tietoEVRY

Response to National Bank of Moldova Open tender #: ocds-b3wdp1-MD-1615975211331 of March 17, 2021

Instant payments software solution

Technical offer

Digitally signed by Mocanu Radu
Date: 2021.06.17 17:08:18 EEST
Reason: MoldSign Signature
Location: Moldova

Table of Contents

Confidentiality terms 5

Subject to final agreement 5

Contact details 5

Executive summary 6

1. TietoEVRY understanding of project objectives 8

2. Description of the proposed solution (functional and technical solution, technologies, description of models/components) 9

2.1 Solution functional description 9

2.1.1 Access to IPS services 11

2.1.2 IPS Participant types 11

2.1.3 Participant work modes (Participant unreachable service) 12

2.1.4 Transaction Validation and Routing 13

2.1.5 Duplicate Checking 13

2.1.6 Timeout Management 14

2.1.7 Batch Processing 14

2.1.8 Cut-off principles 14

2.1.9 Liquidity Management 14

2.1.10 Fee management 15

2.1.11 Risk management 15

2.1.12 Reporting 15

2.1.13 Administration Portal 16

2.1.14 Proxy Service 17

2.2 Solution technology and architecture 17

2.2.1 Logical architecture 17

2.2.2 Scalability 18

2.2.3 Auditability 18

2.2.4 Availability 18

2.3 Physical architecture 19

2.3.1 Reverse proxy/load balancer server 20

2.3.2 Firewalls 20

2.3.3 API Gateway 20

2.3.4 Microservices 20
2.3.5 Database provider 21
2.3.6 Certificate Management 21
2.3.7 Infrastructure monitoring 21
2.3.8 Built-in IPS Monitoring 21
2.3.9 User Access Right Management 21
2.4 Security pillars 22
2.5 Performance 22
2.6 GDPR 23

3. Proposed implementation strategy 24
3.1 General approach 24
3.2 Implementation: phases, milestones, duration, priorities 24
3.3 Description of working principles 24
3.4 Working hypotheses 24
3.5 Risk management 25
3.6 Interoperability approach 26

4. Approach, deliverables, methodology and tools used for project different phases 26
4.1 Project Management related activities 26
4.2 Analysis phase 27
4.3 Design phase 28
4.4 Solution preparation on-site (Build phase) 30
4.5 Testing phase 30
4.6 Training phase 31
4.7 Go live and Final Acceptance phases 32

5. Response to specifications and requirements F4.4 33
5.1 Functional requirements (FR) 33
5.2 Non-functional requirements (NF) 80
5.3 Implementation requirements (IR) 109
5.4 Requirements for post-implementation and support services (MnS) 139

6. Training description 141

7. Project Management description 142
7.1 Project organizational chart 142

7.2 Project management approach, including Quality Assurance and Change Management approach 145
7.3 Project management plan 145
7.4 Original version of project management plan 145

8. Examples of deliverables (other than mentioned above)....145

9. Required additional software and recommended hardware configuration 146

10. Proposal licensing policy 146

11. Appendices of Agreement model 147
11.1 Model of a standard licensing agreement 147
11.1 Model of standard maintenance and support agreement 148
11.2 Service level agreement (SLA) 148
11.3 Model of Product warranty agreement 148

12. Change management process approach 148

13. Solution demonstration LINK (access to IPS DEMO video recording) 150

14. Appendixes and annexes 151

15. Proposal validity 154

16. Signatures 154

Confidentiality terms

This document contains confidential information and is supposed to be used only by the National Bank of Moldova (hereinafter National Bank of Moldova or Customer). This document is the property of TietoEVRY or its subsidiaries (hereinafter TietoEVRY or Supplier). Total or partial circulating of the given document can be allowed only with the written permission of TietoEVRY.

Subject to final agreement

The information provided in this document (TENDER Response) and its appendixes is based on TietoEVRY's current understanding of the Customer`s requirements. Everything not covered in this document and its appendixes is subject to final scoping, discussions and estimations. The proposal is based on the Customer`s TENDER requirements and does not include any additional potential customizations, if not stated in the document otherwise.

The document is not be deemed as self-executing, any binding commitment of TietoEVRY is subject to a final written contract being negotiated by the parties, and after a Pre-study analysis is conducted by TietoEVRY.

The detailed solution design documentation including solution specification (a finalised proposal) and detailed implementation plan will be provided as a result of a Pre-Study analysis as part of a written contract between Parties, which will provide more clarity on the requirements, solution scope, the scope of responsibilities of the parties and other information related to the project business needs and agreed deliverables.

Contact details

Name	Title	E-mail	Phone
Irina	Grinspane	irina.grinspane@tieto.com	+371 29259990
Evalds	Mihalenko	Evalds.mihalenko@tietoevry.com	+371 67510000
Radu	Mocanu	radu@involity.com	+373 79990610

Executive summary

TietoEVRY creates a digital advantage for businesses and society. We are a leading digital services and software company with a local presence and global capabilities. Our values and heritage steer our success.

TietoEVRY employs around 24 000 experts globally. The company serves thousands of enterprise and public sector customers in more than 90 countries. TietoEVRY's annual turnover is approximately EUR 3 billion and its shares are listed on the NASDAQ in Helsinki and Stockholm as well as on the Oslo Børs.

As one of the leading providers of payment technology and software globally, we focus on supporting digital innovation and real-time transformation with cutting-edge solutions.

TietoEVRY is one of the world's leading suppliers for payment and card solutions, well known for platforms in the area of Cards and Account-based Payments and Instant Payments. In the space of Card processing business (Issuing/Acquiring/Switching/Clearing), TietoEVRY is one of the TOP 5 product providers globally covering the needs of >500 financial institutions via multiple installations across banks and 3rd party processors, including Klarna and Worldline.

With more than 25 years of experience in retail and card payments, TietoEVRY focuses on supporting new digital payment paradigms and real-time transformation, with cutting-edge solutions that align with the National Bank of Moldova vision for the country payment ecosystem. More than 500 financial institutions in over 100 countries globally run their retail payment businesses on TietoEVRY's product solutions. TietoEVRY has implementation experience of national card switches in countries like Azerbaijan, Belarus, Latvia, and Lithuania. TietoEVRY has implemented a nation card solution in Ukraine, implemented interoperable national ATM switch and instant payments in Finland, card and account-based instant payments in Kenya. Currently implements Instant Payments and Universal Payment gateway solution in the Maldives.

TietoEVRY has a wide portfolio with solutions that can be combined and adjusted to our customer needs. Along with provided solutions comes our expertise, global experience, and opportunities to become technologically more advanced and up to date with current market trends and requirements.

TietoEVRY Instant Payment Solution (Tieto EVRY IPS) is a powerful platform for account-based payment processing solution, that provides payments business transition for central processors, national or central banks to real-time payments. TietoEVRY Instant Payment Solution provides a platform for centralized payment infrastructure connecting banks and 3rd party PSPs for consistent, real-time, irrevocable money transfers processing, which are settled through the national real-time gross settlement (RTGS) system. Financial interoperability, through TietoEVRY Instant Payment Solution, ensures immediate payments between end-customers of different banks and PSPs. Individuals, businesses, and government organizations may play roles of an end-customer in the solution, thus providing so-called P2X, B2X, and G2X payment processing models.

The TietoEVRY Instant Payments Solution is a platform for real-time account-based payment transactions. By enabling instant transactions for all market participants, you can bring new benefits to businesses and citizens, and ensure payments can flow quickly and safely wherever they are needed, through a variety of payment instruments and methods.

Our Instant Payments Solution offers accessibility via open APIs and international standards, such as ISO20022. This enables payment service providers to easily connect to the system and promotes the creation of new and innovative market services.

The TietoEVRY IPS is based on microservices architecture and creates efficiency gains from the re-use of services, components, and interfaces. High availability, security, data protection and compliance are the key cornerstones of our Instant Payments Solution. TietoEVRY IRPC unit is a product-oriented organisation. Therefore, Product development is organised in separate product development projects according to internal Product development procedure. The stack of possible software development models (approaches) at the moment are:

- Elements of Agile/Scrum methodology;
- Elements of RUP (Rational Unified Process) methodology.

Selecting the right long-term partners to develop or re-shape a national payment system is essential. There is no substitute for knowledge and experience. This makes the selection of partners that have experience in managing similar complex projects and multiple, sometimes competing, stakeholders a pre-requisite. Payments are strongly national, so partners who can draw on what worked and did not work from other markets and have good local and technical knowledge are desirable. TietoEVRY has the experience and will help NBM to implement their Instant payments Solution.

Why TietoEVRY:

- We are a Customer First company;
- We recruited the Best People;
- Experience and Strong reputation building national level retail payments infrastructure solutions.
- More than just software we establish a partnership through our consultancy and advisory divisions;
- Proven software product with numerous live implementations, scalable for future volumes growth and functionally rich).

1. TietoEVRY understanding of project objectives

TietoEVRY fully understands the National Bank of Moldova objective to maintain an innovative and inclusive, real-time national payment ecosystem in benefit for stakeholders - Moldovan banks and customers of banks. The new platform shall be open and support innovations, including seamless and instant payments. The key aspects of the platform are security, compliance, usability and openness for further innovations.

TietoEVRY fully understands the National Bank of Moldova objective to start delivery of the project in 2021 and are ready to fit expected project timelines.

TietoEVRY assumes that a single and measurable short-term objective could be to deliver a solution platform with a single use case that will be available for all market participants.

To realize the project goals following professional services will be provided by TietoEVRY:

- Project Management;
- Pre-Study-Technical & system user training (trainings of participants are excluded from Project);
- Preparation of test environment in TietoEVRY;
- Development of identified GAPs and their implementation;
- Solution installation and configuration on MNB test environment;
- Test scenario preparation;
- Preparation of Project supporting documentation (technical & administrative);
- Validation and Functional tests-Integration tests of implemented solution;
- Integration tests with two Banks participants selected by NBM;
- Support of testing performed by NBM-User Acceptance Tests requested by NBM and agreed in Master Test Plan-Analysis of test results;
- Project GO-LIVE/post GO-LIVEsupport.

This document describes the Instant Payments Solution implementation in the NBM. Before implementation detailed pre-study needed (included in financial offer).

2. Description of the proposed solution (functional and technical solution, technologies, description of models/components)

2.1 Solution functional description

TietoEVRY Instant Payments Solution (IPS) is designed to process millions of payments daily with a response time for every individual payment within just a second.

The IPS operates in 24/7/365 mode with 99.99% availability per month. System components are functioning in active-active mode. The system component upgrade process is performed on-the-fly with zero downtime.

IPS is designed to provide secure payment and information exchange via secure network governance with electronic digital certificates for TLS connections and with transactions seals to ensure that the contents of the message have not been tampered during the transition.

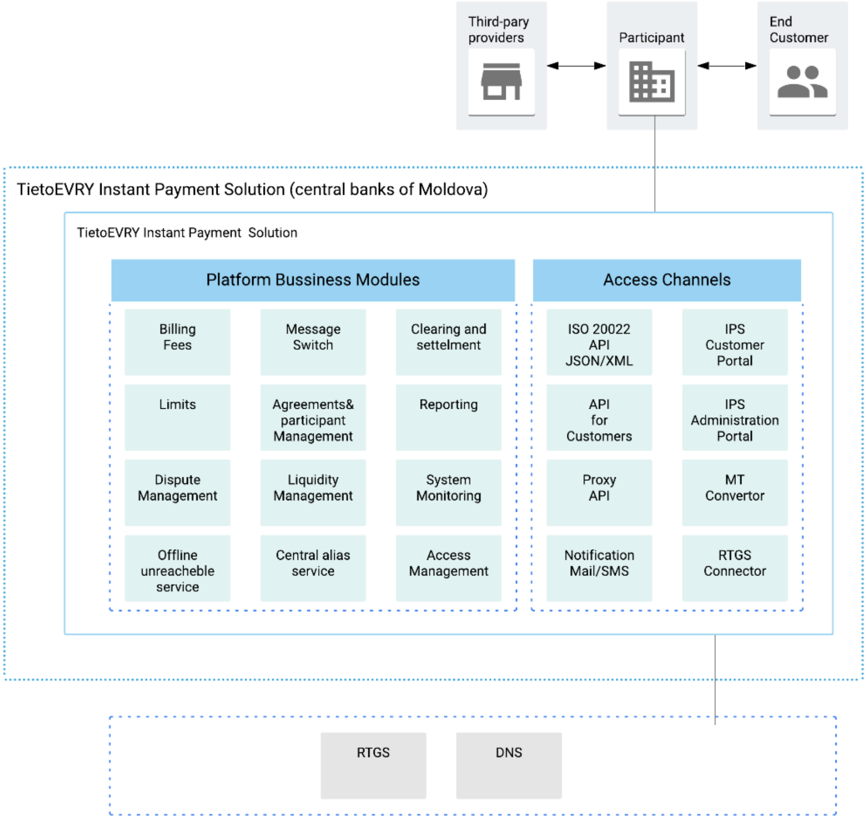
IPS can be integrated with existing data protection infrastructure and master source of user data such as LDAP.

IPS software will be operated by the Central Bank of Moldova as a system operator. IPS software is based on ISO20022 standard. The processing does not need manual intervention, instantly clears and settles individual credit transfer orders.

Instant Payments Solution enables secure ISO20022 message transportation between IPS Participants allowing immediate funds transfer from the payer and immediate funds availability for end beneficiary within seconds. The transaction processing workflows in the core module is implemented according to the SEPA Instant Credit Transfer Rulebook.

- Continuous (24/7/365) processing, validation, clearing, and settlement of individual credit transfer messages (credit transfers' initiation and the corresponding response; recalls' initiation and the corresponding response investigation messages and request to pay).
- Clearing and settlement in the IPS is executed
  - prefunded,
  - continuously (all Calendar Days of the year),
  - in real-time,
  - by individual payment transactions,
  - or by bulk file for batch processing.
- Individual Fee calculation per participants.
- Individual Limit setting up per participant.
- Liquidity management per Direct Participants.
- Reports generation (such as Daily reconciliation reports per Direct Participants, and per Indirect Participant and Cycle Reconciliation report).
- Unified technical connection (All institutions using the IPS service's infrastructure will have the same type of technical connection).
- Participants will be identified by IPS Service via using certificates issued by IPS. (client and seal).
- Business and technical monitoring

The schema below illustrates a high-level functional and integration design of the proposed TietoEVRY Instant Payments Solution based on the requirements:



TietoEVRY IPS Functional owerview

The proposed overall solution offer includes the following functionalities:

- Support of different types of payments (includes Credit transfer and Request to Pay)
- Real-time clearing
- Support the four-layer structure of participants (direct participants, indirect participants, payment initiators and technical service providers)
- Liquidity management
- Risk management for participant transaction value and volume control (Limits)
- Fee management system
- Message routing according to predefined business flow
- Reporting
- Dispute Management
- Central Aliase Service. The purpose of the Central Aliase Service is to ensure the possibility of identifying the account number and BIC corresponding to the Alias (for example, mobile phone number) in order to make the initiation of payments easier by using Alias instead of entering account numbers and other necessary payment details.
- Pre-authorization Service (Stand-in) & Participant unreachable service
- Participant portal

2.1.1 Access to IPS services

Being connected to IPS any Participant immediately receives access to services authorized for this participant (Credit transfer, Batch Payments, Transaction recall, Request to Pay, Smart Addressing) and message routing to/from other connected eligible Participants. The System Operator may define which services are available for the particular Participant (in case it is necessary to restrict access to some of the registered services).

2.1.2 IPS Participant types

Direct Participant

Each Direct Participant has one IPS agreement and one IPS account which is used to reflect the Liquidity Net Position (sum of debit and credit transfers) of this participant in IPS.

Direct Participant's account in the IPS correlates with the Direct Participants account opened in the RTGS system which represents the amount of funds reserved for this Direct Participant to guarantee its final settlement of IPS payments. IPS is using pre-funding settlement model when the processing of the Direct participant is covered by the funds reserved on the account in the Central Bank (RTGS system).

Settlement Agent (Liquidity Provider) is determined in the IPS as Direct Participant, meaning that Direct Participant settings are valid for Settlement Agent. Only Direct Participant is allowed to act as Settlement Agent.

Indirect Participant

Each Indirect Participant can be sponsored by one and only one Direct Participant at a time.

Each Indirect Participant has one IPS account, which is used to reflect the Liquidity Net Position (sum of debit and credit transfers) of this participant in IPS. This Liquidity Net Position is allocated to Indirect participant by its Settlement Agent. Indirect participant Liquidity Net Position is part of Liquidity Net Position of Settlement Agent and is managed by Settlement Agent. Settlement Agent sets and controls Liquidity thresholds for Indirect Participant. Notification messages about Indirect Participant Liquidity Net Position statuses is sent to its Settlement Agent.

Payment Initiator

Payment Initiator is an additional type of the IPS participants, which may submit payment initiation message (pain.001), final status reports (pain.002) and investigation message (camt.028) to IPS. Payment Initiator acts on behalf of its customer (usually merchant), who has an account at one of the participants of IPS. When submitting a payment initiation message, the Payment Initiator indicates the Originator Bank, which account will be debited in the result of the transaction, and the Beneficiary Bank which account will be credited in the result of the transaction.

Payment Initiator has no separate account in the IPS but has its own IPS connections endpoints.

Each Payment Initiator must have only one record in the IPS, meaning it has only one agreement, where total transaction processing limits defined by Schema per Payment Initiator are reflected. IPS does not separate liquidity settings for Payment Initiator. Payment Initiator may have its own limits settings and fees settings in the system.

Currently, there are no requirements in RFP for the Payment Initiator role, so this particular role will not be assigned to any of the Participants at the initial implementation stage.

Technical Service Providers

Technical Service Providers (TSP) is an additional type of the IPS participants, which ensures only technical connectivity to the IPS for other types of participants.

TSP has a technical account in IPS for routing purposes and does not participate in the clearing and settlement procedures. TSP does not initiate messages itself, TSP ensures technical processing of messages initiated by other participants connected to IPS via a particular TSP. TSP is the only technical provider (mediator) for IPS message processing initiated by the participant. TSP must support all message elements that are required by the IPS Interface Specification. Data necessary for the corresponding transaction is provided by the particular participant when initiating the corresponding transaction and TSP creates (or forwards, it depends on integration between TSP and the participant and on TSP provided services) ISO20022 message for the further submission and processing in IPS.

The message must contain BIC of "original" participants - initiator and recipient. Message routing and clearing will be performed based on these data (BIC). As under particular TSP will be registered the list of serviced participants, IPS will know where to route the message based on BIC of instructing and instructed parties.

TSP can provide technical connectivity services for one or several different participants (Direct, Indirect, or Payment Initiator). TSP is not providing settlement services.

TSP does not have separate settings, such as services, transaction processing limits, fees, timeout settings, etc. TSP is allowed to process so many transactions as is allowed to process to the participants connected to IPS via this TSP. IPS processes messages received from TSP according to the processing settings (limits, fees, etc) of the participants connected to the IPS via this particular TSP and initiated this particular message.

Currently, there are no requirements in RFP for the TSP role, so this particular role will not be assigned to any of the Participants at the initial implementation stage.

2.1.3 Participant work modes (Participant unreachable service)

Direct and Indirect Participants may work in “online” and “offline” modes. Online mode means that participants shall validate incoming transactions and sent them to the Central node (IPS) approve or reject response. In case of response is not received in pre-defined time (as configured in the system on the basis of the local in-country rulebook) transaction is rejected.

In offline mode, participants transaction is processed by IPS without prior validation by these participants and based on special limits with special limited-time duration.

The central bank operator or/and the participant can define a limit and timeframe when the participant goes offline. If this offline parameter in the system is the active notification about participant offline (admi.004) not be sent to all participants in the scheme. After the offline period, all accumulated instant payment transactions in IPS will be sent to the participant for final payment execution.

IPS Administration Portal supports functionality for the System Operator to indicate the start and finish date and time for the scheduled maintenance window.

Additionally, IPS supports “heart-beat” service. To check participant's availability, the system periodically (for example, each minute) sends an echo test (API call) to each participant of the Schema. The participant should respond accordingly. If any of the participants are unavailable, the IPS system marks this particular participant as unavailable via monitoring facility at the IPS Administration Portal and automatically sends admi.004 message to all available participants about this event. IPS continues to send echo tests to the participant, and when the participant is back online again, IPS correspondingly changes the participant’s status via the monitoring facility at the IPS Administration Portal. As well corresponding admi.004 is sent to all the available participants to inform them about this event.

Participant may configure (add/modify/suspend/delete) “pre-authorization” profiles for Payments via Participant Portal. The Participant may indicate the conditions (particular sender or/and receiver, transaction amount, aggregated daily amount of transactions, type of instrument, and transaction purpose) when IPS is allowed to authorize the transaction on behalf of the participant when the participant is unavailable.

In addition to the unavailability information message, the IPS service supports optional API features to communicate the unavailability of a Participant. Message admi.004 is used by participants to inform the system and other participants about the unavailability of a participant. When Participant plans to be unavailable for some reason (for example due to a regular system update), it may submit admi.004 message to IPS to inform the system and other participants about planned downtime. IPS will forward this admi.004 to all other participants of the Schema. The message contains participant BIC, start date/time of unavailability, and end date/time of unavailability.

2.1.4 Transaction Validation and Routing

IPS validates each message individually. If the message is successfully validated, it is forwarded in real-time to the receiving IPS Participant.

If it is rejected, the result of the validation process is sent to the sending IPS Participant in real-time. The results of the validation process may contain

- the acknowledgement of a valid transaction, or
- the reporting of invalid data on the transaction level.

IPS validates all messages in the following order:

- XML Schema technical validation
- Message size
- API header environment control
- Duplicate and retransmission control
- Content validations: ISO 20022 rules, Schema special rules.

As soon as any validation fails, IPS stops message processing and responds to the sender with an appropriate error message.

IPS routes all the valid messages it receives to the counterparty, which is determined by the system according to the contents of its routing data. This counterparty is referred to in the IPS as the Instructed Agent.

The Instructed Agent BIC is found using the receiving side BIC (Creditor Agent BIC).

The Instructing Agent is validated when the message is processed. At this point in time, IPS checks that the sending Participant is active. If this condition is not met, in case of a message exchange the entire message is rejected with error code B10.

During Validation of each transaction, and specifically during the Routing process IPS verifies, that the Instructed Agent (derived from the routing process and based on the Instructed Agent BIC) is active on the Acceptance Date/business date.

The Routing process described in this document ensures that the Instructed Agent is active on the Acceptance Date, Interbank Settlement Date, or business date of the transaction according to the message type.

2.1.5 Duplicate Checking

If IPS receives a duplicated Instant Payment Transaction, with the same unique key of an existing transaction, the second one will be rejected. A specific reason code is added to the rejection message. The unique key shall unambiguously identify the transaction throughout the entire interbank chain.

Unique key = Transaction ID + debtor ID + Acceptance date and time (standard configuration, will be configured according to NBM functional requirements)

Duplication checks are performed in IPS and are based on the unique key stored in the IPS repository.

If IPS receive a duplicate response to a transaction or a duplicate response to an investigation, meaning with the same unique key of an existing response, the second one will be rejected to the Beneficiary Bank without making any duplication check and any processing.

The first answer received from the Beneficiary Bank is the one that will cause the update of the status of the payment to final, while other subsequent messages received for the same original payment will be rejected to the Sender, informing the Beneficiary Bank as regards the final status of the corresponding Instant Payment transaction. Additional Confirmation messages will be rejected, irrespective of the confirmation's status, without forwarding the message to the Originator Bank or performing any other processing.

2.1.6 Timeout Management

The Schema must define overall message execution time-outs for all transactions supported by IPS:

- Credit Transfer (pacs.008)
- Payment Activation Request (pain.013)
- Customer Credit Transfer Initiation (pain.001)
- Recall (camt.056)
- Investigation pacs.028

During the first setup of IPS, the time window, during which a transaction is considered successful, is configured by the IPS operator.

2.1.7 Batch Processing

IPS is able to accept Instant Credit Transfers batches such as Salary payments from Payer' Banks and PSPs and provide their processing.

Batches in IPS will be processed in online mode. These batches can contain payments presented to a single Payer Bank or Payer PSP account. Beneficiary participants may be multiple. The batch is split into single payments, each of them is processed separately.

2.1.8 Cut-off principles

IPS operates 24/7/365, and the concept of the business day (cut-offs and end-of-day) is applicable only in the context of availability of the RTGS to performs settlement for participants and the necessity of the bank (participant) to close the business day. End of day mainly concerns processes to be done at changing the settlement date (e.g. generating end-of-day reports, start a new settlement date).

2.1.9 Liquidity Management

IPS ensures service for managing online liquidity positions for direct participants. IPS ensures real-time clearing of processed messages according to available limits within participant accounts. IPS ensures notifications on upper/lower limit positions and automatic initiation with settlement service.

Indirect participant liquidity can be controlled only by its Settlement Service Provider. IPS supports automatic liquidity adjustments for indirect participants as well. Direct participant may initiate liquidity credit/debit on behalf of Indirect participant (camt.050). As result, IPS performs liquidity adjustment and informs Direct participant with camt.025 message and Indirect participant with camt.054 message.

Participant monitors and manages its current IPS liquidity position using the IPS Participant portal provided workplace or/and by sending liquidity management related messages.

Liquidity management related message processing flows in IPS native format ISO 20022. For communication with the RTGS system, SWIFT FIN format messages will be used. IPS native format ISO 20022 liquidity management messages will be converted to the corresponding SWIFT FIN format messages.

2.1.10 Fee management

Fees are defined per participant and reflect specific commission volumes for the processing of different transaction types and other services provided by the IPS. Fees can be defined as recurring fees and fees per transaction. Recurring fees are regular charges that are deducted from the participant's account for different services provided by IPS, such as Credit Transfers, Request to Pay, Recalls, Batch payments, Aliase Services, Reports, Participant Portal, etc. Fees per transaction can be set as a fee for a number of transactions (Credit Transfers and Request to Pay) processed per period or as a fee for a particular amount of single transaction (Credit Transfers, Request to Pay and Recall). Fees based on a particular amount of single Credit transfer and Request to Pay can be defined as fixed price or fixed price plus a percentage of the amount. As well IPS allows setting different fees for intervals for a number of transactions and amount of transaction.

2.1.11 Risk management

The IPS provides an opportunity to define different type of transaction processing limits to ensure effective risk management. The limits are defined by the system operator for a particular participant (direct, indirect and payment initiator) when signing the participant’s agreement.

The IPS supports the following limits:

- Total allowed amount and number of incoming (credit) transactions per calendar day;
- Total allowed amount and number of initiated (debit) transactions per calendar day;
- Maximum allowed amount of single credit transfer transactions.

Additionally, the system allows to define the following limits for a calendar day, week, month, quarter, or year:

- Total allowed number of initiated Credit Transfers;
- Total allowed number of initiated Request to Pay messages;
- Maximum allowed number of transactions during offline hours;
- Maximum allowed number of transactions in the batch.

Additionally, IPS supports limits for requests to Aliase Service system. The schema may define separate limits for:

- Look-up requests
- Alias Management requests.

These values allowed to be defined as “unlimited”.

The limits are registered by the IPS administrator when registering a new participant agreement via the Administration Portal.

2.1.12 Reporting

Direct Clearing Participants (Settlement Agents) receive the following reports from IPS:

- CRR - Cycle Reconciliation Report after each reconciliation cycle
- DRR - Daily Reconciliation Report summary reconciliation data for the completed clearing date.

Additionally, Participant can download the same report from the Portal in CSV format.

The message elements are the same in both reports. The reports contain reconciliation data for the Participant and its affiliated Settlement Serviced Participants. Settlement Agents who did not send or receive transactions in the cycle will receive an empty CRR.

Cycle reconciliation reports are generated per Direct and Indirect Participants on each processed transaction by type (credit transfer, payment return), by direction (debit or credit) and by the final status (cleared and settled or rejected).

Cycle reconciliation reports for indirect participants contain transaction data related only to this particular indirect participant. Reports for direct participants contain all transaction data related to this direct participant and all its Settlement Serviced participants.

Daily summary reconciliation report per Direct Participants contains the following data:

- total amount and number of credits,
- total amount and number of debits,
- total amount and number of erroneous transactions by rejection codes,
- opening and closing balances of a settlement account.

All reports can be adjusted to customer needed.

Available reports for IPS Operator:

- Fee basic report by Participant
- Fee extended report by Participant (by transaction)
- Transaction reports
- Participant reports

The report is generated by IPS Administrator via the IPS Administration Portal. The report can be downloaded in CSV and PDF format.

2.1.13 Administration Portal

The IPS provides a web-based Graphical User Interface where all configurable parameters, business processes, workflows, and access rights can be managed.

The Administration Portal provides the following functions:

- Participant Management - the function that ensures registration and maintenance of the participants, assigning the participant types and defining the relationships between the participants. As well Participant Management ensures necessary functions for participant connection to the system – definition of connection endpoints and access rights setup.
- Transaction processing limit (by transaction total amount and transaction total volumes) configuration per participant - the function that allows defining different types of limits applicable to the transaction processing within the system.
- Fee configuration per participant - the function that allows defining different fees applicable to the participant activities within the system.
- Timeout settings per participant - the function that allows defining timeout settings applicable to the transaction processing within the system.
- Upper, Lower and Base position definition per participant - the function that allows defining participant's individual liquidity monitoring settings applicable to the transaction processing within the system.
- Reports and transaction viewer - the function that ensures the possibility for the system administrator to generate reports supported by the system.
- Calendar - the function that allows to schedule banking working and non-working days and to configure the settlement sessions (cut-off cycles). As well Calendar allows the operator to see and review the results of processed settlement sessions (whether the Net Settlement message was successfully submitted to RTGS).

The Administration Portal supports the four-eyes principle, i.e. any participant data update, agreement data update, or participant status change made by one user must be approved by another user, who is authorized person to confirm the changes.

As part of Administration Portal, the IPS offers system monitoring functionality, which includes monitoring of all applications software modules, technical platform`s modules and activities of participants in the system. Functioning of key solution components supported, such as availability of HW resources (CPU, RAM, disc space), throughput (TPS), participant reachability.

Main data available with monitoring:

- Communication port status
- Real-time transaction statistics
- Approved transaction count;
- Error transaction count;
- Overall message throughput
- Throughput by source – throughput based on direct/indirect participant, BIC number.
- IPS processing time (latency) – average transaction processing time between IPS receiving incoming request/response to IPS sending request/response out.
- Participant Response time – average response time from Participant (from request sending to a participant to IPS receiving the response from participant).
- Full message processing response time (IPS + participant) – average response time between IPS receiving a request to IPS sending a response back.

IPS Monitoring module could integrate with SMS gateway and/or Mail server to send notifications alerts to system administration. Alerts and their delivery channels are configurable.

2.1.14 Proxy Service

Within the framework of the instant payment service, IPS offers Proxy Service (Central Alias Service). The purpose of the Proxy Service is to ensure the possibility of identifying the account number and BIC corresponding to the alias (for example, mobile phone number) in order to make the initiation of payments easier by using an alias instead of entering account numbers and other necessary payment details. The Proxy Service contains information about the aliases, account numbers and the related information of the customers of IPS participants that have applied for using the Proxy Service.

The Proxy Service supports the following features:

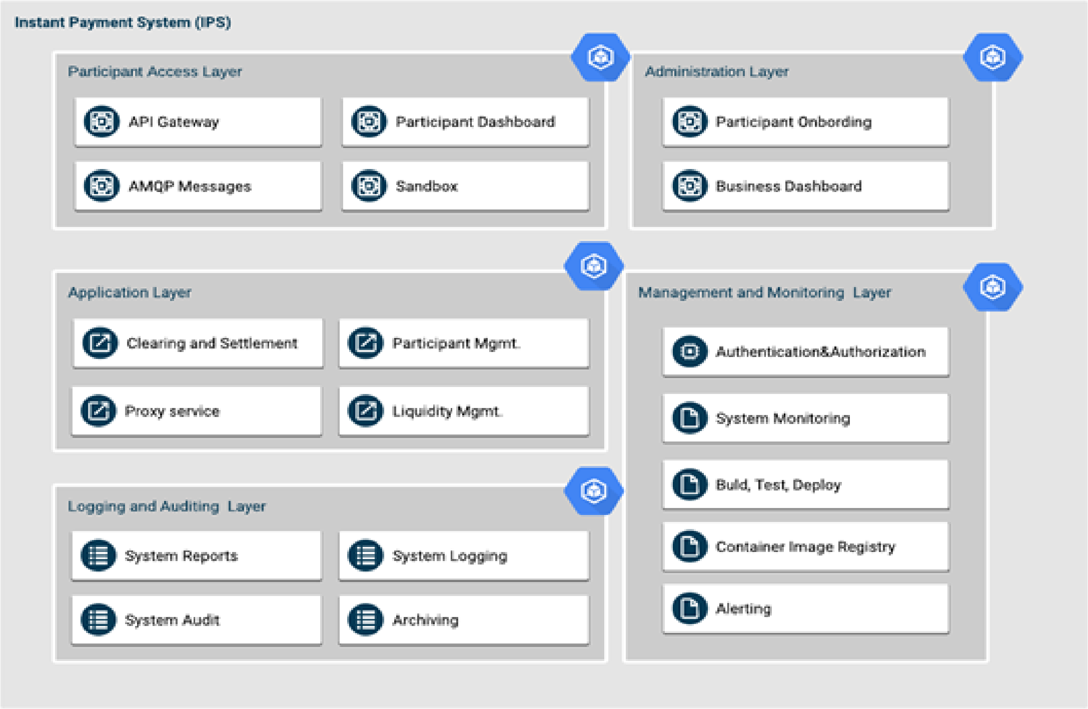
- online service, 24/7/365
- supports only non-financial messages
- response message on alias based look-up
- response message on account number based look-up request (for example, a list of registered aliases for a particular account number)
- response message on the new record registration request
- response message on the deletion of the record

2.2 Solution technology and architecture

2.2.1 Logical architecture

The IPS is a multi-tier application built on open industry standards and frameworks such as the cloud-native framework. The tiers within the application stack are well separated and can be deployed independently. The platform follows the modern, microservices architecture.

Microservices-based architecture: the business logic is implemented as stateless services, deployed as separated applications. The applications are loosely coupled and support hot deployment: installation of fixes, new versions can be done in the live system without any outage. With microservices there are lower requirements on the infrastructure, micro container or containerless approach are also options.



TietoEVRY IPS Logical scheme

2.2.2 Scalability

The IPS system installed with the scalability of the IPS application services to run multiple instances. This is a requirement for performing updates without affecting application availability. By default, the maximum number of Pods that can be unavailable during the update and the maximum number of new Pods that can be created is one. As your IPS deployment grows, you may need to increase the amount of storage available. How you scale up storage depends on which type of file system you are using for your persistent storage.

Scaling up performance is done via the total number of pods. The more hardware resources you have, the more pods you deploy.

The solution can be scaled seamlessly without downtime or service interruption; Kubernetes implies horizontal scaling. The solution design is made for “dedicated” infrastructure and no automatic expansion was foreseen.

2.2.3 Auditability

Auditability is an important concern IPS addresses. The solution is built in such a manner that all the actions made and consents received are logged and stored. If required, it is possible to find who and when made a change or what was actions provided for a particular payment and other services called.

2.2.4 Availability

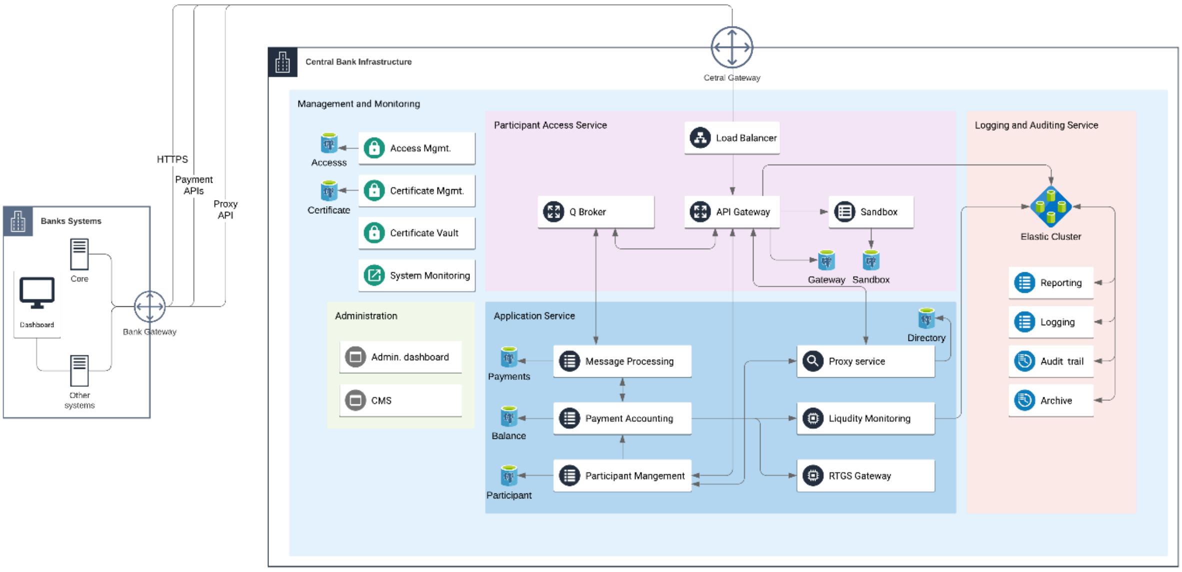
The solution is installed on each site independently. Further, the operator automatically sets all the necessary components and checks the link between sites. Site-to-site connectivity is established using the Discovery service. To achieve the non-functional requirement regarding 24x7 and 99.99 availability Customer needs to comply with provided by TietoEVRY hardware and software requirements.

RECOVERY TIME (RTO) AND POTENTIAL DATA LOSS (RPO)

Event	RECOVERY TIME (RTO)	Potential Data Loss – RPO
Disk failure	Zero	Zero
Machine and recoverable database instance failures	Zero to 60 seconds	Zero
Application instances failure	Zero to 60 seconds	Zero
Data corruption and unrecoverable database outages, availability domain outages (power, network, etc)	60 Seconds	Zero
Site outages	60 Seconds	Zero
Database reorganization, file move, eligible one-off patches	Zero	Zero
Hardware and software maintenance and patching	Zero to 60 seconds	Zero
Database upgrades (patch-sets and full releases)	Zero to 60 seconds	Zero
Application upgrades that modify back-end database objects	Zero to 60 seconds	Zero

2.3 Physical architecture

The following figure shows the physical architecture of the potential proposed solution.



TietoEVRY IPS Physical architecture

2.3.1 Reverse proxy/load balancer server

The communication using HTTPS connection is planned to be intercepted by a Reverse Proxy server, recommended that it is deployed in the DMZ.

2.3.2 Firewalls

The access from the Internet is protected by the first level firewall(s), Usually, the firewalls and reverse proxy servers deployed in the DMZ are either separated software or dedicated hardware devices, in most cases, the firewalls already have RP capabilities. Depending on the availability of these devices we are planning to use existing infrastructure elements.

2.3.3 API Gateway

Handles participants authentications, web sessions, third-party integrations in front of the microservices layer. Responsible for monitoring, authorization, and authentication of users handle user web sessions. API Gateway plays the role of Access Layer for Participants of the Schema to the different components of the solution in Central bank infrastructure of Instant payment solution. API Gateway unites all internal systems and publishes those services via one unified API.

2.3.4 Microservices

Small packages of components, implement business logic, deployed as standard applications in Docker. API of the components are exposed as stateless rest services. Each package has its own responsibility, application as component packages are loosely coupled, using interfaces and queues and inter-calls between the apps.

2.3.5 Database provider

IPS Solution solutions are database agnostic and support traditional relational databases. Oracle DB and IBM DB2, MS SQL, MySQL are supported on a product level, however, through configuration, the customer's preferred database provider is also supported. The solution also supports databases without the more expensive enterprise features, thanks to the built-in data sharing, and the whole application can run on the Oracle Standard Edition licence.

2.3.6 Certificate Management

Certificate Management retrieves, stores and verifies eIDAS (x.509) certificates participant present during communication with a central bank, as well as verifies CA and participants themselves. When participants present their certificates for the first time, data certificates contain are used to enrich participant profile information stored by participant Management. Certificate management gives a possibility to issue and manage self-signed certificates (seal and client). Self-signet certificates also are based on eIDAS (x.509) standard.

2.3.7 Infrastructure monitoring

With the help of Prometheus, the Customer monitors various computer resources, such as memory, CPU, disk, network, and software components and system health metrics. It may also be important for us to count the number of calls to the methods of our API or measure the time of their execution, because the greater the load on the system, the more expensive is its downtime. And this is where Prometheus comes to the rescue.

Each Software Component collect application parameters and check the metrics, then Prometheus will be able to pick up CPU, Memory, and Threads. Reports cover the Alert-Manager module. For graphs, you need to draw a dashboard in Grafana.

Within the Solution TietoEVRY will provide:

- Pre-configuration to collect these logs under Prometheus (Prometheus on their side)
- Configuration for Alert-Manager under these metrics
- Configuration dashboard for Grafana under these metrics.

2.3.8 Built-in IPS Monitoring

IPS built-in monitoring provides a complex predefined view of system metrics include important hardware checks. This a completed monitoring viewer is available via the IPS administration portal. Monitoring consists of one pre-defined dashboard that displays the most important system and business parameters paraments: system health, transactions performance and statuses, participant statuses.

2.3.9 User Access Right Management

IPS access management uses role-based access control defined over data and operations in the System. Upon installation is provided with a predefined set of operational roles per each system part, that are available for composing realm roles to assign to newly defined users according to their intended use of the system. Data access is specified by a list of available participant identifiers, while operational roles are split into administrative, everyday operations and read-only access to each system part.

IPS uses single-sign-on (SSO) mode for user sessions when their effective rights are encoded in jwt bearer tokens and checked by each accessed service according to OIDC protocol.

Different user roles can be defined to configure appropriate access rights according to the central bank and its customers' needs. Each role has its independent configuration that defines which user with the roles assigned is or is not authorized to perform. Configuration can be edited by the central bank if needed. This part is using realms from main access management from IPS.

2.4 Security pillars

Product and the support team independently monitories the OWASP standards, new vulnerabilities, updates of third-party libraries, and known security issues. Periodically the support and product team releases patches for updating security elements of the product and keeping the used third-party libraries, components up to date. In urgent cases, the support provides hotfixes immediately and notifies all of our customers about the hotfix deployment required, and provides further information about the risks, issues which are needed to be fixed immediately.

Following OWASP recommendations:

- Forced Transport Layer Security on remote connections and between the app layers
- JSON Web token is used for clients to enhance the security (API Security based on EBA requirement about API security).
- CSRF token and API Keys.
- All communication is secured with an additional PKI element. The solution can be also integrated with third-party 2FA (eg. Vasco token solutions)
- Audit trail component tracks, stores and validates all requests, responses in the system and provides reports, and provides a searchable interface in the Administrative console.
- Payment data integrity and protection are ensured by encrypted transmission over mutually authenticated connections of digitally signed messages, while data on rest is protected in an ACID-compliant database stored on encrypted data volumes on mirrored drives in raid10 configuration.
- TietoEVRY software follows the recommendation of the PCI Software Security Framework (SSF) for the secure design and development of payment software. As stated earlier, the PIC-SSF replaces the PA-DSS with new requirements that support a variety of payment software types, technologies, and development techniques.

2.5 Performance

The IPS Solution will comply with the performance targets listed below, considering that the customer follows the hardware recommendations set forth by TietoEVRY:

- The System must process an end-to-end transaction within five (5) seconds.
- The System must be able to handle operation at a minimum of at least four hundred (100) transactions/second (TPS).
- The System must support at least twenty (100) concurrent users and must be scalable to add more users in a short period.
- The System must be able to process payments, including payments over the alternate network, through necessary risk controls in less than one (1) second.
- The System must have a general GUI response time within two (2) seconds while moving between functions/screens.
- The System must not take longer than three (3) seconds to complete any one enquiry.
- The System must not take longer than five (5) seconds for any one user to login.
- The System must not take longer than three (3) seconds to generate common reports.
- Any enquiries or reporting must not affect overall system performance.
- The System operates 24/7 with no interruptions.

2.6 GDPR

TietoEVRY has developed and implemented the Global Data Protection Regulation (GDPR) program based on its privacy engineering frameworks adapted with the Regulation and regardless of solution delivery model. Thus, the principles of privacy and security by design and by default are applied. Following the context of Clause 78 of the Regulation, when developing, designing, selecting, and using products and solutions that are based on the processing of personal data or process personal data to fulfil their tasks, TietoEVRY considers the right to data protection with due regard to the state of the art, to make sure that controllers and processors can fulfil their data protection obligations and improve their GDRP-readiness.

3. Proposed implementation strategy

3.1 General approach

The TietoEVRY IPS implementation methodology describes the fundamentals of our implementation approach and execution – see attached **Annex TietoEVRY PPS_NBM_v1.**

3.2 Implementation: phases, milestones, duration, priorities

The allocated TietoEVRY project manager is responsible for preparing the implementation project together with the customer. The project manager coordinates changes and activities into an implementation project plan. The prepared plan describes the project from a calendar view, including task descriptions, project stages, tasks duration, starting and ending milestones, planned time for each task, and a responsibility summary.

It is highly recommended to start with a pre-study analysis to properly scope all requirements and capture any gaps (functional, non-functional and integrations). Only after pre-study efforts, it is possible to fully scope, plan timelines and budget such implementation works precisely. The result of the pre-study will be a detailed Solution Description document prepared by TietoEVRY, based on which implementation effort, including necessary gaps development, can be estimated.

The proposed preliminary implementation plan, phases, duration of steps can be found:

1. **Annex TietoEVRY IPL_Estimation_ips_Moldova_v1.1**, which includes Gantt chart, critical paths.

*(**NOTE**: Microsoft Project Plan (.mpp) format file cannot be electronically signed and submitted via "RSAP / MTender" (achizitii.md), thus we provide a .pdf format file with the tender proposal. Microsoft Project Plan (.mpp) format file can be shared in a different way in addition upon Customer`s request.)*

2. **Annex TietoEVRY IPL_WBS_ips_Moldova_v1.1** – originally Microsoft Excel format exported from .mpp format file, to show the implementation tasks and milestoned in the text list.

*(**NOTE**: Microsoft Excel (.xlsx) format file cannot be electronically signed and submitted via "RSAP / MTender" (achizitii.md), thus we provide a .pdf format file with the tender proposal. Microsoft Excel (.xlsx) format file can be shared in a different way in addition upon Customer`s request.)*

Finalized detailed Project Plan will be submitted to the Bank for approval during Pre-Study Phase of Project implementation.

3.3 Description of working principles

Preliminary working principles are described within **Annex TietoEVRY PPS_NBM_v1**. After the project Pre-Study phase those will be updated according to project specifics and agreed upon between parties.

3.4 Working hypotheses

General working hypotheses and working principles of successful project implementation are described within **Annex TietoEVRY PPS_NBM_v1.**

Working environment requirements are described in the Section Work environment of **Annex TietoEVRY PPS_NBM_v1**

Obligations of parties are divided into two parts:

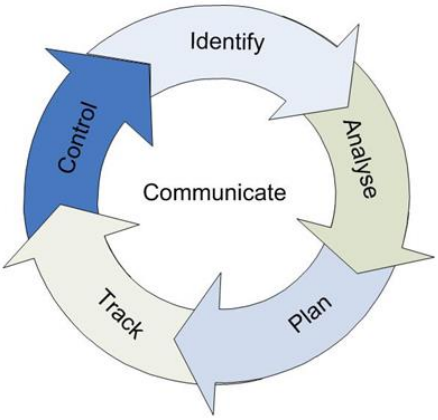
1. In Section Preconditions and outer dependencies of **Annex TietoEVRY PPS_NBM_v1**.
2. In **Annex TietoEVRY IPL_Estimation_ips_Moldova_v1.1 -** the preliminary plan where Customer/Vendors resources are assigned to a specific task.

*(**NOTE**: Microsoft Project Plan (.mpp) format file cannot be electronically signed and submitted via "RSAP / MTender" (achizitii.md), thus we provide a .pdf format file with the tender proposal. Microsoft Project Plan (.mpp) format file can be shared in a different way in addition upon Customer`s request.)*

For successful project implementation, it is recommended to use the TietoEVRY Standard Project management methodology which is described in **Annex TietoEVRY PPS_NBM_v1.**

3.5 Risk management

The TietoEVRY risk management strategy is followed in the project.



Identify: Search for and locate risks before they become problems adversely affecting the project

Analyse: Process risk data into decision-making information

Plan: Translate risk information into decisions and actions (both present and future) and implement those actions

Track: Monitor the risk indicators and actions taken against risks

Control: Correct for deviations from planned risk actions

Communicate: Provide visibility and feedback data internal and external to your program on current and emerging risk activities

The project risks for this project are identified, their impact and probability assessed, and mitigation actions and contingency plans with responsibilities developed when the project estimation process ongoing.

The Project manager analyses the status of each risk and reports it in a project status report. The risks are monitored in every steering group meeting. The basic approach is continuous risk management.

For each of the risks the following information should be provided:

Description – a description of the risk;

Source – risk source can be defined from the following choices:

- Project – e.g. risks related to schedule, scope or costs
- Customer – e.g. risks related to customer dependencies
- Result – product/solution related risks
- 3rd party – risks related to 3rd parties
- ICO / Regulator – risks related to ICO or other regulators (e.g. legal) requirements
- Human resources – risks related to human resources, competencies, resource turn-over etc.
- HW / Environment – risks related e.g. to HW performance, environment readiness
- Technologies – risks related to platforms, open-source SW and other technologies
- Other

Impact on a project – Low, Medium, High, Critical;

Probability – Low, Medium, High. When risk comes true, this has to be moved to section Issues and to be addressed by PDs;

Priority – rated from 1 to 9 where 1 is the highest priority and 9 is the lowest. For the priority calculation the following formula is used:

- Priority = Impact X Probability
- (High=1; Medium=2; Low=3)

Status – short description of status (open, in-progress, closed).

For **Impact on project** the following categories are defined:

- High – project execution may be stopped. (Greater than 20% slip in schedule, greater than 20% cost overrun, greater than 20% reduction of functionality/delivery scope)
- Medium – project execution impacted, though the project can still be executed with medium adjustments (10-20% slip in schedule, 10-20% cost overrun, 10-20% reduction of functionality/delivery scope)
- Low – project execution may continue, with negligible impact on the project.

For **Probability** the following categories of risk becoming true are defined:

- High – 71-99%
- Medium -31%-70%
- Low – 0-30%

In both Internal and External Steering minutes the Risk List must be followed up.

Risk management including risk list and risk analysis information can be found on the project page (extranet).

Risk management principles are described within **Annex TietoEVRY PPS_NBM_v1**, within the section Project risks management.

3.6 Interoperability approach

Interoperability/Integration approach and preliminary testing strategy is described in Section Test strategy of **Annex TietoEVRY PPS_NBM_v1**

4. Approach, deliverables, methodology and tools used for project different phases

The proposed way of implementation with the corresponding project approach is described within **Annex TietoEVRY PPS_NBM_v1** and can be changed during the project Pre-Study phase. The same approach will be applied for each project phase.

4.1 Project Management related activities

Most of the Project Management related activities are described in Section Project development and management processes of **Annex TietoEVRY PPS_NBM_v1**.

To realize the project goals following professional services will be provided by TietoEVRY:

- Project Management
- Pre-Study
- Technical & user training
- Preparation of test environment in TietoEVRY
- Development of identified GAPs and their implementation
- Solution installation and configuration on MNB test environment
- Test scenario preparation
- Preparation of Project supporting documentation(technical & administrative)
- Validation and Functional tests
- Integration tests of the implemented solution
- Integration tests with two participant Banks selected by NBM
- Support of testing performed by NBM
- User Acceptance Tests requested by NBM and agreed in Master Test Plan
- Analysis of test results
- Project GO-LIVE/post-GO-LIVE support

4.2 Analysis phase

Pre-Study Phase (**Business Analysis Phase)**:

ID	Description of Deliverable	Responsible
1	Detailed software requirements specification of the solution proposed for the implementation with clear link/track of the particular requirements to the process(es).	TietoEVRY
2	Detailed acceptance criteria.	TietoEVRY
3	Concept of the data model of the Solution.	TietoEVRY
4	Conceptual architecture of the solution and infrastructure diagrams.	TietoEVRY
5	Detailed and updated (within given timelines) project plan for the rest phases of the implementation.	TietoEVRY
6	Initial version of detailed, accurate and up-to-date task/issue/risk log, which will be updated throughout the full project.	TietoEVRY
7	Project plan with the updated set of deliverables.	TietoEVRY
8	Fit analysis document	TietoEVRY
9	Solution Description	TietoEVRY

Acceptance Criteria's:

- 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 to elimination.
- The deliverables of the analysis phase shall be provided to the NBM in accordance with the project plan.
- NBM shall not have any objections regarding the completeness and correctness of the document, in accordance with agreed quality and other criteria.
- Deliverables meet the NBM expectations and requirements in terms of clarity, level of detail, structure, content, etc.
- Deliverables are aligned with internal standards of the successful Tenderer and best practices.
- Deliverables are easy to use and understandable to the intended beneficiaries.
- Deliverables are aligned with quality standards agreed between the NBM and the successful Tenderer.
- Acceptance documentation for the analysis phase are approved by the Parties.

4.3 Design phase

Environment and solution preparation (**Design Phase)**:

ID	Description of Deliverable	Responsible	Deadline
1	Solution Description to be updated with • Solution overview • integration platform of solution components, interfaces (the name that will be integrated with the solution, the type of interface (e.g., supplier, consumer, symmetric), solution and the impact of the failure of the interfaces); • solution architecture attributes (software and hardware technologies, services, components, portability, capacity, availability and reliability, scalability); • Continuity plan and disaster restoration - BCPDR (specifying architectural attributes necessary to meet solution requirements for BCPDR); • data architecture (context diagrams, logical data model); • security architecture (overview of security solution);	TietoEVRY	TBA
2	Solution configuration and installation guides	TietoEVRY	TBA
3	Testing documentation: • Master Test plan • Test Strategy • Test scenarios for planned test activities	TietoEVRY	TBA
4	Solution validation tests have been successfully finished	TietoEVRY	TBA

Acceptance Criteria's:

- The acceptance criteria shall be revised and agreed upon with the NBM at the initiation phase. The below-mentioned criteria are minimal and shall not be subject to elimination.
- The design phase-related deliverables shall be provided to the NBM as per the project plan.
- NBM shall have no objections regarding the completeness and correctness of the document in accordance with the agreed quality and other criteria.
- Deliverables are in line with the NBM expectations and requirements – in terms of clarity, level of detail, structure, content, etc.
- Deliverables are aligned with successful Tenderer's internal standard and with the best practices.
- Deliverables are easy to be used and understood by the targeted beneficiaries.
- Deliverables are in line with quality standards agreed between the NBM and the successful Tenderer.
- NBM shall have no objections regarding chosen solutions.
- An acceptance report shall be signed by both parties within the agreed time period.

4.4 Solution preparation on-site (Build phase)

ID	Description of Deliverable	Responsible	Deadline
1	Solution, installed and configured in the following environments: • Test environment • Development environment • Training environment • Production environment	TietoEVRY	TBA
2	Solution is installed according to Solution Description document approved in Pre-Study phase	TietoEVRY	TBA
3	Solution support documentation(User and Administrator Guides)	TietoEVRY	TBA
4	Security documentation(user management, roles, encryptions)	TietoEVRY	TBA
5	Technical deployment document prepared	TietoEVRY	TBA

Acceptance Criteria's:

- The acceptance criteria shall be revised and agreed upon with the NBM at the initiation phase. The below-mentioned criteria are minimal and shall not be subject to elimination.
- Deliverables shall be provided to the NBM as per the project plan.
- NBM shall have no objections regarding the completeness and correctness of the document.
- Deliverables are in line with the NBM expectations and requirements – in terms of clarity, level of detail, structure, content, etc.
- Deliverables are aligned with successful Tenderer's internal standard and with the best practices.
- Deliverables are easy to be used and understood by the targeted beneficiaries.
- Deliverables are in line with quality standards agreed between the NBM and the successful Tenderer.
- An acceptance report shall be signed by both parties within the agreed time period.

4.5 Testing phase

ID	Description of Deliverable	Responsible	Deadline
1	Tests conducted according to • UAT scenarios • Master Test plan • Testing strategy	TietoEVRY	TBA
2	Evidence report, test result report	TietoEVRY	TBA

3	Updated testing documentation: • Master Test plan • Test Strategy • Test scenarios for planned test activities	TietoEVRY	TBA
4	Solution validation tests have been successfully finished	TietoEVRY	TBA

Acceptance Criteria's:

- All tests shall be completed without severity levels Critical or Blocker.
- The testing process shall consist of as many test cycles as necessary until all severity Critical and Blocker issues will be eliminated. After Severity Critical or Blocker problems will be fixed, it is for the NBM testing team to decide whether the test cycle will be restarted or continued.
- The number of outstanding defects is below an acceptable upper limit (to be agreed before the acceptance phase) or the faults are minor.
- Acceptance document agreed and "signed-off" by both parties.

4.6 Training phase

ID	Description of Deliverable	Responsible	Deadline
1	Training is conducted in accordance with the agreed Training Scenario	TietoEVRY	TBA

Acceptance Criteria's:

- The training sessions have been organized.
- Knowledge Testing Questionnaires demonstrate that end users have an acceptable level of knowledge.
- The NBM has no objections regarding the integrity and the correctness of the training materials.
- Deliverables correspond to the expectations and requirements of the NBM - in terms of clarity, level of detail, structure, content, etc.
- An acceptance report shall be signed by both parties within the agreed time period.

4.7 Go live and Final Acceptance phases

ID	Description of Deliverable	Responsible	Deadline
1	The solution is ready for launching into production (the solution was installed in a production environment, testing was performed and no severity Critical and Blocker defects were found).	TietoEVRY	TBA
2	Plan for resolution of all found minor issues has been prepared and agreed by parties	TietoEVRY	TBA
3	Self-assessment document	TietoEVRY	TBA
4	UAT conducted by Customer, relevant issues have been reported with all necessary information.	NBM	TBA
5	Issues found during the UAT phase has been solved or an issue resolution plan was agreed	TietoEVRY	TBA
6	Solution supporting documentation(Techincal documentation, user & administrator guides) has been updated and reviewed by NBM	TietoEVRY	TBA

Acceptance Criteria's:

- Successful Tenderer's self-assessment report demonstrates that all business and technical requirements were fully delivered.
- No major bugs identified during the UAT period.
- No discrepancies found between the NBM self-assessment report and the successful Tenderer self-assessment report. In case discrepancies found, these shall be removed prior to the final acceptance of the soak period.

- An acceptance report shall be signed by both parties within the agreed time period.

5. Response to specifications and requirements F4.4

5.1 Functional requirements (FR)

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 to the best practices in the industry.	Mandatory
Answer	Answer: TietoEVRY Instant Payment Solution (IPS) is an end-to-end solution for account-based payment processing, that provides payments business transition for central processors, national or central banks to real-time payments. IPS provides a platform for centralized payment infrastructure connecting banks and 3rd party PSPs for consistent, real-time, irrevocable money transfers processing, which is settled through the national real-time gross settlement (RTGS) system.	
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
Answer	Answer: The system process messages based on ISO 20022:2013 standard. The standard can be accessed here: https://www.iso.org/standard/55005.html.	
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

Answer	Answer: The IPS conducts specified input verifications on messages prior to the further processing of the messages. The following validation is performed: • Security Validation; • Format Validation • XML schema validation, including validation of the existence of mandatory fields defined in the message format, and of optional fields used in one of the processes ; • BIC validation; • Duplicate Validation (the unique key reference is used); • Business and Schema rules validation (such as timeouts and transaction limits). • Timestamp validation against time-out parameters.	
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
Answer	Answer: IPS validation algorithm is based on the approach described in the requirement – as soon as any validation fails, the message will be rejected with an appropriate error message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project.	
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
Answer	Answer: Digital signature existence is proved on connectivity level before technical and business validation. ACK and NACK messages could be processed without digital signatures according to NBM requirements (communication and digital signature requirements could be configured)	
FR.6	IPS enables A2A interface to users. *IPS enables sending messages in A2A mode to users.*	Mandatory
Answer	Answer: The IPS provides secure payment and information exchange via secure network connectivity. All users will use the same type of technical connectivity for exchanging messages in A2A mode.	

FR.7	IPS enables users to use web interface. *IPS allows users to perform monitoring and reconciliation of payments via web interface.*	Mandatory
Answer	Answer: Workplace for Participant provides a Web-based interface accessed through a closed network only for participants (users) and enables the Participants to view system status (events end alerts), manage liquidity, view transaction information and perform transaction reconciliation. From the web interface multiple system reports are available.	
	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
Answer	Answer: For liquidity management, each Participant has one (1) IPS agreement and one (1) IPS liquidity account. Liquidity accounts could be built on hierarchies, to provide sponsor/sponsored or direct/indirect relationships. This functionality enables the required uniqueness of the Participant liquidity account as well as required multi-level hierarchies.	
FR.9	Every IPS account has an account structure, established by operating rules.	Mandatory
Answer	Answer: Yes, every IPS account follows operating rules, and IPS allows to configure account structure according to country-specific operating rules.	
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
Answer	Answer: Yes, every Participant liquidity account can be uniquely identified by means of unique sending and receiving participants unique identification codes such as BIC. IPS Participant management facility allows to set up Instant Payment scheme participants, their processing related data such as BIC code (or pseudo BIC) or any other identifier, as well as assigned authorization roles, participant type and other processing parameters such as processing scenarios, liquidity parameters, limits.	

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
Answer	Answer: In IPS Participant management facility for Direct Participant mandatory field is RTGS systems account number for transaction & liquidity position exchange between IPS liquidity account and correspondent account in RTGS	
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
Answer	Answer: In the IPS Participant management facility for Indirect Participant IPS account is connected to the IPS Direct Participant account, to manage the summary liquidity position of Direct Participant (Direct participant position + attached Indirect Participants positions). But Direct Participants IPS account is connected to exactly one RTGS account. That way it is ensured required functionality, that every Indirect Participant in IPS has an open IPS account connected to exactly one RTGS account of the Direct Participant.	
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
Answer	Answer: Required account relationship model is ensured by in the FR.12 described model. Direct Participant’s account in the IPS correlates with the Direct Participants account opened in the RTGS system. Indirect Participant connects to and settles through a Direct Participant. Each Direct Participant can be Settlement Agent for several (zero to many) Indirect Participants.	
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
Answer	Answer: Limits are set up on participant level, Direct Participant manages own and also connected Indirect Participants limits.	
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

Answer	Answer: Authorized Participants communicates through messages with IPS for liquidity management position adjustments. All messages are validated on technical and business validity. This is a part of IPS liquidity management functionality. Limit and its utilization could be seen from Participant Portal or by API request	
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
Answer	Answer: IPS validation algorithm is based on the approach described in the requirement – as soon as any validation fails, message processing will be disrupted with an appropriate error message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project.	
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
Answer	Answer: Authentication and authorization facility allows to build business rules for required authentication and authorization procedures. All participants must be identified in order to determine if they have the right to use the system, including the setup of account limit and validation against BIC correspondence with RTGS account number. The facility allows to determine participant allowed transactional functionalities: • allowed transaction types; • allowed BICs; • possible to configure additional transaction information related functionality authorization controls.	
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
Answer	Answer: IPS updates the liquidity positions of the Participants in real-time by processing positively confirmed transactions. All messages that would bring Participant's liquidity position below zero, including above described liquidity adjustment messages, will be rejected.	

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. *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).*	Mandatory
Answer	Answer: This functionality is configurable according to central processor business rules. In particular case, IPS will be configured to allow set up independent from coverage limits on IPS accounts. As described, liquidity position towards RTGS account balance will be monitored for each particular transaction.	
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
Answer	Answer: IPS will generate alerts for the Participant if the upper or the lower limit is breached and send a notification to the respective Direct and Indirect Participants.	
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
Answer	Answer: IPS will generate alerts for the Participant if the threshold against the RTGS account (liquidity position in IPS) balance is breached. Alert notification will be sent to the respective Direct Participant.	
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
Answer	Answer: Liquidity position adjustments are executed according to preconfigured liquidity adjustment cycles (multiple times per RTGS working day, which could be configured in IPS to follow existing RTGS cycles). Participants can also send induvial liquidity adjustment transactions in MT202 format or in MX message formats. IPS could receive and process such messages 24/7, so message availability is dependent on RTGS business day and operating hours.	

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
Answer	Answer: Liquidity position adjustments are executed according to preconfigured liquidity adjustment cycles (LAC) - multiple times per RTGS working day, which could be configured in IPS to follow existing RTGS cycles. The system could be configured for the required 2 mandatory cycles as described in requirements or more. The Liquidity adjustment process could be initiated also manually by System Operator.	
	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
Answer	Answer: Actual balance could be seen by authorized users of Participant from Participant portal (U2A) and by API call (A2A) from authorized Participant. Only accounts owned by a particular Participant is accessible.	
FR.25	IPS must enable Direct Participants to view the balance of the RTGS account in IPS. *U2A and A2A*	Mandatory
Answer	Answer: Actual balance on IPS shadow account of RTGS account could be seen by authorized users of Direct Participant from Participant portal (U2A) and by API call (A2A) from authorized Direct Participant. Only accounts owned by a particular Direct Participant is accessible.	
FR.26	IPS must provide all the queries necessary for monitoring the work in the system to Participants.	Mandatory
Answer	Answer: IPS provides the Participant portal where participants can monitor activities, limits, liquidity position and performance on U2A mode. As well the same functionality is available by APIs on A2A mode.	
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. *Statement of account turnover and Statement of account for all Participant accounts.*	Mandatory

Answer	Answer: At the end of the calendar days, at the end of the last Reconciliation cycle, in addition to the current intraday report (CRR), the IPS system generates a so-called DRR (Daily Reconciliation Report), which contains the Outgoing and incoming messages of the Direct Participant and its associated Indirect Participants, number of and aggregated by amount, as well as broken down by sending and receiving party.	
FR.28	IPS should provide generation of reports that contain data available since the last report up to the present moment.	Mandatory
Answer	Answer: Each transaction in IPS is automatically assigned to a Reconciliation Cycle. As for that cycle, the closing date has been reached, the transactions are automatically assigned to the next cycle, so the IPS system ensures that each transaction is included in only one Reconciliation cycle. Reports are made automatically for Reconciliation Cycles ensuring compliance with NBM requirement.	
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
Answer	Answer: IPS will validate the authorisation of Participants according to pre-defined roles, access rights and account ownership. NBM will be assigned a role to query all accounts, while Direct Participants only those connected to particular Direct Participant RTGS account.	
7.1.4. Administrative functions		
FR.30	IPS is required to enable the NBM to connect direct and indirect participants in the system.	Mandatory
Answer	Answer: Operator portal supports Participants management, including registration of participants and setting their allowed products and operational limitations.	
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
Answer	Answer: The IPS supports the Participant’s IPS account blocking/unblocking functionality, including separate blocking for credit and debit functions.	
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

Answer	Answer: Dedicated certification environment will be provided for Participant testing before onboarding. Scope of pre-defined tests to be agreed during pre-study as those depends on provided business functionalities. Certification environment provides a possibility to emulate live environment with test data – providing standard SLA monitoring reports.	
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
Answer	Answer: TietoEVRY IPS provides HTML based Graphical User Interface where all configurable parameters, business processes, validation workflows and access rights can be managed having sufficient rights within dedicated administrative roles.	
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
Answer	Answer: IPS solution allows management of relationships between Participants, including change of direct participant for the indirect participant.	
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
Answer	Answer: System supports functionality for suspending Participant with following capabilities of deactivation and deletion of Participant if all accounts related to Participant is with zero balance.	
FR.36	An appropriate software solution (A2A) needs to be provided for the NBM as a system participant.	Mandatory
Answer	Answer: NBM can be set up in the system as Direct Participant providing to NBM the same functionality as for others Direct Participants.	
FR.37	IPS needs to enable the NBM to define the maximum period for retention of transaction data in the system.	Mandatory
Answer	Answer: 1) IPS architecture provides a possibility to store data in any DBMS (Oracle, MySQL, PostgreSQL, etc.). Data retention in a database is managed by NBM using standard DBMS tools 2) For business logic on data processing availability (for instance time period for recalls; duplicate validation time period) there are system parameters that could be managed from the Administration portal.	

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.002 (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

Answer: Credit Transfer (pacs.008) is sent by Participants representing the Originator Bank to IPS and from IPS to the Participants representing the Beneficiary Bank in order to transfer funds from an originator to a beneficiary. To meet the requirements of the client, the message can contain custom data (e.g. proxy indicator or specific transaction indicator).

The payment status(pacs.002) report is sent by a Participant representing the Beneficiary Bank to IPS and from IPS to Participants representing the Originator Bank:

- Confirm acceptance or rejection of credit transfer that was initiated by Originator Bank
- As a positive or negative response to on status inquiry message that was initiated by the Originator Bank

The payment status(pacs.002) report is sent to both Beneficiary Bank and Originator Bank

- To inform about transfer order execution - positive confirmation messages

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

Answer: Fully support described process flow including pacs.008 and pacs.002.

7.2.1. ***General conditions (*IPS.PMNT.01)**		
FR.38	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
Answer	Answer: IPS processes messages in the order they arrive. Participants by themself couldn't influence IPS to process messages in other order.	
FR.39	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

Answer	Answer: IPS processes messages in the order they arrive using in-memory processing and maximizing straight-through processing ratio.	
FR.40	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
Answer	Answer: The IPS makes the reservation for the Credit Transfer amount on the IPS account of the Originator Bank.	
FR.41	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
Answer	Answer: The IPS support required data fields in transfer order for data source specification from CAS.	
FR.42	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
Answer	Answer: The IPS support the required option to specify data source in the transfer order.	
FR.43	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
Answer	Answer: The IPS support the required option in positive responses to specify/certify data compliance with presented data in payment order.	
7.2.2. ***Validation (*IPS.PMNT.02)**		
FR.44	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 are specified below. In addition to these, technical validations are also carried out.*	Mandatory

Answer	Answer: IPS validation algorithm is based on the approach described in the requirement – as soon as any validation fails, the message will be rejected with an appropriate error message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project. IPS performs several message validations including security, format (mandatory fields, field data), duplicate, BIC, business rules validation. The Error handling functionality allows to define the Error processing scenarios – based on SCT Inst and/or Local (LCT Inst) schema requirements.	
FR.45	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
Answer	Answer: The IPS support the required option to validate transfer order based on BIC and its correspondence of Participant authorisation.	
FR.46	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
Answer	Answer: The requirement correspondents standard IPS algorithm to identify IPS account based on BIC and currency.	
FR.47	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
Answer	Answer: The requirement correspondents standard IPS algorithm to identify IPS account based on Payee BIC and transaction currency.	
FR.48	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
Answer	Answer: The IPS support the required option to validate transfer order based on BIC. In case such BIC is not in the system in "Active" status, the transfer order will be rejected.	

FR.49	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
Answer	Answer: If IPS receives a duplicated Instant Payment Transaction, with the same unique key of an existing transaction, the second one will be rejected. A specific reason code is added to the rejection message. The unique key shall unambiguously identify the transaction throughout the entire interbank chain. Unique key = Transaction ID + debtor ID + Acceptance date and time Duplication checks are performed in IPS and are based on the unique key stored in the IPS repository. If needed, a unique key calculation algorithm will be adopted according to NBM requirements, based on Payer's BIC (AT-06 in DS-02 SCT Inst) and reference (AT-43 in DS-02 SCT Inst).	
FR.50	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
Answer	Answer: Account status checks are performed during transfer order validation. In case the IPS account is blocked, the transfer order will be rejected.	
FR.51	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
Answer	Answer: In case the IPS account is blocked, the transfer order will be rejected and the amount will not be reduced from the account.	
FR.52	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
Answer	Answer: In case the RTGS account is blocked, the corresponding IPS account based on information from RTGS will be blocked and the transfer order will be rejected and the amount will not be reduced from the account.	

FR.53	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
Answer	Answer: Account status checks are performed during transfer order validation. In case the IPS account is blocked for credits, all credit transfer orders will be rejected.	
FR.54	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
Answer	Answer: Account status checks are performed during transfer order validation. In case the IPS account is blocked for credits, all credit transfer orders will be rejected	
FR.55	IPS will not credit the IPS account if its RTGS account is blocked for crediting. *IPS will reject the transfer order if the RTGS account, connected to the IPS account that should be credited, is blocked for crediting.*	Mandatory
Answer	Answer: In case the RTGS account is blocked for credit, the corresponding IPS account based on information from RTGS will be blocked for credit and all credit transfer order will be rejected.	
FR.56	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
Answer	Answer: IPS enables time-out processing according to SEPA Inst. and/or local Instant rule book. Message processing time-out values are configurable parameters. Validation applies for both early and postpones arriving transactions against configurable parameters.	
FR.57	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
Answer	Answer: Account currency and transfer order currency validation are performed during transfer order validation.	
FR.58	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

Answer	Answer: IPS provides validation of operating day of the system and transfer order execution dates as well as account validity for operations in a particular operational day is validated.	
FR.59	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
Answer	Answer: IPS provides validation of operating day of the system and transfer order execution dates and synchronizes IPS account statuses based on account statuses in RTGS based on RTGS provided information.	
FR.60	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
Answer	Answer: IPS will provide validation of transaction amounts – for overall payment schema as well as individual Participant limits.	
FR.61	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
Answer	Answer: IPS will provide validation of both payee and payer IBANs presence in payment instructions according to specified business rules validation criteria.	
FR.62	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
Answer	Answer: IPS validation algorithm is based on the approach described in the requirement – as soon as any validation fails, the message will be rejected with an appropriate error message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project.	
7.2.3. ***Reservation of funds* (IPS.PMNT.03)**		

FR.63	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
Answer	Answer: IPS will reserve funds in Payer's IPS account (and with this also in the corresponding RTGS account) after business rule validation. In case of cancellation of the payment order, the reservation will be released immediately.	
FR.64	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 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.*	Mandatory
Answer	Answer: IPS will reserve funds in Payer's IPS account after business rule validation and reduce the available balance on the account. In case of rejection of the transfer order, the reservation will be immediately released.	
FR.65	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
Answer	Answer: IPS will not execute transfer order if there will be insufficient funds on the corresponding IPS or RTGS account.	
FR.66	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
Answer	Answer: In case the transfer order has been rejected response message will be sent to Payer. A specific reason code is added to the response message.	
7.2.4. ***Transfer order forwarding (*IPS.PMNT.04)**		

FR.67	IPS will forward a transfer order to the Payee if it was successfully validated and reserved.	Mandatory
Answer	Answer: IPS will route all successfully validated and reserved messages to the counterparty according to the content of the routing data.	
	7.2.5. ***Payee's response (*IPS.PMNT.05)**	
FR.68	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
Answer	Answer: The IPS expects the response (positive or negative) during a pre-defined period of time (configurable) and responds with time-out error messages to both parties in case if the response is not received during this period.	
FR.69	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
Answer	Answer: The IPS expects the response (positive or negative) during a pre-defined period of time (configurable) and responds with time-out error messages to both parties in case if the response is not received during this period.	
FR.70	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 a Participant in accordance with the operating rules and based on the functionalities described in section 7.9 "Participant unreachable function and pre-authorisation facility".	Mandatory
Answer	Answer: IPS stand-in functionality allows an administrator to configure described functionality of unreachable Payee pre-authorisation facility when the system credits Payee's account without waiting for a response from Payee.	
FR.71	IPS will notify the Payee in an appropriate message in case of response timeout. *Message sent is in the defined format.*	Mandatory

Answer	Answer: If the response is not received within the timeout, the transfer order is rejected. The IPS submits the negative pacs.002 with rejection reason "timeout" to both parties. The exemption is previously described as "stand-in" functionality when the system is configured to accept transfer orders without waiting for a response from Payee.	
FR.72	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
Answer	Answer: If the response is not received within the timeout, the transfer order is rejected. The IPS submits the negative pacs.002 with rejection reason "timeout" to both parties.	

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.73	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
Answer	Answer: IPS business validation algorithm is based on the approach described in the requirement – as soon as any validation fails, the message will be rejected with an appropriate error message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project. The IPS conducts specified business validations prior to further processing. These controls are based on the respective international (for SEPA Credit Transfer Instant - SCT Inst) and Local (LCT Inst) schemas rules.	
FR.74	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
Answer	Answer: Validation of response sender will be performed according to the BIC of Payee.	
FR.75	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

Answer	Answer: IPS will validate response message towards Payee's BIC and transaction reference, to ensure secure and trusted processing of transactions. All messages with the same reference will be linked to provide transparent monitoring and follow up of the message chain.	
FR.76	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
Answer	Answer: In case of errors both parties will be notified, appropriate reason code will be provided in a response message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project.	
FR.77	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
Answer	Answer: IPS will proceed with process flow according to the business validation procedure. Whenever transfer is executed successfully, transactions are booked as records in corresponding Participant accounts. In case of unsuccessful processing, the reservation in Payer's IPS account is released.	
7.2.7. ***Release of funds (*****IPS.PMNT.07)**		
FR.78	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
Answer	Answer: This is a standard process flow for the release of reserved funds. In case of unsuccessful processing, reservation in Payer's IPS account is released	
FR.79	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 response is negative), the reserved funds should be released for other orders or for liquidity transfer*.	Mandatory

Answer	Answer: This is a standard process flow for the release of reserved funds.	
FR.80	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.*	
Answer	Answer: Both parties will be notified about reasons for rejected order due to validation and in case of Payee rejection, the corresponding Payee code will be forwarded to Payer.	
7.2.8. *Execution – settlement* (IPS.PMNT.08)		
FR.81	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
Answer	Answer: IPS will execute transfer orders individually as they will arrive in the system.	
FR.82	IPS will execute the transfer order through IPS account. *Execution is done by debiting and crediting appropriate IPS accounts.*	Mandatory
Answer	Answer: This is a standard process flow for transfer order execution, initially all amounts are reserved in the Payer account. As soon as the transaction is completed amount is debited and credited to the appropriate Payer and Payee accounts.	
FR.83	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
Answer	Answer: This is a standard process flow for transfer order execution. Transfers are executed as they arrive and execution is done according to the operational date of the system that corresponds to the actual calendar date.	
FR.84	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
Answer	Answer: IPS execute transfer order in full amount. In case of error, the transfer order will be rejected in full amount as well.	
FR.85	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

Answer	Answer: This is a standard process flow for transfer order execution, as soon as the transfer is approved as executes, reserved funds are transferred to booked amount	
FR.86	IPS, by debiting/crediting the Payer's/Payee's IPS account reduces/increases the balance in their IPS accounts.	Mandatory
Answer	Answer: This is a standard process flow for transfer order execution. Every debit transaction decreases available balance and credit transaction increases available balance on IPS and corresponding RTGS accounts according to transfer amount.	
FR.87	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
Answer	Answer: This is a standard process flow for transfer order execution. Every debit transaction decreases available balance and credit transaction increases available balance on IPS and corresponding RTGS accounts according to transfer amount.	
FR.88	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
Answer	Answer: This is a standard process flow for transfer order execution. Future dated transfers and standing orders will be sent to Payee as soon as they arrive and will be processed in the same logic as same-day payments, including reservation of funds in Payer IPS/RTGS accounts on the same day. If needed IPS can provide reporting on future valued transaction balances for Participant liquidity and interest calculation purposes.	
FR.89	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
Answer	Answer: Notifications are sent to both parties in case of successful or unsuccessful transfers. The default language for the message is English, but it could be localized during the implementation project	
FR.90	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
Answer	Answer: This is a configurable option, Direct Participant could be notified if needed on connected indirect participants incoming and outgoing transfer orders.	

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.

Answer: All required recall messages are supported by IPS.

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.

Answer: This is a standard process flow of IPS for processing recalls.

7.3.1. ***Validation of recalls*** **(IPS.RECALL.01)**		
FR.91	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
Answer	Answer: IPS validation algorithm is based on the approach described in the requirement – as soon as any validation fails, message processing will be disrupted with an appropriate error message. Technical validations are performed before the business validations. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project.	

FR.92	IPS validation algorithm is based on the approach described in the requirement – as soon as any validation fails, the message will be rejected with an appropriate error message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project. 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
Answer	Answer: The IPS support the required option to validate recalls based on BIC and original transfer order.	
FR.93	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 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*.	Mandatory
Answer	Answer: The IPS support the required option to validate if IPS can reach Recipient (Based on BIC and list of Participant and their actual connectivity status)	
FR.94	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
Answer	Answer: Duplication checks are performed in IPS and are based on a unique key stored in the IPS repository. A specific reason code is added to the response message.	
FR.95	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
Answer	Answer: In case recall has an error during validation, the recall will be rejected and a response message will be sent to Payer. A specific reason code is added to the response message.	

7.3.2. ***Forwarding of recalls (*****IPS.RECALL.02)**		
FR.96	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). *After the stated validations, IPS does not perform further processing, but only forwards the recall to the Payee*.	Mandatory
Answer	Answer: IPS will route all successfully validated messages to the counterparty according to the content of the routing data.	
7.3.3. ***Validation of recall responses (*****IPS.RECALL.03)**		
FR.97	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
Answer	Answer: The IPS conducts specified business validations prior to further processing and notifies both parties in case of a rejected recall.	
FR.98	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
Answer	Answer: Validation of the response sender will be performed according to the requirements.	
FR.99	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
Answer	Answer: Validation of the response sender will be performed according to the requirements.	
FR.100	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
Answer	Answer: Processing of recalls accepted recalls will be performed according to described requirements. Negative response after validation will be forwarded to Payer	
FR.101	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

Answer	Answer: Positive recalls will be validated and processed according to requirements.	
FR.102	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
Answer	Answer: Positive recalls will be validated and processed according to requirements – BIC and account roles will be switched to proceed with reversal transaction.	
FR.103	If the recall response is positive, IPS will check whether the credit 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 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.*	Mandatory
Answer	Answer: Validation of blocked accounts and available balances will be executed as part of the standard validation process.	
FR.104	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
Answer	Answer: Validation of blocked accounts and available balances will be executed as part of the standard validation process.	
FR.105	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
Answer	Answer: Validation of blocked accounts and available balances will be executed as part of the standard validation process. Transfer order will be reversed in the original amount. Validation against the retention period will be executed.	

FR.106	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
Answer	Answer: Validation of accounts validity for recall by validating accounts opening on closing dates against original transfer will be executed.	
FR.107	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
Answer	Answer: As soon as the first validation fails, IPS rejects recall response and in the case of errors sender will be notified, appropriate reason code will be provided in a response message. Industry-standard error codes are used and text reasons in the English language. Language could be localized during the implementation project.	
FR.108	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
Answer	Answer: In case of negative response, IPS after successful validation of response will forward Payee's negative response	
	***7.3.4. Processing a positive recall response* (IPS.RECALL.04)**	
FR.109	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 relationship between the Payer and the Payee, but not higher than the systemically configured amount for a transfer order).*	Mandatory
Answer	Answer: IPS will execute positive recall transfer order according to requirements.	
FR.110	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
Answer	Answer: IPS will execute positive recall transfer order according to requirements. IPS will use the recalled amount taken from the positive recall response (field AT-46 of dataset DS-06 SCT Inst). Standard validation procedures will be executed, including validation of the maximum amount of transfer.	

FR.111	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
Answer	Answer: IPS will execute transfer order according to requirements.	
FR.112	IPS will reduce/increase the balance in the corresponding accounts (IPS and RTGS accounts) in relation to the recall.	Mandatory
Answer	Answer: IPS will execute transfer order according to requirements. Balance in the corresponding accounts (IPS and RTGS accounts) will be reduced/increased accordingly.	
FR.113	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 • 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.*	Mandatory
Answer	Answer: This is a standard process flow for transfer order execution.	
FR.114	IPS will notify the Payee and Payer that the recall has been successfully executed by sending a confirmation of execution of that recall.	Mandatory
Answer	Answer: This is a standard process flow for transfer order execution, notifications will be sent to both parties.	
FR.115	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
Answer	Answer: This is a standard process flow for transfer order execution, in case of validation errors notifications will be sent to both parties, including the reason for rejection.	
FR.116	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
Answer	Answer: This is a configurable option, Direct Participant could be notified if needed on connected indirect participants incoming and outgoing transfer orders.	
FR.117	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
Answer	Answer: Recall validity period is a configurable parameter (in number of days after original transfer)	

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

Answer: Instant Payment Status Inquiry Message (pacs.028) - the status inquiry message is sent by a Participant representing the Originator Bank to IPS after the timeout limit for a response to a credit transfer has passed, to inquire if the funds have been made available to the beneficiary.

The payment status report (pacs.002) is sent by a Participant representing the Beneficiary Bank to IPS and from IPS to:

- Confirm acceptance or rejection of credit transfer that was initiated by Originator Bank
- As a positive or negative response to on status inquiry message that was initiated by the Originator Bank
- Inform the Beneficiary Bank about the receipt of the confirmation messages

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.

Answer: This is a standard process flow for pacs.028 and pacs.002 execution.

	7.4.1. Validation of a transaction status query	
FR.118	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
Answer	Answer: IPS will provide validation of the status validation query. In case of error, further processing will stop and a corresponding error message will be provided to Payer.	
FR.119	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
Answer	Answer: IPS will provide validation of the status validation query – including validation on Payer's reference and timestamp of the transaction. In case of error, further processing will stop and a corresponding error message will be provided to Payer.	
FR.120	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
Answer	Answer: IPS will provide validation of the status validation query – including validation on original transfer execution data and corresponding retention period. In case of error, further processing will stop and a corresponding error message will be provided to Payer. The transfer retention period is a configurable parameter in the IPS.	
FR.121	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
Answer	Answer: IPS will provide validation of the status validation query. Payer's BIC code in the status validation query will be validated towards the transfer order's BIC. In case of error, further processing will stop and a corresponding error message will be provided to Payer.	
FR.122	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
Answer	Answer: In case of errors sender will be notified, appropriate reason code will be provided in a response message.	
	7.4.2. Processing of transaction status query messages (IPS.IV.02)	

FR.123	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
Answer	Answer: This is a standard process flow for transaction status message. If all validations are successful, a corresponding response message to Payer will be send - a copy of the rejection message or a copy of the message on transfer order execution.	

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

Answer: The Central Alias Service (Proxy service in TietoEVRY product offering) functionality ensures finding a linkage between IBAN account information and end-user alternative ID such as mobile phone, e-mail address, payment card token or any other unique ID numbers.

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

Answer: This is standard functionality in offered product for processing CAS.

7.5.1. ***Technical and business validation of a request for customer details (IPS.CAS.01)***		
FR.124	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
Answer	Answer: IPS will provide validation of the customer details according to the business process flow. Validation will stop on the first error and a corresponding response with an error code will be provided to the requestor.	
FR.125	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
Answer	Answer: IPS will validate the query that a particular type of alias is configured in the system. If not, then a corresponding error message will be sent to the requestor.	
FR.126	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

Answer	Answer: IPS will validate for customer data presence in the CAS. If such customer data will not be found, the request will be rejected and an appropriate error message will be sent.	
FR.127	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
Answer	Answer: In case of errors Payer will be notified, appropriate reason code will be provided in the response message.	
7.5.2. ***Sending of customer details (IPS.CAS.02)***		
FR.128	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
Answer	Answer: IPS CAS functionality ensures finding a linkage between bank IBAN account information and end-user alternative ID such as mobile phone, e-mail address, payment card token or any other unique ID numbers. Functionality ensures proxy/alternate ID mapping to IBAN (payment instrument). IPS will send customer details based on a query on available information in CAS	
7.5.3. ***Processing of a Participant's request for entry of customer details (IPS.CAS.03)***		
FR.129	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
Answer	Answer: IPS will provide business validation for the entry of the customer details according to the business process flow. Validation will stop on the first error and a corresponding response with an error code will be provided to the requestor.	
FR.130	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

Answer	Answer: IPS will provide validation against configured alias types in the system according to the business process flow. Validation will stop on the first error and a corresponding response with an error code will be provided to the requestor IPS will validate customer details according to the configuration in the system.	
FR.131	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
Answer	Answer: IPS will provide validation of the Sender and its authorized rights in CAS and customer account validity for corresponding Sender's BIC. In case of not correspondence, an error code will be responded to Sender.	
FR.132	For each request for entry of customer details, IPS will check whether the data for that alias and the content of that alias have already been entered and whether the entry of a new customer is required or data on an existing customer are updated (based on the flag from the message – field XX). IPS will reject a request for entry by sending an error message in the following cases: • if an entry that already exists in the CAS is added, • if an update of a customer not entered in the CAS is requested, • if the sender is trying to update an entry it did not create. *Based on the alias and the content of the alias (for example, the alias is the mobile phone number, and the content is 79400072), IPS sends a query to the CAS to determine whether the entry exists and, based on the flag from the message, establishes whether the requested action is possible.*	Mandatory
Answer	Answer: IPS will provide validation of the customer details according to the requested business process flow.	
FR.133	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
Answer	Answer: In case of errors Sender will be notified, appropriate reason code will be provided in the response message.	
7.5.4. ***Processing of a recall of customer details (IPS.CAS.04)***		
FR.134	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

Answer	Answer: IPS will provide validation of the customer details according to the business process flow.	
FR.135	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 (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.*	Mandatory
Answer	Answer: IPS will allow only Sender made changes in customer details. IPS operator as administrator can recall any Sender data, still, 4 eyes principle is applied for all of these activities.	
7.5.5. ***Data reading by batch processing (IPS.CAS.05)***		
FR.136	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
Answer	Answer: IPS supports batch data processing. Prior data upload in CAS IPS will perform validation checks of the batch. The batch file has to be encrypted and digitally signed. XML data format is supported in the product standard release. CSV and XLS will be provided according to Bank of Moldova requirements in the scope of project delivery.	

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

FR.137	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; • To initiate Recall process if agreed between Participants; • To provide Reporting on Disputes.	Mandatory

Answer	Answer: Dispute management facility enables possibility from user web screens to process exceptional transactions. The transaction could become exceptional due to different automatic or user-initiated events based on actual business process configuration. Dispute management facility allows to process or manage cases – using the workplace for investigation, retrieving and adding necessary data from Transaction Warehouse, retrieving additional data from participants, changing statuses, adding timers, creating letters, attaching documents. Functionality allows generating a certain result of the case lifecycle step or phase. Results are either outgoing messages (investigation or recall messages), or initial data for creating financial bookings in the accounting system, or a decision to close the case.	

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

FR.138	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
Answer	Answer: The IPS provides multilevel monitoring options for all applications software modules, technical platform`s modules, and activities of participants in the system. From an architecture point of view Logging and Auditing Layer is responsible for the collection and visualization of data. Elasticsearch is used for search engine, Grafana for dashboard monitoring and Kibana for visualization of data. TietoEVRY IPS Monitoring module provides functionality through a graphical user interface that enables the monitoring of operations. Functioning of key solution components supported, such as availability of HW resources (CPU, RAM, disc space), throughput (TPS), participant reachability.	
FR.139	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

Answer	Answer: IPS provides actual monitoring of all Participant by monitoring of “heartbeat” of Participants, as well as planed scheduled unavailability windows reports. Participant status shows if Participant is reachable or in planned or non-planned downtime. Historical reports on Participants availability is available.	
FR.140	IPS provides monitoring facilities for System Operator for unavailability schedules, current unavailability windows opened as well as sudden announcements.	Mandatory
Answer	Answer: IPS provides actual monitoring of all Participant by monitoring of “heartbeat” of Participants, as well as planed scheduled unavailability windows reports. Participant status shows if Participant is reachable or in planned or non-planned downtime. Information is available for Systems Operator in the Monitoring workplace.	
FR.141	IPS provides report for scheduled upcoming unavailability schedule	Mandatory
Answer	Answer: Reporting functionality provides scheduled upcoming unavailability reports.	
FR.142	IPS provides historical report for unavailability start and finish activities (system-wise)	Mandatory
Answer	Answer: Reporting functionality provides detailed reports on system and Participant level about planned and unplanned Participants unavailability with detailed start and end dates & time.	
FR.143	IPS provides historical report for unavailability start and finish activities (Participant-wise)	Mandatory
Answer	Answer: Reporting functionality provides detailed reports on system and Participant level about planned and unplanned Participants unavailability with detailed start and end dates & time.	
FR.144	IPS issues alerts concerned Participants at pre-defined time before planned windows start and finish	Mandatory
Answer	Answer: IPS Monitoring module has the ability to integrate with the SMS gateway and Mail server to send notifications alerts to system administration. Alerts and their delivery channels are configurable.	
FR.145	IPS issues alerts to Participants when unavailability windows start and finish	Mandatory
Answer	Answer: IPS Monitoring module has the ability to integrate with the SMS gateway and Mail server to send notifications alerts to system administration. Alerts and their delivery channels are configurable.	
FR.146	IPS issues alerts to System Operator when unavailability windows start and finish	Mandatory
Answer	Answer: IPS Monitoring module has the ability to integrate with the SMS gateway and Mail server to send notifications alerts to system administration. Alerts and their delivery channels are configurable.	

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

Answer: IPS Request To Pay (RTP) functionality supports all requested message types:

Pain.013.001.08 - The CreditorPaymentActivationRequest message is sent by the Creditor sending party to the Debtor receiving party, directly or through agents. It is used by a Creditor to request the movement of funds from the debtor account to a creditor.

Pain.014.001.08 - The CreditorPaymentActivationRequestStatusReport message is sent by a party to the next party in the creditor payment activation request chain. It is used to inform the latter about the positive or negative status of a creditor payment activation request (either single or file).

Pain.001.001.10 - The CustomerCreditTransferInitiation message is sent by the initiating party to the forwarding agent or debtor agent. It is used to request the movement of funds from the debtor account to a creditor.

Pain.002.001.11 - The CustomerPaymentStatusReport message is sent by an instructed agent to the previous party in the payment chain. It is used to inform this party about the positive or negative status of instruction (either single or file). It is also used to report on pending instruction.

List of processes

Process code	Description
IPS.RTP.01	General conditions
IPS.RTP.02	RTP and PIR business process (validations)

Answer: Standard process flow for Request to Pay is supported by offered IPS RtP functionality.

	7.8.1. General conditions (IPS.RTP.01)	
FR.147	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
Answer	Answer: The Request to Pay module enables end-users of the Payee to initiate payment transactions from the Payee side. The Payer may reply to the request initiated by the Payee with a standard instant credit transfer transaction. The payer may reject it, sending an appropriate rejection message.	
FR.148	IPS processes Payment initiation Request received from Third Party, registers it and routes for Processing by Payer. *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.*	Mandatory
Answer	Answer: IPS will process RTP, register request and routes accordingly configured business process flow. Only one transfer request could be issued by Payer, in case of error, the same request couldn't be resent.	
FR.149	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
Answer	Answer: IPS will process RTP or PIR according to the configuration in the system. All configurations will be done based on required process rules. The validity term of response time is a configurable parameter in the system	
FR.150	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
Answer	Answer: IPS supports standard requirements for RTP/ PIR processing. RTP/PIR does not include any funds movements or obligations, it is assumed to be an informative message.	
FR.151	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
Answer	Answer: Transfer order initiated based on corresponding RTP/PIR is validated against actual RTP/PIR message and if the message does not exist or if time out is reached, the particular message is rejected by appropriate error code. IPS supports unique reference for each transaction. Duplication checks are performed in IPS and are based on a unique key stored in the IPS repository.	

FR.152	The Payer will specify the data source in the field (xx) of the RTP created based on the data in the CAS. *The RTP order contains fields (flags) that serve to specify the data source for the payer and/or payee from the CAS.*	Mandatory
Answer	Answer: The IPS supports requested data fields in RTP/PIR messages as well in credit transfer messages to provide data of CAS.	
FR.153	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
Answer	Answer: The IPS supports requested data fields in RTP/PIR messages as well in credit transfer messages to provide data of CAS and other informative fields, as requested for bill reference.	
FR.154	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
Answer	Answer: The IPS supports the exchange of requested data fields in RTP/PIR messages as well in credit transfer messages between Participants. By receiving data, Payee needs to present data to the end-customer and assure, that the end-customer approves compliance with data. IPS can ensure correct data exchange between Participants.	
	7.8.2. ***Validation (IPS.RTP.02)***	
FR.155	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
Answer	Answer: IPS will provide validation of RTP/ PIR according to business process flow. IPS ensures the processing of all required business validations and rejects message on first error appearance.	
FR.156	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
Answer	Answer: IPS will validate the authorisation of Sender and BIC according to the business process flow.	
FR.157	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

Answer	Answer: Transfer order will be processed according to standard credit transfer processing flow, including all required validations supporting required functionality.	
FR.158	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
Answer	Answer: Transfer order will be processed according to standard credit transfer processing flow, including all required validations supporting required functionality.	
FR.159	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
Answer	Answer: Transfer order will be processed according to standard credit transfer processing flow, including all required validations supporting required functionality. In addition, if a transfer order is initiated based on RTP/PIR, then validation of corresponding RTP/PIR will be executed.	
FR.160	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
Answer	Answer: IPS will check and validate correspondence of RTP/PIR currency and accounts for processing of transfer order.	
FR.161	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
Answer	Answer: IPS will validate correspondence of attributes of transfer order according to configurated requirements.	
FR.162	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
Answer	Answer: IPS will provide validation of the correct syntax of account numbers and their presence in the transfer order.	
FR.163	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
Answer	Answer: In case of errors Sender will be notified, appropriate reason code will be provided in a response message.	

FR.164	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
Answer	Answer: In case of errors Sender will be notified, appropriate reason code will be provided in a response message.	
FR.165	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
Answer	Answer: IPS stand-in functionality allows an administrator to configure described functionality of unreachable Payee pre-authorisation facility when system credits Payee's account without waiting for response from Payee.	

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.

Answer: The unreachability function is part of core IPS services within Participant management. A separate pre-authorisation service will be provided by offered stand-in functionality.

Interconnection 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 order payment processing.

Answer: Interconnection with other IPS schema processes will be provided, and in case of “unreachability” of Participant particular payment flow could be processed in stand-in (pre-authorisation) mode.

List of processes for “unreachability” window

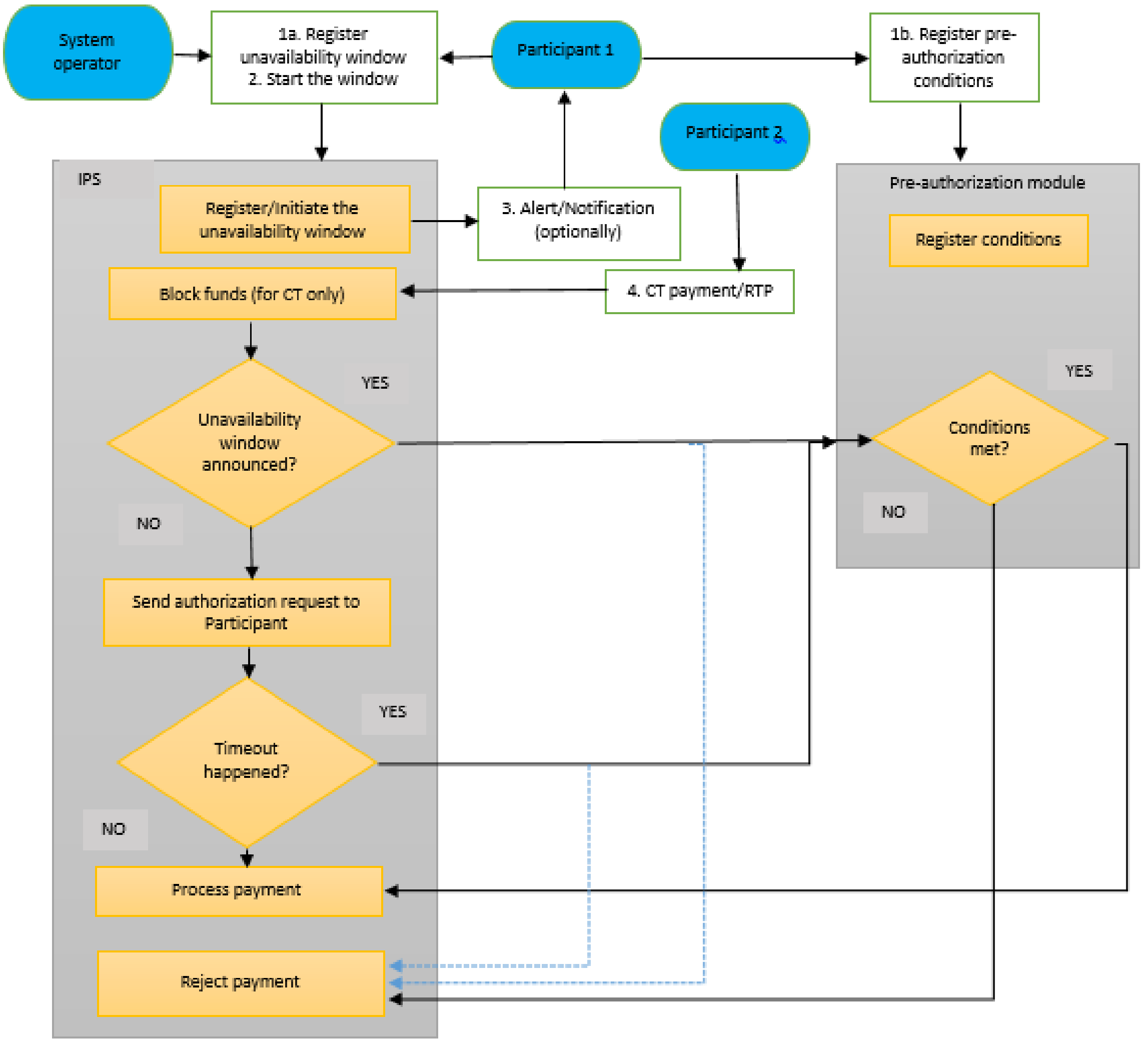
Process code	Description
IPS.OUT.01	In case of scheduled unreachabilty, Business process starts from registration of future unreachability event (window) in the IPS
IPS.OUT.02	At predefined time interval before planned time, IPS (optionally) issues a system event notification to “unreachable” Participant 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

Answer: Required flows will be implemented during the implementation project.

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) - Type of instrument - Transaction Purpose (if available).

Answer: Required flows will be implemented during the implementation project. The overall business process is presented in the diagram below:


System operator
1a. Register unavailability window
2. Start the window
Participant 1
1b. Register pre-authorization conditions
Participant 2
IPS
Register/Initiate the unavailability window
3. Alert/Notification (optionally)
Block funds (for CT only)
4. CT payment/RTP
Pre-authorization module
Register conditions
YES
Unavailability window announced?
NO
YES
Conditions met?
NO
Send authorization request to Participant
YES
Timeout happened?
NO
Process payment
Reject payment

7.9.1. Unavailability schedule management (*IPS.OUT.01*)		
FR.166	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* - *Narration data with description* - *Audit information* - *Pre-authorization conditions in pre-authorization module.*	Mandatory
Answer	Answer: PS supports API calls (ISO 20022 admi.004 messages) to communicate the unavailability of a Participant. When Participant plans to be unavailable for some reason (for example due to a regular system update), it may submit admi.004 message to IPS to inform the system and other participants about planned downtime. IPS will forward this admi.004 to all other participants of the Schema. The message contains participant BIC, start date/time of scheduled unavailability, and end date/time of scheduled unavailability. Pre-authorization conditions should be configured via the Pre-authorization module of Participant Portal.	
FR.167	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
Answer	Answer: IPS System Operator may set up scheduled maintenance window on behalf of Participant via IPS Administration Portal.	
FR.168	IPS allows Participant to manage unavailability schedule (delete scheduled maintenance window announced earlier) *Participant shall be available to do it via API call*	Mandatory
Answer	Answer: ISO 20022 admi.004 message is supported by IPS to allow the participant to delete the scheduled maintenance window announced earlier.	
FR.169	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
Answer	Answer: IPS System Operator may delete scheduled maintenance window on behalf of Participant via IPS Administration Portal.	
7.9.2. Unavailability window start and finish announcement (*IPS.OUT.03)*		
FR.170	Participant initiates unavailability window start for scheduled maintenance window *Participant shall be available to do it via API call*	Mandatory

	Answer: Participant will be able to access and manage data through API, including initiate unavailability window start for the scheduled maintenance window	
FR.171	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
Answer	Answer: IPS Administration Portal supports functionality for the System Operator to indicate the start and to mark the finish for the scheduled maintenance window.	
FR.172	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
Answer	Answer: ISO 20022 admi.004 message supported by IPS to allow the participant to announce and indicate the start of the unscheduled downtime.	
FR.173	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
Answer	Answer: IPS Administration Portal supports functionality for the System Operator to indicate the start and to mark the finish for unscheduled downtime.	
FR.174	Participant finishes unavailability window (announced earlier) *Participant shall be available to do it via API call*	Mandatory
Answer	Answer: ISO 20022 admi.004 message supported by IPS to allow the participant to indicate the finish of the scheduled maintenance window announced earlier.	
FR.175	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
Answer	Answer: IPS Administration Portal supports functionality for the System Operator to indicate the start and to mark the finish for the scheduled maintenance window.	
	7.9.3. Pre-authorization service (*IPS.AUTH.01)*	
FR.176	To allow Participant to configure (add/modify/suspend/delete) “pre-authorization” profiles for Payments and RTP requests under normal conditions	Mandatory
Answer	Answer: IPS allows Participant to create and afterwards configure preauthorization/stand-in profiles for Payments and RTP requests.	

FR.177	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
Answer	Answer: Participants will be able to access and modify preauthorization profiles 24/7, including during unavailability windows for event “when “unavailability window” is opened”.	
FR.178	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
Answer	Answer: Participants will be able to access and modify preauthorization profiles 24/7, including during unavailability windows for event “if response for RTP or Payment didn’t come in pre-defined timeout”	
FR.179	To allow System Operator to monitor “pre-authorization” profiles defined by Participants	Mandatory
Answer	Answer: System Operator will be able to monitor pre-authorized profiles defined by Participants, but will not able to modify limits and values within profiles.	

7.10. ***Billing***

FR.180	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 - 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)	Mandatory
Answer	Answer: IPS supports the following commission types: • one-time fee (registration, penalty/fine etc.); • transaction-based fee – by transaction type and volume; • periodic fee (monthly, yearly, etc). • Value-added services fee – Proxy database fee (CAS fee), unavailability window management fee, stand-in/preauthorization service fee The Fee Management model will be clearly specified and implemented during the project implementation phase.	

5.2 Non-functional requirements (NF)

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
Answer	Answer: Microservices-based architecture: the business logic is implemented as stateless services, deployed as separated applications. The applications are loosely coupled and support hot deployment: installation of fixes, new versions can be done in the live system without any outage. With microservices there are lower requirements on the infrastructure, micro container or containerless approach are also options.	
NF. 2	The solution will have an open and modular architecture, which will allow easy implementation and integration with different systems.	Mandatory
Answer	Answer: It is a Java-based solution providing ultimate control and flexibility: customers can easily customize it without vendor involvement. The solution has a flexible connector layer enabling seamless integration to multiple backends and front-end systems. This means the customer can create integration via system component own backend systems and publish via API gateway own API services.	
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
Answer	Answer: The solution is designed with full high availability in mind, using self-healing Kubernetes manifests and a cross-site disaster recovery mechanism.	
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
Answer	Answer: A "connectors" microservices are used by the IPS solution for communication with the Central Bank and external systems. A "connectors" microservices is used as a mediating software for integration and configuration of the message routing and conversion between systems in real-time, possible message transformation, logging, etc or can be set as Straight-through message processing. A "connectors" microservices supports transport switching, rule-based mediation, priority-based mediation for advanced integration requirements. By default, the system has necessary integration connection possibilities via SOAP, REST, XML, and MT formats.	

NF. 5	Due to the high amount of processed data, to ensure increased productivity, the solution shall have natively integrated capabilities such as in-memory processing, multi-thread processing, parallel execution of jobs, etc.	Mandatory
Answer	Answer: We split the solution into a set of non-blocking microservices to ensure smooth parallel processing of all data; each component is capable of scaling independently depending on its current workload, without delaying other operations. The use of in-memory and streaming technologies is a part of the IPS microservice design. Provides an in-memory store that ensures you are not adding unnecessary latency to your pipeline when reading and writing data.	
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
Answer	Answer: The Solution is developed based on OWASP principles which describe how applications create input and output validation and error handling. These are OWASP C5 input and output validation principles and C10 for error handling.	
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
Answer	Answer: For users of the multi-tenant application, users simultaneously have access to data and can change it. If external applications are using the API, then it is the same with users. In some cases where needed, a four-eyes verification sends a notification for approvers. Participant data is saved in revisions that can be applied and rolled back via the management GUI. transaction locking is in place to prevent simultaneous modification of entries.	
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
Answer	Answer: ISP system is a very open system and allows using parameters in system change a lot of business needs such us: limits, timeouts, reports, statistics and etc, this allows very fast adapt the system to particular business needs without changes in code.	
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

Answer	Answer: Users of the Solution expect applications to be available all the time. In Kubernetes, this is done with rolling updates. Rolling updates allow Deployments' update to take place with zero downtime by incrementally updating Pods instances with new ones. Updates do not affect existing architecture and related infrastructure and interfaces including customization. Special customization is controlled at the K8S CRD level and during updates is can't be changeable.	
NF. 10	The solution will be based on web interfaces, shall have user-friendly interfaces, be simple and intuitive in use.	Mandatory
Answer	Answer: All IPS system interfaces are web-based and build on material UI baselines and TietoEVRY guidelines regarding UX in payment software.	
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; d. prevent loss, modification or misuse of information within the system;	Mandatory

Answer	Answer: TietoEVRY is following three security approaches OWASP, PCI SSF (related to payment data processing, storing, and data lifecycle), and GDPR related to sensitive personal data storing and processing. Confidentiality: IPS uses a data description, passwords, Two-factor authentication. Integrity: IPS uses encryption, User access controls, Version control, Backup, and recovery procedures. Availability: IPS uses Redundancy in the micro-service software level, K8S clustering, Monitoring. For preventing unauthorized access IPS uses role-based access control, Role-based access control is centred around the role of the entity. The main advantage of role-based access control is that it allows business owners and team leaders to control access in the context of their organizations' respective role structures. Together with monitoring data access give an effective instrument for access prevention. Audit trail component tracks, stores, and validates all requests, responses in the system and provides reports, and provides a searchable interface in the Administrative console. With detailed management of access right in the system Operators can very detailed provide access rights to system operations and data. For IPS operations related to financial and confidential operation can be implemented a four-eyes principles.	
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
Answer	Answer: IPS systems achieve modularity using microservice architecture principles. Each system module is responsible for one or more business operations. Microservices being small, functional stand-alone applications that can be managed and updated independently.	
NF. 13	The architecture of the solution will be service-oriented (SOA).	Mandatory
Answer	Answer: The IPS is Microservices-based architecture: the business logic is implemented as stateless services, deployed as separated applications. A microservices architecture takes this same approach and extends it to the loosely coupled services which can be developed, deployed, and maintained independently. Each of these services is responsible for the discrete task and can communicate with other services through simple APIs to solve a larger complex business problem. Also, we want to refer to Q&A where NBM stated "Yes, microservice architecture will be compliant and welcomed"	

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
Answer	Answer: IPS system is based on a micro-architecture approach and the solution is divided into 5 (five) system logical layers: Participant Access Layer, Application Layer, Administration Layer, Logging and Auditing Layer and Management and Monitoring layer.	
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
Answer	Answer: TietoEVRY uses MTLS encryption and XML document signing for participant communication; all external communications are covered by industry-grade cyphers. Internal communication between micro-services is secure and covered by K8S.	
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
Answer	Answer: A "connectors" microservices are used by the IPS solution for communication with the Central Bank and external systems. A "connectors" microservices is used as a mediating software for integration and configuration of the message routing and conversion between systems in real-time, possible message transformation, logging, etc. A "connectors" microservices supports transport switching, rule-based mediation, priority-based mediation for advanced integration requirements. By default, the system has necessary integration connection possibilities via SOAP, REST, XML, and MT formats.	
NF. 17	Interaction based on Web-services must be available as an integration capability in IPS. *List of interfaces available and integration approach must be specified by Vendor.*	Mandatory
Answer	Answer: The IPS Interface definition follows the REST service approach. The content parameters in the corresponding HTTP body will be encoded in JSON. • SWIFT MX ISO 20022 for integration to RTGS and other systems (payment, notifications, and cash management messages only). • MT Interface for integration to RTGS (payment, notifications, and cash management messages only). • JSON API for payment and participant data (export/import).	

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*	Recommended
Answer	Answer: More than 70 % of all SWIFT transactions in the Nordics processed by TietoEVRY's SWIFT messaging hub. We provide SWIFT connectivity through SWIFT Alliance access, SWIFTNet connector as well as providing connectivity service for banks through TietoEVRY SWIFT Service Bureau. We are open to provide existing SWIFT services to customers and develop new services according to SWIFT's new service roadmap. Still, as in tender there are no detailed requirements on services required and expected volumes are not provided, TietoEVRY is not able to provide pricing for these services as part of the answer on this tender.	
NF. 19	The IPS must support SWIFT MX ISO 20022 messages for interaction with external systems.	Mandatory
Answer	Answer: The IPS system support SWIFT MX ISO 20022 messages related to Instant payment and cash management messages and can be used to interact with external systems.	
NF. 20	The IPS must be capable to interact with external systems by means of web services via private network.	Mandatory
Answer	Answer: The IPS in most cases has APIs over HTTP and APIs are protocol-agnostic and can be used in any network includes a private network.	
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
Answer	Answer: The IPS Interface definition follows the REST service approach. The content parameters in the corresponding HTTP body will be encoded in JSON. • IPS APIs for IPS Participant (payment, R2P) • IPS APIs for Participant related to Directory service (Proxy service) • IPS APIs for Participant related to liquidity management • IPS APIs for participant related to technical messages • SWIFT MX ISO 20022 for integration to RTGS and other systems (payment, notifications, and cash management messages only). • MT Interface for integration to RTGS (payment, notifications, and cash management messages only). All interfaces are included in the offered proposal.	
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
Answer	Answer: a) All business rules in the system are parameterized and configurable by IPS Administrator. b) IPS system has a full function scheduler service where IPS admin can schedule a system and business events. c) Business workflow regarding instant payment messages can only customize with pre-defined parameters. Workflows regarding users IPS administrators can create new, change existing. Workflows regarding APIs IPS admin can define a lot of parameters (trolling, policies and etc.) d) A new report in the IPS system can be created via the Kibana tool where the IPS administrators can define and create any reports based on all data including logs of what the IPS system is stored. With this approach, we give an openness regarding reports.	
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
Answer	Answer: IPS system has three layers of user forms. The first layer presents IPS Admin UI with strongly pre-defined web UI designed based on the best UX approaches and this UI can change only TietoEVRY because a lot of verification, authentication, and security features are included. IPS admin can create/ change user realms and define rights and roles. The second Layer is Kibana who allows customizing views on the system, create dashboards with systems and business data. The last layer - is the participant portal and this layer is specially designed as a content management system where you can change/add text, pictures, web pages, API documentation, and reference manuals.	
NF. 24	The application will allow customizing existing reports (e.g. adjust data set, formatting).	Mandatory

Answer	Answer: Customization level of reporting should be done via the Kibana tool which is part of TietoEVRY solution delivery. Using the Kibana tool IPS administrators can define any parameter to monitor transaction processing in full payment flow and visualize data via histograms, line graphs, pie charts. In Kibana IPS administrators can see predefined "index patterns" by all system components and based on this can create IPS own transaction dashboards and monitor other IPS system parameters if necessary. IPS administrator for reporting of data visualization can use export functions and create custom reports based on own data.	
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
Answer	Answer: In the IPS system is possible to manage normative reference information including integration to external systems as well as internal systems.	
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
Answer	Answer: IPS UI is designed based on the last best practices in UI/UX designs using the material UI approach. Our UI/ UX design approach gives a possibility to create all operations via mouse only or keyboard only or mix.	
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
Answer	Answer: The IPS system allow the setting of available business function and access controls but with technical limits. Usually, TietoEVRY during the pre-study phase investigates this requirement with the customer and decides the right approach.	
2.4. Requirements for usability		
NF. 28	All business functions available to users of application must be accessible through web interfaces.	Mandatory
Answer	Answer: All IPS UIs are web-based using ReactJS technology.	
NF. 29	All user interfaces must be in English language. *It is recommended the user interfaces to be available also in Romanian language*.	Mandatory
Answer	Answer: The IPS UIs using a flexible language library and can support any language. If the customer can provide a translation from English to Romanian of IPS UIs then it can be done with a “one-click” transition. The Default UI language is English.	
NF. 30	Application will have user-friendly interfaces that are intuitive and convenient to use for business users and users with administrative roles.	Mandatory

Answer	Answer: IPS UI is designed based on the last best practices in UI/UX designs using the material UI approach and TietoEVRY more than 20 years of experience in the financial area. Our design is convenient for business and technical users.	
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
Answer	Answer: IPS UI is designed that can be very understandable without extra training.	
NF. 32	Documentation related to the solution shall contain complete guides, detailed and updated for all groups of users.	Mandatory
Answer	Answer: IPS has Administration manual sets, User Guide manual sets, and How-to manual sets. These sets are updated during every delivery of patches or product version.	
NF. 33	Users shall have access to context-sensitive help.	Recommended
Answer	Answer: In the IPS UIs there are series of “hints” available to UIs users which help to understand the system features, as well the necessary links to the user and administrative guides.	
NF. 34	The solution shall allow saving intermediate work and operations initiated by the user (automatically or at user request).	Recommended
Answer	Answer: Intermediate work states can be saved only by user request this is needed because all-important operations in the system have four-eye principles.	
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
Answer	Answer: The IPS administrative workplace is not customizable by the user. IPS can save all user settings from previous sessions and the admin can customize for the particular users a workplace based on user roles.	
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
Answer	Answer: Our UI/ UX design approach gives a possibility to create all operations via mouse only or keyboard only or mix. Additionally implemented easy search mechanisms.	
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
Answer	Answer: The IPS Administration UI is presented as dashboards divided into business areas.	
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 NBM (further into institutional model of CSD) for information security management (based on ISO 27000 family of standards).	Mandatory
Answer	Answer: IPS has possibilities of integration to secure tools on the customer site and ability to integrate into institutional model of NBM. TietoEVRY follows ISO27000 family of standards. Detail security integration requirements to be described and agreed during pre-study phase.	
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
Answer	Answer: All credentials and roles are setting up in IP Access Management UI. The IPS system does not have any hardcoded credentials.	
NF. 40	None of the solution components shall contain stored access credentials in open form (in databases, configuration files).	Mandatory
Answer	Answer: All access credentials are stored on “Vault” under secure keys and cryptography.	
NF. 41	All solution related system processes shall run with minimum privileges needed to execute the tasks assigned.	Mandatory
Answer	Answer: Each IPS` system process is isolated in separate containers, and runs with limited user privileges even inside the container.	
NF. 42	All external interfaces of application will be accessed by using secure authentication methods (e.g. X.509 certificate-based authentication).	Mandatory
Answer	Answer: IPS uses two certificates (all certificate is based on X.509 and eIDAS requirements) "client" usage as part of a mutual authentication TLS session, "client-TLS": One way of identifying participant by the use of a "client" is that the IPS sends a CertificateRequest in the ServerHello message during the TLS handshake and the participant responds with its 'client" (with id-kp-clientAuth). IPS can then verify the "client" and know the identity of the participant. "seal" usage, "seal-header": use of a "seal" is that the participant signs the data it intends to send to IPS with its "seal" and attaches the signature as an HTTP header. IPS can then verify the "seal" and know the identity of the participant. Also in order to guarantee confidentiality, the data could be sent over TLS but the TLS connection itself would not need to contain identification of the participant.	
NF. 43	The solution will be able to encrypt sensible data stored in the database.	Recommended

Answer	Answer: Payment data integrity and protection ensured by encrypted transmission over mutually authenticated connections of digitally signed messages, while data on rest protected in an ACID-compliant database stored on encrypted data volumes on mirrored drives in raid10 configuration.	
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
Answer	Registration of system users covered by admin who issues roles, rights to IPS users. After the particular user has a role and right, the user can log on to the system and manage passwords.	
NF. 45	Application should support strong authentication mechanisms, including two factor authentication. *Vendor will describe all supported mechanisms for user authentication.*	Mandatory
Answer	The IPS support two-factor authentication and can be integrated into a public authenticator such as Google and Microsoft authenticators or use customer proprietary tool for strong authentication as well can be generated an OTP via SMS or eMail. 1. standard (username or email + password) 2. with two-factor authentication (username or email + password + code from authentication mechanisms linked to particular session).	
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
Answer	After the IPS system is configured, any new passwords (for new users) or modified passwords (for existing users) are encrypted before they are stored in the directory database. For applications that require retrieval of clear passwords, the directory administrator needs to configure the server to perform two-way encrypting encryption on user passwords. In this instance, the clear passwords returned by the server are protected by the directory ACL mechanism. A two-way encryption option, AES, is provided to allow values of the userPassword attribute to be encrypted in the directory and retrieved as part of an entry in the original clear format. It can be configured to use 128, 192, and 256-bit key lengths.	

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
Answer	The IPS Access Management system in a new realm created has no password policies associated with it. Access Management has a rich set of password policies you can enable through the Admin Console. 1. Password Policy Types 2. HashAlgorithm 3. Hashing Iterations 4. Digits 5. Lowercase Characters 6. Uppercase Characters 7. Special Characters 8. Not Username 9. Regular Expression 10. Expire Password 11. Not Recently Used 12. Password Blacklist The administrator can create different groups with different password policies using Access management UI. Users in IPS UI can change passwords.	
NF. 48	Application will allow to block, disable or suspend user accounts at the application level.	Mandatory
Answer	The IPS Access Management via User Manager menu allow the system administrator to suspend, delete, re-activate a user accounts.	
NF. 49	Application will allow users to access application only through an authentication procedure.	Mandatory
Answer	By default, IPS for any access require an authentication procedure.	
NF. 50	Application will allow differentiated use of authentication methods, depending on different categories of users.	Recommended
Answer	The IPS Access management allows to set up a different authentication method for any selected user groups.	

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
Answer	The IPS Access management allows to set up and control of the number of sessions for the user account.	
NF. 52	Application will permit to set user session timeout in case of inactivity.	Mandatory
Answer	The IPS Access management allows you fine-grain control of the session timeouts for user inactivity.	
NF. 53	Application will provide mechanisms to prevent unauthorized take-over of active sessions initiated by legitimate users.	Mandatory
Answer	If a resource is protected by a policy enforcer, it responds to client requests based on the permissions carried along with a bearer token. Typically, when you try to access a resource server with a bearer token that is lacking permissions to access a protected resource, the resource server responds with a 401 status code and a WWW-Authenticate header.	
NF. 54	Application will provide the necessary mechanisms for implementation of Single Sign-On (e.g. Kerberos).	Mandatory
Answer	You may want to give users the option to login via Kerberos or disable or enable various built-in credential types. Access management supports login with a Kerberos ticket through the SPNEGO protocol. SPNEGO is used to authenticate transparently through the web browser after the user has been authenticated when logging in to his session. For non-web cases or when the ticket is not available during login, Access also supports login with Kerberos username/password.	
2.5.3.Authorization		
NF. 55	Authorization method in the application will be based on the principle "everything not expressly permitted is forbidden".	Mandatory
Answer	IPS authorization methods are based on the principle "everything not expressly permitted is forbidden. Access management Authorization Services can improve the authorization capabilities of your applications and services by providing: • Resource protection using fine-grained authorization policies and different access control mechanisms • Centralized Resource, Permission, and Policy Management • Centralized Policy Decision Point • REST security based on a set of REST-based authorization services • Authorization workflows and User-Managed Access	

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
Answer	Groups in Access Management allow you to manage a common set of attributes and role mappings for a set of users. Users can be members of zero or more groups. Users inherit the attributes and role mappings assigned to each group. In Access Management, Groups are just a collection of users that you can apply roles and attributes to in one place. Roles define a type of user and applications assign permission and access control to roles.	
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
Answer	Groups are hierarchical. A group can have many subgroups, but a group can only have one parent. Subgroups inherit the attributes and role mappings from the parent. This applies to the user as well. So, if you have a parent group and a child group and a user that only belongs to the child group, the user inherits the attributes and role mappings of both the parent and child.	
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
Answer	We have role-based access right management and with special access, user/admin rights can share a right to another user. But this very much depends on customer security guidelines.	
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
Answer	The IPS system have a report regarding existing access right by users and user groups including all rights to IPS applications in details.	
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
Answer	The IPS have four-eye principles for verification for all user operations (this is configurable) and in some case can be adjusted to plus one verification layer. All verification is managed by IPS notification services.	
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

Answer	User and external application Input and output are protected by end-to-end TLS protected and signature for critical and financial activities.	
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
Answer	Integrity protection is ensured using PKI and digital signatures for sender messages as well as the validation of the digital signature by the recipient. All transactions are cryptographically signed and transferred via MTLS connections.	
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
Answer	Confidentiality protection is provided by using PKI and traffic encryption between system participants and the operator at the application level.	
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
Answer	We provide documentation and assistance to participating parties for establishing a secure connection; no connections are possible without a fully configured 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. • 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.	Mandatory

Answer	Management of public-key certificates IPS uses HashiCorp Vault solutions who provide Public Key Infrastructure (PKI) provides a way to verify the authenticity and guarantee secure communication between applications. Vault provides a unified interface to any secret while providing tight access control and support with detailed recording from integrated audit logs. A centralized CA must be established by the IPS or system operator. The PKI secrets engine generates dynamic X.509 certificates. With this secrets engine, services can get certificates without going through the usual manual process of generating a private key and CSR, submitting to a CA, and waiting for a verification and signing process to complete. Vault's built-in authentication and authorization mechanisms provide the verification functionality. HSM support is available for devices that support PKCS#11 version 2.20+ interfaces and provide integration libraries and is currently available for linux/amd64 platforms only. It has successfully been tested against many different vendor HSMs; HSMs that provide only subsets of the full PKCS#11 specification can usually be supported but it depends on available cryptographic mechanisms. TietoEVRY software follows the recommendation of the PCI Software Security Framework (SSF) for the secure design and development of payment software. As stated earlier, the PIC-SSF replaces the PA-DSS with new requirements that support a variety of payment software types, technologies, and development techniques.	
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. 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.	Mandatory

Answer	A strong audit facility allows businesses to audit IPS system activity by the statement, by use of system privilege, by the object, or by the user. You can audit activity as general as all user connections to the IPS, system events, and specific operations. You can also audit only successful operations or unsuccessful operations. For example, auditing unsuccessful statements may catch users on "fishing expeditions" for data they are not privileged to see. Audit trail records can be stored in an Elastic for ease of management. Audit trail records stored in an Elastic can be viewed through Kibana UI. Storing certain audit trails separately enables an enterprise to audit the actions of even the most privileged users. Audit records convert records and save this without sensitive data, sensitive data can be deleted in the archive as well. Security of audits is based on system certificates.	
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
Answer	The Audit records can view in two UI: IPS UI where we show flirted and important actions and in Kibana UI customer have the possibility to drill down under details to each record.	
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
Answer	The system has a possibility to integrates into SIEM via API • Detections API: Manage detection rules and signals • Cases API: Open and manage cases	
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
Answer	The snapshot and restore module allow the creation of snapshots of individual indices or an entire cluster where audit records. These snapshots are great for backups because they can be restored relatively quickly. Frequency, the destination can be parameterized. As well in the system available partially restore.	
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; 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.	Mandatory
Answer	IPS supports and maintains all components shipped as part of the solution; local infrastructure to be defined and maintained by its owners. All development is accomplished in-house by TietoEVRY and delivered to the customer. The TietoEVRY has a fully functional monitoring tool to monitor and prevent any problems in the IPS system.	
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
Answer	The IPS system design and monitoring capabilities focus on proactive problem identification. Timely deliveries of IPS system updates including security updates are minimized problems across system components.	
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
Answer	IPS built-in monitoring provides a complex predefined view of system metrics include important hardware checks. This a completed monitoring viewer is available via the IPS administration portal. Monitoring consists of one pre-defined dashboard that displays the most important system paraments: • System Health dashboard • Transaction throughput dashboard • Connection status dashboard • Error detection dashboard • Average processing time dashboard • Success rate dashboard With the help of Prometheus, TietoEVRY monitors various computer resources, such as memory, CPU, disk, network, and software components and system health metrics. It may also be important for us to count the number of calls to the methods of our API or measure the time of their execution, because the greater the load on the system, the more expensive is its downtime.	
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
Answer	Based on infrastructure requirements and taking into account IPS design, the IPS system can process peak 100 A2A transactions with an execution time of less than 1 second. The performance is guaranteed according proposed technology platform.	
NF. 74	IPS must support a configuration to operate on a 24/7 basis. *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*.	Mandatory
Answer	The solution supports a high availability configuration running in multiple data centre facilities for failover and disaster recovery. 24/7 mode of operation fully supported. In order to achieve fault tolerance, the customer is required to deploy multiple independent facilities with full high availability set up for underlying sites, database and storage infrastructure. A load balancer device running in high availability configuration forwards all incoming traffic to the primary site. If a failure is detected at the primary site, the load balancer switches all connections to one of the failover sites where the solution is readily available to process transactions without downtime. Since the database is separate, the solution itself can be switched back and forth by pointing to the correct backend on the load balancer device.	

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
Answer	The IPS system installed with the scalability of the IPS application services to run multiple instances. This is a requirement for performing updates without affecting application availability i.e. update to take place with zero downtime by incrementally updating Pods instances with new ones.	
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
Answer	The solution can be scaled seamlessly without downtime or service interruption; Kubernetes implies horizontal scaling. The solution design is made for “dedicated” infrastructure and no automatic expansion was foreseen.	
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

<table>
<tr>
<td>Answer</td>
<td>To achieve an RPO value of zero customer needs to comply with provided by TietoEVRY hardware and software requirements.
<table>
<tr><th>Event</th><th>RECOVERY TIME (RTO)</th><th>Potential Data Loss – RPO</th></tr>
<tr><td>Disk failure</td><td>Zero</td><td>Zero</td></tr>
<tr><td>Machine and recoverable database instance failures</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Application instances failure</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Data corruption and unrecoverable database outages, availability domain outages (power, network, etc)</td><td>60 Seconds</td><td>Zero</td></tr>
<tr><td>Site outages</td><td>60 Seconds</td><td>Zero</td></tr>
<tr><td>Database reorganization, file move, eligible one-off patches</td><td>Zero</td><td>Zero</td></tr>
<tr><td>Hardware and software maintenance and patching</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Database upgrades (patch-sets and full releases)</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Application upgrades that modify back-end database objects</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
</table>
</td>
<td></td>
</tr>
<tr>
<td>NF. 78</td>
<td>IPS must ensure a RTO (Recovery time objective) not longer than 15 minutes.
<i>In case of a system failure, maximum recovery time must not be longer than 15 minutes.</i></td>
<td>Mandatory</td>
</tr>
</table>

<table>
<tr><td>Answer</td><td>TietoEVRY proposed RTO is within 1 minute, based on TietoEVRY recommended software and hardware requirements
<table>
<tr><th>Event</th><th>RECOVERY TIME (RTO)</th><th>Potential Data Loss – RPO</th></tr>
<tr><td>Disk failure</td><td>Zero</td><td>Zero</td></tr>
<tr><td>Machine and recoverable database instance failures</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Application instances failure</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Data corruption and unrecoverable database outages, availability domain outages (power, network, etc)</td><td>60 Seconds</td><td>Zero</td></tr>
<tr><td>Site outages</td><td>60 Seconds</td><td>Zero</td></tr>
<tr><td>Database reorganization, file move, eligible one-off patches</td><td>Zero</td><td>Zero</td></tr>
<tr><td>Hardware and software maintenance and patching</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Database upgrades (patch-sets and full releases)</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
<tr><td>Application upgrades that modify back-end database objects</td><td>Zero to 60 seconds</td><td>Zero</td></tr>
</table></td><td></td></tr>
<tr><td>NF. 79</td><td>The IPS system will have suitable instruments for executing backup procedures and the management of the historical backup copies.</td><td>Mandatory</td></tr>
<tr><td>Answer</td><td>All IPS temporary data plus IPS cluster states are located in SQL Database under customer responsibilities and Elasticsearch is under IPS delivery and contains all IPS system data. The only reliable and supported way to back up a cluster is by taking a snapshot. A snapshot is a backup taken from a running Elasticsearch cluster. You can take snapshots of an entire cluster, including all its data streams and indices. You can also take snapshots of only specific data streams or indices in the cluster.</td><td></td></tr>
<tr><td>NF. 80</td><td>The IPS system will have defined operational recovery procedures, to ensure the availability and accessibility of the solution in case of major incidents.</td><td>Mandatory</td></tr>
</table>

Answer	The IPS system will have defined operational recovery procedures, to ensure the availability and accessibility of the solution in case of major incidents. Propoper testing and training will be executed as part of implementation project. All IPS temporary data plus IPS cluster states are located in SQL Database under customer responsibilities and Elasticsearch is under IPS delivery and contains all IPS system data. You can restore snapshots to a running cluster, which includes all data streams and indices in the snapshot by default. However, you can choose to restore only the cluster state or specific data streams or indices from a snapshot. Kubernetes recovery itself is based on standard K8S recovery procedures and capabilities.	
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
Answer	The solution can be scaled seamlessly without downtime or service interruption; Kubernetes implies horizontal scaling. The solution design is made for “dedicated” infrastructure and no automatic expansion was foreseen.	
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
Answer	The solution can be scaled seamlessly without downtime or service interruption; Kubernetes implies horizontal scaling. The solution design is made for a “dedicated” infrastructure and no automatic expansion was foreseen. Scale horizontally if necessary, can set up independently within the frame of business logic and reserved compute resources.	
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
Answer	Autoscaling the prerogative of “Cloud” solutions, where you can buy an additional resource at any time. IPS currently do not support an Autoscaling function.	
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
Answer	IPS provides system requirements and an overview of possible deployment scenarios, including network hardware, supported database layouts, and high availability options. The solution itself does not have any specific external version requirements and is expected to run on a general Kubernetes cluster.	
NF. 85	Platform technologies presented in the solution architecture shall be open technologies or widely used technologies.	Mandatory
Answer	IPS uses the most popular technological stack today. IPS uses industry-standard software whenever possible, the entire solution is deployed via Kubernetes operators and relies on commonly available libraries and components.	
NF. 86	To run the application it will require only standard equipment, available to be purchased by NBM freely on the market.	Mandatory
Answer	The solution runs on commonly available hardware and third-party software components.	
NF. 87	The application must support the creation, modification, processing, storage and access for text data in Unicode format.	Mandatory
Answer	The IPS solution uses UTF-8 as a default across the board.	
NF. 88	The IPS system must include clearly defined system administration procedures, which should be automated as far as possible.	Mandatory
Answer	The IPS system includes the tools and necessary automation for its administration in form of a GUI and Kubernetes configuration.	
NF. 89	The IPS system must include clearly defined system maintenance procedures. *Vendor shall describe required maintenance procedures and periodicity of those procedures.*	Mandatory
Answer	TietoEVRY provides a user manual for the solution itself and recommendations for datastore management; Kubernetes, database and underlying hardware are considered customer's infrastructure and are managed by the customer's team. Update of software can be related to security, functional, and bug fixes. Delivery of these updates is based on CI/CD approach. Customers can choose a time to update a production environment. Any updates processed without any downtime.	

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
Answer	Answer: Considering the minimal infrastructure requirements we provide our recommended HW sizing in Annex TietoEVRY F4.5 TOTAL COST OF OWNERSHIP (TCO), Table 4: Requirements towards infrastructural specifications	
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
Answer	This is a configurable parameter and the customer fully manages the retention times of the system data. The amount of data does not affect the performance of the IPS application.	
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.*	
Answer	The IPS will after snapshot procedures can be archive data labelled as “old” in another disk space and can be managed separately as “recent” data. Data in hot storage -> Take a snapshot -> transfer to cold storage in Elastic.	
NF. 93	The IPS system must support the efficient data archiving procedures. *Vendor has to describe archiving approach and automated/manual procedures*	Mandatory
Answer	Snapshots are simple one command in the IPS system. Customers can schedule and automate it based on internal banks' procedures.	
NF. 94	The IPS system must maintain sufficient information for audit purposes for a period of at least seven (7) years.	Mandatory
Answer	In the IPS system retention data is configurable and based on customer backup procedures. An IPS system is DB agnostic and DB maintenance and running is a customer responsibility and based on this all DB data retention can be configurable by the customer. Regarding operational data (transactions data, logs, audit) in IPS, IPS has export/import mechanisms of data. By default in "hot" data IPS operate and manages danda in the range of one year, older data goes to archive, but this is configurable parameters.	
NF. 95	The IPS system must provide an efficient data archiving solution for data protection based on flexible backup-restore approach	Mandatory

Answer	The Take and restore snapshots are built in the instrument under Elasticsearch what IPS has. Snapshots are backups of a cluster's indices and state. State includes cluster settings, node information, index settings, and shard allocation. Elasticsearch snapshots are incremental, meaning that they only store data that has changed since the last successful snapshot. The difference in disk usage between frequent and infrequent snapshots is often minimal. In other words, taking hourly snapshots for a week (for a total of 168 snapshots) might not use much more disk space than taking a single snapshot at the end of the week. Also, the more frequently you take snapshots, the less time they take to complete. Some Elasticsearch users take snapshots as often as every half hour.	
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
Answer	TietoEVRY recommends and proposes to use a provided by your environments with active/ active failover deployment architecture. TietoEVRY IPS licensing policy does not limits number of environments in use. Still limitations applies to 3rd party products, in particular if NBM is going to use Oracle database, then Oracle licensing needs to be counted for each environment. It is calculated in proposed technical offer of 3rd party products.	
NF. 97	The solution will have in place mechanisms to assure the transfer of data between different environments.	Mandatory
Answer	IPS are based on small packages of components, implement business logic, deployed as standard applications in Docker enabling easy management of application components between different environments. Data transfer between environments are ensured by using select database tools.	
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
Answer	IPS doeas not generates any personalized data as it receives messages from participants and transports messages to another participants. It is expected that participants during the onboarding tests will provide IPS with already depersonalized data.	

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, reorganization etc.). In the event that the source code can not be transmitted, it is necessary to provide an escrow commitment.	Mandatory
Answer	TietoEVRY is able to deliver the source code to an escrow, held by an independent third party, which can later be accessed in case of liquidation, insolvency or bankruptcy, in order to provide guarantees to NBM business continuity on IPS product maintenance in case of absolute and objective TietoEVRY unavailability to maintain proposed solution. It would be TietoEVRY's own responsibility to hand over source code in predefined cases as well as enter in Escrow agreement on the costs of the customer.	

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.

Answer: Considering the minimal infrastructure requirements we provide our recommended HW sizing in **Annex TietoEVRY F4.5 TOTAL COST OF OWNERSHIP (TCO), Table 4: Requirements towards infrastructural specifications.**

5.3 Implementation requirements (IR)

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
Answer	TietoEVRY uses the TietoEVRY Project Management Model which is described in **Annex TietoEVRY PPS_NBM_v1** which assures project successful implementation, including monitoring, control and clear status of the project to both parties.	
IR.2.	The Tenderer is responsible for the implementation project management, as well as for the 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
Answer	TietoEVRY is assigning a Project Manager for each project which ensures successful project delivery as per the signed agreement.	
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
Answer	TietoEVRY Project manager is responsible for all activities which are needed from successful project delivery, this includes and not limit: • Administrative related tasks(budgets, meeting minutes, finances management) • Contracting changes/reviews	
IR.4.	A well-known project management methodology or standards (e.g. PRINCE2, PMBOK etc.), or an internal developed methodology, based on these standards or methodologies, shall be used for the implementation project and shall be appointed specifically.	Mandatory

Answer	TietoEVRY uses TietoEVRY Project Management Model which is described in **Annex TietoEVRY PPS_NBM_v1** is the PMBOK (Project Management Body of Knowledge) methodology with minor changes.	
IR.5.	In order to organize the project, the Tenderer shall appoint a Project Manager, who will manage the project team.	Mandatory
Answer	TietoEVRY Project manager is responsible for all activities which are needed from successful project delivery and it is assigned to this Project.	
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
Answer	The organizational chart can be found in **Annex TietoEVRY PPS_NBM_v1,** Project Organization section**.**	
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
Answer	TietoEVRY Project manager is responsible for all activities which are needed from successful project delivery, in case of delays in project those are escalated to Steering Group for decision.	
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
Answer	TietoEVRY Project manager is responsible for all activities which are needed from successful project delivery and will use described methodology in **Annex TietoEVRY PPS_NBM_v1,** in addition to that Project Manager will prepare all needed reports to ensure a clear picture of project status to stakeholders.	
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 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.	Mandatory
Answer	The communication plan described is Section Communications management of **Annex TietoEVRY PPS_NBM_v1**.	
IR.10.	The Project Manager of the Tenderer has the authority and responsibility to conduct daily project activities.	Mandatory
Answer	TietoEVRY Project manager is responsible for all activities which are needed for a successful project delivery.	

<table>
<tr><td>IR.11.</td><td>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</td><td>Mandatory</td></tr>
<tr><td>Answer</td><td>TietoEVRY Project Manager is responsible for resource organization for successful project delivery. Communication plan and tools are described in Section Communications management of <b>Annex TietoEVRY PPS_NBM_v1</b>.</td><td></td></tr>
<tr><td>IR.12.</td><td>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.</td><td>Mandatory</td></tr>
<tr><td>Answer</td><td>TietoEVRY Project Manager will appoint needed Team Leaders within Project, for example, the Testing Team lead and Development Team lead.</td><td></td></tr>
<tr><td>IR.13.</td><td>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.</td><td>Mandatory</td></tr>
<tr><td>Answer</td><td>Defect (Issue) classification/prioritization and handling process during the project implementation is described in Section Defect Management of <b>Annex TietoEVRY PPS_NBM_v1.</b> TietoEvry JIRA is used to manage Defects (Issues) originating from testing and review activities. Testing task can be closed only when all subtasks are resolved. All fixes for Issue/defects must be retested.
Issue escalation level and timeframes mentioned below:
<table>
<tr><th>Escalation Level</th><th>Time period for escalation</th><th>Customer’s Contact Person</th><th>Tieto Latvia Contact Person</th></tr>
<tr><td>0</td><td></td><td>Named PM</td><td>Project Manager</td></tr>
<tr><td>1</td><td>2 Working Days</td><td>Jana Jansone</td><td>Implementation and Consulting Unit Manager</td></tr>
<tr><td>2</td><td>4 Working Days</td><td>Valdis Janovs</td><td>Head of Instant, Retail Payments and Cards</td></tr>
</table></td><td></td></tr>
<tr><td colspan="3"><b>2. Project management activities and deliverables requirements</b></td></tr>
</table>

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
Answer	Project Management activities are described in **Annex TietoEVRY PPS_NBM_v1.**	

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. 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.*	Mandatory

Answer	Project Management activities are described in **Annex TietoEVRY Training_NBM_v1** and those fully match with the proposed activities**.** **<u>The below-mentioned templates used in the project:</u>** • Project management plan – **Annex TietoEVRY Project Plan template ver 3.1A** • Support presentation for the kick off meeting – **Annex TietoEVRY Project kick off meeting_TPM00301_eng_1.6A** • Weekly reporting comprising status report – **Annex TietoEVRY Status report of project short presentation_TPM00011_eng** • End of phase reports containing the following/Monthly (or when required) report/Exception Reports - **Annex TietoEVRY Project_status_report_TE_v.1.4**	
IR.16.	Acceptance criteria for project management deliverables: 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.	Mandatory
Answer	Project Management deliverables must be approved by the Steering Group as those are critical for successful project delivery.	
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: 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	Mandatory

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.)	

Answer	Project Management activities are described in **Annex TietoEVRY PPS_NBM_v1.** **Templates:** • Minutes of the meeting - **Annex TietoEVRY Minutes of meeting_TPM00012_engV1.5A** • Weekly report – **Annex TietoEVRY Status report of project short presentation_TPM00011_eng** • End of phase report/steering group presentation – **Annex TietoEVRY Project_status_report_TE_v.1.4** • Risk registry – **Annex TietoEVRY Risk Management template V4.1-6D** • Project kick-off template - **Annex TietoEVRY Project kick off meeting_TPM00301_eng_1.6A** • Change log - **Annex TietoEVRY Change Log template** • Minutes of delivery - **Annex TietoEVRY Minutes of delivery_TPM00306_eng** • Project Plan - **Annex TietoEVRY Project Plan template ver 3.1A**	

9.2. Software development lifecycle requirements

It is expected that software development lifecycle will be the standard V-model with elements of prototyping and incremental development. The following requirements are applicable for each of implementation stage.

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 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.	Mandatory

Answer	TietoEVRY calls it a Pre-Study phase of the project and it is included in the current project.	
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 instruments used for analysis phase and shall provide sample of deliverables.	Mandatory
Answer	These requirements are met during the Pre-Study phase of the Project.	
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

Answer	At the end of the Pre-Study phase, this list of deliverables will be provided and must be approved by the Customer.	
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. 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.	Mandatory
Answer	Formal approval is held during the Steering group meeting and the Acceptance note must be signed by both parties.	
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
Answer	TietoEVRY calls this phase Off-site preparation, during which solution is being prepared/designed for Delivery.	

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 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.	Mandatory
Answer	TietoEVRY calls this phase Off-site preparation, during which solution is being prepared/designed for Delivery.	

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., 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.	Mandatory
Answer	TieroEVRY will provide all needed Solution Supporting documentation which will help both parties to maintain the solution.	

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.	
Answer	Formal approval is held during the Steering group meeting and the Acceptance note must be signed by both parties.	
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
Answer	TietoEVRY calls this phase as Solution Preparation on-site	

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. 6. Test analysis is further detailed – complete set of test scripts is elaborated and finalized.	Mandatory
Answer	Works mentioned are included in Project WBS and will be completed as required.	
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
Answer	Deliverables are included in the project scope. All deliverables are presented to the Customer and appropriate Minutes/AN is signed by parties. Examples can be found in **Annex TietoEVRY Minutes of delivery_TPM00306_eng**	

IR.29.	***Acceptance criteria:*** 1. The acceptance criteria shall be revised and agreed upon 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. 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.	Mandatory
Answer	Formal approval is held during the Steering group meeting and the Acceptance note must be signed by both parties.	
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. 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.	Mandatory
Answer	The test approach has been described in **Annex TietoEVRY PPS_NBM_v1**, Section Testing.	

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. 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.	Mandatory

	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.	
Answer	Test approach has been described in **Annex TietoEVRY PPS_NBM_v1**, Section Testing and additionally required tests for solution are included into WBS.	
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. 3. Test results documents.	Mandatory

<table>
<tr><td>Answer</td><td>Deliverables are understood and are included in the Project scope.</td><td></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.
5. Acceptance document agreed and ‘signed-off’ by both parties.</td><td>Mandatory</td></tr>
<tr><td>Answer</td><td>Formal approval is held during the Steering group meeting and the Acceptance note must be signed by both parties.</td><td></td></tr>
<tr><td colspan="3"><b>5. Training</b></td></tr>
</table>

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
Answer	The training approach (incl. training objectives) is described in **Annex TietoEVRY IPS_Training_plan_v2**	
IR.35.	***Main activities:*** 1. The Tenderer shall develop and agree with the Beneficiary the following elements of the training component: - 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.	Mandatory
Answer	The training approach (incl. activities) is described in **Annex TietoEVRY IPS_Training_plan_v2**	

IR.36.	***Deliverables:*** 1. Plan / program and training curriculum. 2. Documentation of training by category. 3. Questionnaires for knowledge testing. 4. Results of training quality assessment.	Mandatory
Answer	The training approach (incl. deliverables) is described in **Annex TietoEVRY IPS_Training_plan_v2**	
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.	
Answer	Formal approval is held during the Steering group meeting and the Acceptance note must be signed by both parties.	
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

Answer	In addition to that TietoEVRY would like to add the Pilot GO-LIVE stage to achieve a more smooth full Solution production launch.	
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
Answer	GO-LIVE preparation phase must be confirmed and accepted by the Steering Group.	

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
Answer	During this phase, TietoEVRY prepares a Deployment plan. The attached **Annex TietoEVRY Deployment_plan_template_ver_1.1A** provides a brief overview of the planned activities.	

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
Answer	In addition to that formal report is provided by TietoEVRY which will contain the necessary information to formally approve the delivery.	
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
Answer	Formal approval is held during the Steering group meeting and the Acceptance note must be signed by both parties.	
6.2.	***Soak period***	
IR.43.	***Phase objectives:*** 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.	Mandatory
Answer	This period is included in the system roll-out activities.	

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. 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.	Mandatory
Answer	During the pre-GO-LIVE period, all resources must be available to solve all major issues which were reported by the Customer.	
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
Answer	At this stage, TietoEVRY suggests arranging daily report meetings to have a full picture of both sides of the work that is done during the day.	
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

Answer	Formally accepted by Steering Committee and no critical issues are allowed for production launch.	
6.3.	***Final acceptance***	
IR.47.	***Phase objectives:*** 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.	Mandatory
Answer	Final acceptance is included in the project scope.	
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: 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)	Mandatory

Answer	Exact list to be agreed upon during the Pre-Study phase and signed-off by both parties.	
IR.49.	***Deliverables:*** 1. Criteria list revised and agreed by both parties.	Mandatory
Answer	Exact list to be agreed upon during the Pre-Study phase and signed-off by both parties.	
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
Answer	Formal approval is held during the Steering group meeting and the Acceptance note must be signed by both parties.	
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 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.	Mandatory
Answer	All Solution Supporting documentation will be provided during the Project and will cover TENDER requirements.	

5.4 Requirements for post-implementation and support services (MnS)

<table>
<tr><th>Req. ID</th><th>Requirements</th><th>Classification</th></tr>
<tr><td>MnS.1.</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>Answer</td><td>We will provide the requested post-implementation guarantee for the delivered solution during the warranty period of 12 months from the date of final acceptance of the solution.</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><i>Critical</i></td><td>30 min</td><td>2 h</td></tr>
<tr><td><i>High</i></td><td>2 h</td><td>6 hours</td></tr>
<tr><td><i>Ordinary</i></td><td>1 day</td><td>4 days</td></tr>
<tr><td><i>Low</i></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>Answer</td><td>We agree to include the SLA conditions in the Scope of Maintenance Services to be provided for the delivered solution. The SLA conditions for the offered TietoEVRY Instant Payments Solution are explained in Section 4 Scope of Maintenance Services of Appendix D: Maintenance Services of the <b>Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN</b> (a standard (model) licencing Agreement). The Agreement provided as a standard model and its clauses and appendixes can be negotiated by agreement parties.</td><td></td></tr>
</table>

MnS.3.	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
Answer	For all our customer we ensure post-implementation maintenance and support services on multiple levels, including Service Desk, 1st line and 2nd line support and maintenance services provided by Continues Services Unit. More detailed information available in Appendix D: Maintenance Services of the **Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN** (a standard (model) licencing Agreement).	
MnS.4.	The Support Centre shall be contacted at least by the following means: e-mail, phone, web, etc.	Mandatory
Answer	We provide our Service Desk email: support.lv@tietoevry.com We will provide telephone support after the Customer has been reported an issue via email to the Supplier Central Service desk email Support.lv@tietoevry.com In case of A (critical) class issues please contact us by 24x7 on-call: +371 67771743 (the hotline available beyond working hours) Customer Ticketing System (JIRA) also available via secure web channels: https://support.lv.tieto.com/secure/Dashboard.jspa In addition, a dedicated Customer team with dedicated specialists (direct contacts for contacting) for each of our customers is provided. Meaning regardless of the customer chosen Maintenance&Support Service level, a Single Point of Contact for all support related issues, change requests, invoices, etc. will be assigned to every customer. Each customer will have its own Customer team assigned: - Customer Team Manager - Dedicated Account manager, - Dedicated Technical Account manager - Dedicated Business analysts Issues are registered through the Service Desk and depend on the issue type and category overtaken by the Technical support team or Customer Team.	

MnS.5.	Maintenance and support services shall be provided remotely.	Mandatory
Answer	Remote Maintenance and support services will be provided. In addition, on-site Maintenance and support services can be ordered for an additional charge	
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
Answer	Customer Ticketing System (JIRA) is available as the customer-oriented interaction platform concerning support and maintenance issues: https://support.lv.tieto.com/secure/Dashboard.jspa	
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
Answer	Our post-implementation customer support and maintenance services are ensured by Continues Service Unit (consisting of Service Desk, Technical support unit and Customer teams but not limited to) All Maintenace and support processes are based on ITIL (v3) best practices.	

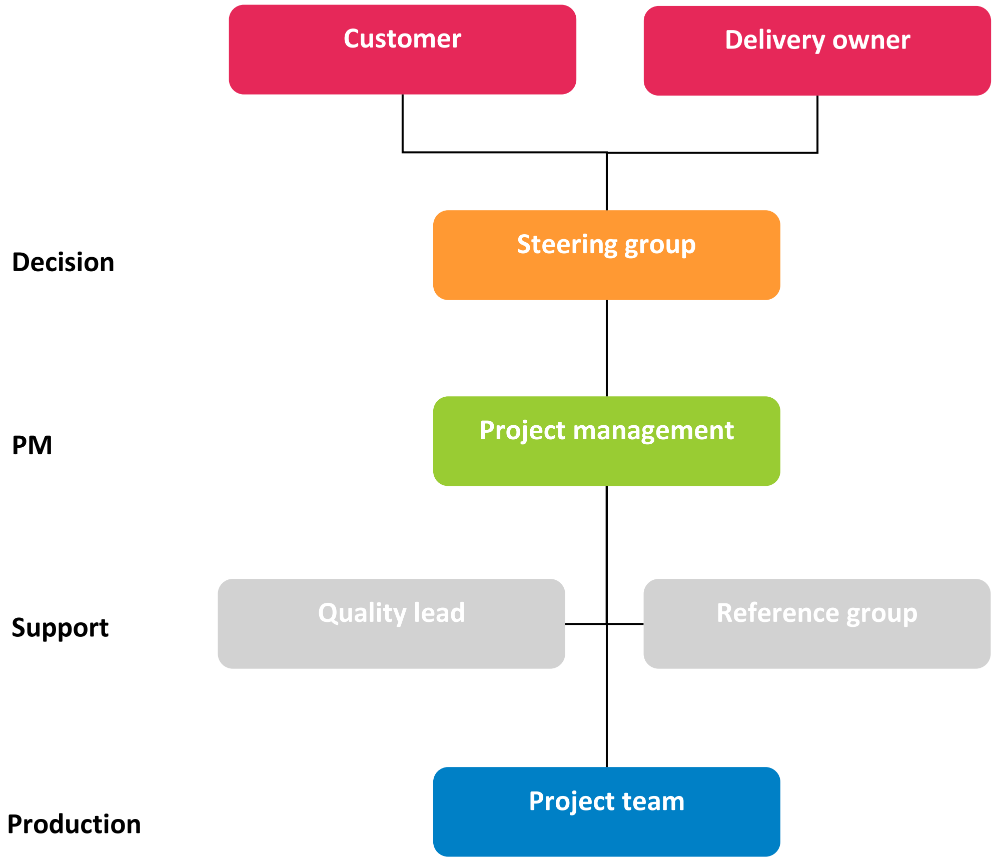
6. Training description

Training methodology, including training agenda, training tools, deliverables etc. are provided in **Annex TietoEVRY IPS_Training_plan_v2** (the default Training plan). However, before it will come to the Training phase of the implementation project, a more precise training program can be developed and agreed upon with the Customer.

7. Project Management description

7.1 Project organizational chart

The stuffing high-level structure is presented below:



Role	Responsibilities	Authorities	Person(s) in role (sub-role, if any)
Project manager	• Heads the project team. • Is responsible for all commitments made by the project and described in the project plan. • Is a member of project's steering group and internal steering group.	• Control of allocated resources • Decision-making issues, approval of agreed work results	
Customer	• Orders and pays for the project. • Ensures that set project objectives will contribute to business needs/expected benefit of his organisation. • Is a member of project's steering group and is its chairman.	• Highest decision-making mandate on behalf of Customer's organisation • Approval of project-related agreements from the Customer side (including project plan).	
Agreement owner	• Initiates the project (in external deliveries). • Ensures that the project-related agreements contribute benefits to the business. • Is a member of project's steering group and internal steering group.	• Highest decision-making mandate on behalf of the delivery organisation • Approval of project-related agreements (including project plan)	
Delivery owner	• Initiates the project (in internal deliveries). • Gives resources for the project. • Ensures that the project-related agreements contribute benefits to the business. • Is a member of project's steering group and internal steering group.	• Highest decision-making mandate on behalf of the delivery organisation • Approval of project-related agreements (including project plan)	
Steering group	• Monitors and controls that the project will conform to the terms and conditions of the agreement and its appendices • Ensures that project priority and project objectives steer the project all the time	• Decision-making concerning the contents, execution and method of implementation of the project to the extent that such decisions do not affect the contents of the project as set forth in the agreement • Start, change and closure of the project • Request for external project audit or assessment in order to ensure the right status of the project	

Role	**Responsibilities**	**Authorities**	**Person(s) in role (sub-role, if any)**
Internal steering group	• To steer and support project management proactively in managerial questions. • To monitor and control the project progress from an internal perspective. • To act as the 1st escalation step within the project (e.g. related to changes or issues hindering the proper progress of the project).	• Decision-making concerning contents, execution and method of implementation of the project as long as they do not affect the project priority and project objectives negatively. • Request for external audit or assessment in order to ensure the right status of the project.	
Quality lead	• Supports project management in project quality management (quality planning, quality evaluation, quality improvement and quality awareness) as a delivery-internal P&Q person. The main focus is on quality assurance (i.e. assuring management that defined standards, practices, procedures and methods of the process are applied). • Reports in a matrix to the project management and P&Q country and unit organisations. • Is a member of project's internal steering group.	• Raising of issues and non-conformities in the implementation of the project during its whole lifecycle. • Escalation of issues to higher levels of management if the handling of them is not sufficient within the project.	
Project team (member)	• Produces verified work results according to tasks delegated to single members of the project team	• Performance of tasks according to the project plan and other agreed working procedures, guidelines and standards	
Reference group	• Provides advice and other kinds of support to the Project manager and project team on the area of own expertise. • Ensures that work results fulfil the requirements in order to achieve project objectives successfully	• Reporting of deviations, other inputs that do not satisfy the requirement in the project to the Project manager	

Staffing plan

Resources	Estimated requirements	Competence centre
Maris Zandersons	Project Manager	TietoEVRY Latvia
Gustavs Galdiņš	Solution Architect	TietoEVRY Latvia
Jelena Čekušina Natalija Maļuhina	Business Analyst	TietoEVRY Latvia
Natalija Maluhina	Instructor (Trainer)	TietoEVRY Latvia
Vadims Lamovs Konstantins Feofantovs Ivars Jaunozolins	Software Developers	TietoEVRY Latvia
Sergejs Tammeoja	Test Team lead	TietoEVRY Latvia
Vadims Lamovs	Lead Technical consultant	TietoEVRY Latvia
Andris Eiduks	Lead Security Specialist	TietoEVRY Latvia
Maris Zandersons Sergejs Tammeoja	Quality Assurance specialists	TietoEVRY Latvia

7.2 Project management approach, including Quality Assurance and Change Management approach

The project management approach is described in **Annex TietoEVRY PPS_NBM_v1**, covering Project development and management processes description including Section Deviation Change Management and Project quality objectives and management description including Section Quality Assurance.

7.3 Project management plan

The project management plan is supposed to be **Annex TietoEVRY PPS_NBM_v1** document itself. It contains all relevant descriptions for the successful project implementation.

7.4 Original version of project management plan

The Project management plan is supposed to be **Annex TietoEVRY PPS_NBM_v1** document itself. It contains all relevant descriptions for successful project implementation.

8. Examples of deliverables (other than mentioned above)

The list of examples (Templates) to be delivered as the project management supporting documentation mentioned below with the corresponding attachments to this Technical proposal:

- Minutes of the meeting - **Annex TietoEVRY Minutes of meeting_TPM00012_engV1.5A**
- Weekly report - **Annex TietoEVRY Status report of project short presentation_TPM00011_eng**
- End of phase report/steering group presentation - **Annex TietoEVRY Project_status_report_TE_v.1.4**
- Risk registry - **Annex TietoEVRY Risk Management template V4.1-6D**
- Project kick-off template - **Annex TietoEVRY Project kick off meeting_TPM00301_eng_1.6A**
- Change log - **Annex TietoEVRY Change Log template**
- Minutes of delivery - **Annex TietoEVRY Minutes of delivery_TPM00306_eng**
- Project Plan - **Annex TietoEVRY Project Plan template ver 3.1A**

9. Required additional software and recommended hardware configuration

We provide our recommended HW sizing and required additional Software in **Annex TietoEVRY F4.5 TOTAL COST OF OWNERSHIP (TCO), Table 4: Requirements towards infrastructural specifications**.

10. Proposal licensing policy

The proposed solution includes IPS licence according to the functionalities described in the Tender response. All costs related to IPS and described value-added functionalities are included in the price proposal.

The proposed licencing model is volume-based (transactions & participants). Volume-based pricing offers a fair and effective win-win relationship between parties. The approach is based on TietoEVRY long-term experience in providing payment solutions for central infrastructures. For low transaction volumes and a low number of Participants, the system requires less involvement from TietoEVRY experts for support and maintenance tasks. As well potential fee/commission income for a central operator is relatively low. By growing volumes, both involvement of TietoEVRY experts, as well as central operator income, grows. This leads to a fair and transparent increase in the license price. Usually, central infrastructure operators charge Participants with a fixed participation fee per annum (covering Participant license fee) and with individual transaction fee (covering transaction volume license fee). TietoEVRY is flexible to adapt the licensing model for the NBM business model towards Participants.

TietoEVRY will issue the license according to the following scheme:

a. The licenses will be issued in the name of NBM;

b. The NBM will have the right upon its decision to initiate the transfer of license rights procedure without any additional costs imposed by the TietoEVRY.

All the provided licenses related to the solution will be perpetual, which will allow the Purchaser / Beneficiary to use the licensed software indefinitely.

The licenses for IPS will be handed over to NBM on hard copy support, as part of the agreement between parties.

TietoEVRY licence proposal is included in **Annex TietoEVRY F4.5 TOTAL COST OF OWNERSHIP (TCO)**. Licensing includes required 30 registered participants, 5 million payment messages per month and an **unlimited number of users** and covers requirements regarding the performance and characteristics of the resilience of the solution. Also, the license will cover all the specified types of interfaces described in response to the functional and non-functional requirements (F4.4).

The following additional licencing extensions are available for future business growth:

Licence extension	Short description
1 additional participant (will be applied after 30 participants registration in IPS)	Additional participant registration in IPS
100 000 additional messages (will be applied after 5 000 000 messages exceed per/month)	Payment messages in IPS per / months

Pricing information on the available licence extensions arise specified in table 2 “Licenses of the IPS software solution” of **Annex TietoEVRY F4.5 TOTAL COST OF OWNERSHIP (TCO).** The licence extension can be provided at the NBM request.

The annual maintenance fee is calculated based on the total licence fee, and by purchasing additional licence extensions, the maintenance fee is increased accordingly.

The solution will not refuse the initiation and execution of transactions or any other business-critical operations in case of exceeding volumetric licensing.

IPS licencing policy does not limit the number of operational environments and the number of hardware deployments. The proposed solution is compliant with the requirement for multiple IPS instances and active-active high availability deployment.

The software licenses will be delivered according to the implementation needs, but not earlier than the completion of the design specifications and no later than the system acceptance phase.

All delivered software licenses will include the price for one year of support and maintenance, provided by the licenses manufacturer (Supplier), which will start from the system acceptance date. In case of earlier activation of licenses, all the costs for support and maintenance services, provided by the licenses manufacturer (Supplier) during the implementation stage, will bear TietoEVRY.

11. Appendices of Agreement model

11.1 Model of a standard licensing agreement

Our standard (model) licencing Agreement is provided in **Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN**. The provided Agreement is a Master agreement which is constituted by General contractual terms and conditions and several Appendixes, like Solution specification, Pricing and Payment terms, Maintenance and support services, Change request process conditions etc. The Agreement provided as a standard model and its clauses and appendixes can be negotiated by agreement parties.

11.1 Model of standard maintenance and support agreement

The model of the standard Maintenance and support services for the proposed solution described in Appendix D: Maintenance Services of the **Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN** (a standard (model) licencing Agreement).

11.2 Service level agreement (SLA)

The SLA conditions for the offered TietoEVRY Instant Payments Solution are explained in Section 4 Scope of Maintenance Services of Appendix D: Maintenance Services of the **Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN** (a standard (model) licencing Agreement).

11.3 Model of Product warranty agreement

Model of Product (Solution) Warranty is fully covered by standard Software Maintenance Service terms and conditions described in Appendix D: Maintenance Services of the **Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN** (a standard (model) licencing Agreement). That means the same principles of Maintenance and support scope and SLA conditions are applied to the successfully delivered to the Customer Product (Solution) during the agreed Warranty period. Our delivery centre is qualified and has the expertise and will continue to be qualified and have the expertise to render the Services as stipulated in Appendix D: Maintenance Services of the signed Agreement during the Warranty Period.

12. Change management process approach

REQUEST FOR CHANGE

CUSTOMER may request to the Supplier to make any change, modification, addition or deletion to, in, or from the in Software. The Supplier and CUSTOMER agree that this Section specifies the procedures, the terms and conditions applicable to any Change Request made, and any changes to be brought to the Software subsequent to a Change Request.

For the avoidance of doubt, the Change Request when subsequently agreed by both Parties shall serve as an addendum to the Agreement, including but not limited to functional and non-functional specifications of the changes.

For the avoidance of doubt, any change so requested as per this Section shall be deemed to have been included within the definition and scope of the Software once the change is accepted by CUSTOMER, and terms and conditions of the Agreement applies.

PROCEDURE FOR CHANGE REQUEST AND CHANGE MANAGEMENT

Where CUSTOMER wants to bring any changes to the Software **post-Go-Live**, such requests shall be raised in accordance with this Section and shall be made through the Change Request Form, which is attached to the **Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN** (a standard (model) licencing Agreement).

The Supplier, subject to available competencies on the Change Request date, shall honour such Change Request at a reasonable price agreed by both Parties.

Upon receipt of a Change Request by CUSTOMER, the Supplier shall fully assess the change requested and its impact, and provide within a reasonable time a proposal to CUSTOMER which includes, at minimum, the following:

a) The proposed solution
b) Risk analysis, if any
c) Hardware and software requirements, if any
d) Implementation plan, time schedule and delivery date
e) The price, if any, and payment terms
f) Maintenance fee, if any
g) Installation and testing plan
h) Deployment plan
i) Back-out plan

Upon receipt of proposal from the Supplier, CUSTOMER may accept the proposal or request the Supplier to revise any part of the proposal or reject the proposal. The Supplier shall only commence any development work in relation to the Change Request once the CUSTOMER accepts the Supplier's proposal in writing.

Where the change requires CUSTOMER to purchase additional Third-Party Hardware and Software, CUSTOMER agrees to purchase such hardware and software, as well as the necessary licenses and support services as may be required for it.

Supplier shall provide all Documentation necessary for CUSTOMER and participants, to properly deploy the change into the System, as well as effectively operate, manage and maintain the change including release notes, installation manual and updated user guide.

The Supplier shall provide all required trainings related to the respective changes made, as may be required and requested by CUSTOMER.

Where the price of the change requested exceeds xxxxx EUR/USD (amount in word), both Parties may mutually agree to enter into a separate agreement with special terms to govern such changes.

MAINTENANCE

All Changes once implemented become a part of the Software for the purpose of provision of Maintenance Services under the Agreement.

Where a Change Request increases the cost of maintenance of the Software, the Supplier charges a maintenance fee for the respective change in the amount of twenty per cent (20%) of the total price of the respective change.

The Maintenance fee quoted for the changes enacted shall be automatically added to the Software's Annual Maintenance Fee and shall be paid as per the Agreement, from the date the change is accepted.

CHANGE DELIVERY, ACCEPTANCE AND QUALITY

As soon as the change is ready to be tested, the Supplier shall send a notice to CUSTOMER to commence testing of the change in accordance with the agreed testing plan. The testing of such changes shall be the responsibility of CUSTOMER, but shall be conducted with the full cooperation of the Supplier, to ensure that the changes are compliant with the agreed specifications and are particularly validated for no impact to non-changed parts of the Software and the System. CUSTOMER has the right to undertake additional tests or experience-based testing to ensure the quality of such changes. The testing shall demonstrate to CUSTOMER the functionality, performance standards and data integration of the change.

CUSTOMER will inform the supplier in writing of any defects, software errors or any other issues being the reason for the failure of the acceptance after testing. Upon such notification, the Supplier shall promptly correct indicated defects, software errors and other issues. Once such corrections are made by the Supplier, Supplier will inform CUSTOMER, and CUSTOMER shall with the full cooperation of the Supplier promptly carry out retesting of the System. The procedure set out in this Section shall be repeated until all the issues are corrected and the change is compliant with the requirements of this Section.

Changes made shall be deemed accepted for the purpose of this Appendix, in any of the following events:

a) CUSTOMER confirms in writing that the testing has been successful and the change has been deployed to the System.

b) The date following thirty (30) days after the notice served by the Supplier if CUSTOMER fails to start testing the change within the same period.

c) When the CUSTOMER starts to use any part of the change for commercial use for thirty (30) consecutive days before the acceptance is confirmed in writing by the CUSTOMER.

In the event that the Supplier delivers a change which does not conform to the specifications agreed or the change has an impact on the non-changed parts of the Software and System, CUSTOMER may decide not to proceed with the change due to such reasons and CUSTOMER shall not be liable to pay the remainder of the payments in relation to the change.

Additional information on the approach for the change request process during post-Go-live/post Warranty period is available in Appendix E: Change request of the **Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN.**

The approach for the change management process during the project implementation (Delivery phase) is described in Section Deviation and change management of **Annex TietoEVRY PPS_NBM_v1.**

13. Solution demonstration LINK (access to IPS DEMO video recording)

TietoEVRY IPS DEMO access link: https://vimeo.com/563068286

Access to the link will be provided by TietoEVRY by communicating to the contracting authority the password separately upon request.

14. Appendixes and annexes

The following Appendixes and annexes are part of the **TECHNICAL** response:

- Annex TietoEVRY PPS_NBM_v1
- Annex TietoEVRY IPS_Training_plan_v2
- Annex TietoEVRY IPL_WBS_ips_Moldova_v1.1
- Annex TietoEVRY IPL_Estimation_ips_Moldova_v1.1

- Annex TietoEVRY Change Log template.xlsx
- Annex TietoEVRY Deployment_plan_template_ver_1.1A
- Annex TietoEVRY Minutes of delivery_TPM00306_eng
- Annex TietoEVRY Minutes of meeting_TPM00012_engV1.5A
- Annex TietoEVRY Project kick off meeting_TPM00301_eng_1.6A
- Annex TietoEVRY Project Plan template ver 3.1A
- Annex TietoEVRY Project_status_report_TE_v.1.4
- Annex TietoEVRY Risk Management template V4.1-6D.xlsx
- Annex TietoEVRY Status report of project short presentation_TPM00011_eng

Note: Response to Chapter IV – Requirements (F4.4) is provided within this document **section Response to specifications and requirements F4.4**

The following Appendixes and annexes are part of the **FINANCIAL** response:

- Annex TietoEVRY F4.3 STRUCTURE OF THE FINANCIAL PROPOSAL
- Annex TietoEVRY F4.5 TOTAL COST OF OWNERSHIP (TCO)

The following Appendixes and annexes are part of the **QUALIFICATION** response:

- TietoEVRY EPSD _Duae
- Annex TietoEVRY F3.1 Offer form
- Annex TietoEVRY F3.2 Offer guarantee _SEB Bank
- Annex TietoEVRY F3.4 Original offer conformity
- Annex TietoEVRY F3.5 Participant quality statement
- Annex TietoEVRY F3.8 Recommendation letter IPSL KENYA
- Annex TietoEVRY F3.8 Recommendation letter Maldives Monetary Authority

- Annex TietoEVRY F3.9 Similar projects statement
- Annex TietoEVRY F3.10 List of key experts

- Annex TietoEVRY F3.11 CV Andris Eiduks
- Annex CISM-Eiduks-certification-1424848_exp_2024
- Annex CISSP_Eiduks_digitalcert_from_2020_exp_2023
- Annex PCIP-Certificate-AndrisEiduks-1002-080

- Annex TietoEVRY F3.11 CV Gustavs Galdins
- Annex Documenting SW Architectures _GG
- Annex SW Architecture Design & Analysis _GG
- Annex SW Architecture Principles & Practices _GG
- Annex SW Product Lines certificate _GG

- Annex TietoEVRY F3.11 CV Ivars Jaunozolins
- Annex 2019-ET-0122_Ivars Jaunozolins_Certificate
- Annex Java dev training _cert IJ

- Annex TietoEVRY F3.11 CV Jelena Cekusina
- Annex 2019-ET-0120_Jelena Cekusina_Certificate
- Annex CBAP JC

- Annex TietoEVRY F3.11 CV Konstantins Feofantovs
- Annex 2020-ET-0101_Konstantins Feofantovs_Certificate

- Annex TietoEVRY F3.11 CV Maris Zandersons

- Annex TietoEVRY F3.11 CV Natalija Maluhina
- Annex 2019-ET-0119_Natalija Maluhina_Certificate
- Annex IIBA CBAP Certificate NM

- Annex TietoEVRY F3.11 CV Sergejs Tammeoja
- Annex ISTQB Cert Tester Advanced Level Test Manager ST
- Annex ISTQB Cert Tester Foundation Level ST

- Annex TietoEVRY F3.11 CV Vadims Lamovs
- Annex 2019-ET-0118_Vadims Lamovs_Certificate
- Annex Certified Penetration Testing Engineer (CPTE)_v.lamovs_2013
- Annex Oracle db_11g_Admin_Worshop_II_v.lamovs_2012

- Annex TietoEVRY F3.12 Team availability statement
- Annex TietoEVRY F3.13 Structural validation list
- TietoEVRY Qualification requirements (F3.14)
- Annex TietoEVRY F3.15 Customer questionnaire
- Annex TietoEVRY F3.16 Disputes statement
- Annex TietoEVRY F3.17 No offence declaration

- Annex TietoEVRY F4.1 TECHNICAL SPECIFICATIONS
- Annex TietoEVRY F4.2 PRICE SPECIFICATIONS

- Annex Tieto Latvia Absence of arrears Lursoft from State Revenue Service
- Annex Tieto Latvia CERTIFICATE OF RESIDENCE
- Annex Tieto Latvia NACE classificatory report Lursoft
- Annex Tieto Latvia Registration (incorporation) certificate_LV_ENG_apostille
- Annex Tieto Latvia State Revenue Service statement in Latvian (original)
- Annex Tieto Latvia UR Statement_LV_ENG_apostille
- Annex TietoEVRY CC_pesa link_ENG_A4_v2
- Annex TietoEVRY Central Bank of Azerbaijan_EN
- Annex TietoEVRY TietoEVRY National Bank of Ukraine_RU
- Annex TietoEVRY CC_Siirto_ENG_A4
- Annex TietoEVRY IPS_roadmap
- Annex TietoEVRY Tieto Latvia Account statement certificate - Danske bank
- Annex TietoEVRY Tieto Latvia IPS_SW_License_Impl_Maint_agr _CLEAN
- Annex TietoEVRY Tieto Latvia Power of Attorney - Radu Mocanu
- Annex TietoEVRY Tieto Latvia SRS _statement confirmation EN
- Annex Tieto-latvia-40003193130-izzina Lursoft

- Annex Tieto Latvia ISO 9001
- Annex TietoEVRY Infrastructure services _ISO9001
- Annex TietoEVRY ISO 9001 FSS

- Annex TietoEVRY ISO 14001 FSS
- Annex TietoEVRY ISO 14001
- Annex TietoEVRY ISO 22301 FSS
- Annex TietoEVRY ISO 27001 FSS
- Annex TietoEVRY ISO 27001

- Annex Tieto Latvia BALANCE SHEET 2017
- Annex Tieto Latvia BALANCE SHEET 2018
- Annex Tieto Latvia BALANCE SHEET 2019
- Annex Tieto Latvia PROFIT OR LOSS STATEMENT 2017
- Annex Tieto Latvia PROFIT OR LOSS STATEMENT 2018
- Annex Tieto Latvia PROFIT OR LOSS STATEMENT 2019

15. Proposal validity

Proposal valid till October 31, 2021.

16. Signatures

Date: 08.06.2021

Riga, Latvia,

Tieto Latvia SIA, a subsidiary of TietoEVRY

Board member Valdis Janovs

Board member Evita Ozola