

Forbis

Instant payment system technical offer



Table of Content

1.	Introduction	5
1.1	Definition, acronyms and abbreviations	5
1.2	Purpose of this document.....	6
1.3	History and competence	6
1.4	Versions and roadmap	7
2.	General description.....	7
2.1	Project objectives.....	8
2.2	Project scope.....	8
3.	Proposed IPS solution	8
3.1	Functional solution	8
3.1.1	General.....	8
3.1.2	Transfer Orders	12
3.1.3	Recalls	12
3.1.4	Investigation.....	12
3.1.5	Central alias service	13
3.1.6	Dispute Management Module	13
3.1.7	Statistics, monitoring, reporting, alerts	14
3.1.8	Request To Pay and Payment Initiation Request.....	15
3.1.9	Participant “unreachable” function and pre-authorisation facility	15
3.1.10	Billing.....	17
3.2	Solution architecture	18
3.2.1	General high-level description	18
3.2.2	Security	19
3.2.3	Confidentiality and Integrity	21
3.2.4	Availability.....	22
3.2.5	Performance.....	22
3.3	Security architecture.....	23
3.3.1	Security solution overview.....	23

3.3.2	Identity and Access control.....	23
3.4	IPS environments	24
3.5	Technical architecture.....	25
3.6	Integration platform	29
3.7	Technical characteristics of the IPS environments (For One Node)	30
3.8	3rd party software specification	32
3.9	Technical solution and characteristics of the environment for IPS Participants	35
3.10	Justification of Technology Selection.....	37
3.11	Data strategy.....	41
3.11.1	Data categories	41
3.11.2	Data retention.....	42
3.11.3	Archiving	42
4.	Implementation project.....	42
4.1	Major phases.....	43
4.2	Project deliverables and other expected results	45
4.3	Quality.....	46
4.3.1	Quality Management Approach.....	46
4.3.2	Quality Assurance and Internal Controls	46
4.3.3	Continued Service Improvement	47
4.3.4	Quality policy of Forbis	47
4.4	Risk-analysis	48
4.4.1	Description of risk management method	48
4.4.2	Risk analysis.....	48
4.4.3	Risks related to project management.....	49
4.4.4	List of potential risks	50
5.	Attachments.....	56

Tables

Table 1: High-level architecture components.....	21
Table 2: IPS environments' components	25
Table 3: Architecture solution components	28

Table 4: Environments, machines and technical parameters	31
Table 5: 3 rd party software	33
Table 6: Web Management Console.....	35
Table 7: HSM	37
Table 8: Data categories	41
Table 9: 7 work streams.....	44
Table 10: Go-live and final acceptance phase	44
Table 11: project phases	46
Table 12: Probability of the risk	49
Table 13: Risk impact	50
Table 14: Risk priority	50
Table 15: The risk analysis results and possible risk mitigation measures	56

Schemes

Figure 1: CT Inst workflow	9
Figure 2: High-level solution architecture.....	18
Figure 3: IPS communication scheme	20
Figure 4: IPS environments	25
Figure 5: Standard infrastructure.....	26
Figure 6: High-level solution architecture.....	27
Figure 7: Architecture of integration platform	29
Figure 8: Architecture of integration platform	29
Figure 9: High availability architecture of universal integration platform	29
Figure 10: Data Guard	34
Figure 11: Participant. Message exchange with IPS. Option 1	36
Figure 12: Participant. Message exchange with IPS. Option 2	36
Figure 13: Participant. Message exchange with IPS. Option 3	37
Figure 14: The initial Programme plan.....	43

1. Introduction

Forbis is ready to implement a full ecosystem of instant settlement system. Our proposition includes the software and integration technology, technical infrastructure, legal and regulatory input, as well as the preparation of regulatory technical standards, related processes, and documentation.

Current document contains a detailed description of the proposed infrastructure.

1.1 Definition, acronyms and abbreviations

Terminology presented in alphabetical order.

Abbreviation	Description
ACL	Access Control List
Bank	National Bank of Moldova (in the tender documents sometimes referred to as 'Beneficiary')
CSM	Clearing and Settlement mechanisms.
CT	Credit Transfer.
Deliverable	Function or deliverable, a tangible or intangible thing that needs to be created during the Project, for example software deliverable package, instruction, etc.
FCA	Financial collateral account – an account handled by the National Bank in which funds are held as financial collateral under a security financial collateral arrangement. Financial collateral is designated to ensure the liabilities of an IPS participant.
FI	Financial institution.
Forbis	Forbis group and its affiliated companies.
HSM	Hardware security module.
IPMP	Initial Project Management Plan
IPS	Instant payment system.
ISO 20022	ISO standard for electronic data interchange between financial institutions.
Inst	Credit Transfer Instant payment message.
IT	Information technology
NB	National Bank or other regulatory authority responsible for implementation, maintenance and supervision of the payment system.
OSS	Open Source Software.
Participant	A financial institution (FI) that participates in the Instant payment scheme.
Solution	Instant payments system
Solution implementation	Means the activities and all works that are necessary to be performed by Forbis (Supplier) under the statement of work and work orders in order to implement the Solution in accordance with National Bank or Moldova (Bank) requirements
Supplier	Forbis, Forbis Solutions (in the tender documents sometimes referred to as 'Tenderer') and subcontractors
XAdES	XML Advanced Electronic Signatures.
X.509	A standard defining the format of public key certificates.



1.2 Purpose of this document

The purpose of this document is to describe technical offer for IPS solution implementation: project objectives and overview on the implementation project, functional and technical architecture, technologies and modules description.

1.3 History and competence

Forbis is a leading developer of banking software in the Baltics. Established since 1995, the company has been offering cutting-edge technology and innovative financial products and solutions to financial institutions, which range from large banks to small payment companies.

Forbis delivers a wide range of software development, implementation, and support services for banking and finance sectors. Our company ensures provision of the services and their continuous improvement in compliance with the ISO/IEC 20000 standard – the international standard for IT service management, and ISO/IEC 27001 – the information security management standard.

The goal for 2021 was set to achieve one more ISO certificate - ISO/IEC 9001 for Quality management – and in May 2021 we have successfully completed ISO certification of ISO/IEC 9001.

The Forbis Group has a long, proven track-record of successfully delivering complex IT projects, for example national currency conversions (Litas to Euro, implementation of European Central Bank directives (PSD2, Open banking and etc.) and core banking system migrations.

Forbis has a proven track record of implementing systemically important projects:

- Euro currency conversion in Latvia and Lithuania.
- Introduction of IBAN accounts numbers in Belarus.
- Denomination in Belarus.

Among important and large-scale projects related to Instant Payment system and similar to the scope of the Tender are:

- Development, implementation, and support of FORPOST system products related to provision of SEPA Instant Payments in multiple banks.
- Transition of Lithuanian, Latvian, and Estonian branches to the Single Pan-Baltic Instance, so-called BALIN.
- Implementation of new generation of FOPROST products in multiple banks.
- Implementation, support and development and of banking system to fit Software-as-a-Service model.

Detailed list of the projects together with respective recommendation letters is provided in the *“Statement on the list of main similar goods delivered and services rendered in the last 5-7 years (F3.9).”*

1.4 Versions and roadmap

Number of companies using current version: 20+

Number of companies using Instant Payment functionality: 5

Current FORPOST version is 4.7.3. The release date was September 30th, 2020.

Previous versions:

- Version 4.7.0. The version was released on August 31, 2017.
- Version 4.7.1. The release date was on October 31, 2018.
- Version 4.7.2. The release date was on September 30, 2019.

Upcoming version – FORPOST 4.7.21 – will be released on the 30th of September, 2021. This version will be applicable to the Oracle Database versions 19c and Oracle Forms 12c.

The key product of Forbis is banking information system FORPOST. Our development efforts are focused on a few strategic directions:

- **Integration platform Forbis Connection Gate** that embraces various B2B solutions and Open Banking, and digital channels including Internet Banking and Mobile Banking.
- **Instant Payment Solution**, that enables commercial and central banks provide Instant payment services. Major update planned for this product is developing of Request-to-Pay functionality. At the moment, the European Payment Council has announced a 90-day public consultation on possible changes to the SEPA Request- to-Pay rulebook. Based on the results of this consultation, a new version of the Request-to-Pay rulebook is expected to be released in November 2021. Respectively, the requirements of the European Union thereof have not been finally formulated and their implementation at the moment is not feasible, therefore we are waiting for the final version of the Rulebook.
- **A new banking solution**, which combines reliable, stable, and time-tested core of the system and the selected line of products together with the modern technologies contained within the front-end application. We are aware of the challenges of the nowadays financial landscape; therefore, we focus our attention on the security requirements for a financial IT system and the convenience of the end user – an employee of a financial institution.

2. General description

The scope of the acquisition and implementation of an Instant payments system (IPS) is to provide clearing and instant settlement of retail payments, initiated by individuals, corporates and government. The IPS system shall become a cross platform that offer interoperability for all PSP in the local market, by processing their payment messages originated from different channels: pc, mobile, acceptance network etc.

2.1 Project objectives

The implemented solution for the IPS shall meet the following main objectives:

- a. The features of the IPS, the scheme organization as well as the legal framework should meet requirements as set out in SCT Instant Rulebook.
- b. The IPS shall include such functionalities as central alias service (CAS) and request to pay (RTP). It would also have the capacity to provide new functionalities as payment markets develop.
- c. The system would use modern, off-the-shelf and proven technology. The new software and hardware infrastructure will be operated and administrated by Bank, as well as integrated in the Bank environment to benefit from economies of scope.
- d. The IPS shall have a close integration with RTGS system of AIPS, the latter being a funding source for all IPS payments.
- e. The system would be able to offer flexible participation and provision of access rules (direct/indirect participation).

2.2 Project scope

Services and products included in the scope of the Project:

- a. Software licenses for IPS solution
- b. Implementation services
- c. Post implementation services

The following elements are out of scope of the Supplier responsibilities:

- a. Bank organizational change management and whole Programme management;
- b. procurement of the infrastructure platform needed to run the IPS solution.

3. Proposed IPS solution

3.1 Functional solution

3.1.1 General

The IPS system of Forbis has been developed in compliance with the SEPA Instant Credit Transfer rulebook version 1.0, thus, this system completely complies with the rules and standards of European Payments Council. The system is updated in accordance with the amendments to the SCT Instant rulebook. Currently the system update processes are being carried out in accordance with the 2021 SCT Instant rulebook amendments.

IPS uses the ISO20022 standard version. All the messages in the system are xml messages.

The communication between IPS and participant is realized in A2A and U2A models. The A2A is the main way of system-to-system communication via messages. Direct and indirect participants of the IPS can login to their IPS accounts using a browser (U2A model).

3.1.1.1 Conceptual workflow of Instant message

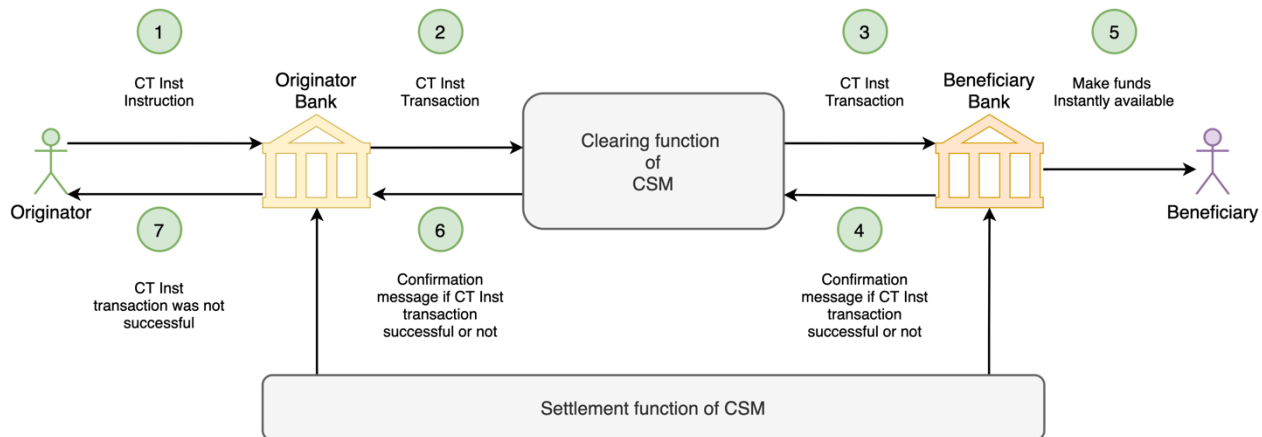


Figure 1: CT Inst workflow


Note: Figure 1 displays the distinction between the Clearing function and the Settlement function of a CSM. The steps of workflow:

Step 1: the Originator Bank receives a CT Inst instruction from the Originator. The Originator Bank then instantly executes all processing conditions and funds availability checks. When these validation checks are successful, the Originator Bank instantly makes a reservation of the amount on the Originator's payment account with this information instantly accessible to the Originator, instantly prepares an CT Inst transaction based on the CT Inst instruction and puts the time stamp in the created CT Inst transaction.

Step 2: the Originator Bank instantly sends the CT Inst transaction message to the CSM of the Originator Bank. Via this message, the Originator Bank gives the authorization to the CSM of the Originator Bank to reserve funds on its account as cover for the CT Inst transaction. This provides upfront settlement certainty.

Clearing function of CSM: out of scope of the scheme: the CSM of the Originator Bank instantly reserves funds from the Originator Bank as settlement cover for the CT Inst transaction. The CSM of the Originator Bank instantly sends the CT Inst transaction to the CSM of the Beneficiary Bank.

Step 3: the CSM of the Beneficiary Bank Instantly sends the CT Inst transaction message to the Beneficiary Bank. For the Beneficiary Bank, this message under Step 3 implies that the Beneficiary Bank



has the settlement certainty for this CT Inst transaction in case the Beneficiary Bank accepts the transaction for further processing. The Beneficiary Bank instantly verifies if it can apply the CT Inst transaction to the Beneficiary's payment account and executes various validation checks.

Step 4: the Beneficiary Bank sends the confirmation message to the CSM of the Beneficiary Bank indicating that the Beneficiary Bank:

- has received the SCT Inst transaction, and
- is either able to process the CT Inst transaction Instantly (positive confirmation) or not able (negative confirmation with an immediate Reject).

For the Beneficiary Bank, this message under Step 3 implies that the Beneficiary Bank has a settlement certainty for this CT Inst transaction in case the Beneficiary Bank accepts the transaction for further processing. The Beneficiary Bank Instantly verifies if it can apply the CT Inst transaction to the Beneficiary's payment account and executes various validation checks. The CSM of the Beneficiary Bank gives a certainty of receipt for the confirmation message that the Beneficiary Bank has sent.


Clearing function of CSM: out of scope of the scheme: based on the message received in Step 4:

- In case of a negative confirmation: the CSM of the Beneficiary Bank passes on this confirmation message to the CSM of the Originator Bank. The CSM of the Originator Bank releases the reservation of Funds for the cover done between Steps 2 and 3.
- In case of a positive confirmation: the CSM of the Beneficiary Bank initiates the final settlement processing for this specific CT Inst transaction with the CSM of the Originator Bank.

Step 5: only when the Beneficiary Bank has sent a positive confirmation via the message in Step 4 and it has the certainty that the message under the Step 4 has been successfully delivered to the CSM of the Beneficiary Bank, the Beneficiary Bank instantly makes the funds available to the Beneficiary. The Beneficiary Bank relies on the settlement certainty covered by the message in Step 3. The information about the new available funds is instantly accessible to the Beneficiary. This action means that the Beneficiary has immediate use of the funds subject to the terms and conditions governing the use of the payment account of the Beneficiary.

Step 6: the CSM of the Originator Bank Instantly reports to the Originator Bank if the CT Inst transaction has been successful (or not). The basis for this report is the contents of the confirmation message in Step 4, which the CSM of the Originator Bank had received via the CSM of the Beneficiary Bank.

Step 7: in case the Originator Bank receives a negative confirmation about the CT Inst transaction which indicates that the funds has not been made available to the Beneficiary, the Originator Bank is obliged to immediately inform the Originator. The Originator Bank lifts the reservation of the amount made in Step 1.



Settlement function of a CSM: out of scope of the scheme: when a positive confirmation is received, the amount of the CT Inst transaction is included in the settlement procedure between the Originator Bank and the Beneficiary Bank, and as such credited by the CSM to the Beneficiary Bank during the settlement process.

3.1.1.2 Liquidity

Each direct and indirect participant has at least one account in the IPS. Every direct participant in the system has a special account opened in the RTGS system. Accounts are created according to certain set rules, linked to the Participant's BIC, there is a possibility to set limits to these accounts. Monitoring of the limit values ensures a sufficient balance of each participant's in the IPS account. It is also possible to calculate and ensure a sufficient RTGS account balance by describing the account limits of each participant. The direct IPS participants have the possibility to manage funds in RTGS accounts. A direct participant in the IPS, can make transfers between own RTGS main account and the RTGS account for instant payments. Payments are validated against business days, business hours, and account balances.

3.1.1.3 Reporting

Direct and indirect participants can view the balance of the IPS accounts in A2A and U2A. Direct participants in the IPS can view the balance of RTGS accounts.

In the IPS, there is implemented sending of the following messages to the participants (messages can be sent at set intervals or at the request of a participant):

- camt.052 – the account balance in the beginning and in the end of the day;
- camt.054 – a notification about the completed transactions within the set period;
- pacs.010 – a request received from a direct participant to replenish or reduce the IPS account balance;
- camt.052 – a notification intended for a participant and informing about the reached min/max limit in the IPS and RTGS accounts;
- pacs.010 – a notification about the IPS account replenishment or reducing.

3.1.1.4 Administrative functions

The IPS operator is provided with an interface for connecting the participants to the system, their creation, removal, and administration. Besides graphical interfaces are provided for configuring of all the IPS parameters: parameterization of the messages and their routes, storage of the system parameters, parameterization of the system's connection gate, and other forms of parameterization, and etc.. The IPS participants are provided with the tests that they must execute in the system to meet the requirements. The Communications Gateway solution is also available and may be used as a software solution (A2A).

The system is multilanguage and supports everything within the UTF encoding and can switch to any language. English is officially supported, as for other languages, the translations must be done and entered into the database.

3.1.2 Transfer Orders

The messages used by the IPS comply with the ISO20022 standard, the additional information may be filled in as separate message tags, provided that this does not contradict to the XSD validations. Payment messages are processed automatically without queuing. Verification of the messages is carried out according to the rules described in the route, in a consistent manner, according to their priority.

Once the first error (a non-compliance with the check) has been detected, the message is moved to the *Negative Answer* point, then the negative response is generated and sent. After the successful validation, the IPS reserves the funds and forms a message to the Payee (PACS.008 OUT) using the export procedure. The PACS.008 OUT message sent to Payee will only be executed when the PACS.002 confirmation (ACCP) is received from the Payee. If it has been determined that the payment cannot be executed (RJCT), the block is removed from the Payer's IPS account, the corresponding message (RJCT) is sent to the Payer and the Payee with indicating the reason for the rejection. Each payment message generates only one transaction.

3.1.3 Recalls

The Recalls functionality is implemented in the IPS. The used message types are: Recall (CAMT.056), Recall rejection (pacs.002), Recall response (CAMT.029 or PACS.004), Rejection of a recall response (pacs.002), Recall response confirmation (pacs.002).


The system performs technical and business validation of the Recall messages. If the internal Recall checks do not reveal any errors, the received message is moved to the archive, and a new Recall message is formed and sent to the Payee. All the received Recall responses (positive (PACS.004) and negative (CAMT.029)) are checked according to the established procedure. After performing all the necessary checks and detecting no errors, the ISP automatically generates a transaction (when PACS.004 is received) – *a Transfer of Funds From the Payee to the Payer*. Upon having completed the operation between the participant's accounts, the IPS sends the positive Recall response to the Payer.

3.1.4 Investigation

In the IPS, there is implemented Investigation functionality. The used message types are:

- query about the status of a transaction (transfer order) (pacs.028);
- rejection of a transaction status query (pacs.002 with error code);
- response to a transaction status query (pacs.002 ACCP or RJCT).

the system performs technical and business validation of a transaction Status Query. Upon receipt of the Status Query, the ISP checks whether or not the pacs.008 payment, whose status is being requested in the Status Query, is known. If no such payment is found, a *Rejection of a Transaction Status Query* with the corresponding error code is sent to the Payer. If no errors are found in the pacs.028 (Status Query) message, the IPS searches in the archive for the corresponding pacs.002 already sent to the payer by the



pacs.008 payment, whose status is being requested. Based on pacs.002, a new pacs.002 is formed and sent to the Payer.

3.1.5 Central alias service

The central alias service (CAS) allows the Payer to obtain information required for creating a transfer order by using attributes such as the ID, card number, mobile phone number, e-mail, etc..

The IPS has its own solution for storing/managing and providing access to customers' aliases. The system allows creating, updating or deleting customer alias via S2S services. Separate S2S service provides access to customers' aliases database in order to lookup customer's information by the certain criteria. The information exchange is ensured in secure manner only for authorized consumers (users). The IPS system is in charge of secure consumer authorization, request validation, its processing and formation of response.

CAS ensures such functionalities:

- Technical and business validation of a request for customer details: the message PLGET is sent to IPS to get customer details that are necessary to execute a transfer order.
- Sending of customer details: the message PLRETRN is sent by the IPS to the Sender and contains the original identifier of the Sender's request PLGET and the elements that are necessary for a transfer order – customer's IBAN, Nm, BICFI.
- Processing of a Participant's request for entry of customer details - the message is sent by the IPS Participant to the IPS to initiate a process for setting a new relation for the phone number and the account related to the alias.
- Processing of a recall of customer details - the message PLSWTCH is sent by the IPS Participant to the IPS to remove the customer details in CAS.
- Data reading by batch processing - the IPS allows senders to import files with detailed customer information in xml, csv or xls formats.

3.1.6 Dispute Management Module

IPS has Dispute Management Module which allows Participants to initiate and resolve disputes after processing of transfer orders and recalls.

This module ensures such functions:

- 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.

3.1.7 Statistics, monitoring, reporting, alerts

The system has its own built-in Dashboard and Monitor, and it is also open to such systems as Zabbix and ELK.

All messages data or over data required to be monitored will be shipped to ElasticSearch (ELK Stack):


- Each transaction will be saved in ElasticSearch as document, which will be updated during payment process.
- Dashboard can be arranged according the needs of data representation. And each employ can have separate dashboards with payments statistics and process information from perspective on his role (System administrator, Analyst...)
- Dashboards will represent statistics in required cuts for selected period.
- Dashboards allows to filter data to get rapid view of information from a different perspectives.
- Events displayed graphically with payments can be investigating by checking messages exchange information.
- Graphical alert displaying in dashboards can be displayed as alerting graphic with some sort of thresholds. Can have separate coloured indicators which will identify payment or system status. Also rejected payments or over process errors can be identified by separate dashboard components.

There are two types of the IPS logs – DB layer and applications. DB logs are based on automatically registered records using DB/tables triggers. Application logs are collected in ELK for display and analysis. There are tools for responding to critical or threshold values, both internal (within the application) and external.

The IPS' most relevant logs:

- Logs of payment data exchange with external systems:
- The IPS' universal audit mechanism for internal (DB) purposes, which keeps track of the following:
 - Who (username and session id) performed an action;
 - What action was performed (inserted, updated, deleted);
 - On which table;
 - On which columns;
 - Old and new value.
- The IPS' log dashboard for users data audit:
- Important tables with sensitive data have journaling tables for all actions with records. These tables store the exact copy of the record at the moment of change. Thus, it is possible to see, how records have changed over time.
- Reports logs. The IPS keeps track of launching reports: who, when launched what report, what parameters were used. The same concerns launching interfaces, but the parameters or queries, performed on the form, are tracked selectively.
- Additional objects for auditing of web applications are:
 - User's parameters;
 - User's security means.

The solution has 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.



IPS has its own subsystem of notifications. The concept of the notification subsystem is to provide the data of a certain content and purpose and certain conditions according to certain regulations to certain recipients. It is possible to select required data for the formation of a notification, set the recipients of messages and possible transfer channels, transfer the formed notification to the recipient and monitor and control the course of processes of notification formation and sending.

The IPS solution ensures the reporting in the PDF, EXCEL, XML, TXT, and CSF formats with such tools:

- Microsoft Office reports: MSO documents' reports by the required template;
- JasperReports;
- XSR reports (SQL based with xsl transformation).

The main monitoring and reporting facilities for unavailability used:

- The UI for monitoring of unavailability schedules, current unavailability windows opened as well as sudden announcements;
- The report for scheduled upcoming unavailability schedule;
- The historical report for unavailability start and finish activities.

There are the possibilities:

- to alert concerned Participants at pre-defined time before planned windows start and finish.
- to alert Participants when unavailability windows start and finish.

Alert can be send by:

- e-mail;
- SMS message;
- notification via Participant web interface.

3.1.8 Request To Pay and Payment Initiation Request

At the moment, the EPC (European Payment Council) has announced a 90-day public consultation on possible changes to the SEPA Request to Pay rulebook. This consultation has already begun and will last until the end of August 2021. Based on the results of this consultation, a new version of the Request to Pay rulebook is expected to be released in November 2021. Respectively, the requirements of the European Union thereof have not been finally formulated and their implementation at the moment is impossible – we are waiting for the final version of the Rulebook.

In the system, it is possible to implement *Request to Pay* and *Payment Initiation Request* functionalities based on the already existing functionalities. The following messages types are used for this purpose: Pain.013, Pain.014, Pain.001, Pain.002. The IPS executes the exchange of the messages between the Creditor, Third party, and the Payer, performs technical and business validations of these messages, and executes corresponding transactions in the accounts.

3.1.9 Participant “unreachable” function and pre-authorisation facility

Unavailability management

There is a possibility to create scheduled maintenance window with such parameters via API call (S2S is used):

- 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

If scheduled maintenance window was created successfully System returns Unique scheduled maintenance window code.

There are the possibilities:

- to get list of scheduled maintenance window with all parameters via API call (S2S is used) together with Unique scheduled maintenance window code;
- to delete scheduled maintenance window created earlier via API call (S2S is used);
- to initiate scheduled maintenance window created earlier via API call (S2S is used);
- to finish scheduled maintenance window created and started earlier via API call (S2S is used).

System Operator can manually create scheduled maintenance window. Using UI System Operator can manage unavailability schedule: delete scheduled maintenance window created earlier, initiate scheduled maintenance window created earlier.

Pre-authorization service

There is UI in IPS system, which allows under normal conditions/during the time when “unavailability window” is opened/for timeout events to set (add/modify/suspend/delete) different "pre-authorization" profile types using parameters/predefined criteria:

- Sender
- Receiver
- Individual amount
- Aggregated amount (daily)
- Type of instrument
- Transaction Purpose (if available)

Possible profile types:

- at any time
- during unavailability window
- in case of RTP/Payment timeout event

There is UI for monitoring of “pre-authorization” profiles defined by Participants. The following information is displayed:

- participant;
- profile type;

- predefined criteria.

3.1.10 Billing

The IPS contains the billing functionality:

- to define fees for services provided by the IPS;
- to automatically apply fees for participants; to debit fees/total fee amount on monthly/quarterly/yearly basis;
- to prepare monthly fee report for participants.

The Fee Management module of the IPS is intended for centralized management of fee tariffs in the IPS and base for creating variants of pricing packages, applicable to all participants/for group of participants or individually. Different tariff schemes can be set up for different type of the transaction. A fee payable for a certain IPS service must be parameterized for the service type as a tariff scheme.

The IPS has the functionality for setting up:

- a fee for registration of participants (contract conclusion fee);
- a monthly/yearly fee (contract administration fee);
- penalties.

There are the functions:

- to define fees for “unavailability window”;
- to define fees for pre-authorization services;
- in the IPS by postponing the Pricing Package contract of the Participant.

The report on monthly/quarterly/yearly fees can be prepared for the Participant by using Additional conditions setup of the contract.

There is the possibility of notification of participants or IPS manager about certain events of lifecycle of contract if necessary.

3.2 Solution architecture

3.2.1 General high-level description

The architecture of our system has been field-proven to deliver reliable and secure service that may be easily scaled and adapted to growing business needs and changes of the industry and regulation.

The functionality of Forbis solution for IPS that would be deployed and run by the Regulator is shown in the Figure 2.

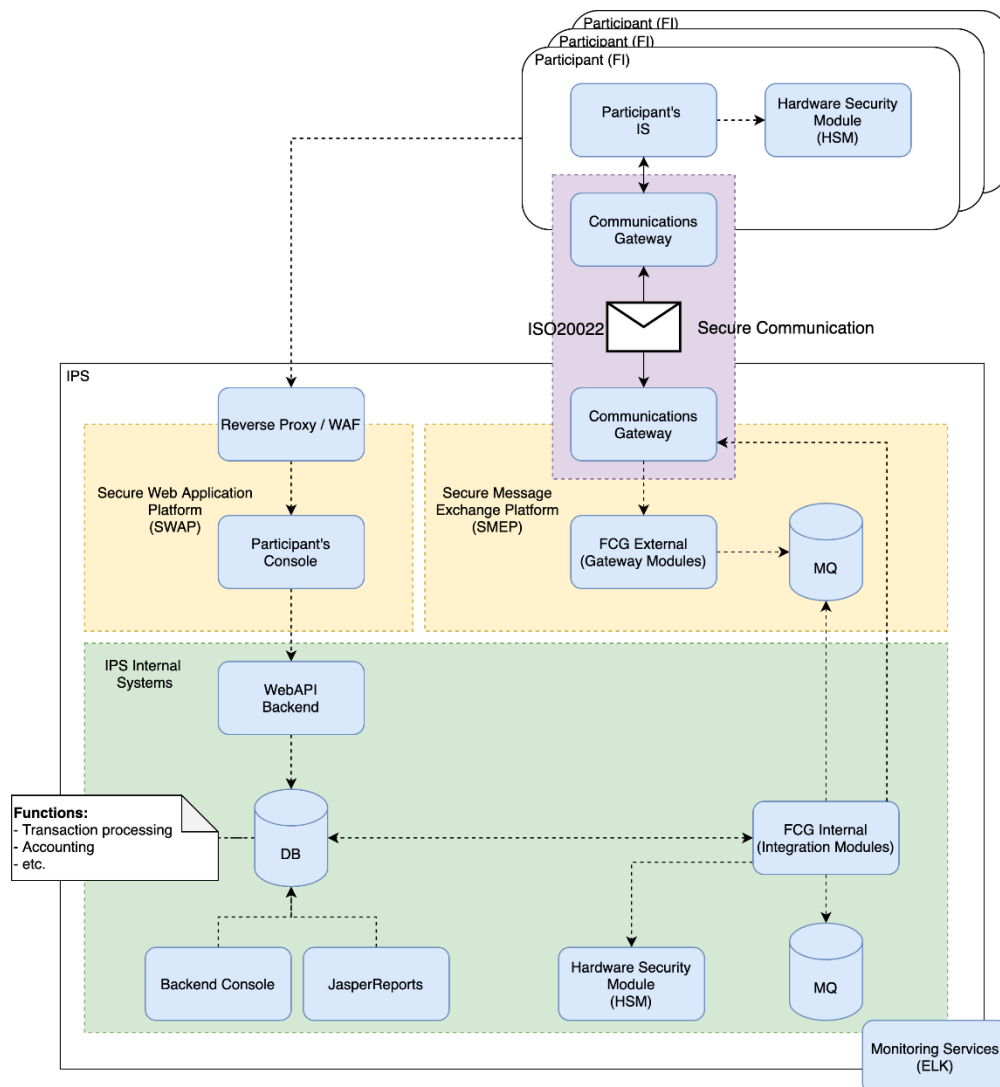



Figure 2: High-level solution architecture



The diagram above (Figure 2) shows a high-level conceptual definition of the architecture and the main components used in it. The arrows show the dependencies between the components. They also mean that these components communicate with each other in a certain way (the details of such communication are not presented in the diagram).

The proposed solution contains three main high-level components:

- SMEP – Secure Message Exchange Platform. It is used for the reliable and secure exchange of messages between the financial institutions.
- SWAP – Secure Web Application Platform. It is used for providing Web Management Console to IPS participants.
- IPS Internal Systems. The systems in which the entire logic of message processing and business will be implemented.

3.2.2 Security

The message exchange between IPS and Participants will be executed in a secure and reliable manner.

The security will be based on the following principal aspects:

- The messages will be exchanged via a secure channel. Both communicating parties (IPS and Participant's IS) will be authenticated using cryptographic keys (X.509 certificates and TLS Mutual authentication protocol). A secure channel will be implemented via Reverse Proxies (see *Communications Gateway*). Optionally, an IP ACLs (*Access Control Lists*) can be used to further limit the access to the IPS. Also, the alternative solutions may be used, such as VPN tunnels.
- An intermediate layer will be used to separate the external network (e.g. the internet) from the IPS local network. In a diagram above, this layer is called SMEP – Secure Message Exchange Platform. It will be implemented using conventional DMZ (*Demilitarized Zone*) solutions. Additionally, no direct TCP connections will be allowed between the SMEP and IPS LAN where connection initiator is SMEP. Only IPS LAN will be able to connect to SMEP, and messages will be delivered for processing via MQ (*Message Queue*). This limits the possibility that malicious agents will be able to penetrate into IPS LAN.

Figure 3 below presents a diagram, which shows the communication between the IPS that is located and run by the Regulator and the financial institutions (*Participants*).

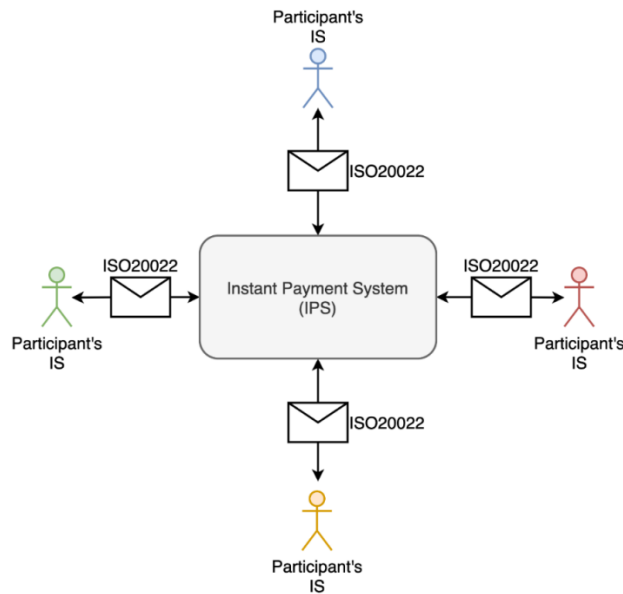


Figure 3: IPS communication scheme

All Participants communicate with each other via ISO 20022 financial messages which are digitally signed (e.g., XAdES - XML Advanced Electronic Signatures v1.1.1, <http://uri.etsi.org/01903/v1.1.1/>). All communications happen via IPS which provides the necessary clearing and settlement functions.

Name	Description of the components
Participant (FI)	Participant's organization
Participant's IS	Participant's Information System
SWAP – Secure Web Application Platform	An infrastructure and software solution that allows serving Web Applications in a secure manner.
SMEP – Secure Message Exchange Platform	An infrastructure and software solution that allows the exchange of messages between the parties in a secure manner.
IPS Internal Systems	Instant Payment System's applications that are internal and not directly accessible to external entities.
Hardware Security Module (HSM)	A physical computing device that manages cryptographic keys and provides cryptographic functions such as encryption and digital signature.
Communications Gateway	A reverse proxy that enables a secure channel via the internet where both communicating parties are mutually authenticated using certificates issued by IPS. Note: alternative secure channel solutions also may be used (e.g. VPN).
Secure Communication	The private communication between two parties.
Reverse Proxy / WAF	Web Application Firewall. An enhanced firewall that is capable to inspect Application layer data and prevent suspicious or malicious activity.

Name	Description of the components
Participant's Console	A management console of the Instant Payments Scheme participant.
WebAPI Backend	A component which serves RESTful style web services. These services will be consumed by Participant's management console.
DB	A database. This is the main component in which the message processing and business logic is implemented, such as: <ul style="list-style-type: none"> - Account management - Contract management - Transaction management - Auditing - Bank Identification Codes classifier, etc.
Backend Console	A backend management console.
JasperReports	Reporting engine based on OSS JasperReports library.
FCG External	Gateway modules of Forbis Connection Gate that accept incoming messages for further processing.
FCG Internal	Integration modules of Forbis Connection Gate that are responsible for the processing of incoming / outgoing messages.
MQ	Message Queue / Message Oriented Middleware. It is used for inter-application communication.
Monitoring Services	System monitoring tools used for online system availability reporting, log management, and analytics.

Table 1: High-level architecture components

3.2.3 Confidentiality and Integrity

To ensure the confidentiality of the data, the following measures are applied:


- Encryption;
- Restriction of access rights.

The following measures are used for ensuring integrity:

- Hash;
- MAC;
- Digital signature.

Algorithms for cryptographic operations (hashing, symmetric/asymmetric encryption, MACs, digital signatures) are selected considering all of the following:

- NIST (National Institute of Standards and Technology) "[Cryptographic Standards and Guidelines](#)"
- [FIPS](#) (for instance FIPS 140-2 [Annex A: Approved security functions](#)).
- Local regulatory standards and requirements, if any
- HSM usage:
 - If cryptographic operation is performed by HSM, only HSM supported algorithms, which comply with FIPS 140 [Security Requirements for Cryptographic Modules](#), are used;
 - Otherwise, priority is being given to the algorithms, which are natively supported by the Oracle database crypto API (dbms_crypto). This way no calls to Forbis Remote Services



(FRS) or other services are required (reduced network traffic, passwords or other sensitive information does not leave the database).

Inside the IPS, the data integrity and confidentiality are ensured by access control:

- Access to the database tables and API is controlled using password-protected database roles.
- Access to specific IPS entities (customers/participants, accounts, interest schemes etc.) and operations (create customer/participant, view customer/participant, open account, view balance, close account etc.) is controlled using the IPS user groups and object groups.

Additionally, changes of the data can be tracked using a customizable IPS audit mechanism. Audit tables are protected according to "Protecting IPS Audit":

- View privilege is granted to administrators (a specific DB role, the role is password protected);
- Depending on the Bank's business processes, View privilege can also be granted to other Bank's employees;
- Only the database schema user (object owner) can directly insert, update, delete operations in the audit table;
- The schema user must be locked;
- The data is recorded into the audit table automatically using the database table triggers on the tracked tables.

When the data leaves the Bank network, its confidentiality and integrity is protected according to "Protecting Data Outside Bank Network":

- Confidentiality and integrity of the data, which are transferred outside the Bank's network, is protected by using a secure channel (HTTPS, SSL, VPN). In this case, no additional encryption is required.


When transferring the data over insecure channels, the data should be encrypted. Additionally, the data can be digitally signed or MAC-calculated.

3.2.4 Availability

The IPS system is fully ready to operate 24h a day. Continuous availability is ensured by RAC/DATAGUARD at the Oracle level, and by clustering and load balancing on the level of the application/service. Suggested system architecture ensures that system will be available in case of failure of hardware and/or software components.

3.2.5 Performance

Executing an account-to-account transfer on a modern platform would take 0.008 seconds. At a speed of 0.008 seconds, one flow will execute 100 transactions per second. 5,000,000 transfers per day is an experimentally proven fact with our clients in the course of real exploitation. When performing load and stress tests, the load like "obtain online account balance", "enter a debit/credit transaction", "obtain basic information on account parameters" does not exceed one second. We do not take into account reports and statements, as this much depends on the number of lines, which can be numerous. Basic operations are based on primary keys and a small number of records to process.



The signing speed depends on the HSM speed, however, there is a possibility to parallelize calls to several HSMs.

3.3 Security architecture

3.3.1 Security solution overview

Security should be ensured by using administrative and technical means.

Security architecture goals are:

- To secure the system from unauthorized access;
- To secure the system from unauthorized actions by registered users or personnel;
- To prevent unauthorized access to sensitive business data;
- To prevent data leaks;
- To provide a mechanism to manage user rights, access privileges, access to business data and functions.

The system has multi-layered security approach. IPS Core data integrity and confidentiality is ensured by access control. Access to data is organized in the hierarchical manner.

The IPS uses its own key storage for administration of the access credentials. The keys can be stored either locally (Oracle DB) or in the external HSM (Physical security, administration, backup, and other HSM administrative tasks are the Bank's responsibility, since HSM is physically located on Bank's side). The IPS API operates only with the metadata of the relevant keys.

None of the user passwords are stored as a plain text in the database or other external applications that are configured on the server; the sensitive information is encrypted.

Every system process may be run with its own dedicated user that has a limited access to the system resources, such as: file system, network, or memory.


API requires that the client be authenticated with its X.509 Certificate and a digital signature. This is achieved at the transport layer using TLS. Both sides are authenticated when the TLS handshake is established and X.509 Certificates are exchanged. The technologies used are: TLS1.2, TLS1.3, and up to date secure encryption algorithms.

3.3.2 Identity and Access control

IPS core

Each IPS Core user is an Oracle RDBMS user e.g. it has an account (username and password) at the DB level. This is the first level of the access control.

Each IPS Core user is granted Oracle DB roles to be able to access the data in DB. Each role grants access to certain data structures (tables, views) and API (packages). Each role, except for the one which allows to login to DB, is password-protected and disabled by default. Thus by just logging in DB



user does not see any data in IPS Core. These roles are enabled only if user logs in using IPS Core interface. This is the second level of access control.

The third level embraces rights' management at the application level. Each IPS Core user is assigned to one or more IPS Core user groups. Each user group has access rights to customers/participants, transactions, accounts, applications etc. Also each user group has different access to IPS Core menu – the menu can be restricted so that different user group would have access to different IPS features and screens.

The user can access the IPS only by the authentication procedure. For back-end, a standard Oracle authentication procedure is used, for front-end, the Keycloak functionality for authentication is used. Both of them support Multi-Factor Authentication.

Keycloak allows adding different policies, required actions for each case, for individual users, or globally.

Participant console

Each Participant user has username and password. User logs in application using these credentials and additional security means (multi-factor authentication).

Each operation performed by the user in application must be confirmed by using user's additional security means. There is also operation confirmation in a group e.g. depending on the amount of the operation or the user rights, the operation may require confirmation from several users. Only after all of them are confirmed the transaction is executed.

Gateway

Each message sent to the Communication gateway is an encrypted message which must be digitally signed. If the message has been signed by an unknown or invalid/expired certificate, it is rejected. The cryptographic certificate is on the HSM. Both communicating parties (IPS and Participant's IS) will be authenticated using cryptographic keys (X.509 certificates and TLS Mutual authentication protocol).

Moreover, Keycloak Authorization Services can help improve the multi-level authorization capabilities on 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;
- The infrastructure to help avoid code replication across projects (and redeploys) and quickly adapt to changes in your security requirements.

3.4 IPS environments

Forbis recommends to set up four environments:

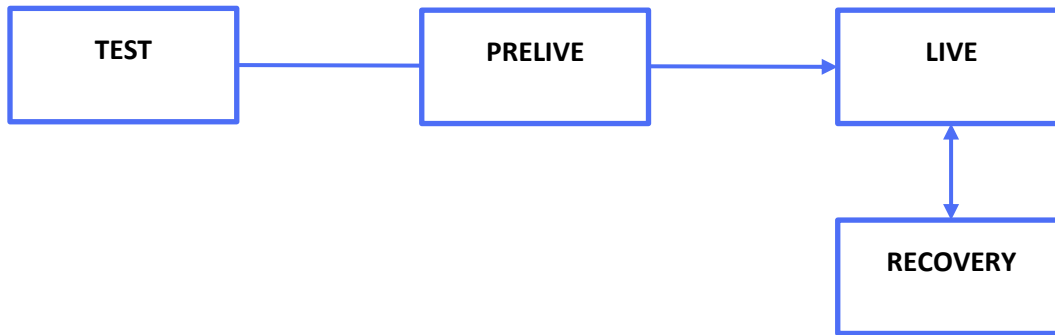


Figure 4: IPS environments

Technical characteristics for each component presented below in Table 4: Environments, machines and technical parameters and Table 5: 3rd party software.

Name	Purpose	Capacity
TEST	The environment used for complex testing of new features and changes.	Approx. 10-20% of LIVE resources for database, and 50% of other servers
PRELIVE	The environment is intended for final testing of implemented functions, new features and other changes before going live.	Capacity of 10-20% of LIVE resources for database, and of 50% of other servers
LIVE	Main production environment.	Full
RECOVERY	Reserved environment for disaster recovery. Preferably, it should be located in a different geographical location than the main site.	Capacity around 50-100% of LIVE resources

Table 2: IPS environments' components

For certain extra-complex projects, it might be necessary to create additional short-lived environments (for a period of up to 3 months).

3.5 Technical architecture

The diagram below shows the architecture of a standard infrastructure without HA (High Availability) and Load Balancing. All communications with external entities is performed using only strong encryption (at least TLS v1.2).

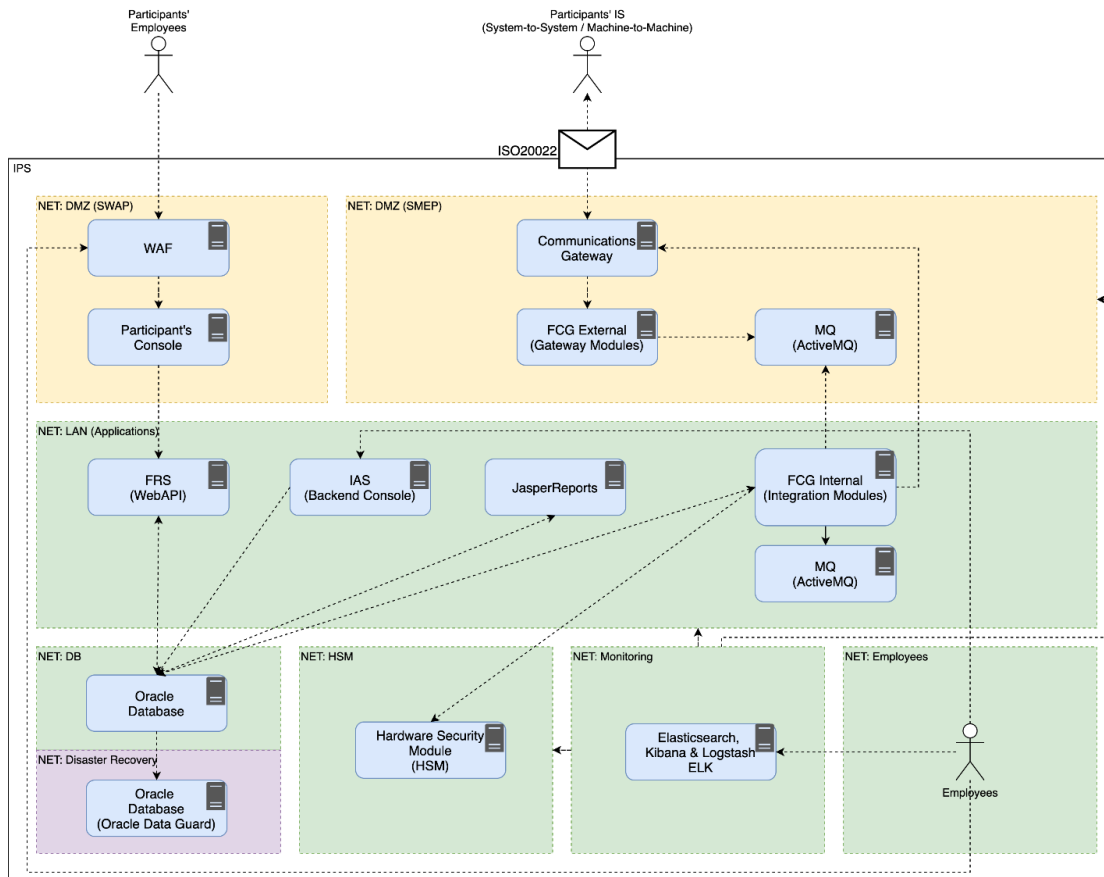


Figure 5: Standard infrastructure

It should be noted that both scalability and high availability can be achieved by adding redundant nodes to the infrastructure together with the necessary load balancing & failover mechanisms. Below is an example diagram, which shows how both scalability and reliability features can be achieved by adding redundant components and configuring them in a way that enables failover and load balancing.

The reliability and performance requirements are defined by the client. Having the requirements, the performance and reliability testing is carried out in order to select the most efficient and appropriate solution, therefore, the infrastructure topology may be subject to change during the process of project implementation.

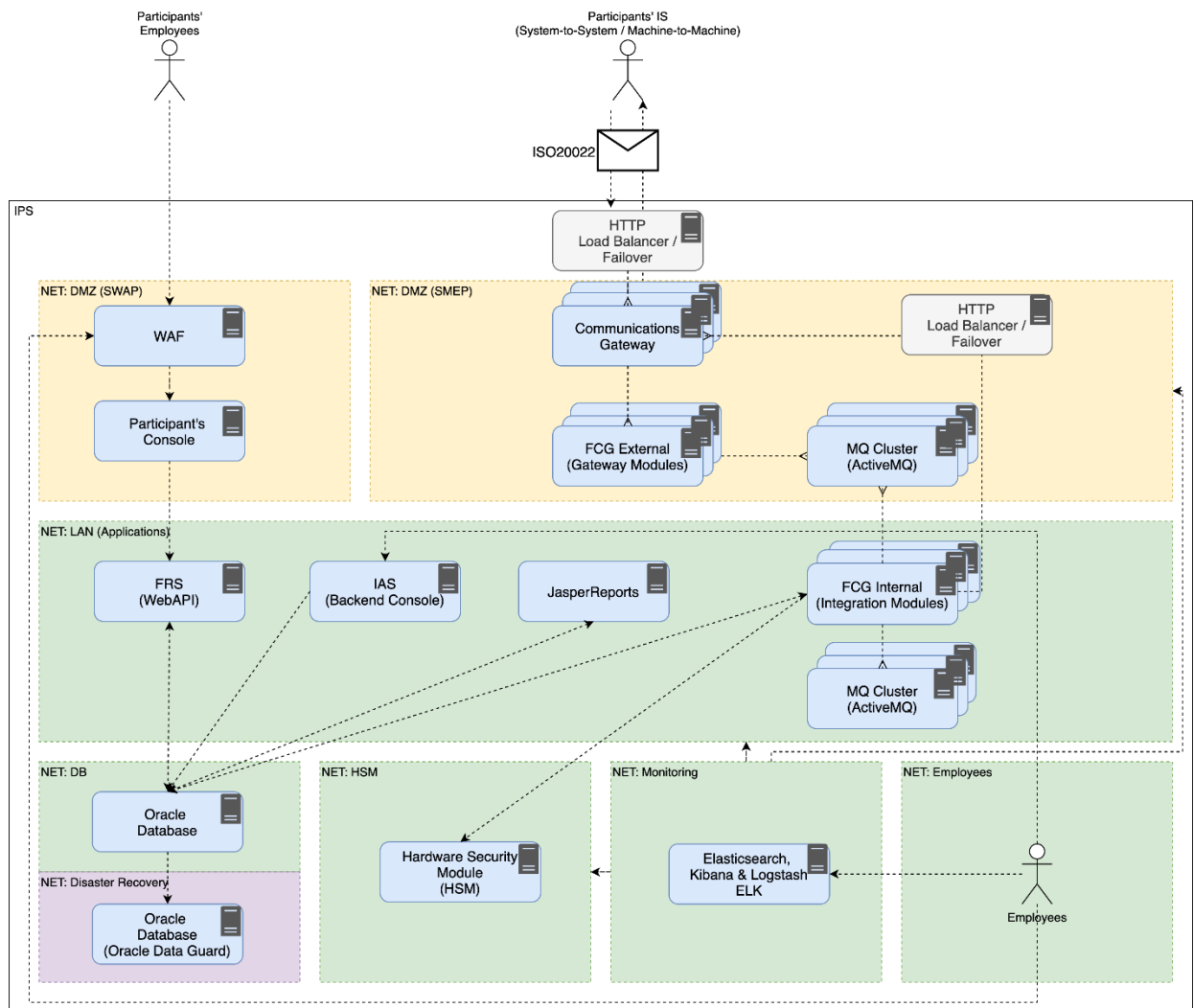


Figure 6: High-level solution architecture

Note: The bigger part of the components is deployable as Linux containers using Docker technology. Although the containerization is not a requisite for this solution, it is recommended as it makes the delivery and deployment of software products a lot easier.

Technical characteristics for each component presented below in Table 4: Environments, machines and technical parameters and Table 5: 3rd party software.

#	Name	Purpose
1	Oracle Database	The main database of the system kernel. High availability is ensured by the Oracle Real Application Cluster (RAC) technology: in case of the failure of any of the cluster nodes, the access and operation of the available nodes is ensured. With the help of the TAF (Transparent Application Failover) technology, the user

#	Name	Purpose
		sessions are redirected to the operating nodes; in case of failure of any of the nodes, this allows transferring of the entire context of the session available on the node copy, to another active node.
2	IAS (Backend Console)	Oracle Application Server. The availability and distribution of sessions are ensured by the load balancing.
3	JasperReports	Reports server based on OSS JasperReports library.
4	FRS	Forbis Remote Services, additional Web API services for the DB. The availability and distribution of sessions are ensured by the load balancing.
5	Participant's Console	Management console for external users (commercial banks and other payment service providers, participants of IPS scheme). The availability and distribution of sessions is ensured by the load balancing.
6	Communications Gateway	Reverse Proxy which enables the secure communication between two endpoints. Both communicating parties are authenticated using a TLS mutual authentication protocol.
7	HSM	Hardware Security Module for storing cryptographic keys and providing cryptographic functions such as data encryption and digital signatures.
8	FCG External	Forbis Connection Gate (gateway modules) for accepting incoming messages from external systems and passing them to FCG Internal for processing.
9	FCG Internal	Forbis Connection Gate (integration modules) for processing both incoming and outgoing messages. This is the main component which implements integration with external systems. Integrations are created using EIP (Enterprise Integration Patterns).
10	MQ	Message Queue / Message Oriented Middleware.
11	WAF	Web Application Firewall / Reverse Proxy.
12	ELK	Collection and processing of logs, monitoring.
13	Oracle Data Guard / Remote Standby Site	A geographically remote data centre with redundant hardware. Oracle Standby/Dataguard technology is applied. The data centre is maximally protected from various unforeseen influences and full failure of the main data centre as well as from data corruption.

Table 3: Architecture solution components

3.6 Integration platform

The IPS system uses the standard native expandable integration platform Forbis Connection Gate which will ensure all required integration interfaces between the IPS system and the network of other services.

Third parties can easily integrate with our system via our API. API is based on industry-wide standards and uses technologies such as HTTP, Mutual TLS, REST API, JSON, HATEOAS, and Digital Signatures. API provides fine-grained services for better customization and flexibility, and, in addition, it provides coarse-grained services for more specific workflows that ensure better performance.

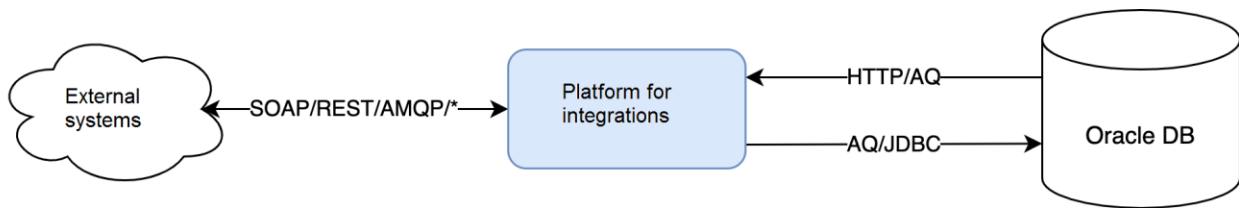


Figure 7: Architecture of integration platform

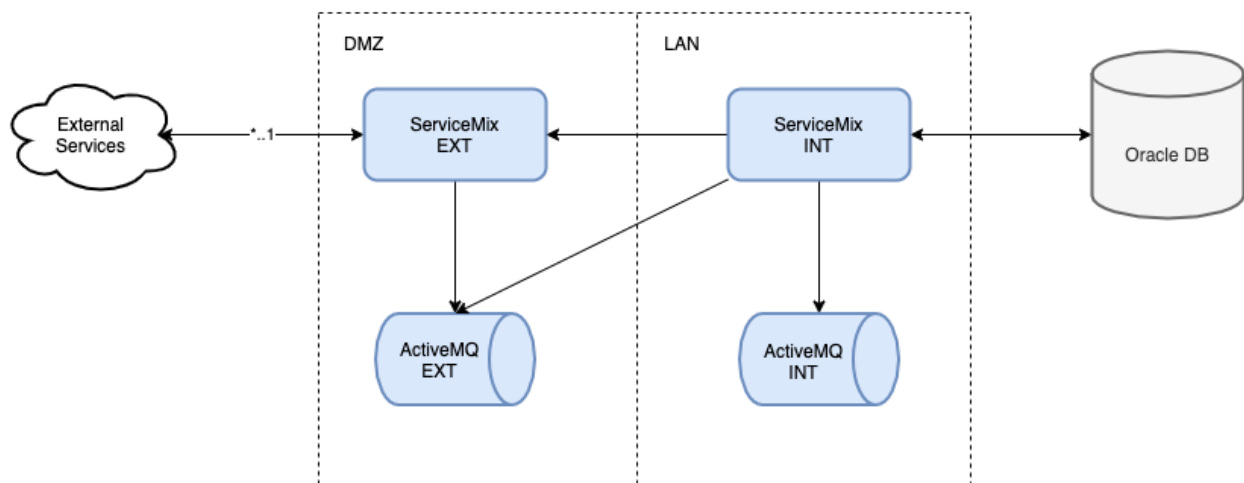


Figure 8: Architecture of integration platform

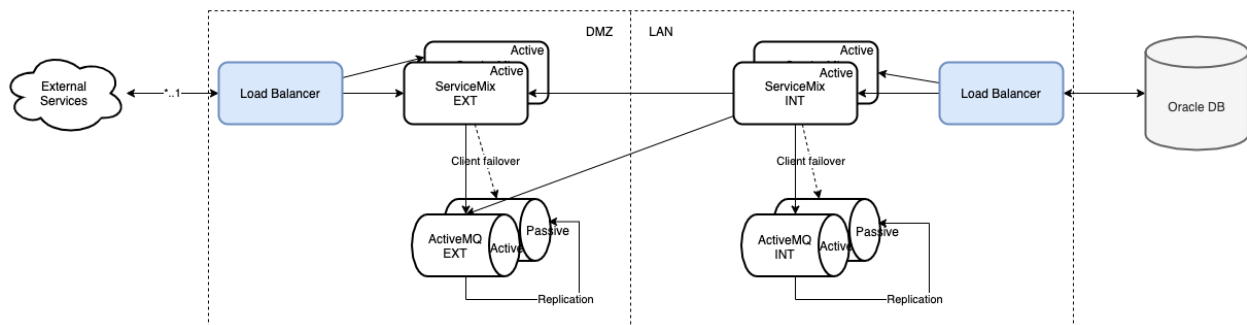


Figure 9: High availability architecture of universal integration platform

System supports a set of standard interfaces with other systems:

- HTTPS as the main protocol for system interaction
- Integrations with SFTP, SMTP, SMPP, JMX
- ActiveMQ and RabbitMQ (the stand at the client)
- Working with WSDL, RESTAPI (SWAGGER)
- SOAP protocol
- WSS (WebSocket Secure) protocol
- Integration with WEBSPPHERE (the stand at the client)
- UDP operation via ISO-8583 gateway

3.7 Technical characteristics of the IPS environments (For One Node)

#	Server name	Purpose	Minimal configuration
LIVE			
1.	IAS	Web-Interface for Internal users	<u>For 300 users</u> 1 node Intel Xeon 2.5 V3 GHz 4 core, RAM 32 GB, HDD 100 GB
2.	Oracle	Core backend	<u>For 300 users</u> Intel Xeon V3 16-24 CPU CORE, RAM – 80 GB, SSD RAID 10 – 500 GB for 1 st year
3.	FRS	Forbis Remote Services; external JVM /Web Services	Oracle unbreakable Linux 7.1 1 node 4 vCore Core (> 2 GHZ), 12 GB RAM 100 GB HDD
4.	Participant's Console	Web Console for external users	Oracle unbreakable Linux 7.1 1 node 8 vCore V3 (> 2 GHZ), 16 GB RAM 100 GB HDD
5.	JasperReports Server	Report server	Oracle unbreakable Linux 7.1 1 node 4 vCore Core (> 2 GHZ), 12 GB RAM 50 GB HDD
6.	HSM	Hardware Security Module	Utlimaco CryptoServer Se12 PCIe CP5 or other models with higher performance capabilities
7.	FCG Internal	Enterprise Service Bus LAN	Intel Xeon 12 vCore V3 (> 2 GHZ), 24GB RAM

#	Server name	Purpose	Minimal configuration
			HDD 500GB
8.	FCG External	Enterprise Service Bus DMZ	Intel Xeon 12 vCore V3 (> 2 GHZ), 24GB RAM HDD 500GB
9.	WAF	Web Application Firewall / Reverse Proxy	4 vCore Core (> 2 GHZ), 12 GB RAM 50 GB HDD
10.	ELK Monitoring	Log mining, monitoring	4 vCore Core (> 2 GHZ), 12 GB RAM 500 GB HDD
TEST/PRELIVE			
11.	IAS	Web-Interface for internal users	The server must have at least 10-20% or more of production server resource capacity
12.	Oracle	Oracle	The server must have at least 50% or more of production server resource capacity
13.	FRS	Forbis Remote Services; external JVM /Web Services	The server must have at least 50% or more of production server resource capacity
14.	Participant's Console	Web Console for external users	The server must have at least 50% or more of production server resource capacity
15.	JasperReports Server	Report server	The server must have at least 50% or more of production server resource capacity
16.	HSM	Hardware security module	Utimaco CryptoServer Se12 PCIe CP5
17.	FCG Internal	Enterprise Service Bus LAN	The server must have at least 50% or more of production server resource capacity
18.	FCG External	Enterprise Service Bus DMZ	The server must have at least 50% or more of production server resource capacity
19.	WAF	Web Application Firewall / Reverse Proxy	The server must have at least 50% or more of production server resource capacity
20.	ELK Monitoring	Log mining, monitoring	The server must have at least 50% or more of production server resource capacity
21.	WTS (+ optional)	Terminal Server for remote Forbis connections (for troubleshooting, optional)	Intel Xeon 2.5 GHz CPU*2 core, RAM 4 GB, HDD 5 GB
RECOVERY			
22.	IAS	Web-interface for internal users	The server must have at least 50-100% of production server resource capacity
23.	Oracle	Core backend	The server must have at least 50-100% of production server resource capacity

Table 4: Environments, machines and technical parameters

3.8 3rd party software specification

The following table provides the technical requirements and recommendations for 3rd party software configuration.

Forbis uses the products of the Oracle Corporation for database management. It allows ensuring the high speed of system operation, fault-tolerant DBMS, and the highest standards of data integrity, security and impenetrability.

Forbis is Oracle Golden partner, and has been granted the right to distribute Oracle products with a partner discount. Forbis is ready to offer exclusive conditions for Oracle products for this project, however, the exact configuration and respective cost of Oracle applications is out of scope of current proposal.

#	Server name	OS	3 rd party products	Licensed software	Freeware
LIVE					
1.	IAS	Windows Server 2012 x64	Oracle Application Server Forms and Reports Services 11g Release 2 OR Oracle Forms 12	For 1 node Min 1 CPU Oracle Forms and Reports	
2.	Oracle	Oracle unbreakable Linux 7.1	Oracle 19 EE Oracle Data Guard* with Switchover option	For 1 node Min 2 CPU Oracle Enterprise Editions	
3.	FRS	Oracle unbreakable Linux 7.1	Java 1.8 + TomCat 8.X +		
4.	Participant's Console	Oracle unbreakable Linux 7.1	Java 1.8 + TomCat 8.X +		
5.	Jasper Reports Server		Java 1.8 + TomCat 8.X +		
6.	HSM	FIPS 140-2 Level 3 HSM	Utimaco** Security Server Se12+		
7.	FCG Internal	Oracle unbreakable Linux 7.1	Java 1.8 Apache service mix 6.x+		

#	Server name	OS	3 rd party products	Licensed software	Freeware
			Docker 19.x+ Active MQ 5.x		
8.	FCG External	Oracle unbreakable Linux 7.1	Java 1.8 Apache service mix 6.x+ Active MQ 5.x		
9.	WAF		Apache HTTPD or alternative		
10.	ELK Monitoring	Oracle unbreakable LINUX 7.1	ELK 7.7.X +		
TEST/PRELIVE					
Same as in LIVE environment, except the following:					
11.	IAS			Can be 20 NUP Oracle Forms and Reports	
12.	Oracle			Can be 1-2 CPU Oracle Enterprise Editions	
13.	WTS (+ optional)	Windows Server + Terminal Service CALL (5 RDP users) + Java Enabled Browser	Oracle Client PL/SQL Developer		
RECOVERY					
14.	IAS			For 1 node 1 CPU Oracle Forms and Reports	
15.	Oracle			For 1 node Min 2 CPU Oracle Enterprise Editions	

Table 5: 3rd party software

HSM

* Our IPS solution is integrated with the HSM models Utimaco Security Server Se12 PCIe, Utimaco SecurityServer Se12 LAN V4. The offer is prepared taking into account the integration with these models or others Ultimaco equivalent models. Utimaco is a worldwide supplier of professional cybersecurity solutions. Company has been developing hardware-based, high-security appliances (Hardware Security Modules) since 1983. Integration with other HSH models is also possible, in this case an additional evaluation of works is required.

ORACLE Data Guard

** For reliability, disaster tolerance, as well as for the purposes of the fastest possible transition to a backup database without the cost of copying and restoring, it is strongly recommended to use the ORACLE Data Guard technology (formerly called STANDBY). This technology allows, by transferring the redo logs (transaction log), to transfer the changes from the Primary Database to the Standby Database and keep it up to date.

Limitations: ORACLE Enterprise Edition only.

Thus, the Database can be dispersed geographically, and the Downtime and the Data Loss are significantly minimized. This allows solving the following tasks: the disaster recovery allows performing transition to a geographically remote Data Center (DC)); the switchover allows changing the database roles to check the remote site, thus to service the Primary site, to update the server, to update the OS on the server, to install the ORACLE patch, to check the operability of the remote server room; it is possible to automatically switch to the Standby Database if the Primary Database is unavailable. Snapshot Standby allows making a test database for a short time, trying incident/bug critical/high, roll-backing, and continuing STANDBY.



Figure 10: Data Guard

It is possible to use and to purchase an additional Active Data Guard option, then the Reporting tasks can be effectively resolved (load balancing is ensured, the Standby Database can be opened for reading (select/query) and report generating, it is possible to direct the load to costly queries from the main database). This option also has the Automatic Block Repair.

Disclaimer: The deeper technical analysis may bring amendments to the above-described infrastructure in relation to currently existing infrastructure and different technical requirements.

3.9 Technical solution and characteristics of the environment for IPS Participants

Requirements for IPS participants:

– **Browsers for Web Management Console:**

OS	BROWSER	SUPPORTED versions
Windows	Edge	Current major version and two versions before
Mac/iOS	Safari and Safari Mobile	Current major version and one versions before
Windows	Mozilla Firefox	Current major version and one versions before
Windows/Mac/Android	Google Chrome or Google Chrome Mobile	Current major version and one versions before

Table 6: Web Management Console

– **For messages exchange with IPS:**

- Message to be signed with X.509 certificate.
- Strongly recommended certificates issued to HSM.
- Recommendations for HSM:

Option 1. Only HSM		
OS	BROWSER	SUPPORTED versions
Requirements for HSM standard: FIPS 140-2 Level 3 HSM.	<ul style="list-style-type: none"> – The API to work with HSM depends on the HSM and must be developed by participant side and integrated with participant IS. – The participant's IS is responsible for message exchange with IPS. 	

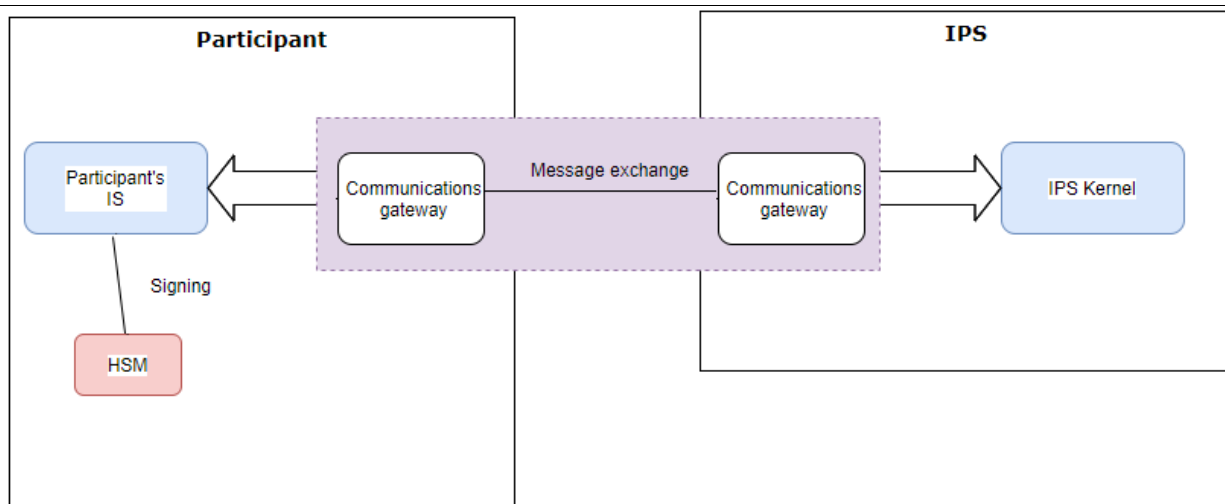


Figure 11: Participant. Message exchange with IPS. Option 1

Option 2. HSM with Forbis provided adapter

OS	BROWSER	SUPPORTED versions
Requirements for HSM standard: FIPS 140-2 Level 3 HSM with PKCS#11 application programming interface.	<ul style="list-style-type: none"> Java based adapter to work with HSM. Using PKCS#11 interface standard for interaction with HSM. Developed by Forbis. The participant's IS is responsible for message exchange with IPS. 	Java 1.8 or higher, HSM related software.

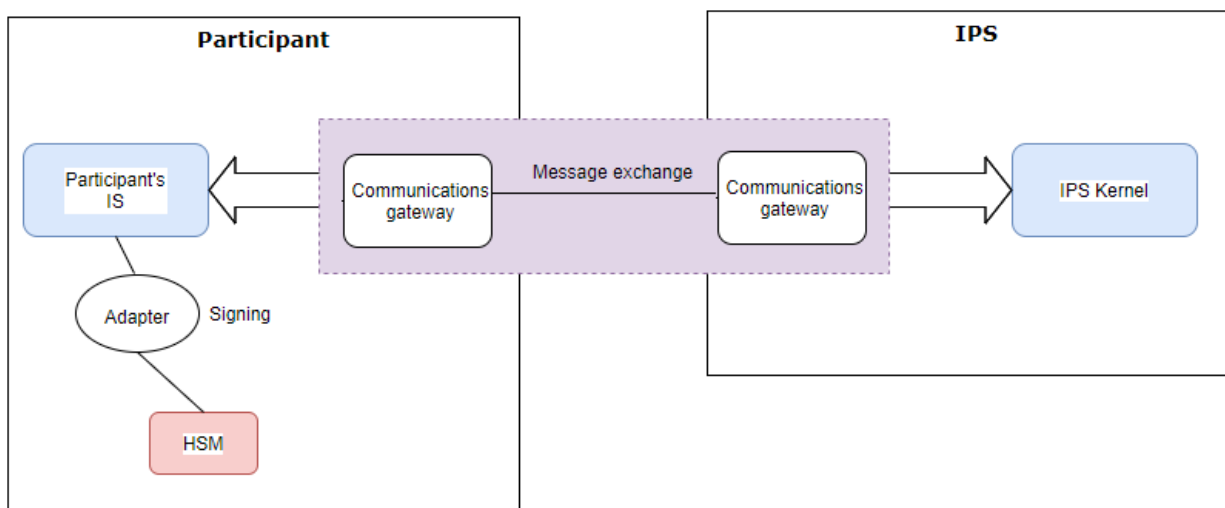


Figure 12: Participant. Message exchange with IPS. Option 2

Option 3. HSM with Forbis provided adapter and Forbis Participant's Connection Gate

OS	BROWSER	SUPPORTED versions
Requirements for HSM standard: FIPS 140-2 Level 3 HSM with	<ul style="list-style-type: none"> PCG (Participant's Connection Gate) solution developed by Forbis. Gateway and integration 	Java 1.8 or higher, HSM related software, Oracle unbreakable Linux 7.x,

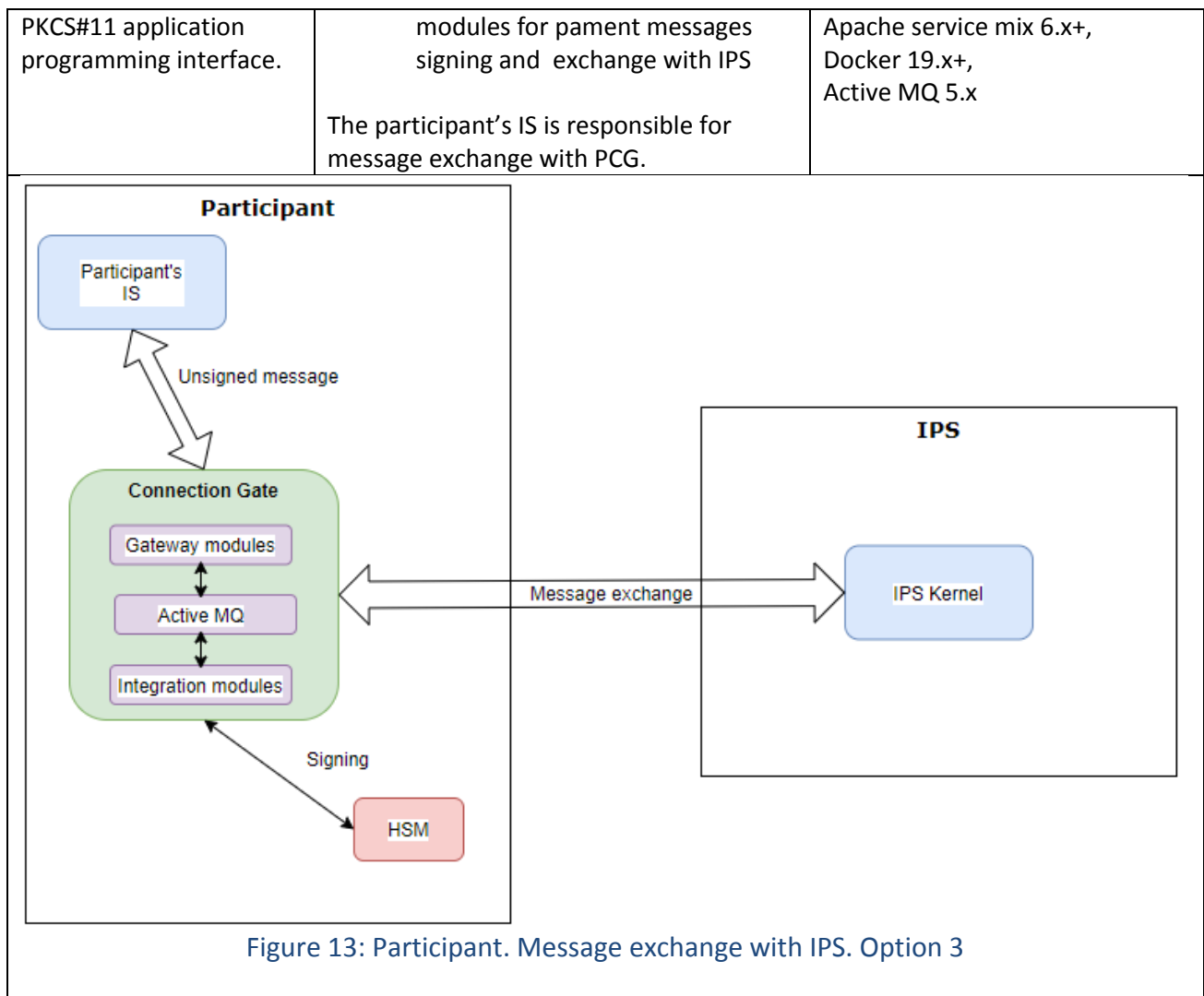


Table 7: HSM

3.10 Justification of Technology Selection

Oracle DB (Oracle 19)

- Multiplatform
- Breadth of services
- Product functionality and performance
- Strong consulting partnership
- Strong user community
- Strategic partnership
- Session concurability
- Overall cost
- High rating at Gartner Inc. (<https://www.gartner.com>)

Oracle Forms (Oracle Forms 12)

- Native Oracle service
- Network traffic optimizations
- HTTP/HTTPS support
- Rapid application development
- Tight integration with Oracle Database Server
- Record locking out-of-the-box functionality

WebLogic Server

- Mandatory for Oracle Forms

Windows Server OS

- Mandatory for Oracle Forms

Java

- One of the most popular programming languages (<https://www.tiobe.com/tiobe-index/>)
- Object oriented: encapsulation, abstraction, polymorphism, inheritance
- Multi threading
- Platform-independent
- Robust, strong memory management
- Portable
- Distributed service
- Strong consulting partnership
- Strong user community
- Wide frameworks and libraries selection
- Native Oracle service
- Tight integration with Oracle Database Server

Javascript

- Main programming language for modern web-based application development
- One of the most popular programming languages (<https://www.tiobe.com/tiobe-index/>)
- Multi-paradigm: event-driven, functional, imperative, object-oriented (prototype-based)
- Supports development for client and backend systems
- Strong user community
- Provides a lot of popular web frameworks (e.g. React)

Linux OS

- Recommended by Oracle
- Portable (multiplatform)
- Multitasking
- Multi user
- Multiprocessor (SMP) support
- Multithreading support
- Virtual memory

- Hierarchical file system
- Graphical user interface
- Wide hardware support
- Dynamically linked shared libraries as well as static libraries
- POSIX compliant
- Multiple virtual consoles
- Multiple file system support
- Multiple networking protocols (TCP/IP, IPX/SPX, Appletalk, AX.25)
- Shell
- Strong security model
- Open source

Apache Tomcat

- One of the most popular web application servers for Java platform
- Open-source (The Apache Software Foundation)
- Supports Java Servlet specifications up to (and including) 4.0
- Clustering
- Easy load balancing with Apache HTTPD (via HTTP and AJP connectors)
- Monitoring and management
- JMX
- Supports WebSockets
- JNDI
- Virtual Hosting
- Advanced IO (blocking and non-blocking)

Apache ActiveMQ

- One of the most popular and powerful open-source messaging server (MOM – Message-Oriented Middleware)
- Supports JMS 1.1
- Supports transient, persistent, transactional and XA messaging
- Open-source (The Apache Software Foundation)
- Clustering
- Enterprise Integration Patterns
- JMX

Apache ServiceMix

- Integration container, which provides a unified solution for developing integration applications
- Open-source (The Apache Software Foundation)
- It unifies the features and functionality of the following:
 - Reliable messaging with Apache ActiveMQ
 - Messaging, routing and Enterprise Integration Patterns with Apache Camel
 - WS-* and RESTful web services with Apache CXF
 - OSGi-based server runtime powered by Apache Karaf

Jasper Reports Lib

- One most popular open-source reporting engines for Java platform
- Layout and Interactive Features:
 - Pixel-perfect page-oriented or continuous output for web or print
 - Dashboards, tables, crosstabs, charts, gauges and widgets
 - Sub-reports easily handle highly complex layouts
 - Integrated barcode support
 - Visual text rotation
 - Styles library
 - Drill-through / hypertext links, including support for PDF bookmarks
 - Interactive table elements and sub-reports for interactive and complex layouts
 - Conditional printing
- Flexible Deployment and Output:
 - Report output in PDF, XML, HTML, CSV, XLS, RTF, TXT
 - Internationalized and localisable for global deployments
- Variety of data sources:
 - Database JDBC connection
 - XML file data source
 - File CSV data source
- Scalable architecture:
 - No limit to report size
 - Report virtualizers to optimize for memory utilization and I/O performance
 - Query governors to protect system resources

Docker

- One of the most popular open-source containerization technologies
- Allows rapid development, shipping, and running applications
- Isolates applications from the underlying infrastructures:
 - Operating systems
 - Networking
 - Filesystems
- Ensures solution portability across different environments
- Allows flexible resource allocation management via Linux control groups (cgroups):
 - CPU time
 - System memory

ELK

- the open source, distributed, RESTful, JSON-based search engine
- easy to use
- scalable and flexible
- powerfull visualization tool.
- worldwide community

The ELK Stack is a collection of three open-source products:

- ElasticSearch: used for storing logs;
- LogStash: used for both shipping as well as processing and storing logs;
- Kibana: is a visualization tool (a web interface) which is hosted through Nginx or Apache.

3.11 Data strategy

3.11.1 Data categories

The following attributes for data may be defined:

- Manageability – an ability to edit or manipulate the data.
- Availability – a period of time needed to provide data (make it available) to the user.
- Accessibility – constraints to access data, e.g.:
 - Online – constant access.
 - On demand – data can be accessed according to business needs.
 - On request – user must submit official request to access data.
- Interface – what way the user can access data.

According to such attributes the data falls under the following categories:


- Operational
- Operational Archive
- Archive
- Historical

Data category	Manageability	Availability	Accessibility	Interface	Responsibility
Operational	Editable by user	According Business continuity plan category	Online	Application	Forbis
Operational Archive	Not Editable by user	Next business day	Online	Application	Forbis
Archive	No	1 week	On demand	Application + additional user action	Forbis
Historical	No	1 month	On request	Archive documents	Bank

Table 8: Data categories

Operational data is data actively used in a day-to-day work to ensure business functionality. Users have the rights to insert, update or access the data using IPS UI.

Operational archive means historical data, which quite rarely (from time to time) might be required for business functionality or reporting. It is stored in archive tables in _ARCH tablespace separately from the



operational data. This data is not editable (read-only). The operational archive data is accessed using IPS UI. The operational data is transferred to the operational archive automatically using table triggers or scheduled jobs, which transfer the data from the operational tables to the archive tables.

Archive data is read-only data, which is no longer used in day-to-day work, but is valuable as a proof. There is no access to this data in IPS UI – only using custom reports or any Oracle RDBMS client software. This data is stored in another archive table (not in the same as the operational archive) in _LTA tablespace. Usually after the data is exported to the historical archive these archive tables should be cleared. Transfer from the operational archive to the archive is done using IPS API manually or employing scheduling jobs.

Historical archive means an archive of the exported data intended for a very long storage term usually on external carriers like magnetic tapes (manually managed). Forbis IPS does not provide means for such activity, but this can be done under an additional agreement.

3.11.2 Data retention

The IPS is designed and developed to comply with the General Data Protection Regulation (GDPR), which automatically obliges the IPS to ensure data retention periods according to their importance and type. To ensure the speed of operation of the IPS, the system has been designed applying the best known practices for data storage and data flow distribution (indexing, use of the Oracle hint, data structure partitioning, data structure normalization and denormalization methodologies, parallelization of the system processes, transfer of the system processes to lower load periods).

In addition, the system allows to unload some historical data in a denormalized way to other locations in the system, thus increasing the system speed of operation when working with the recent past data within the system itself, and improving report loading time when it is required to generate reports for some long past periods.

3.11.3 Archiving

The IPS uses all standard Oracle means for archiving. The IPS has the mechanism of automated archiving of the tables; the archived tables are partitioned.

The IPS allows collecting all the historical data, including the system audit records and logs.

4. Implementation project

In the course of Project implementation, there will be applied project management standards, which are provided by the “Project Management Body of Knowledge” (PMBOK) and “Agile” practice guides.

More details regarding the implementation project are provided in “Initial Project Management Plan”.

4.1 Major phases

The initial project plan is prepared based on functional requirements, non-functional requirements, software development lifecycle requirements, other information. Programme plan start date is set at 03-01-2022. This date has been chosen as indicative, and it can be changed by mutual agreement between Bank and Supplier.

The initial Project plan consist of 8 phases:

1. Business Analysis phase,
2. Design Phase,
3. Build Phase,
4. Testing Phase,
5. Training,
6. Go-live and final acceptance,
7. Solution documentation,
8. Non-functional requirements implementation.

The initial Programme plan is provided below, it can be changed by mutual agreement between Bank and Supplier:

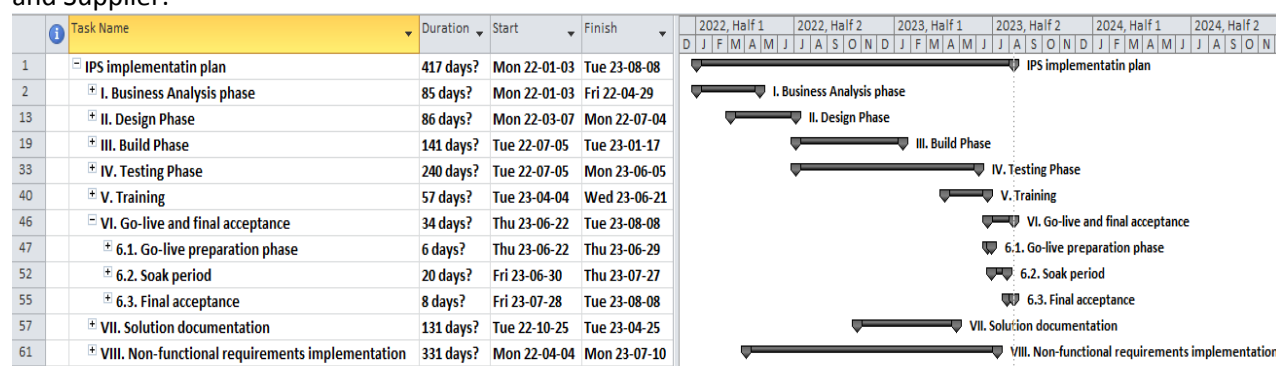


Figure 14: The initial Programme plan

Business Analysis phase will start with the GAP analysis and continue with preparation of all the required documents. All documents will be aligned and confirmed by Bank. Total phase duration is 4 months.

Design Phase will start in the middle of the business analysis phase, as some GAPs will be already aligned with Bank and ready for detail design. At the end of the design phase, all the documents will be aligned and confirmed by Bank. Total phase duration is 4 months.

Build phase will start after the accomplished design phase. The phase will be divided into 7 work streams:

Stream 1	(IPS core (7.1. Transfer Order, 7.2 Recalls, 7.3. Transaction status validation (Investigation), 7.4. General functional Requirements);
Stream 2	CAS (7.5. Central Alias Service);
Stream 3	Dispute Management (7.6. Dispute Management Module (IPS.DM.01));
Stream 4	Monitoring, unavailability management and pre-authorization (7.7. Statistics, monitoring, reporting, alerts (IPS.SM.01), 7.9. Participant “unreachable” function and pre-authorization facility);
Stream 5	RTP (7.8. Request to Pay and Payment Initiation Request (IPS.RTP));
Stream 6	Billing (7.10. Billing).
Stream 7	Non-functional requirements

Table 9: 7 work streams

The streams are divided based on their functionality relationship and interdependencies. The first and the main stream is the IPS core, which will create a subsystem of transfers’ management. Some other streams will be executed in parallel, as they do not have a direct relationship. Total phase duration is 7 months.

Testing Phase will start together with the design phase as some testing phase activities, like testing plan, need be prepared in the early development stage. Testing will be done in a couple of stages: the initial testing (performed by the developers), then the alfa-testing (performed by the testing team, analysts), and finally, the UAT (user acceptance testing). On the UAT stage, both Bank and Supplier will take part. Total phase duration is almost 11 months.

Training Phase will start at the second part of Testing phase. It will ensure timely Bank key persons preparation for testing activities. There will be separated trainings session for IT administrators /super user, IT analyst and end users. Total phase duration is approximately 3 months.

Go-live and final acceptance phase will start after the Training and Testing phase are completed. The phase may be divided into the following three parts:

Go-live preparation phase	The purpose of this phase is to review and assess readiness from the point of view of IT and Business readiness criteria, and deploy the whole solution into production environment.
Soak period	It is the system’s hyper care period when the system is stabilized after go-live, and involves fixing defects.
Final acceptance	Documentation/deliverables for all phases’ acceptance by Bank team.

Table 10: Go-live and final acceptance phase

During the **Solution documentation phase**, all the required documents will be prepared including User instructions and User guides, system operating instructions/work instructions, documentation relating to end-users and technical trainings, and other project documentation. This phase will start in the middle of the Build phase.

Non-functional requirements implementation phase will start at the beginning of the Business analysis phase and will continue until go-live.

4.2 Project deliverables and other expected results

Deliverables can be grouped depending on its context:

- Supplier's **documentary deliverables** for Bank – for example: software requirements specification (SRS), user guide, base description of functionality, admin guide, patch installation instruction etc.
- Bank's input **data provision** for Supplier – for example: requirements document, use cases, examples etc.
- Supplier's **software deliverables** for Bank – for example: patches, installation frameworks etc.
- **Testing material deliverables** – for example: test plan, test cases, test summary report etc.
- **Project material deliverables** between both Parties – for example: project plan, project timeline, project Gantt, meeting minutes, weekly/monthly report, end of phase report, risk registry, questionnaire, follow up status on previously agreed actions etc.
- **Presentation deliverables** – for example: MS power point with overall Programme /sub-project progress
- **Process scheme deliverables** – for example: scheme where stated responsibilities and actions according to particular staff functions

No.	Project Phase	Deliverable name	Description /goal /content
1	Business analysis phase	GAP's list	GAPs identification in details, consolidation and final scope sign-off
		Software requirements specifications	Detailed software requirements specifications of the solution proposed for the implementation with clear link/track of the particular requirements to the process (-es)
2	Design phase	Design /architecture documents	Documents on the detailed functional specification of the solution, which shall cover both technical and functional aspects
		Test environment	Test environment preparation on Bank and Supplier's sides
3	Build phase	Software solution	Solution according to GAPs development in Work Streams [1-7]
4	Testing phase	Supplier's testing	Supplier's internal testing of developed GAPs in Work Streams [1-7]
		Bank UAT	Bank user acceptance testing (UAT) in Work Streams [1-7]
5	Training phase	Trainings	Supplier shall conduct Bank staff training to ensure an adequate level of knowledge and skills to use and manage efficiently the solution
6	Go-live and final acceptance	Go-live	Solution implementation to production environment after testing was performed and no severity 1 and 2 defects remains.

7	Solution documentation	User guides	User instructions and users guide providing
		Admin guides	System operating /instructions - work instructions /admin guides providing

Table 11: project phases

4.3 Quality

4.3.1 Quality Management Approach

Forbis has implemented the quality management to identify and manage the overall quality assurance. The quality management plan provides both guidance and direction on how the quality will be managed and validated throughout major projects.

The quality management is based on principles of standard programme/project management methodologies, as IT enabled major programme transformation method and Project Management Institute framework. Worldwide known standards and best-practice methodologies, such as ISO 20000, ISO 9001, ISO 27001 apply where appropriate.

A project team will be assigned with respective roles and responsibilities for coordination of general process of quality management, decision and approval of all the changes in the respect of quality assurance. A purpose of the quality management plan is to ensure that the results of completed tasks (deliverables) which are approved will meet requirements in accordance with prescribed scope and budget.

The procedure of quality management control will be applied by:

- monitoring the progress towards objectives of the development project;
- monitoring the project documentation quality (overall project management documents, questionnaires, specifications, manuals etc.);
- monitoring the project management quality;
- processing the results of quality control.

4.3.2 Quality Assurance and Internal Controls

Forbis undertakes to implement a mechanism of the Quality Assurance and internal control. In accordance with such standards, quality assurance system and procedures applied by top-tier IT service provider, Forbis will develop, implement and maintain the mechanisms, processes and procedures of quality assurance and internal control (including organizational controls, input/output controls, system modification controls, processing controls, system design controls and access controls).

Such processes will also cover verification, checkpoint reviews, testing and other procedures for service recipients to assure the performance quality and timeliness.

Forbis will implement tools and methodologies to perform the Project in an accurate and timely manner in compliance with accepted industry standards of first tier providers of similar services and the local laws applicable to the performance of the services.



4.3.3 Continued Service Improvement

Forbis will improve the provision of services by using the up-to-date technologies considering the latest trends available.

Forbis will ensure the continual service improvement by permanent reviewing its performance and by continuous developing Forbis products and services to ensure that the products and services would maintain a relevant technological level and relevant level of service – this will allow the service recipients to get more competitive technological advantages for supporting their business and will provide the efficient and cost effective solution resulting in the leadership on the technological market.

Forbis has implemented and maintained high security standards, facilities and procedures. Forbis will ensure that each of the Sub-contractors and each of Forbis employee will follow the service-related rules on reasonable safety and security.

4.3.4 Quality policy of Forbis


Forbis undertakes to ensure the quality and continuous activity improvement in all areas of company business activity. The highest priority of the company is to satisfy customer's expectations. By applying this policy, it is endeavoured to provide a basis to determine the goals oriented to the implementation of customer requirements and continuous improvement of the processes.

Forbis operates as a team and strives to involve all the company specialists into the continuous process of quality improvement. Striving to achieve strategic targets, Forbis uses a consistent and systematic quality management method and is constantly self-improving. The company strives to satisfy the customers in the fullest possible manner by applying effective work methods including the comprehensive improvement of business processes.

Quality goals of Forbis are as follows:

- To strive to understand the customer expectations as best as possible and to precisely follow their requirements when implementing new technologies.
- To continuously monitor and assess the quality planning and implementing process, to increase its efficiency and outcome to avoid failures as well as to effectively remedy consequences of such failures, if any.
- To select those service providers who follow both quality and security requirements in the best possible manner.
- Train competent employees helping the company attain goals of the quality management system.
- To analyse the worldwide technological progress in the area of company activity and to implement up-to-date solutions in the products developed by Forbis.

Striving to achieve the above-mentioned goals, Forbis in its activity uses the quality management system which provides an opportunity of providing the customers with high quality products and services satisfying customer expectations and needs. The company makes provision for required resources for



continual monitoring and improvement of the quality system that helps in creating a professional long-term cooperation atmosphere between company employees, customers, partners and other privies.

Forbis monitors the applicable local laws and regulations in the countries the company works in. The company develops its services and products considering customer needs, security requirements and applicable legal regulations.

The present policy is applicable to Forbis and its subsidiaries as an imperative policy.

Executives of the Forbis company are responsible for the determination and implementation of policy objectives, installation and implementation of the quality management system as well as definition of the responsibility for specific functions of quality assurance. All the employees are personally response for reading, understanding and following this policy.

Every employee is obliged to inform about current or probable violations of this policy.

4.4 Risk-analysis

4.4.1 Description of risk management method

The purpose of risk management is to anticipate factors that could have a negative impact on project outcomes, timing or costs. The risks and malfunctions of the project have to be managed in order to reduce their impact and ensure the smooth running of the project.

In this section we present a main description of the risk management methodology; a list of organizational, project-related and technological risk factors that could influence successful project implementation; risk assessment; and measures for risk avoidance and mitigation.

The risk management method consists of the following steps:

- Risk analysis:
 - Risk identification (the detailed list of risks is determined by examining not only the technical aspects of the project, but also the institutional and physical environments).
 - Prioritization of risk (estimation of probability of risk occurrence and impact on the project).
- Risk management:
 - Risk management planning (creation of a risk management plan. The plan specifies measures of management and control for identified risks);
 - Risk management (implementation of risk management plan).

4.4.2 Risk analysis

The following risk attributes are used for the risk analysis and management:

- Source of risk – the source the risk is coming from.
- Risk probability – the chance the risk will materialize.

- Risk impact – the possible impact of materialized risk.

4.4.3 Risks related to project management

These are the risks associated with poor project management: inappropriate project planning, inadequate controls, inadequate communication or collaboration.

Organizational risks

Organizational risks – limited resources of the organization, personnel problems, reorganization, changing priorities of the programs under implementation, disturbances of financial flows.

Technical risks

These are risks directly related to the system being implemented. It covers a wide range of issues:

- Requirements for system functionality (functional and non-functional);
- System adaptation and successful development;
- System integration with external systems;
- User assistance system;
- Infrastructure: hardware, network, system environment.

External risks External risks are changes in the external environment that may have a negative impact on the success of the project. External risk factors arise from adverse actions by suppliers or subcontractors, overall economic situation in the state and, in the framework of this project, a major role is to be played by changes in legislation or delays in those changes.

Probability of the risk

We distinguish the following categories of risk probability:

Probability	Explanation
Low	A small probability to influence the project plan, increase costs or impair the quality.
Moderate	An average probability to influence the project plan, increase costs or impair the quality.
High	Major changes to the project plan, increase of costs or quality deterioration are possible.

Table 12: Probability of the risk

Risk impact

Risk impact is the extent to which the duration of the project, costs, scope of work, and the quality of the results are affected by the risk. We distinguish three levels of exposure - low, moderate and high; the meaning is explained in the table below.

Impact	Explanation
Low	Project duration and / or costs increase up to 10%. The change in scope is modest and does not affect the essential expected results. Quality degradation does not affect essential functionality.

Impact	Explanation
Moderate	Project duration and / or costs increase by 10–20%, the change in scope affects the essential functionality.
High	Project duration and costs increase by more than 20%, the impact of scope changes and / or quality degradation is unacceptable in relation to project objectives.

Table 13: Risk impact

Risk priority

A risk priority is identified by assessing the likelihood and impact of each risk factor. Risk priority = Probability x Impact.

Risk priority		Impact		
		Low	Moderate	High
Probability	High	Moderate	High	Critical
	Moderate	Low	High	High
	Low	Low	Moderate	Moderate

Table 14: Risk priority

4.4.4 List of potential risks

The table below represents the risk analysis results and possible risk mitigation measures.

#	Risk owner	Risk	Risk source	Probability	Impact	Priority	Consequences	Risk mitigation
1.	Bank	Implementation of integration with other systems can be delayed due to the modification of third-party systems, lack of testing environment, or unavailability.	T, E	H	H	C	Possible consequences: <ul style="list-style-type: none"> System integration is not possible; Delays in project delivery. 	Possible risk mitigation measures: <ul style="list-style-type: none"> Integration with a third party is carried out using an approved protocol; The supplier ensures timely escalation of problems if such occur during the project implementation; All external data that is to be used in the system has to be defined during the analysis.
2.	FORBIS, Bank	Risk associated with	P	H	H	C	Possible consequences: <ul style="list-style-type: none"> Poor cooperation 	Possible risk mitigation measures: <ul style="list-style-type: none"> Project

#	Risk owner	Risk	Risk source	Probability	Impact	Priority	Consequences	Risk mitigation
		coordination of large number of project participants (the project will involve specialists with different professional qualifications)					between project participants; <ul style="list-style-type: none"> Poor project coordination; The project involves professionals with different professional qualifications; Different perception of objectives and needs; Delays in project delivery; Incorrect results of the project. 	management plan. <ul style="list-style-type: none"> Building a project working group from the Bank side, involving representatives of all stakeholders. Appointment of one person for daily contacts and communication.
3.	FORBIS	Incorrect evaluation of system architecture	T	M	H	H	Possible consequences: <ul style="list-style-type: none"> A change in implementation strategy is required. Delays in project delivery. 	Possible risk mitigation measures: <ul style="list-style-type: none"> Selection of highly qualified specialists; All requirements and external factors, etc. have to be clearly defined during the analysis. Alignment of architectural design with Bank and obtaining required approvals.
4.	FORBIS	Low reliability of the system	T	M	H	H	Possible consequences: <ul style="list-style-type: none"> If the system will operate unreliably (failures, information security incidents), users will have no trust with the system. Malfunctions and 	Possible risk mitigation measures: <ul style="list-style-type: none"> Special attention has to be given to the reliability and trustworthiness of the system during both development and testing.

#	Risk owner	Risk	Risk source	Probability	Impact	Priority	Consequences	Risk mitigation
							security incidents may also have serious political and financial implications.	
5.	FORBIS	Inaccurate assessment of the scope	P	M	H	H	Possible consequences: <ul style="list-style-type: none"> • Incorrect assessment of the initial scope; • Incorrect final results. 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Reciprocal alignment of scope by developing and approving the requirements specification. • Iterative project execution.
6.	FORBIS	Budget overrun	P	M	M	H	Possible consequences: <ul style="list-style-type: none"> • Overrun of project budget. 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Work and term control; • Effective use of resources; • Appointment of qualified specialists.
7.	FORBIS, Bank	Factor of project team	O	L	H	M	Possible consequences: <ul style="list-style-type: none"> • Inappropriate people are selected for the project implementation; • Misunderstanding of scope and tasks by project team members. 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Team is selected taking into account competences required for project implementation; • Periodic and additional team interaction; alignment of goals and plans.
8.	FORBIS	Unacceptable project deliverables	P	L	H	M	Possible consequences: <ul style="list-style-type: none"> • Inappropriate decisions are made; • Deterioration of quality of project 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Active participation of all project participants in the implementation of

#	Risk owner	Risk	Risk source	Probability	Impact	Priority	Consequences	Risk mitigation
							deliverables.	the project; <ul style="list-style-type: none"> • Timely submission of information; • Adherence to deadlines; • Validation and verification of results with the client.
9.	Bank	Delayed decisions: delays in decision making, review and acceptance of project documentation.	P	M	M	M	Possible consequences: <ul style="list-style-type: none"> • Project delays, additional costs, ineffective work of the project team. 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Approval of the work plan at the beginning of the project, strict control over the work process, prioritization, and focus on timely decision making.
10.	FORBIS	System errors	T	L	M	M	Possible consequences: <ul style="list-style-type: none"> • Errors in data or certificates issued, incorrectly generated reports, additional costs for eliminating the consequences of errors. 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Full system testing; test quality control and test coverage control; continuous quality control.
11.	FORBIS, Bank	Complex management of project environments	T	L	M	M	Possible consequences: <ul style="list-style-type: none"> • Incompatible, inefficient project team work (work with interruptions). 	Possible risk mitigation measures: <ul style="list-style-type: none"> • The work will be performed using the technology of private cloud service provider. Forbis has developed the virtual environment management practices and is currently managing a total of 14 projects with a working volume

#	Risk owner	Risk	Risk source	Probability	Impact	Priority	Consequences	Risk mitigation
								of approx. 20TB.
12.	Bank	The analysis may reveal additional functionality is required.	T	L	H	M	Possible consequences: <ul style="list-style-type: none"> • Additional interfaces will appear, changes will be made to approved decisions; • Project terms may be affected, solution changes will be needed; • Delays in project delivery. 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Clear definition of functional requirements during the analysis; • Establishment of change management procedure; • Clear allocation of responsibilities, introduction of time buffer for rotation; • Introduction of a reserve time buffer for risk management.
13.	FORBIS, Bank	Loss of key experts (holidays, staff changes)	O	M	M	M	Possible consequences: <ul style="list-style-type: none"> • If the main experts of Bank or implementer were unable to continue working on the project (due to illness, job change or other reasons), this could result in loss of knowledge and time. 	Both the implementer and the Bank have to ensure a sufficient documentation of the experts' work in order to transfer the work to another person effectively. Possible risk mitigation measures: <ul style="list-style-type: none"> • Early warning about possible team changes; • The appointment of alternate for responsible person, if needed; • Clear documentation of performed work.
14.	FORBIS	Inaccurate, poor planning	P	L	H	M	Possible consequences: <ul style="list-style-type: none"> • Incorrectly determined project activities; 	Possible risk mitigation measures: <ul style="list-style-type: none"> • Preparation of a detailed project plan;

#	Risk owner	Risk	Risk source	Probability	Impact	Priority	Consequences	Risk mitigation
							<ul style="list-style-type: none"> Incorrectly scheduled deadlines for project activities; Delays in project delivery. 	<ul style="list-style-type: none"> Alignment of the detailed project plan with the client; Approval of the detailed project plan.
15.	Bank	Insufficient control	P	L	M	M	Possible consequences: <ul style="list-style-type: none"> Lack of control of the project plan; Delays in project delivery and poor compliance of project delivery to project objectives. 	Possible risk mitigation measures: <ul style="list-style-type: none"> Selection of appropriately qualified project managers both from the client and from the supplier; Reports, time sheets, additional internal controls.
16.	FORBIS, Bank	Inadequate or ineffective communication	P	L	H	M	Possible consequences: <ul style="list-style-type: none"> Inconsistencies in understanding the overall project objectives and progress; Poor compliance of project delivery to project objectives. 	Possible risk mitigation measures: <ul style="list-style-type: none"> Preparation and implementation of the communication plan. Regular meetings, alignment and approval of interim results.
17.	FORBIS, Bank	Non-performance of contractual obligations	P	L	H	M	Possible consequences: <ul style="list-style-type: none"> Non-performance of contractual obligations; Non-observance of deadlines; Violation of the confidentiality agreements; Delays in project delivery. 	Possible risk mitigation measures: <ul style="list-style-type: none"> Clear definition of obligations in the agreement, which is signed between the supplier and the client; Establishment and approval of a detailed work plan; Establishment and approval of a project implementation

#	Risk owner	Risk	Risk source	Probability	Impact	Priority	Consequences	Risk mitigation
								procedures; <ul style="list-style-type: none"> Regular monitoring of work execution and discussion of results.
18.	FORBIS, Bank	Other external factors and their effects, force majeure	E	L	H	M	Possible consequences: <ul style="list-style-type: none"> Delays in project delivery; Failure to finish the project due to force majeure. 	Possible risk mitigation measures: <ul style="list-style-type: none"> Continuous tracking of areas affecting the project; Active participation of all project participants and timely decision-making.
19.	FORBIS	Insufficient presentation of information to the client and other interested external parties	P	L	L	L	Possible consequences: <ul style="list-style-type: none"> Failure to ensure accountability to external bodies Insufficient information. 	Possible risk mitigation measures: <ul style="list-style-type: none"> Establishment and approval of project implementation procedures; Project progress reporting; Presentation of the final project implementation report.

Table 15: The risk analysis results and possible risk mitigation measures

5. Attachments

- Answers to the tender requirements from F4.4, section 7-10. Description for the project management. Documents: Annex_1. FR.1-180, Annex_2. IR.1-51, Annex_3. NF.1-99, Annex_4. MnS.1-7.
- Initial project management plan with deliverables.
- Proposed service level agreement (SLA) with appendices:
 - Model of standard maintenance and support agreement
 - Model of standard licensing agreement
 - Model of Product warranty.