methodology in the process.	YES
IR.15.	The main Project Management deliverables: a. Initial project management plan. The detailed requirements concerning the project management plan are listed further. b. Updated project management plan.	Mandatory

	c. Support presentation for the kick off meeting and for other project management meetings such as Steering Committee presentations. d. Weekly reporting comprising status report (including decisions that need to be taken at project management and/ or Steering Committee level), issue list, risk register, changes register. The weekly progress reports will comprise at least the following: date, reporting period, implementation schedule status, performed activities, forecasted activities, completed deliverables, identified issues and risks, remediation measures, deliverables to be completed during the next reporting period, raised change and their impact analysis, "to do" list. e. End of phase reports to contain the following: overview of the completed phase, overview of the project plan for the next period, deviations from the project plan, acceptable deliverables, risk analysis, status of project issues, project quality register. The end of phase reports will be presented in the format agreed with the Beneficiary. f. Monthly (or when required) report – special reporting for the Steering Committee of the project. The Progress report on a monthly (or as required) basis to the Steering Committee Group must reflect an overview of the status of the project at the time of reporting, completed stages, deliverables, next project activities, deviations from the project plan, risks , problems and remedial measures, change requests (if any) and other relevant elements for the beneficiaries of this report. Progress reports on a monthly or as-needed basis to the Steering Committee Group will be submitted in the format agreed with the Beneficiary. g. Exception Reports to contain the following information: description of the causes of deviations, the impact of deviations, proposed problem-solving options and their impact on the general tolerances of the project, recommended option by the Project Manager of the Tenderer. *The Tenderer shall include in his Tender models samples for each of these reporting items.*	
Reply	A template of the Weekly Project Report is embedded within the draft PMP. A template Project Kick-off Presentation can be provided, on request. We have no specific standard templates for Monthly and Exception Reporting, but formats can be agreed as part of Project Initiation.	YES
IR.16.	Acceptance criteria for project management deliverables:	Mandatory

	a. The deliverables are provided to NBM according to the agreed terms. b. NBM has no observations regarding completeness and correctness of the document in accordance with quality and other agreed criteria.	
Reply	This is understood and accepted.	YES
3. Project management plan requirements		
IR.17.	The Tenderer shall submit as part of his tender the initial version of the initial management Plan of the project. The Content of these documents will be: 1. Introduction – project context 2. Project description: a. Project objectives b. Project scope of work and out of scope c. General approach (methodology and tools used, own team or subcontracting, etc.) d. Project deliverables and other expected results e. Constraints f. Key success factors 3. The project organizational chart – chart and description of roles and responsibilities 4. The work breakdown structure **5. The major deliverables description sheets** a. The deliverables description shall cover: deliverable name and/ or code, goal, contents, format and presentation, deliverable responsible, quality criteria for the deliverable and the method in which the quality will be tested by the quality responsible, resources required for testing the quality of the deliverable. b. The presented quality criteria will not be ambiguous and present measurable aspects. c. Criteria for deliverables approval shall be:	Mandatory

i. Compliance with requirements submitted to the deliverable.

ii. The extent to which responds to the objectives of the project.

iii. Performance indicators as appropriate.

6. Project plan

a. The initial project plan will list the major phases and work packages, major activities, start and end date, duration, milestones, together the responsibilities, interdependences, external dependencies; also the critical path will be shown.

b. In case the Tenderer will subcontract the activities to obtain some deliverables, he will present Work Packages associated to these activities. The structure of a Work Package will comprise: date, responsible, description of the work package, quality inspection methods to be used, level of resources that will be allocated, begin and end date, constraints, method of reporting. The work packages will be signed by both the subcontractor and the prime Tenderer.

c. The project plan will clearly show the total planned duration of the IPS implementation project. The project plan will also include the activities such as review and coordination of deliverables and acceptance documents by the parties (Bidder and Beneficiary), with the allocation of the necessary time terms

d. The working hypotheses for drafting the initial plan will be presented. Given the complexity and long duration of the project, the months of July and August will be considered as a holiday period for the NBM team.

e. The Tenderer will present the tolerances for the overall project plan and for each of the major phases. The Tenderer will present the method by which the Project Manager will ensure the tolerance control at each stage and procedure that will be applied when these tolerances are exceeded. For this project, the cost tolerances are not permitted, the project budget being fixed.

f. Time tolerances for the entire lifetime of the project is plus 40 working days. The tolerances level phases/activities shall be distributed as needed throughout the project by mutual agreement of the Parties, at the project manager level of both Parties. If a stage is completed later from the time tolerance account, the next stage can be started later on account of this tolerance, but the tolerances for the whole project cannot exceed 40 working days.

g. A Gantt diagram is required for the project plan. Along the project, the project Manager shall use a dedicated project management software/ instrument which will be indicated in the tender.

h. During the contract execution, each stage of the project will be preceded by a review and update and, where appropriate, a further detail of the stage plan to ensure its optimal management.

7. Quality management plan

a. The quality management plan will comprise:

i. Responsibilities for quality assurance.

ii. Reference to the standards to be met.

iii. Identifying the key quality criteria to be achieved.

iv. Control and audit methods for quality of project management deliverables and for those technically specialized.

v. Other tools for quality assurance.

b. In order to register the quality checks to be made on deliverables, the Tenderer shall keep a Quality Register, which will contain the following: deliverable, quality inspection method, results of verification, corrective activities, planned date and actual date of approval.

8. Resource management plan

a. The resource management plan will include for each proposed activity the amount of resources (expressed in man-days/hours) expected to be allocated by the Tenderer, on-site

	and off-site, and number of persons by categories to be allocated. b. The resource allocation plan will also detail the reserve component mentioned in Chapter 4, section 1 “1.4. Financial tender and other costs”. c. The resource management plan will include for each activity proposed the necessary resources to be involved from the Beneficiary, describing the functions and duties of each team member of the Beneficiary and the estimated workload for each task for each staff category. **9. Risk management plan** a. The risk management plan will describe the risk management processes, risk management strategies, risk management responsibilities and specific procedures for risk identification, reporting, escalation etc. b. The Tenderer shall submit the initial Risk Register as part of project management plan. The Risk Register will be filled in with project specific risks and will contain for each identified risk, at least the following information: risk ID, type of risk, identification date, date of last revision, risk description, probability, impact, severity, counter-measures, the risk responsible, risk status (e.g. open, closed). The risk register will structure the risks identified based on categories, e.g. Project management/ Resources/ etc. and also based on project phases, e.g. Analysis/ Design/ etc. **10. Change management plan** a. Change management plan will treat the situations that might appear due to scope change, inclusive scope extension based on reserved resources according to Chapter 4, section 1 “1.4. Financial tender and other costs”. b. The Tenderer shall provide a change process map and also shall describe the process - the steps, roles involved and templates to be used, including the mechanism of identifying/ monitoring/ reporting/ approving/ rejecting change requests, responsibilities and escalation procedure.	

	c. The Tenderer must include an impact analysis in the change process. d. The Tenderer shall provide an example of change requests register. **11. Communication plan** a. The communication plan refers to the interactions between the Beneficiary's project manager, the Tenderer /project manager and other project stakeholders. b. The communication plan will comprise: i. identifying the project stakeholders ii. information needed per each group of stakeholders iii. information source iv. frequency of communication v. content of the communication vi. the responsible persons for the development and the transmission of communications. **12. Project controlling and monitoring mechanism** a. Description of the how the project monitoring & controlling will be performed during the project (e.g. Reporting mechanisms – weekly and monthly reporting, end of phase reporting, exception reporting). b. Description of weekly/monthly reports comprising model c. The procedure for handling project deviations and exceptions d. Contingency plans 13. **Approval plan**, which will present in a condensed form each type of deliverable and how this deliverable is approved. 14. **Project library** – description of how the project documents and deliverables will be stored, found and retrieved.	

	15. **Appendixes** – will include all the templates used for project management (e.g. minutes of the meeting, weekly report, end of phase report, risk registry, questionnaires, etc.)	
Reply	The provided draft PMP covers almost all of these items. Typically items such as a Quality Plan are not separate documents – though this could be arranged, if required. We have indicated elsewhere in our response that we anticipate a duration of 18 months – though opportunities exist to shorten this. A Detailed Project Plan (Schedule) with start/end dates, dependencies – specific to NBM is not possible at this time, as a fixed starting date is unknown, the exact scope is not fully agreed and many other project details have yet to be discussed. Whilst we can share an 'example' plan, we prefer to avoid 'guessing' with regards to many aspects of the project. We do, however, feel confident – based on what we currently know, alongside the strength of our solution and experience in delivery – that we can comfortably achieve the target timeline. We look forward to working in partnership with you to develop a realistic and though-through planning, that all parties can support – in due course.	YES

9.2. Software development lifecycle requirements

Req. ID	Requirements	Classification
1. Business Analysis Phase		
IR.18.	***Phase objectives:*** 1. The purpose of this phase is to create common understanding of the target solution, explain the priorities within review them against the chosen solution and to create detailed software requirements specification (SRS) and acceptance criteria of the solution. This documentation shall ensure a common understanding of the processes, requirements and major gaps in the chosen solution in order to implement a solution that meets the expectations of the NBM. 2. It is expected, that this phase will build upon requirement specifications available in already in this RFP and on the proposal of the	Mandatory

	Tenderers, which will identify to which extent the target solution will cover the requirements within out of the box functionality and which will require customization/custom development of the target solution. 3. Each one requirement will be identified and tracked through the whole development lifecycle in order to be able to map it anytime to the functional specification, acceptance criteria, test cases/scripts and particular parts of the system itself. The responsibility for the requirements traceability is on the Tenderer and this activity must be executed continuously during the implementation.	
Reply	The process, as described, is accepted – though our SRS is typically „embedded" within our FSD. A Requirements Traceability Matrix is good „best practice" software development – though the vast majority of functions will be delivered by the „out of the box" product – so may be harder to trace. We are, however, generally fine with the approach.	YES
IR.19.	***Main activities:*** 1. NBM will present thoroughly current and future requirements regarding the project scope. 2. For each part of the designed process and requirements successful Tenderer will demonstrate vanilla version of the solution and explain the way how the system works. For all core functionalities, Tenderer will prepare prototyped screens adjusted to NBM requirements. 3. All gaps identified during the RFP will be reviewed in detail and adequate solution will be proposed by the Tenderer. 4. Define the data quality assurance strategy / model. 5. Analyze the information about users and their roles. 6. Review the existing IT and network technical infrastructure and to develop proposals / recommendations for architecture and related infrastructure of the Solution, considering keeping under control the complexity of IT infrastructure and reusability of existing resources. 7. The work will be performed mainly via interviews, workshops with business and technical staff from the NBM, analysis of relevant detailed documentation. The Tenderer shall describe the methodology and	Mandatory

	instruments used for analysis phase and shall provide sample of deliverables.	
Reply	This approach is generally acceptable to us. Sample deliverables cannot be shared, due to customer confidentiality – though a standard FSD template can be provided, if required.	YES
IR.20.	***Deliverables:*** At the end of this phase, the following will be delivered: 1. Detailed software requirements specification of the solution proposed for the implementation with clear link/track of the particular requirements to the process(es). 2. Detailed acceptance criteria. 3. Concept of data model of the Solution. 4. Conceptual architecture of the solution and infrastructure diagrams. 5. Detailed and updated (within given timelines) project plan for the rest phases of the implementation. 6. Detailed, accurate and up-to-date task/issue/risk log. 7. Updated set of deliverables. 8. Other documents according to the best-practice and delivery methodology of the Tenderer necessary for the achievement of project objectives.	Mandatory
Reply	This is acknowledged and accepted. Further detailing of the process and the various project artefacts in which they will appear can be discussed at a later point.	YES
IR.21.	***Acceptance criteria:*** 1. The acceptance criteria shall be revised and agreed with the NBM at the beginning of the initiation stage. The below mentioned criteria are minimal and shall not be subject of elimination. 2. The deliverables of the analysis phase shall be provided to the NBM as in accordance with the project plan.	Mandatory

	3. NBM shall not have any objections regarding the completeness and correctness of the document, in accordance with agreed quality and other criteria. 4. Deliverables meet the NBM expectations and requirements in terms of clarity, level of detail, structure, content, etc. 5. Deliverables are aligned with internal standards of the successful Tenderer and best practices. 6. Deliverables are easy to use and understandable to the intended beneficiaries. 7. Deliverables are aligned with quality standards agreed between the NBM and the successful Tenderer. 8. Acceptance documentations for the analysis phase are approved by the Parties.	
Reply	We are happy to confirm these requirements as acceptable to us.	YES
2. Design Phase		
IR.22.	***Phase objectives:*** 1. The purpose of this phase is to define the design and settings of the solution proposed to be implemented. During this phase, the successful Tenderer shall translate functional requirements into a workable design (functional specification), support the analysis by delivering prototypes of designed features and shall prepare the necessary environment for the development / configuration of the solution.	Mandatory
Reply	Design details are generally contained within our FSD. Prototypes are possible, in line with agile delivery.	YES
IR.23.	***Main activities:*** 1. Define and produce a functional specification that would meet the requirements, given the functional and technical constraints imposed. 2. Document design specifications for solution functionalities based on the software requirements specification (including the link of them to keep clear traceability). 3. Document detailed specifications of the solution: interaction interfaces and diagrams (Data Flow Diagrams), Use Cases, retrieval	Mandatory

	scenario, validation scenario, data uploading scenario, analysis scenario, etc. 4. Document test strategy and test analysis in connection to the acceptance criteria and functional specification. 5. Establish the applicable configuration parameters. 6. Transform data model from previous phases into logical and physical data model. 7. Review the changes to be made in the data model. 8. Review and confirm data sources. 9. Define the specifications for customization, configuration and integration with other sources of data/applications. 10. Develop/improve the system architecture to support technical requirements of the previous stage. 11. The Tenderer shall describe the methodology and instruments used for the design phase and shall provide a sample of deliverables.	
Reply	This approach is generally acceptable to us. Sample deliverables cannot be shared, due to customer confidentiality – though a standard FSD template can be provided, if required. Please also refer to the provided test scripts, as well as information on our approaches to Design and Testing, documented within this response.	YES
IR.24.	***Deliverables:*** 1. Document on the detailed functional specification of the solution, which shall cover both technical and functional aspects. From a technical standpoint, the deliverable shall document the solution architecture (applications/tools, model integration of these, data model, interfaces and interaction diagrams, security, etc.), and technology platform agreed and signed by both parties. The document shall include the following information: a. solution overview (diagrams that provide an overview of the solution architecture accompanied by a narrative description); b. integration platform of solution components, interfaces (the name that will be integrated with the solution, the type of interface (e.g.,	Mandatory

	supplier, consumer, symmetric), solution and the impact of the failure of the interfaces); c. solution architecture attributes (software and hardware technologies, services, components, portability, capacity, availability and reliability, scalability); d. Continuity plan and disaster restoration - BCPDR (specifying architectural attributes necessary to meet solution requirements for BCPDR); e. data architecture (context diagrams, logical data model); f. security architecture (overview of security solution); g. other aspects. 2. Document on solution configuration/setting up, which will document in detail all the parameters set for all components of the solution. 3. Document High Level Test Plan (HLTP) and test analysis that will link to and cover all above mentioned specifications. The HLTP shall prescribe the scope, approach, resources and schedule of the testing activities. It shall also identify the items to be tested, the testing tasks to be performed, the person responsible for each task and the risks associated with the test plan.	
Reply	This is generally acceptable, though we would like the opportunity to discuss this further – in order to better align our deliverables with your expectations.	YES
IR.25.	***Acceptance criteria:*** 1. The acceptance criteria shall be revised and agreed with the NBM at the initiation phase. The below mentioned criteria are minimal and shall not be subject of elimination. 2. The design phase related deliverables shall be provided to the NBM as per the project plan. 3. NBM shall have no objections regarding the completeness and correctness of the document in accordance with the agreed quality and other criteria.	

	4. Deliverables are in line with the NBM expectations and requirements – in terms of clarity, level of detail, structure, content, etc. 5. Deliverables are aligned with successful Tenderer's internal standard and with the best practices. 6. Deliverables are easy to be used and understood by the targeted beneficiaries. 7. Deliverables are in line with quality standards agreed between the NBM and the successful Tenderer. 8. NBM shall have no objections regarding chosen solutions. 9. An acceptance report shall be signed by both parties within the agreed time period.	
Reply	This is accepted.	YES
3. Build Phase		
IR.26.	***Phase objectives*** The purpose of this phase is to transpose functional requirements into application functionalities by applying the agreed solutions in analysis and design phase.	Mandatory
Reply	This is understood and accepted.	YES
IR.27.	***Main activities*** 1. Install the production, test, development and training environments (OS/DB/apps). 2. Implement customization, integration and configuration of the solution, according to specifications of the deliverables accepted at design phase. 3. Prepare backup and maintenance procedures. 4. Produce the blueprint for the logical and physical architecture of the application and database servers. 5. The Tenderer shall describe the methodology and instruments used for build phase and shall provide sample of deliverables.	Mandatory

	6. Test analysis is further detailed – complete set of test scripts is elaborated and finalized.	
Reply	This is generally understood and accepted – though we cannot be responsible for your operational procedures in relation to backup/maintenance – though we can offer advice.	YES
IR.28.	***Deliverables*** 1. Solution, configured and installed in: a. Production Environment b. Test and development environment c. Training environment 2. Solution shall meet the requirements agreed in the above chapters and that shall include: a. Functional and non-functional requirements provided in the analysis document; b. Validation rules, workflows, analysis scenarios, reports provided in the analysis document; c. Interfaces specified in the analysis document; d. Security (user rights, backup); e. Documentation provided as per NBM request; 3. Solution architecture document updated as necessary	Mandatory
Reply	This is generally understood and accepted – though "documentation… as per NBM request" needs to be further detailed.	YES
IR.29.	***Acceptance criteria:*** 1. The acceptance criteria shall be revised and agreed with the NBM at the initiation phase. The below-mentioned criteria are minimal and shall not be subject to elimination. 2. Deliverables shall be provided to the NBM as per the project plan. 3. NBM shall have no objections regarding the completeness and correctness of the document.	Mandatory

	4. Deliverables are in line with the NBM expectations and requirements – in terms of clarity, level of detail, structure, content, etc. 5. Deliverables are aligned with successful Tenderer's internal standard and with the best practices. 6. Deliverables are easy to be used and understood by the targeted beneficiaries. 7. Deliverables are in line with quality standards agreed between the NBM and the successful Tenderer. 8. An acceptance report shall be signed by both parties within the agreed time period.	
Reply	This is understood and accepted. Refer to our approach to the Implementation/Build Phase found in our response.	YES
4. Testing Phase		
IR.30.	***Phase objectives:*** 1. The purpose of this phase is to test the quality of all the functional and technical elements of the solution. During this phase, the successful Tenderer shall establish the testing method and shall prepare testing scripts for all testing activities that will cover the entire software development and implementation lifecycle. 2. The successful Tenderer shall include the proposed approach and methodology for testing in the technical proposal in line with the testing principles described below. The proposed testing approach shall be validated/ agreed with the NBM at project initiation phase. The successful Tenderer shall indicate in its technical proposal the software instruments that will be used in order to track and monitor the potential open tickets for defects repair. It is obvious must that NBM representatives need to have access to this application. 3. The successful Tenderer is also advised that for non-functional requirements testing, where applicable (e.g., performance testing, stress testing, etc.) an automated test solution shall be provided to the NBM.	Mandatory

	4. In case test results are poor (high rate of “failed” tests, more than 3 failed tests per application module), the entire module shall be considered “unaccepted” and sent back to successful Tenderer for testing purposes.	
Reply	This is understood and accepted. Refer to our approach to the Testing Phase found in our response.	YES
IR.31.	***Main activities:*** 1. Testing shall be performed according to the best practice (for ex. ISO/IEC/IEEE-29119or similar, and the test activities covered shall include: test planning, test specifications, test execution, recording of results, checking for test completion. 2. All testing to be performed shall be appropriately planned, prior to being executed. For each application, a High Level Test Plan (HLTP) shall be created (in design phase), according to the best practice (for ex. ISO/IEC/IEEE – 29119-3:2013) or similar - The Standard for Test Documentation. The HLTP shall prescribe the scope, approach, resources and schedule of the testing activities. It shall also identify the items to be tested, the testing tasks to be performed, the person responsible for each task and the risks associated with the test plan. 3. Test Specifications shall be developed, which are detailed descriptions of the tests to be carried out and are prepared on the basis of a HLTP. These shall include the test data specification to be used, the actual test steps, including actions and expected results. The test manager shall sign off test specifications prior to test execution. Test scripts shall be created from the test specifications. 4. Activities that will include validation of the test environment, running/re-running the test scripts, logging any issues and production of test reports. The test result shall be recorded for each test in the test script and the expected results shall be unambiguous, so that the testing process to be simple to determine whether each step has passed or failed. The result of each test shall be recorded and shall include the identity and version of each item subject to testing. The actual outcome shall be compared with the expected outcome and discrepancies logged. 5. Activities that are used to determine when testing is complete. Test results are compared with the exit criteria detailed in the test specification and when these correlate testing can be deemed complete.	Mandatory

	6. The proposed strategy of testing is presented below: 7. Unit test shall be carried out by the successful Tenderer' developers. This testing shall be performed directly at code level and shall be related to the ability of individual components of a system to function in the desired manner. 8. Integration testing shall cover the components that are assembled into subsystems and subsystems are linked to form complete systems. This type of testing shall be performed by successful Tenderer's team. 9. System testing covers the activities of testing to determine whether the system meets specified requirements. It shall be subdivided into functional and non-functional system testing: a. Functional System Testing ensures that the system operates in the way in which the business requires it to do so, while keeping in line with the design of the business process for which it was created. b. Non-functional system testing ensures that the system operates to a predefined quality level. The following set of tests shall be performed: i. Load – testing to ensure that a system can handle large volumes of users and data in line with the specification from Tender Documents. ii. Performance – performance testing to verify the performance of a system against expected numbers of users and transactions, measured against expected performance criteria. iii. Stress – as performance testing but the limits of a system are identified by increasing the frequency of transactions, the number of users and the amount of data flowing through the system until any further increase in load results in system degradation and/or failure. iv. Security – testing to ensure that data security (confidentiality, integrity, availability, non-repudiation) is provided in accordance with the stated requirements, respectively all security mechanisms are working properly. v. Usability – testing based on whether the users will actually like the system, includes screen and report layouts and the practicality of running the day to day business processes. vi. Storage – testing to ensure that the database at the backend of the system is capable of handling the expected amount of data once the system	

	goes live, allowing for archiving frequencies and unexpected data requirements. vii. Volume – testing that subjects the system to large amounts of data to ensure it can be handled and there is no unacceptable degradation of system performance. viii. Installation – testing to ensure that the system can be installed as required on all supported platforms/environments. ix. Documentation – testing to check whether the system documentation matches the actual software, including training and support documents. x. Recovery and continuity – testing to check the procedures to recover the system after a crash. 10. Developer (successful Tenderer) shall be responsible for documenting and delivering system tests scenarios with logs and results, as a prerequisite for the NBM acceptance process. During system testing, the NBM testing team shall participate as an observer (if applicable and/or possible). 11. Integration testing shall be performed to expose faults in the interfaces and in the interaction between integrated components. It will be carried out after functional system testing and prior to acceptance testing. Developer (successful Tenderer) shall be responsible for performing these tests. 12. Acceptance testing shall be the final stage of validation in the software development lifecycle (SDLC). NBM, with the successful Tenderer's support, shall perform this activity and the main objective is to ensure that the final system matches the original requirements defined by the business. NBM may choose to do any tests it needs, based on the usual business process. Testing shall be carried out based on users' requirements. It shall be performed under the responsibility of NBM to enable their determination as to whether accept the system software or not. 13. Developer (successful Tenderer) shall support NBM in UAT efforts to help identify problems and communicate them to the relevant team(s) for resolution. Developer's (successful Tenderer) Business Analysts shall act as the first line of support to the NBM testing team and help to resolve system usage problems and minor issues.	

	14. Re-Testing shall cover the repetition of a failed test after a fix has been implemented to ensure that the fix has worked. All tests that have failed shall be formally re-tested and signed off by the test manager. 15. Regression testing shall be performed to ensure that fixes introduced to software have not had side effects on the unchanged software and that the modified system still meets the original requirements. Regression testing shall be performed whenever the software or its environment is changed. 16. The successful Tenderer shall ensure the necessary services for all testing levels described above and also services that will cover at least: a. Prepare UAT documentation/ test scenarios, which shall be revised by the NBM and business consultants. After the NBM validates the test scenarios, these documents can be used for testing purposes. b. Agree acceptance criteria and testing strategy. c. Conduct acceptance test. d. Documentation of the testing results. e. Agree the issue list by categories. f. Agree the action plan for solving the issues. 17. The successful Tenderer shall describe the methodology and instruments used for testing phase and shall provide sample of deliverables.	
Reply	This is understood and accepted. Refer to our approach to the Testing Phase found in our response, as well as provided test scripts. Note – we would not typically produce UAT documentation/test scenarios for clients.	YES
IR.32.	***Deliverables:*** 1. Acceptance test plan agreed and 'signed-off' by both parties. 2. UAT documentation/ test scripts and scenarios agreed and 'signed-off' by both parties.	Mandatory

<table>
<tr><td></td><td>3. Test results documents.</td><td></td></tr>
<tr><td>Reply</td><td>This is understood and accepted.

Refer to our approach to the Testing Phase found in our response.</td><td>YES</td></tr>
<tr><td>IR.33.</td><td>Acceptance criteria

1. All tests shall be completed without severity levels 1 or 2. The severity of the problems found shall be defined according to the criteria below:

<table>
<tr><th>No.</th><th>Severity</th><th>Description</th></tr>
<tr><td>1</td><td>Critical

(fatal problem)</td><td>Central system functions fail completely and constantly or are missing. Complete and continuous central system failure.</td></tr>
<tr><td>2</td><td>High

(serious problem)</td><td>Vital or critical functionality for the intended use is missing or failing continuously or repeatedly. Vital or critical functionality for the intended use cannot be activated or fails continuously.</td></tr>
<tr><td>3</td><td>Medium

(general problem)</td><td>Important but non-critical or vital for the intended use system functionality is completely missing or failing continuously or repeatedly.</td></tr>
<tr><td>4</td><td>Low

(minor problem)</td><td>Certain functions are missing or failing. System works correct but esthetical problems occur. Certain functions work but not completely correct.</td></tr>
</table>

2. Issues with severity level 1 and 2 shall require immediate bug fixing, and it shall be mandatory for testing process to be continued.

3. Testing process shall consist of as many test cycles as necessary until all severity 1 and 2 is-sues will be eliminated. After a Severity 1 or 2 problems will be fixed, it is for the NBM testing team to decide whether test cycle will be restarted or continued.

4. The number of outstanding defects is below an acceptable upper limit (to be agreed before the acceptance phase) or the faults are minor.</td><td>Mandatory</td></tr>
</table>

	5. Acceptance document agreed and 'signed-off' by both parties.	
Reply	This is understood and accepted. Refer to our approach to the Testing Phase found in our response.	YES
5. Training		
IR.34.	***Phase objectives:*** 1. The Tenderer shall conduct staff training to ensure an adequate level of knowledge and skills to use and manage efficiently the solution. 2. The Tenderer shall conduct training sessions for the administration and maintenance and also for development teams designated by the Beneficiary to ensure a proper level of knowledge and skills as to be able to efficiently use the development tools available within the solution and to design and develop individually new scenarios for data source integrations, validation rules, data model, reports, screen forms, etc. 3. For some modules, the NBM reserves the right to require the Tenderer to test the participants' knowledge of the training. Modules for which the NBM will require the testing of knowledge will be agreed upon during the implementation of the project. For such cases, the Tenderer will prepare appropriate questionnaires.	Mandatory
Reply	This is understood and accepted. Refer to our approach to the Training Phase found in our response.	YES
IR.35.	***Main activities:*** 1. The Tenderer shall develop and agree with the Beneficiary the following elements of the training component:	Mandatory

	- Tenderer's strategy on training and knowledge transfer (including categories of users, optimal stages for their delivery, etc.); - Structure and content of the training course and manual for each user category. 2. The training course shall consist of different types of training, such as: - Training courses; - Presentations; - Workshops; - Self-learning materials or remote training; - Individual consultations. 3. The Tenderer shall use logistic facilities of the Beneficiary for organizing training sessions (room for presentations, projector, microphones, headphones for translation, Internet connection). If other technology or logistics facilities than those above-mentioned will be required when organizing training sessions, these shall be provided by the Tenderer. 4. The accepted languages for training sessions and documentation are Romanian or English.	
Reply	This is understood and accepted. Refer to our approach to the Training Phase found in our response. Note: Covid-19 limitations must be accounted for in relation to any classroom training.	YES
IR.36.	***Deliverables:*** 1. Plan / program and training curriculum. 2. Documentation of training by category. 3. Questionnaires for knowledge testing.	Mandatory

	4. Results of training quality assessment.	
Reply	This is understood and accepted. Refer to our approach to the Training Phase found in our response.	YES
IR.37.	***Acceptance criteria:*** 1. The training sessions have been organized. 2. Knowledge Testing Questionnaires demonstrate that end users have an acceptable level of knowledge. 3. The NBM has no objections regarding the integrity and the correctness of the training materials. 4. Deliverables correspond to the expectations and requirements of the NBM - in terms of clarity, level of detail, structure, content, etc. 5. An acceptance report shall be signed by both parties within the agreed time period.	
Reply	This is understood and accepted. Refer to our approach to the Training Phase found in our response.	YES
6. Go-live and final acceptance		
IR.38.	System operation in the production environment and final acceptance shall be made according to the following scheme: a) Go-live preparation phase; b) Soak period; c) Final acceptance;	Mandatory
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
6.1. ***Go-live preparation phase***		
IR.39.	***Phase objectives:*** 1. The purpose of this phase is to facilitate the decision making process in regard with lunching the solution into production.	Mandatory

Reply	This is understood and accepted.	YES
IR.40.	***Main activities:*** 1. Review and assess readiness from multiple perspectives: a. IT readiness criteria: i. production system fully delivered and functional; ii. configuration document and design specification written and a handover made to the future Service Manager of the software; iii. User manual and Admin manual for the application delivered; iv. maintenance process agreed; v. backup process agreed, documented and tested; vi. technical training delivered; vii. no critical defects present after moving into productive environment, unless they are known and approved by the Beneficiary; b. Business readiness criteria: i. all functionalities required are present in the application; ii. no critical or high defects present; maximum of 15 medium and 30 low defects are acceptable; iii. reports are running and generating the correct output; iv. the data loss possible if the application crashes is not exceeding the RPO; v. help mechanisms for users are available; vi. user rights implemented according to the specifications; vii. user training performed. 2. Remediation Plan for defects is developed (defect list may contain defects with severity level 3 and 4). 3. The Tenderer shall describe the methodology and instruments used for go-live preparation phase and shall provide sample of deliverables.	Mandatory

Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response. No sample of deliverables of this nature can be shared at this time – as they tend to be very client specific.	YES
IR.41.	***Deliverables:*** 1. The solution is ready for launching into production (the solution was installed on production environment, testing was performed and no severity 1 and 2 defects were found). 2. Remediation plan for defects. 3. Successful Tenderer's self-assessment report of business and technical requirements (this document shall cover at least the following information: requirement identifier, solutions associated with the requirement, % of requirement coverage in the application).	Mandatory
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
IR.42.	***Acceptance criteria:*** 1. All above-mentioned criteria (as assessment activity) have status "passed". 2. The remediation plan is defined and agreed by both parties. 3. Successful Tenderer's self-assessment report demonstrates that all business and technical requirements were fully delivered. 4. An acceptance report shall be signed by both parties within the agreed time period.	Mandatory
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
6.2.	***Soak period***	
IR.43.	***Phase objectives:***	Mandatory

	1. The purpose of this phase is to extensively test solution behavior in daily operation to determine whether the solution meets the required qualities of capacity and stability. 2. This phase shall be performed during a minimum period of 20 business days. 3. During this phase, the NBM shall draft its own self-assessment report, which will be compared with that provided by the Successful Tenderer at the end of Go-live phase. 4. In case significant discrepancies are found (between the NBM assessment and successful Tenderer assessment), NBM reserves that right to ask the successful Tenderer to fix or improve the coverage degree of certain business & technical requirements.	
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response. Note: Your "Soak Period" is similar to typical "Pilot Testing".	YES
IR.44.	***Main activities:*** 1. Provide extensive offsite and if needed onsite support during the entire soak period for bug fixes and performance issues: log inspection and analysis/ problem prevention/ fine tuning. 2. For defects identified during soak period, a remediation plan shall be agreed. 3. Solving of defects identified in remediation plan approved prior to go-live phase and also identified during soak period. 4. Providing assistance (help desk support) for end users. 5. Assistance for active monitoring of system's parameters. 6. If needed, the Tenderer shall provide any additional configuration or customization required in the solution, in order to comply with the formal requirements set. 7. If needed, the Tenderer shall provide improvement works for system performance with regard to its accessibility and efficiency.	Mandatory

	8. The Tenderer shall assist the Beneficiary in system administration/management. During the soak period, the Tenderer shall ensure full transfer of knowledge to the Beneficiary for proper system administration/management. 9. The Tenderer shall assist the Beneficiary in providing I and II line support to the internal users of the Beneficiary and the reporting entities.	
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
IR.45.	***Deliverables:*** 1. Remediation plan fully executed and all defects removed. 2. Status on remediation plan for defects occurred prior to and during soak period (weekly reports).	Mandatory
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
IR.46.	***Acceptance criteria:*** 1. All defects included in remediation plans are fully removed. 2. No major bugs identified during soak period. 3. No discrepancies found between the NBM self-assessment report and successful Tenderer self-assessment report. In case discrepancies found, these shall be removed prior to final acceptance of soak period. 4. An acceptance report shall be signed by both parties within the agreed time period.	Mandatory
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
6.3.	***Final acceptance***	
IR.47.	***Phase objectives:***	Mandatory

	1. The purpose of this phase is to formalize the complete delivery of system functionalities, documentation and services. 2. Such acceptance shall be signed after formally closing the soak period for the solution. 3. After this final acceptance, the NBM shall approve the final instalment payment and the contract of guarantee will become active.	
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
IR.48.	***Main activities:*** 1. Review and assess the criteria defined below for final acceptance of the solution. 2. Criteria list for solution final acceptance is provided below. NBM shall align and detail together with the successful Tenderer the acceptance criteria at project initiation stage. a. Documentation/ deliverables for analysis phase provided and accepted by the NBM; b. Documentation/ deliverables for design phase provided and accepted by the NBM; c. Documentation/ deliverables for build phase provided and accepted by the NBM; d. Documentation/ deliverables for test phase provided and accepted by the NBM; e. Documentation/ deliverables for soak phase provided and accepted by the NBM; f. Documentation/ deliverables for training phase provided and accepted by the NBM; 3. Criteria list for general acceptance is provided below. NBM shall align and detail together with the successful Tenderer the acceptance criteria at project initiation stage:	Mandatory

	a. All above-mentioned documentation & deliverables are updated and fully provided by the successful Tenderer. b. Services included in the tender were fully executed by Successful Tenderer. c. All deliverables meet the quality criteria (quality assessment)	
Reply	This is understood and accepted. Refer to our approach to the Go Live & Final Acceptance Phase found in our response.	YES
IR.49.	***Deliverables:*** 1. Criteria list revised and agreed by both parties.	Mandatory
Reply	We are happy to discuss and agree this.	YES
IR.50.	***Acceptance criteria:*** 1. All acceptance criteria were met. 2. An acceptance report shall be signed by both parties within the agreed time period.	Mandatory
Reply	This is understood and accepted.	YES
7. Solution documentation		
IR.51.	As deliverables of the project, the successful Tenderer shall provide at least the following documentation: 1. User instructions and users guide: this document shall provide sufficient details, understandable by end users regarding functionalities, operations. The document shall describe the steps and actions to be performed in application and also print screens shall be included, tips & trick, FAQ etc. The purpose of the document is to represent a basis for learning process and also a reference point for users in case information about operating applications is needed. The user guide shall be provided in Romanian or English. 2. System operating instructions - work instructions: a. Maintenance instructions/service management troubleshooting guide: this document shall include all known errors and solutions associated	Mandatory

	and shall provide sufficient technical details in order to correct potential errors. b. Installation manuals, including system modifications at the level of application and database. The document shall cover installation requirements, installation steps and parameters setup for the NBM, post installation tasks, tips & trick, FAQ. c. Documentation relating to application administrators shall cover roles, tasks (e.g., back-up, tuning, patching), utilities, logging, tools for developers, etc. d. Documentation relating to application customization/development (conditions and methodology for solution customization by the NBM). e. Backup & recovery processes and related documentation. f. Archive & retrieval processes and related documentation. g. Documentation relating to security, covering access control, user management, auditing and monitoring, security reports. h. Documentation relating to system configuration – customized installation guide (if this information is not covered by item 2.b above). 3. Documentation relating to end users and technical trainings - support materials for end user and technical trainings. The basic documentation for the solution will be provided at early stages of the project, at least before training and testing phases, in order to assure a better understanding of the solution by the key users.	
Reply	We are generally in agreement, though operational procedures documentation would be your responsibility – though we can guide and advise you regarding these.	YES

CONDITIONS FOR WARRANTY, MAINTENANCE AND POST-IMPLEMENTATION SUPPORT

Req. ID	Requirements	Classification
MnS.1.	**As part of the initial contract for the delivery and implementation of the solution, the successful Tenderer shall provide a post-implementation guarantee, which involves the provision of support services and**	Mandatory

<table>
<tr><td></td><td>maintenance services for a period of 12 months from the date of final acceptance of the solution.</td><td></td></tr>
<tr><td>Reply</td><td>This is our standard policy for post-implementation services as described on section # and ‘BPC AG MAINTENANCE AGREEMENT.docx’ document</td><td></td></tr>
<tr><td>MnS.2.</td><td>Maintenance and support services shall be provided on basis of a Service Level Agreement, which shall be attached to the contract signed between the Parties. The agreement shall establish the post-implementation maintenance and support services level, based on the following minimal requirements:
a. Support days: 7 days per week
b. Support hours: 24/7
c. Response Time (RT) and Solving time:
<table>
<tr><th>Classification of the NBM request*</th><th>Response Time (RT)</th><th>Solving Time (ST)</th></tr>
<tr><td>Critical</td><td>30 min</td><td>2 h</td></tr>
<tr><td>High</td><td>2 h</td><td>6 hours</td></tr>
<tr><td>Ordinary</td><td>1 day</td><td>4 days</td></tr>
<tr><td>Low</td><td>3 days</td><td>The best effort</td></tr>
</table>
* NBM requests for post-implementation maintenance and support services are classified in terms of their importance for the NBM. The importance for the NBM is estimated by the impact (inflicted or potential) of the event that has created the need for the request on the quality parameters of the solution operation.</td><td>Mandatory</td></tr>
<tr><td>Reply</td><td>Our standard policy is described in ‘BPC AG MAINTENANCE AGREEMENT.docx’ document, article 2.2.7. For the current project the policy will be in-line to MnS.2 specification.</td><td></td></tr>
<tr><td>MnS.3.</td><td>The successful Tenderer shall have a customer support center where all requests from the NBM will be directed to. The work program and organization of the Support Centre shall ensure post-implementation maintenance and support services at the level established in these tender documents.</td><td>Mandatory</td></tr>
</table>

Reply	BPC Support consists of three (3) Level; First Level support which is provided throuhg our helpdesk Second Level support which is provided through remote intervention and/or on-site presence depending on the type of support ticket Third Level which consists of patch or hotfix to be applied on the system	
MnS.4.	The Support Centre shall be contacted at least by the following means: e-mail, phone, web, etc.	Mandatory
Reply	BPC Support provieds the following streams; - Telephone - Email - Ticketing system (JIRA ESM)	
MnS.5.	Maintenance and support services shall be provided remotely.	Mandatory
Reply	As described on MnS.3. reply and our Standard Maintenance Agreement	
MnS.6.	For the provision of post-implementation maintenance and support services, the successful Tenderer shall provide NBM with access to a ticketing solution, available through the Internet. The ticketing system shall be properly secured. All interactions between the successful Tenderer and the NBM while providing post-implementation maintenance and support services shall be carried out by means of the respective platform.	Mandatory
Reply	BPC provides access on JIRA ESM web based ticketing tool	
MnS.7.	NBM expects that the proposal for post-implementation maintenance and support services will be based on best practices for Project Management and IT Service Management (e.g., ISO 20000, ITIL v3.0.).	Recommended
Reply	JIRA ESM is ITIL v3 capable	

VIII. Users training approach

Learning a new solution can be a daunting exercise for business and IT staff members, and that is why we offer a wide range of training courses. Designed specifically to rapidly transfer the knowledge needed to ensure the solution runs optimally, our training approaches have proven successful across all our customers worldwide.

Note that we also offer tailored and bespoke training courses.

Training philosophy and requirements

BPC standard training courses have been designed to provide the customer' staff with a comprehensive understanding of all the capabilities of the system and demonstrate the whole structure, possibilities and functionality to all the employees involved in SmartVista projects from top business managers to operators and IT specialists.

We have also developed a customer certification program in order to ensure and maintain the customer knowledge of SmartVista.

BPC understands that Bank expects the training to cover both business and administrative/ operational usage, and that users may be of different 'types': Back-office, IT Management, Business, etc.

Proposed approach

The detailed training agenda, its approach and schedule will be discussed and agreed with KB Bank before the training commences. However, given the complexity of the solution, it is felt that taking a "train the trainer" approach would not be effective for all (types of) members of staff.

BPC, therefore, proposes the following more specific approach at this stage:

- All the users undergo BPC's **e-Learning** program and must then pass a test.
- If required, and depending on the number of staff members, IT staff will be trained **onsite** in groups, each following 1 week of training on the system.
- Alternatively, a "train the trainer" approach can be followed whereby (groups of) participants will follow a 2 to 5 days' **workshop**, followed by a test. The goal being to have "expert" participants that are able to deliver the knowledge further to their teams.
- Each workshop will include some evaluation tools, and these evaluation tools can then be given to the KB Bank team for further internal use.
- BO users will have a set of **videos** to watch (covering all the typical operations) and up to three remote **Q&A sessions** will be organized (gather questions, prepare answers, deliver webinar).
- In addition, **onsite training** can be provided as "train the trainer" to (groups of max. 8) participants to ensure all the expertise is present to consult other colleagues. The duration of this course will be up to 10 days and will be followed by an evaluation (test).

All courses will be accompanied with the dedicated training materials. Generally, the training sessions are conducted after system installation, configuration and acceptance (UAT). So the client's staff will have training sessions on an already pre-configured system.

NBM involvement

NBM team would consist of the following groups, involved in the project:

1) Operations team - they will perform operational tasks with the components.
2) Administrators team - responsible for configuration management and administrative tasks with the applications (e.g. connections management, user management).
3) Infrastructure team - caring about hardware and system-level software, backup, performance.
4) QA team (testing group) – responsible for system testing, e.g. for SIT and UAT execution.
5) Security testing group – caring about security issues.
6) BA group for requirements discussion and helping with test-cases creation.
7) Management group (of different level), who may be interested in high-level information about the solution (terminology, objects, processes) for decision-making and management tasks.

NMB team will be trained about SmartVista products to be capable doing the following:

1) participation in implementation project activities (e.g. SIT, UAT);
2) system exploitation, operational activities;
3) system administration.

Processing system fundamentals

Processing fundamentals (T-01)

This course will provide a high-level understanding in the principles of the card processing business, main participants or entities involved, describes software and hardware used, and provides a general idea of information exchange. This course is independent from the SmartVista system.

Aimed at: Participants who are new to the payment card industry.

Working with EMV (T-02)

This course deals with the overview of EMV specification, data formats, and their application. It will highlight what are the EMV specifications and standards. Participants are expected to have an idea about payment card industry standards or have to at least have completed the “Processing Fundamentals” course.

Aimed at: Card issuing specialists with no or little experience with EMV who will be working with EMV card issuing.

SmartVista suite training

SmartVista essentials (T-03)

This course introduces basic concept of SmartVista, its architecture, capabilities and principles used to solve main business tasks. The course is based on presentations that depict operation of the real system. Independent trainees’ interaction with the system is not intended.

Aimed at: Everyone who is starting to work with SmartVista.

SmartVista user training (T-04)

This course is intended for users who have already adopted the basic concept of the system (for those who have completed the "Essentials" course, or have independently studied the documentation). The course introduces the principles of system configuration and day-to-day business operations. It includes both in-depth theoretical part with presentations and demonstration of the system, and numerous practical exercises to reinforce theoretical skills and to strengthen practical skills required to use SmartVista. The course allows participants to participate in selected topics according to their job specialization.

Aimed at: SmartVista end users.

SmartVista configuration (T-05)

This course focuses on the various features and tools available in SmartVista for system setup and configuration. On completing this course, participants will be able to configure new products and processing rules in order to fulfill business requirements, and manage the system independently with minimal support from BPC for such activities.

Aimed at: Business, operational and IT team members who have SmartVista configuration tasks. Participants must possess knowledge in payment cards processing and also must have completed at least the “SmartVista Essentials” course to qualify for this course.

SmartVista credit card management (T-06)

This course is for specialists who are responsible for credit card product set up and maintenance, carrying out customer registration and maintenance tasks, and for those who directly deal with customer and service them. Participants are expected to have a general business idea of credit cards, their institution’s business requirements for products, and internal operational process and procedures, and also must have completed “Transaction processing” course to qualify for this course.

Aimed at: Business, operational and IT team members who will configure credit card products in SmartVista.

SmartVista administration (T-07)

This course introduces system administration and set-up of user workplaces. The switch and the bank-end processing systems are covered. As for the back-end processing system, the course provides information on operation with processes and their logs, and also basic recommendations on database servicing. The main emphasis is focused on the description of the switch’s architecture, methods of system management and the list of key actions of the

administrator on switch operation and system recovery. Also, key protocols of online interaction are described. At the end of the training, the participants will be able to troubleshoot basic errors experienced during day-to-day activities.

The course is conducted with presentations and demonstration of the real system. Independent users' interaction with the system will be minimal.

Aimed at: Technical specialists (i.e. system administrators).

Transaction processing (T-08)

The key goal of this course is to understand algorithms of SmartVista system operation when processing transactions. It describes the involved processes, logic of transaction processing stages; both during authorization in the switch, and during final processing in the back-end processing system, and also indicators of processing results. Also, the course will cover recommendations for diagnostics and possible actions when having processing errors.

The course is introduced based on presentations, with demonstration of the real system and a few practical tasks.

Aimed at: Business, operational and IT team members who are involved in transaction processing task solving.

SmartVista training for trainers (T-09)

The course provides basic knowledge and skills on how to exchange the knowledge, and a set of tools that allows carrying out SmartVista training. For competent and effective exchange of knowledge with other people it is necessary not only to accumulate this knowledge, but also to understand the basic particularities when working with information during the training course. Training of trainers includes an example of real training situation to show how the course organized, how to structure and to introduce information correctly, how the people perceive it, what methods shall be used to make people remember the shared information, what types of practical exercises exist, how to work properly with questions, and other essentials.

To make this training course useful for trainers, it is important that attendants possess knowledge of SmartVista system.

Aimed at: Trainers who will be conducting trainings on SmartVista.

Dispute management (T-10)

This course deals with basic terms of conducting disputes with Visa and MasterCard networks, dispute logic, message types and rules for their generation. By the end of the course, participants will be able to manage disputes by themselves.

Aimed at: Specialists involved in disputes activities.

Encryption and keys (T-11)

This course will focus on keys and check values used in issuing and acquiring activities. The following will be covered during the training:

Terminal keys and data protection during communication with terminals
Issuing keys, transaction protection, card authentication
Zone keys and use of cryptography for information exchange with payment networks

Pre-requisites to participating in this course, knowledge on the following is necessary:
Processing fundamentals,
Card product configuration steps,
Card issuing steps,
Terminals registration steps,
Transaction processing,
Cryptography fundamentals.

Aimed at: Technical specialists (i.e. system administrators, ATM management staff).

ATM scenarios (T-12)

This course will help specialists to familiarize themselves with ATM scenario terms and concept, as well as the scenario structure. It describes operation of the scenario and data exchange between the ATM and the processing system. The course may be attended by participants without basic knowledge, and by experts who are already familiar with ATMs scenarios. The knowledge level of the participants will impact on the duration of the training.

At the end of the course, participants will be able to edit ATM scenarios. However, to create ATM scenarios, extra training with the scenario developer is required.

Levels of training:
Intermediate – Participants will be trained on how to understand scenarios and edit basic components.
Advanced – Participants will be trained on how to modify scenarios with all the technical aspects.

Aimed at: Technical specialists working with ATMs. Participants must possess some background knowledge in standard ATM protocols like Diebold 912, NDC+, Wincor DDC and Wincor NDC to participate in this course.

Supplementary modules training

Access control server (T-13)

This training is targeted at specialists who will be working with the ACS module. Participants are expected to have a general idea of how 3D-Secure works, the participating systems and international payment network regulations before taking part in this training.

Aimed at: Specialists who will be involved in the ACS operation and administration.

E-commerce solution (T-14)

This course will train the participants on how to use the solution for their day-to-day business activities, such as e-commerce merchant registration, e-commerce merchant management and servicing, and working with e-commerce transactions. Participants are expected to have an idea of e-commerce transactions, 3D-Secure technology.

Aimed at: Specialists who will be involved in the solution's operation, e-commerce merchant management and merchant service support.

Fraud management (T-17)

(optional) This course covers areas specific to fraud management like creation and management of rules, conducting investigations, reporting fraud and also managing notifications. Participants are expected to have a general idea of different types of fraud, experience in fraud management, managing rules and analyzing fraud reports provided by payment networks.

Aimed at: Operators who will be involved in the solution's operation (fraud prevention specialists, risk managers, financial auditors).

SmartVista Integration Platform user training (T-21)

The course introduces the principles of system working and configuration. It includes in-depth theoretical part with presentations and demonstration of the system. Practical exercises can be added to the training upon client request to reinforce theoretical skills required to use SmartVista Integration Platform.

Aimed at: SmartVista Integration Platform end users

SmartVista Integration Platform configuration training (T-22)

This course focuses on configuration features and tools available in SmartVista Integration Platform. The course is based on demonstration of various configuration cases followed by practical exercises. Upon completion of this course participants will be able to configure the interaction and message conversion between different types of SVIP external systems. This is to help fulfilling business requirements managing the system independently with minimum support from BPC side.

Aimed at: Business, operational and IT team members. Participants must possess knowledge of how bank systems communicate to each other, and be aware of the message formats used for systems interaction. Completion of “SVIP User training” (T-21) is mandatory to qualify for this course.

System Monitoring user training (T-23)

This course is an overview of the System monitoring and its features which allows providing centralized health monitoring of the SmartVista platform infrastructure and components (FE/BO) using a single tool. Participants will be provided with the information about the basic architecture of the system components, system’s metric scope and source, notification possibilities and working with GUI

Aimed at: IT or business support specialists responsible for system monitoring activities

IX. Recommended platform

Software

Component	Version
Virtualization	Oracle VM 3.4
OS	Oracle Enterprise Linux 8.3
Cluster	Oracle VM HA
Application Server	WebLogic 12c Standard Edition 12.2.1.4
Java	Oracle JDK 1.8 update 281
Database	Oracle 19c Enterprise Edition

Hardware

Production

Component	Cores	CPU type	RAM Gb	HDD Gb with FRA	FRA Gb	HDD IOPS
BO DB	*4*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*1305*	*700*	*5912*
SVIP DB	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*600*	*400*	*196*
DP DB	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*600*	*400*	*150*
Notif DB	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*600*	*400*	*150*
PPortal DB	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*700*	*400*	*150*
GUI App	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*120*	*0*	*120*
SVIP App+Logstash	*3*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*210*	*0*	*87*

SVIP Elastic	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*559*	*0*	*196*
DP App	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*300*	*0*	*130*
Notif App	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*300*	*0*	*40*
PPortal App	*2*	*Intel Xeon-Gold 6248R @3.0GHz(24c)*	*16*	*300*	*0*	*40*
Summary	***25***		***176***	***5494***	***2300***	***7171***

Development / Test

Env	Component	Cores	CPU type	RAM Gb	HDD Gb with FRA	FRA Gb	HDD IOPS
Test	*Test Apps*	*2*	*Intel Xeon-Silver 4110 @ 2.1GHz (8c)*	*32*	*300*	*0*	*40*
	Test DBs	*2*	*Intel Xeon-Silver 4110 @ 2.1GHz (8c)*	*32*	*400*	*0*	*50*
	Summary	***4***		***64***	***700***	***0***	***90***

OVM Manager & Monitoring Server

Component	Cores	CPU type	RAM Gb	HDD Gb with FRA	HDD Gb	HDD IOPS
OVM Manager	*2*	*Intel Xeon-Bronze 3104 @ 1.7GHz (6c)*	*16*	*300*	*300*	*20*

Component	Cores	CPU type	RAM Gb	HDD Gb with FRA	HDD Gb	HDD IOPS
SVMON (zabbix)	*2*	*Intel Xeon-Bronze 3104 @ 1.7GHz (6c)*	*16*	*600*	*600*	*20*

PKI

Device/VM	OS	Role	Requirements
Root CA	Windows Server 2016	Active Directory Certificate Services	CPU: 2 Core RAM: 8 Gb HDD: 50 Gb
Issuing CA	Windows Server 2016	Active Directory Certificate Services	CPU: 2 Core RAM: 8 Gb HDD: 50 Gb
RCL Server	Windows Server 2016	N/A	CPU: 2 Core RAM: 8 Gb HDD: 50 Gb

X. Proposed SLA

<table>
<tr><th>Req. ID</th><th>Requirements</th><th>Classification</th></tr>
<tr><td>MnS.8.</td><td>As part of the initial contract for the delivery and implementation of the solution, the successful Tenderer shall provide a post-implementation guarantee, which involves the provision of support services and maintenance services for a period of 12 months from the date of final acceptance of the solution.</td><td>Mandatory</td></tr>
<tr><td>Reply</td><td>This is our standard policy for post-implementation services as described on section # and ‘BPC AG MAINTENANCE AGREEMENT.docx’ document</td><td></td></tr>
<tr><td>MnS.9.</td><td>Maintenance and support services shall be provided on basis of a Service Level Agreement, which shall be attached to the contract signed between the Parties. The agreement shall establish the post-implementation maintenance and support services level, based on the following minimal requirements:
d. Support days: 7 days per week
e. Support hours: 24/7
f. Response Time (RT) and Solving time:
<table>
<tr><th>Classification of the NBM request*</th><th>Response Time (RT)</th><th>Solving Time (ST)</th></tr>
<tr><td>Critical</td><td>30 min</td><td>2 h</td></tr>
<tr><td>High</td><td>2 h</td><td>6 hours</td></tr>
<tr><td>Ordinary</td><td>1 day</td><td>4 days</td></tr>
<tr><td>Low</td><td>3 days</td><td>The best effort</td></tr>
</table>
* NBM requests for post-implementation maintenance and support services are classified in terms of their importance for the NBM. The importance for the NBM is estimated by the impact (inflicted or potential) of the event that has created the need for the request on the quality parameters of the solution operation.</td><td>Mandatory</td></tr>
</table>

Reply	Our standard policy is described in 'BPC AG MAINTENANCE AGREEMENT.docx' document, article 2.2.7. For the current project the policy will be in-line to MnS.2 specification.	
MnS.10.	The successful Tenderer shall have a customer support center where all requests from the NBM will be directed to. The work program and organization of the Support Centre shall ensure post-implementation maintenance and support services at the level established in these tender documents.	Mandatory
MnS.11.	The Support Centre shall be contacted at least by the following means: e-mail, phone, web, etc.	Mandatory
MnS.12.	Maintenance and support services shall be provided remotely.	Mandatory
MnS.13.	For the provision of post-implementation maintenance and support services, the successful Tenderer shall provide NBM with access to a ticketing solution, available through the Internet. The ticketing system shall be properly secured. All interactions between the successful Tenderer and the NBM while providing post-implementation maintenance and support services shall be carried out by means of the respective platform.	Mandatory
MnS.14.	NBM expects that the proposal for post-implementation maintenance and support services will be based on best practices for Project Management and IT Service Management (e.g., ISO 20000, ITIL v3.0.).	Recommended

XI. Appendices

Model of standard maintenance and support agreement

Please refer to ‘BPC AG MAINTENANCE AGREEMENT.docx’ and ‘BPC AG PROFESSIONAL SERVICES AGREEMENT.docx’ documents.

Model of standard licensing agreement

Please refer to ‘BPC AG MASTER AGREEMENT.docx’ and ‘BPC AG SOFTWARE LICENSE AGREEMENT.docx’ documents.

Model of product warranty

Please refer to ‘BPC AG MASTER AGREEMENT.docx’ document, article #7.

Model of escrow agreement

Please refer to ‘NCC Escrow Agreement Template_updated.docx’ document.

Name: Vasily Volynskiy

Position: SVP

Date: 16.6.2021

Address: Neuhofstrasse 5a, 6340 Baar, Switzerland

Signature