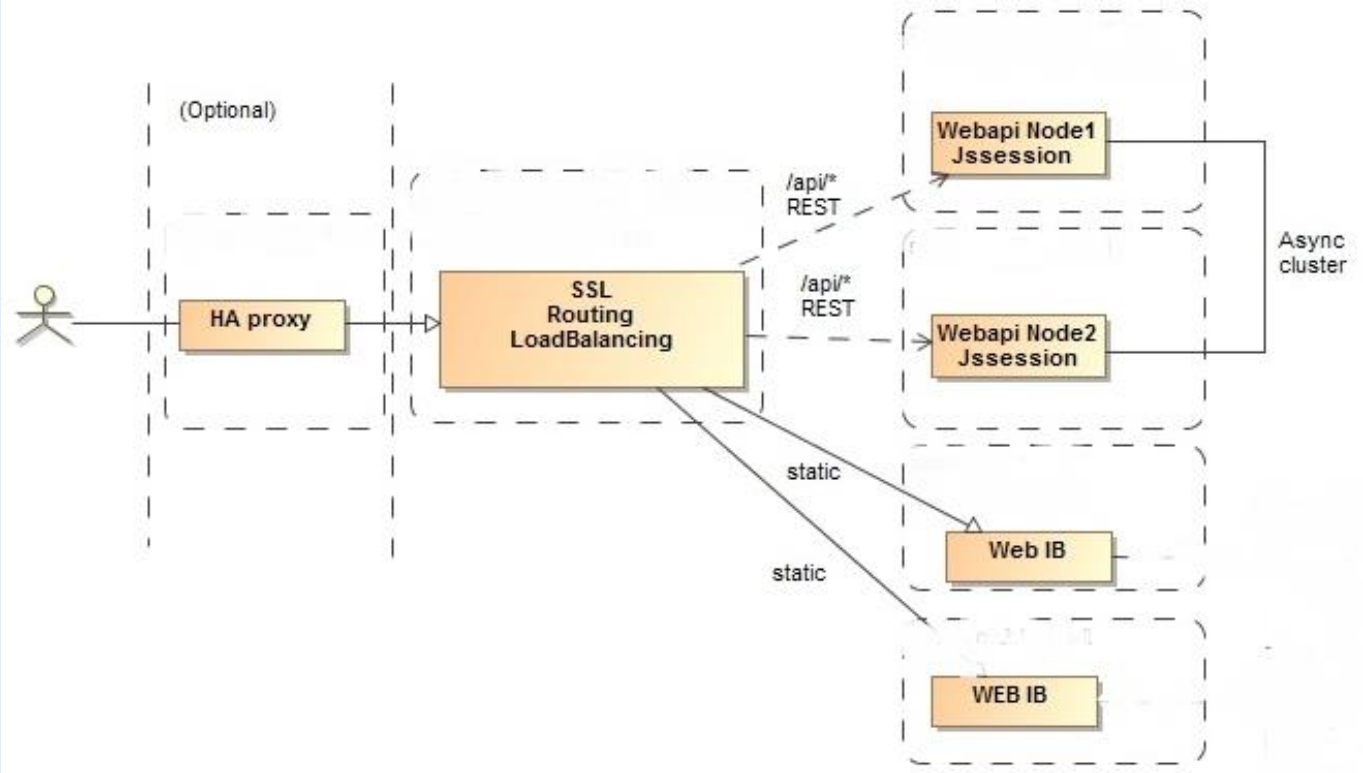
Forbis Solutions, Ltd

ANSWERS TO NON-FUNCTIONAL REQUIREMENTS

8.1. Requirements

Req. ID	Requirements	Classification
1. Requirements for the main characteristics of the solution		
NF. 1	The architecture of the solution shall be aligned to best practices and standards to meet the highest criteria for integrity, compatibility, performance and reliability.	Mandatory
Forbis has thirty years of experience in developing secure and reliable solutions for banking industry, the Oracle partner's status and certificates of ISO 27001 and ISO 20000 standards. 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.		
NF. 2	The solution will have an open and modular architecture, which will allow easy implementation and integration with different systems.	Mandatory
Yes, in the database, the modules act as schemes of different products. Modules for different external applications are also available. Modules are build up and adjusted for each client individually, according to his business needs and the purchased set.		
NF. 3	The technological architecture of the application must have a high level of resistance to failures, and should not contain single points of failure (SPOF).	Mandatory
The goal of our system and subsystems is high availability and reliability against any failures. In most cases, we add redundancy (clustering) in all potential places. For example:  		
NF. 4	The IPS system must provide native integration capabilities with other systems such as automatic interbank payments systems (AIPS), Participant systems, etc. *NBM expects that Vendor will explain in details how proposed IPS solution:* • *Supports STP approach for interaction with external systems* • *Distribute information to external systems*	Mandatory

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.		
NF. 5	Due to high amount of processed data, to ensure increased productivity, the solution shall have native integrated capabilities such as in-memory processing, multi-thread processing, parallel execution of jobs, etc.	Mandatory
System has our own means for parallelizing jobs, i.e. parallel execution of jobs. In-Memory processing is performed algorithmically. In addition, it is a possibility to use Oracle an In-Memory option if applicable.		
NF. 6	The solution shall ensure a high level of stability and operational performance. In this regard, the solution shall have effective mechanisms for handling errors, in order to avoid data loss, system-wide blocking processes, system failure etc.	Mandatory
The error handing is implemented using internal Oracle mechanisms that ensure proper error processing (integrity constraints, tirggers, oracle transactions).		
NF. 7	The application architecture must ensure the integrity and accuracy of the data when data are being accessed and modified simultaneously by multiple entities (users, internal processes, external applications), with notification of user.	Mandatory
We have worked a lot on the concepts of the transaction mechanism - "all or nothing" in case of a failure. If there are several levels, then the principle is observed that after a failure, the processing continues from the moment of a successfully completed processing phase.		
NF. 8	The solution shall have the ability to be timely adapted to the new business needs. It is very important that this will be possible only through parameterization and configuration adjustments in the applications (versus changes in code), thus minimizing adjustment costs supported by the IPS.	Mandatory
At the database level this is provided by reference manuals, additional parameterization (BEFORE_EXECUTE, AFTER_EXECUTE), also the system has a lot of templates for business entities, accounts, transfers. In addition to that, the system embraces dynamically customizable workflow, product system, and dynamically configurable group access system.		
NF. 9	The solution shall be easy maintainable. In this regard, the solution architecture shall allow implementation of new versions delivered by the software provider without affecting the architecture of existing customizations, components implemented by the NBM and interfaces with other external applications.	Mandatory

- The IPS is fully compatible with the suppliers' software (Oracle). The IPS' compatibility with the supplier's software releases is determined in the course of the IPS software development and support. The IPS releases have their own lifecycle and rules set out by the IPS software developer and aligned with the Bank alongside with the contractual obligations. The software developer supports a minimum of two IPS versions. Prior to the release of the IPS version, there are distinguished those supplier's software versions that the IPS operates smoothly with, then the version is fully tested, and, besides, the support of the supplier's software is evaluated in terms of whether it does not interfere with the IPS version support terms. This process is repeated with each IPS version release.
- Improvement and enhancement of the process of the IPS version installation is one of the most important objectives set to the IPS. Therefore, the process is reviewed annually, the problem areas are identified, and the development work is carried out. Similarly, not only the IPS version installation procedure, but also the process of updates' installation is constantly being developed and improved in order to fully automate the entire course of the release transfer and installation.
- There are some Oracle limitations related to compilation of PL/SQL objects. Small patches do not affect the user experience, however, during the version release, 2-4 hours of downtime might be necessary. Nonetheless, this would be covered by stand-in solution.

As software vendors, we provide APIs available to client (external) systems that are isolated in separate Oracle DB schemes, and for whose backward compatibility and stability we are fully responsible.

NF. 10	The solution will be based on web interfaces, shall have user-friendly interfaces, be simple and intuitive in use.	Mandatory
One of the most important phases of our design process is the work of the team of our analysts, when the experts analyse the real user needs, raise the problematic issues, and suggest possible solutions. The result of this process is the application structure, information architecture, and layout of functional components in a simplified prototype and diagrams of actions. In parallel to this process, technical documentation is written. By selecting and arranging the information so that the user would have clear navigation throughout the process of working with the application, we aim at facilitating the implementation of the user tasks.		
NF. 11	The solution shall ensure a very high level of security, taking into account the integrity, confidentiality, availability and non-repudiation concerns regarding the data to deal with, so that control measures provided at the system level is proportional to the risks involved. In this regard, the most important objectives security to be achieved are: a. ensure an adequate level of confidentiality, authenticity, integrity and availability of data during its entire lifecycle and ensure non-repudiation of each single transaction in the system; b. ensure an effective control of logical access and prevent any unauthorized access to its data; c. ensure an effective auditing by monitoring and logging user activities at the system level; d. prevent loss, modification or misuse of information within the system.	Mandatory

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, accounts, interest schemes etc.) and operations (create customer, view customer, 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.

2. Detailed requirements

2.1. Architecture requirements

NF. 12	NBM opts for an open and modular architecture, based on pre-integrated components. These principles must be visible at all levels of the architecture of application that is part of the offered solution.	Mandatory

At the DB level, modules are separate schemes. The set of schemes depends on the client delivery set.
At the level of external applications, this is a set of different applications or a set of FCG (connection gate) modules.

NF. 13	The architecture of the solution will be service-oriented (SOA).	Mandatory

As for the core, it is in the DB; this is a modular system designed to work in a secure environment and provide high-speed service to many users. It is a fast client server.
SOA is ensured through services and external applications that are built around the database for the necessary integration and communication. There are queue servers via which messages are sent and processed, micro-services, and other SOA attributes.

NF. 14	The architecture of application will be client-server type, organized in at least 3 vertical layers, clearly divided so that each higher level will depend only on its lower level.	Mandatory

For the user interface:

1. GUI application.
2. REST API.
3. IPS integration layer (DAO).
4. IPS Kernel.

For integrations:

1. An external cascade (External Forbis Connection Gate).
2. An internal cascade (Internal Forbis Connection Gate).
3. IPS integration layer (DAO).

IPS Kernel.

NF. 15	Communication between all application components will be done in a secure manner, using for this purpose of the internal interfaces of the application components.	Mandatory

On external networks, inside we work via http having in mind that this is an isolated access network and there is no connection between hosts via ASCL.
As an alternative, the mechanism of Oracle HTTPS operation with the entire middle tier might be considered for development.

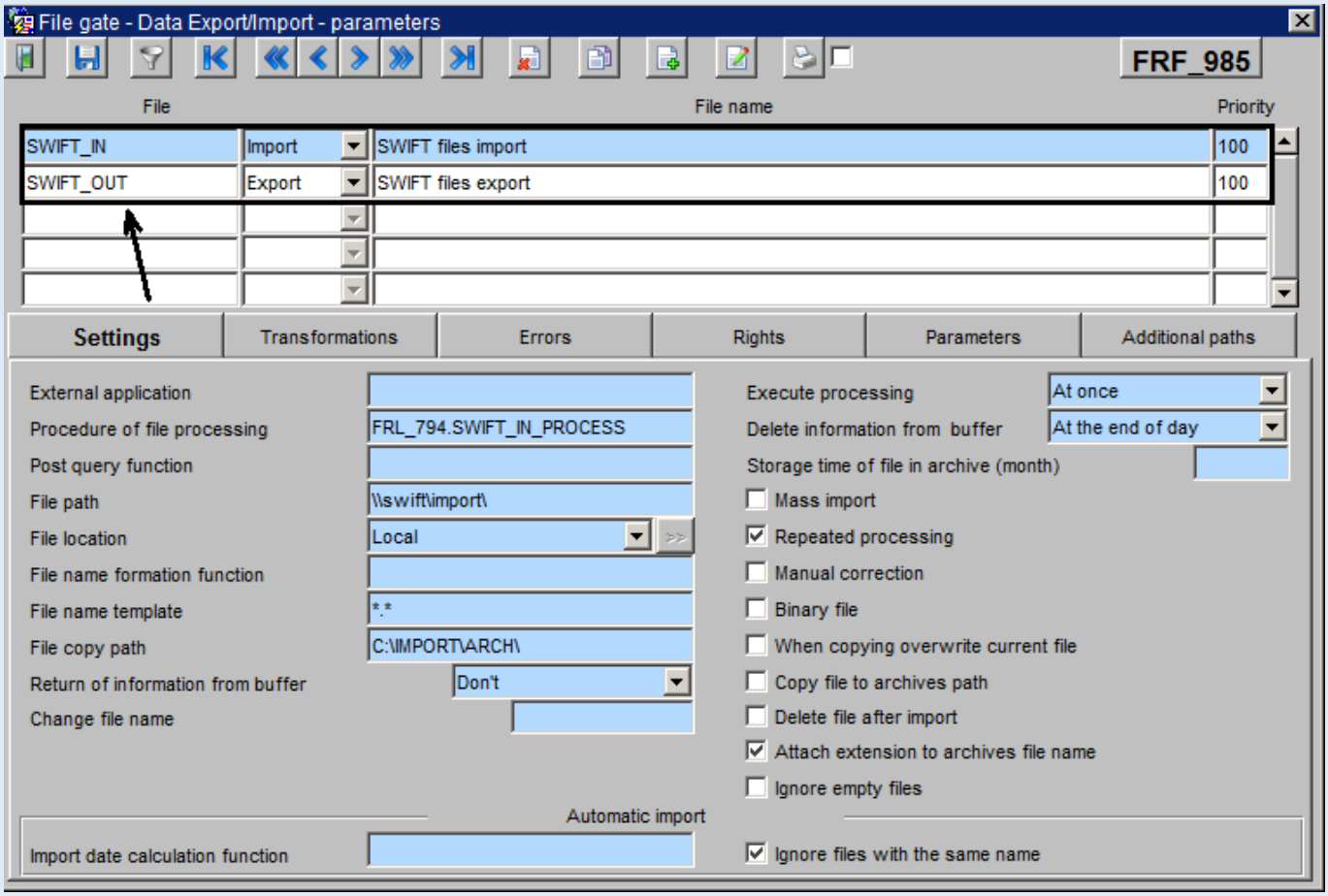
2.2. Requirements for interoperability

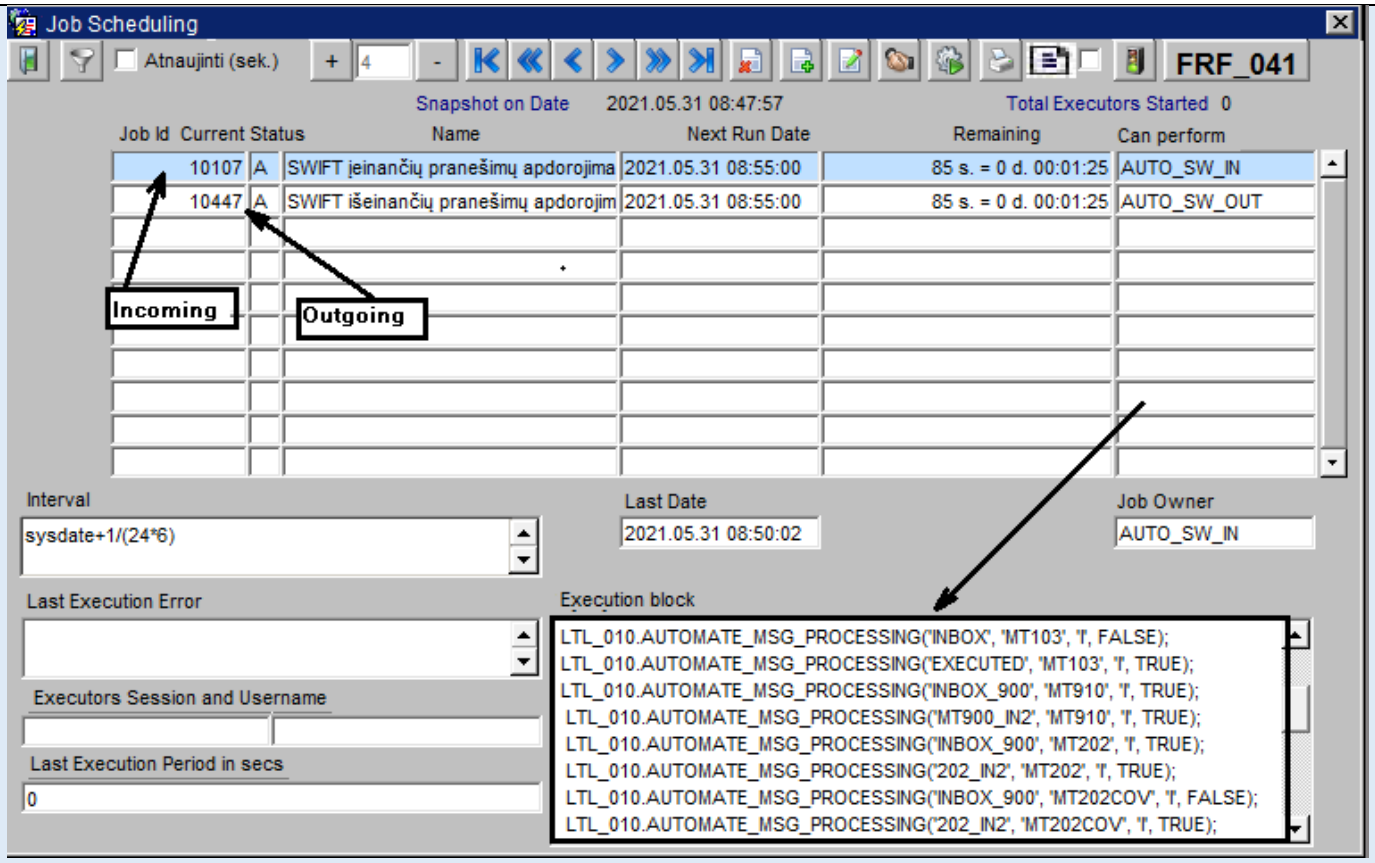
NF. 16	The IPS must have native integration capabilities which will easily allow the integration with different systems. *In the project scope will be included the integration with the AIPS (RTGS module) system installed at NBM, via online messaging interfaces. There will be also available the option to integrate with other IT systems of the NBM, via web services and XML file formats.*	Mandatory

The payments are XML messages, often signed with an electronic signature, and they move according to different payment system standards.

NF. 17	Interaction based on Web-services must be available as an integration capability in IPS. *List of interfaces available and integration approach must be specified by Vendor.*	Mandatory
We work over HTTP/HTTPS, SFTP, SMTP, SMPP, JMX. The rest are possible as well.		
NF. 18	The IPS must be capable to interact with external systems via SWIFT network. *Vendor is requested to:* • *Explain how proposed solution is connected to SWIFT network* • *Provide full list of SWIFT protocols and services supported by proposed solution*	Recommended

The IPS supports MT messages MT012, MT019, MT100, MT101, MT102, MT103, MT191, MT192, MT195, MT196, MT199, MT200, MT202, MT202COV, MT204, MT299, MT300, MT320, MT360, MT535, MT700, MT900, MT910, MT920, MT940, MT942, MT950, MT970, MT999 files import and export via SFTP or FTP channels. The IPS also supports fully automated SWIFT data processing for the data exchange with SWIFT.





NF. 19	The IPS must support SWIFT MX ISO 20022 messages for interaction with external systems.	Mandatory
Will be available in the end of 2021/in 2022.		
NF. 20	The IPS must be capable to interact with external systems by means of web services via private network.	Mandatory
Organization of a private network using third-party standard network tools, for example APACHE, SOPHOS and the like.		
NF. 21	System must support a set of standard interfaces with Participants and other systems. *Vendor must provide full list of standard interfaces being a part of the proposal.*	Mandatory

- 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 WEBSPHERE (the stand at the client).

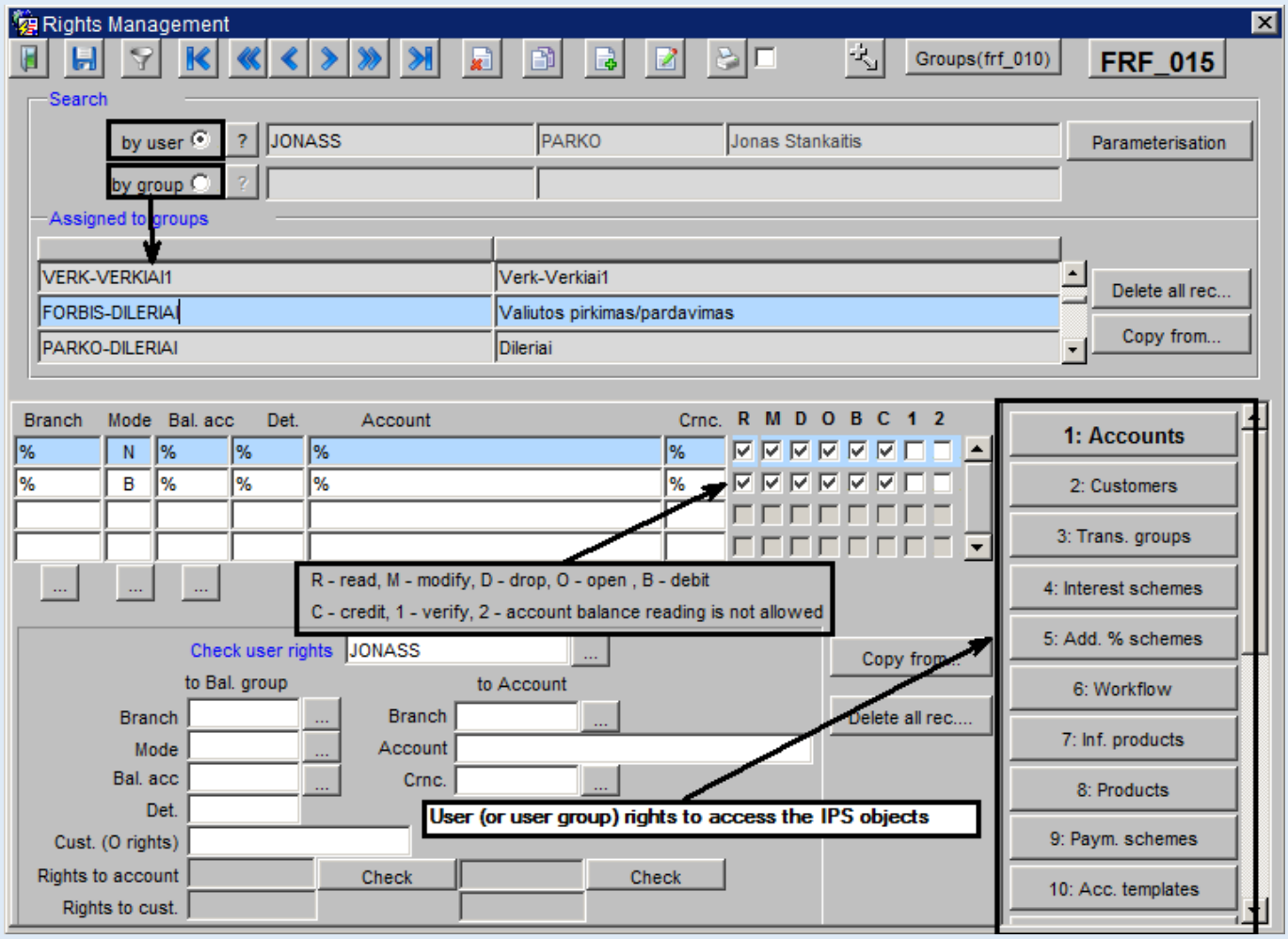
UDP operation via ISO-8583 gateway.

2.3. Requirements for flexibility

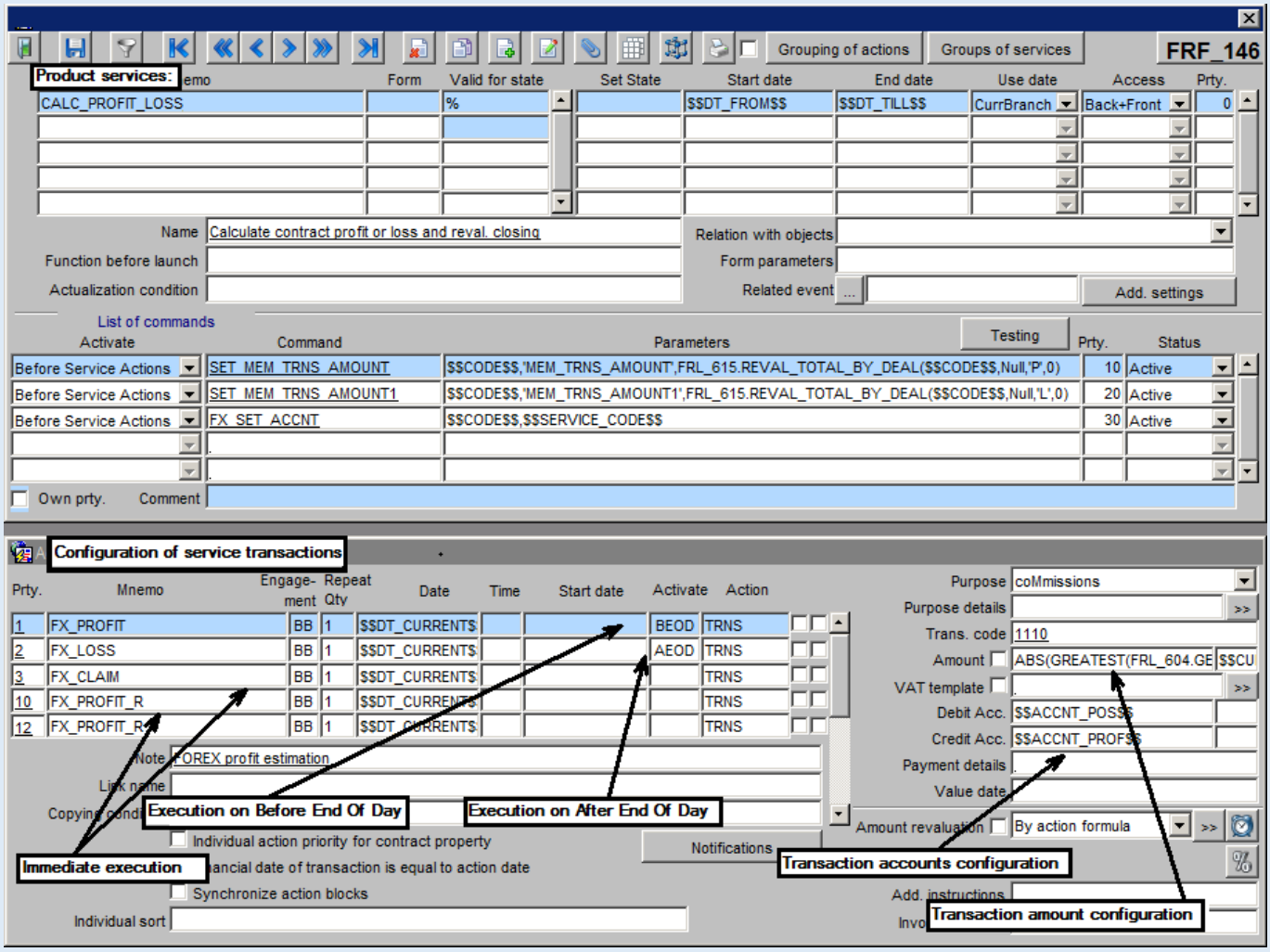
NF. 22	The solution shall allow at least the following user configurable operations: a. define/customize business rules; b. define/customize automated actions based on different events, time schedule; c. define new business workflows, or customize the existing ones; d. define new reports, based on customizable templates.	Mandatory

As needed, the IPS allows the user to configure/create:

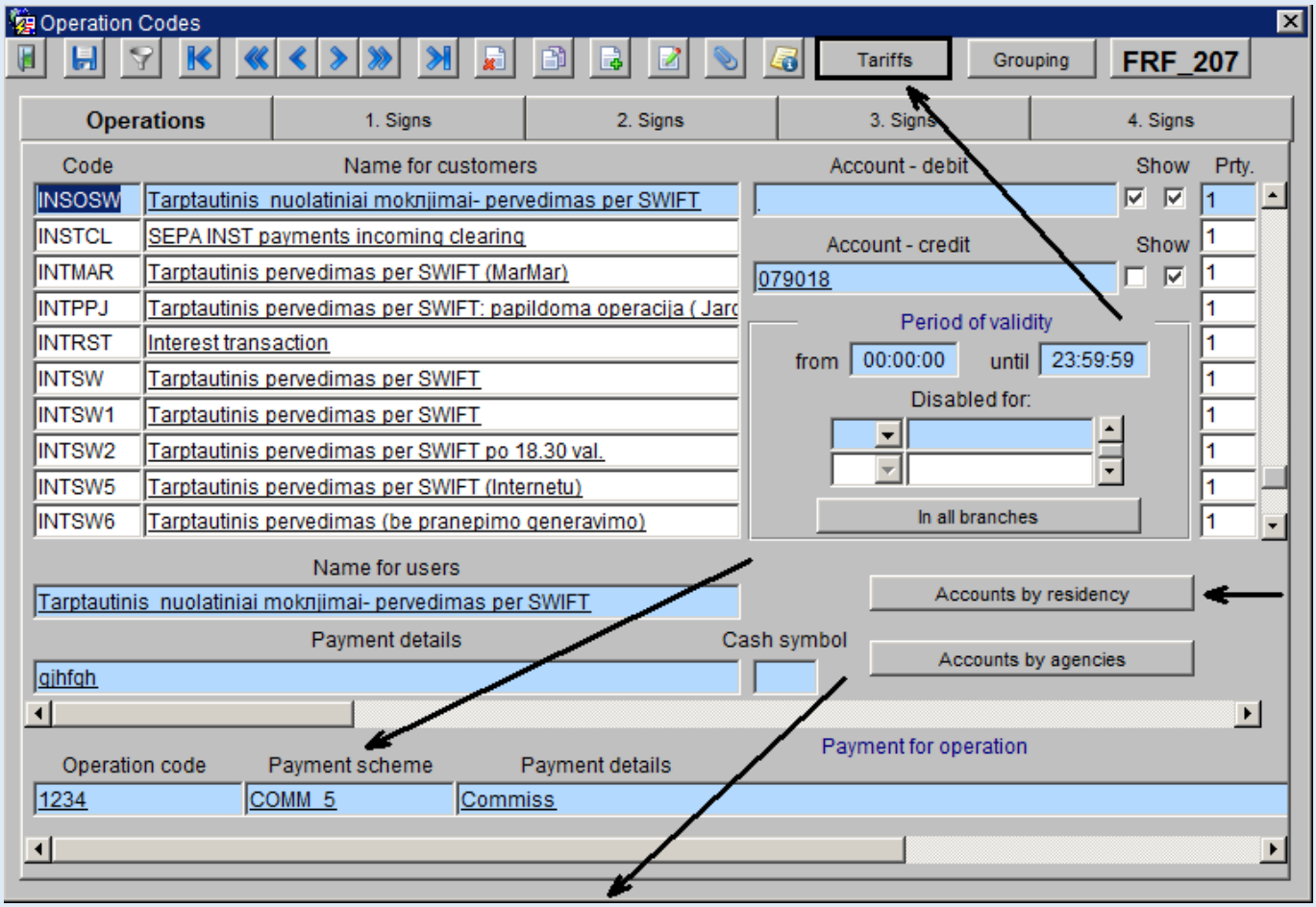
- User access rules to IPS objects:

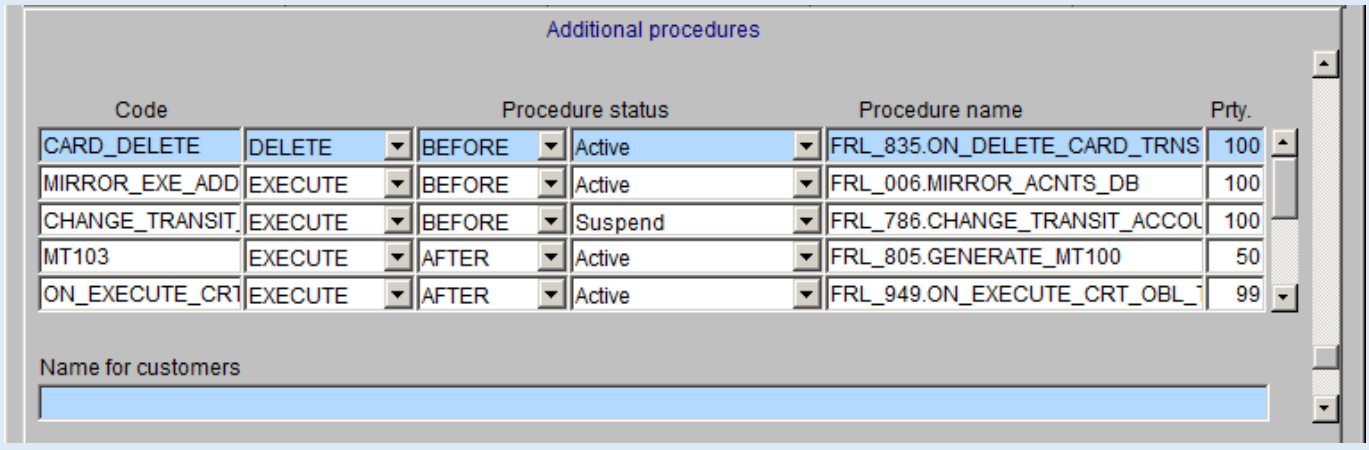


- Banking products (to perform actions with them, to configure payments according to the product business rules):

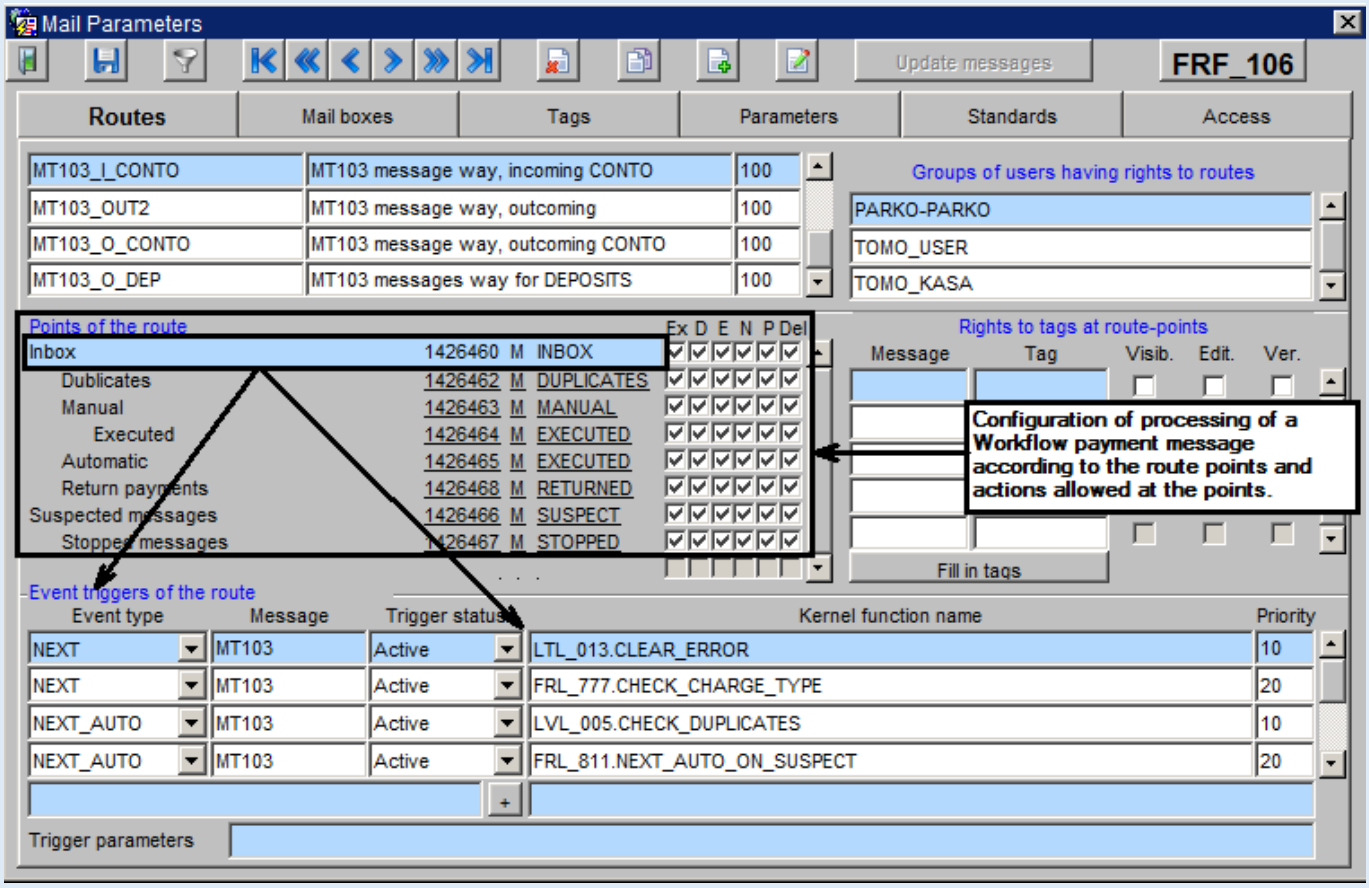


- Financial transactions' execution actions:

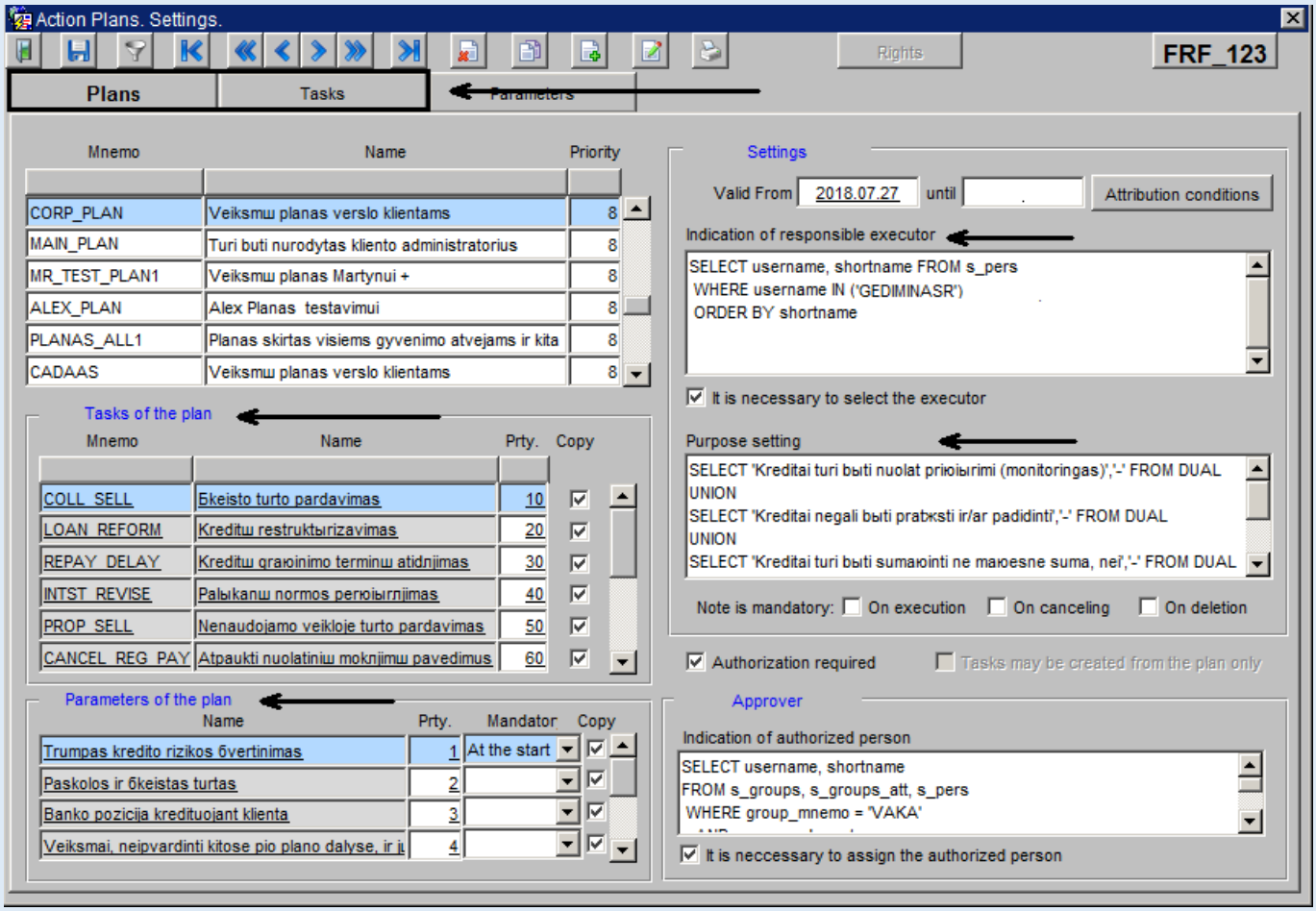




- Payment processing actions according to the Bank's internal requirements and the payment system's requirements:

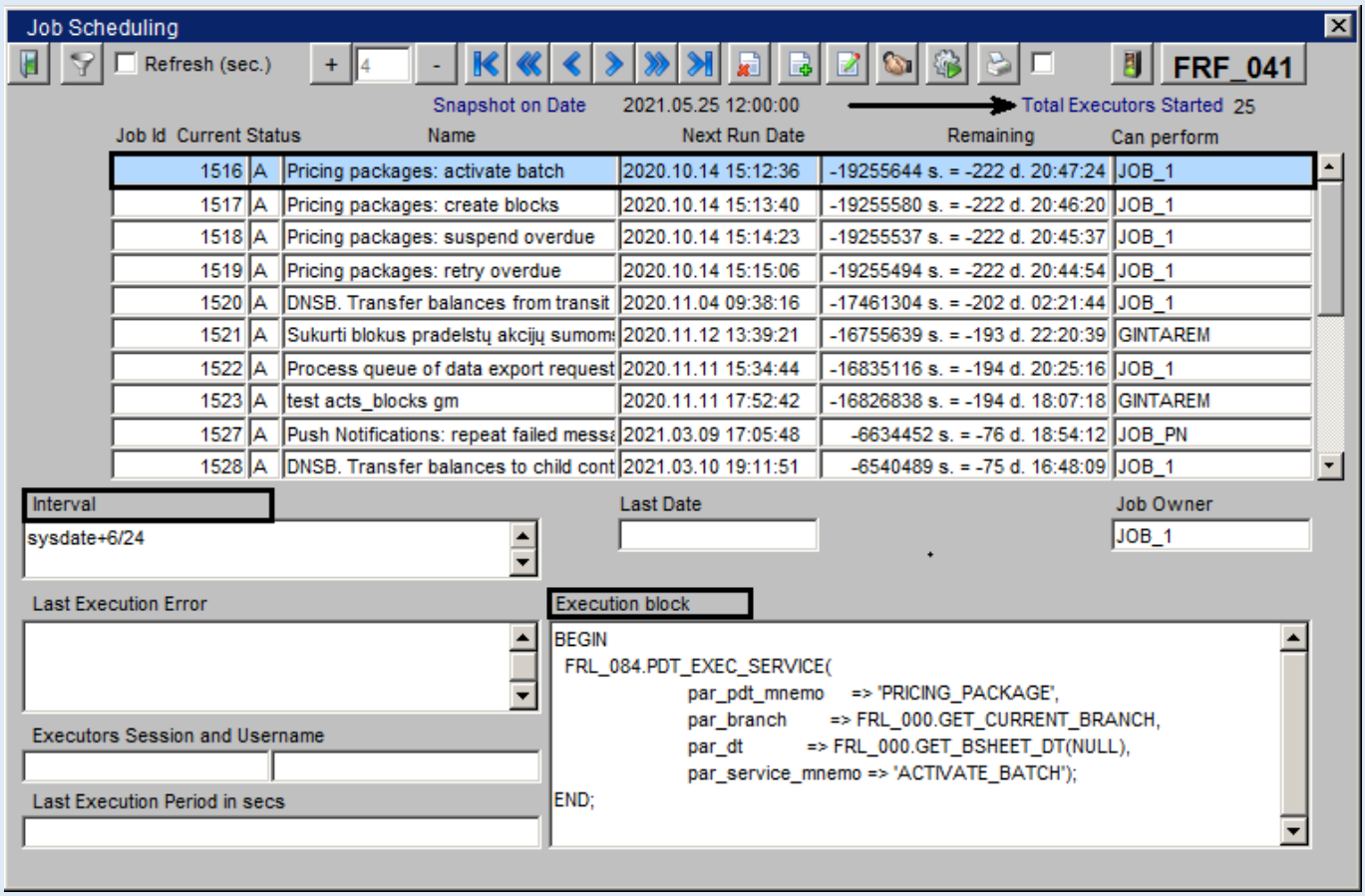


- Internal tasks' management processes:



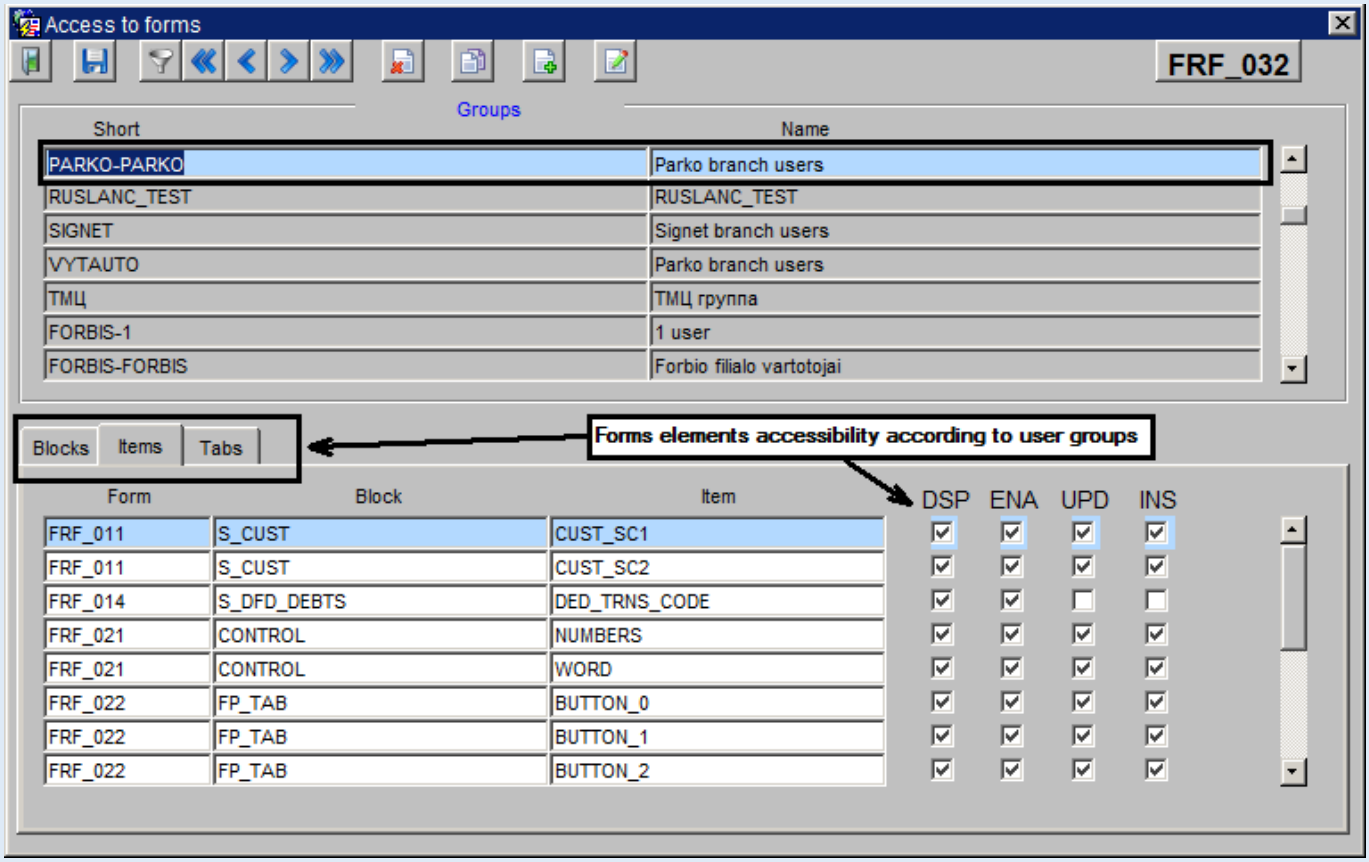
- Processes of report creation and connecting them to the required GUIs:
  - MSO documents' reports by the required template.
  - Reports in the PDF, EXCEL, XML, TXT, and CSF formats.

- Customer notification processes.
- Execution of the system's jobs:

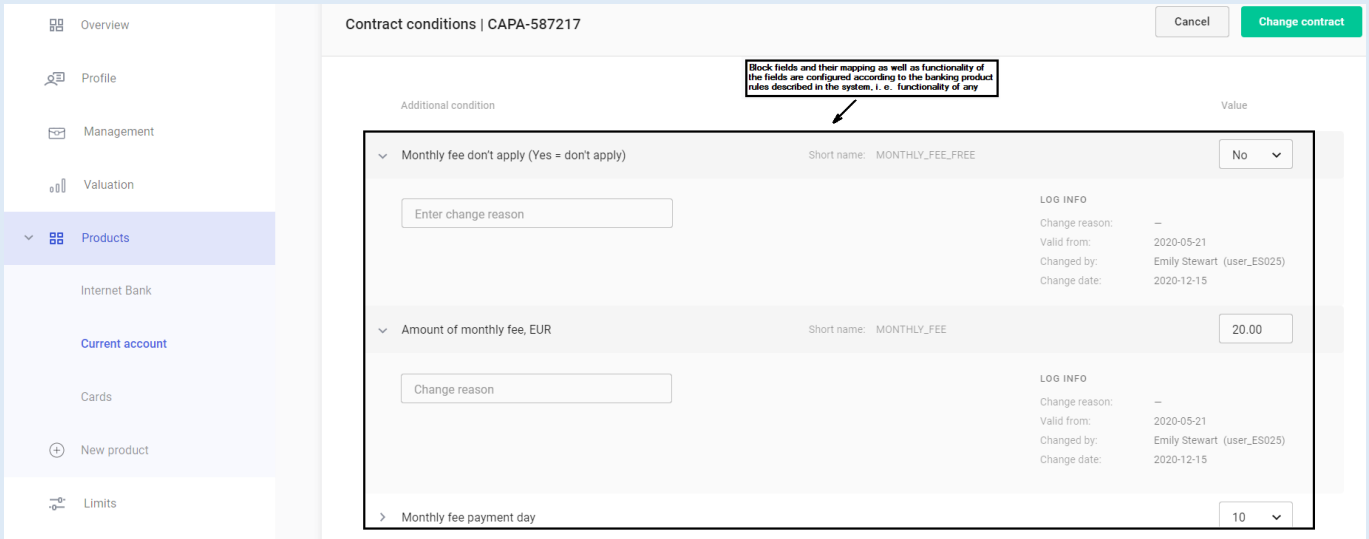


NF. 23	The application will allow to customize views and user forms. The application will allow to create new user forms for accessing the business logic of the application.	Mandatory

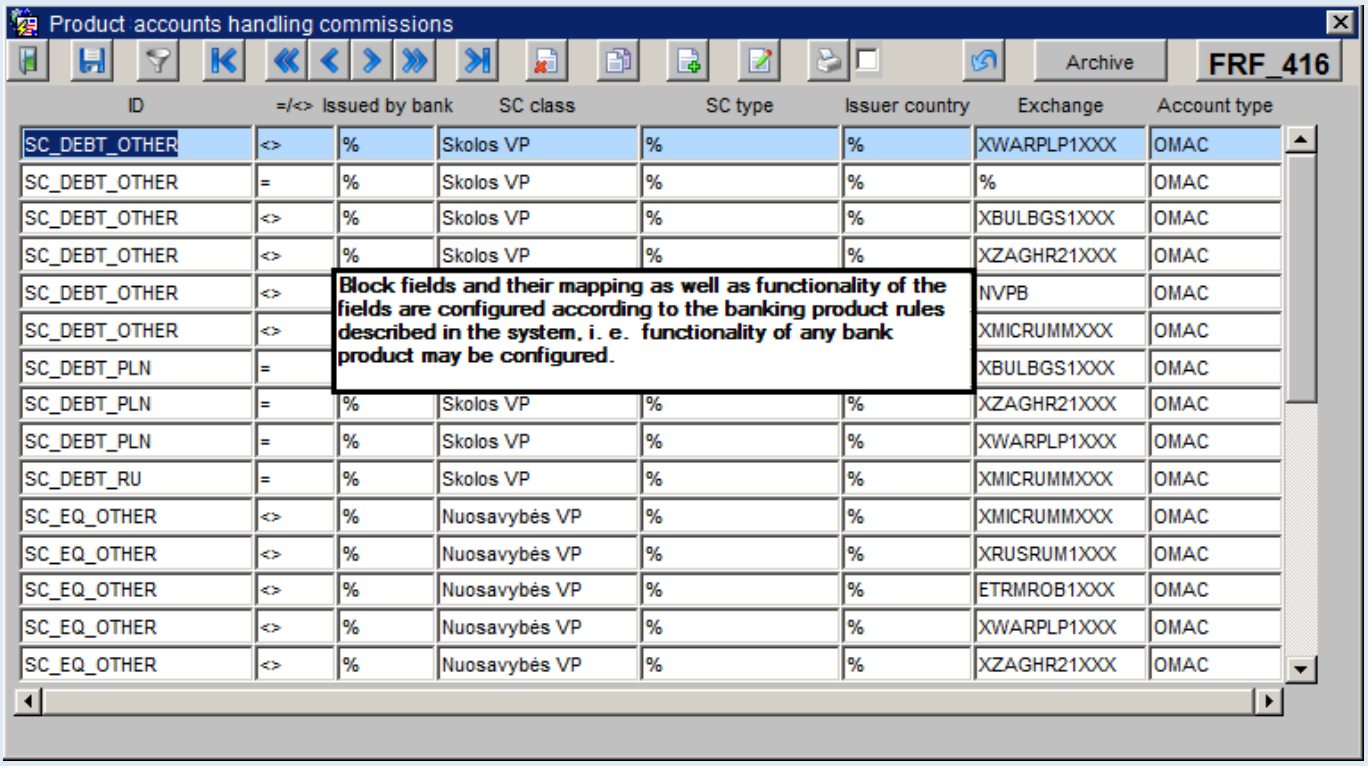
- A possibility to customize access to all elements of the IPS forms according to the user rights:



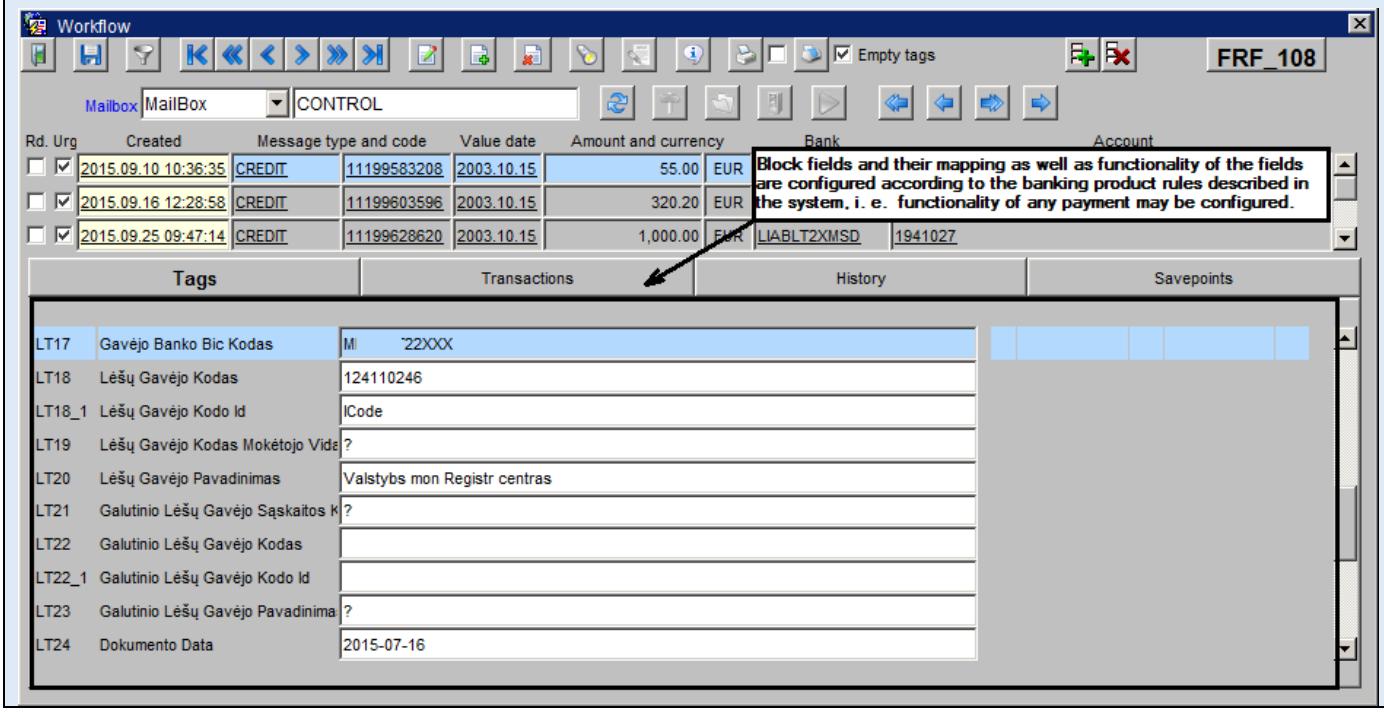
- A possibility to create a screen for servicing of the IPS banking products according to the business requirements:



- A possibility to create a form for handling the datasets of the IPS banking products:



- A possibility to set the initial default values of all the IPS form's fields, and to differentiate them by the user.
- A possibility to customize the form of management of the accounts of the IPS banking products by the business requirements.
- A possibility to customize the form of the fees of the IPS banking products by the business requirements.
- A possibility to customize the forms of servicing and viewing of the IPS payments:

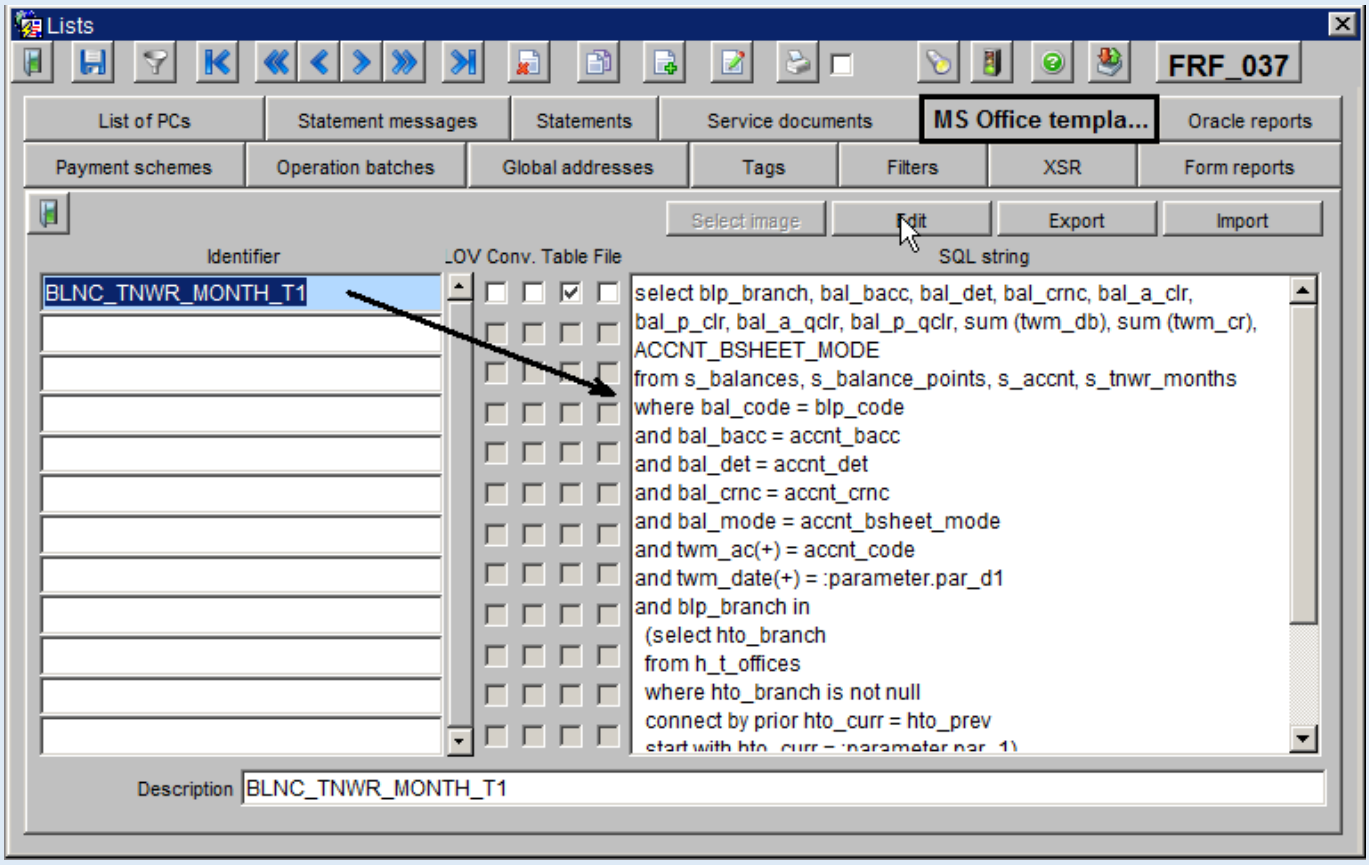


NF. 24	The application will allow customizing existing reports (e.g. adjust data set, formatting).	Mandatory

The IPS allows creating new or customizing the existing reports:

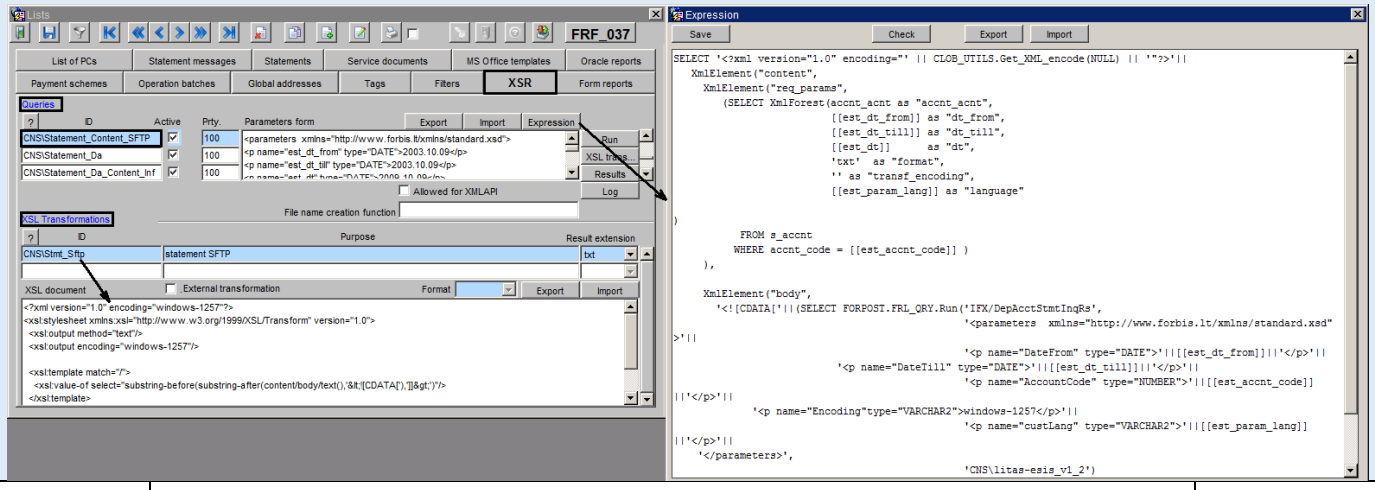
- Microsoft Office reports

Available reports; source for customization:



- XSR reports

Available reports; source for customization:

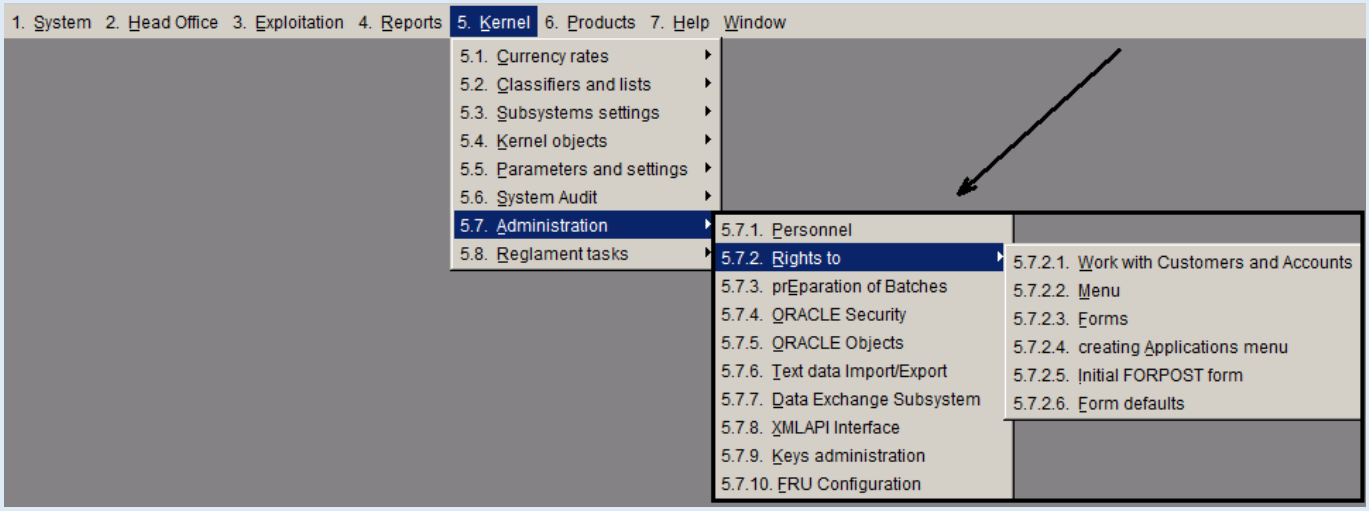


NF. 25	The application will allow the definition and management of normative reference information used within the application. The data source for reference information may be internal or external (e.g. external database, external web service, external file).	Mandatory

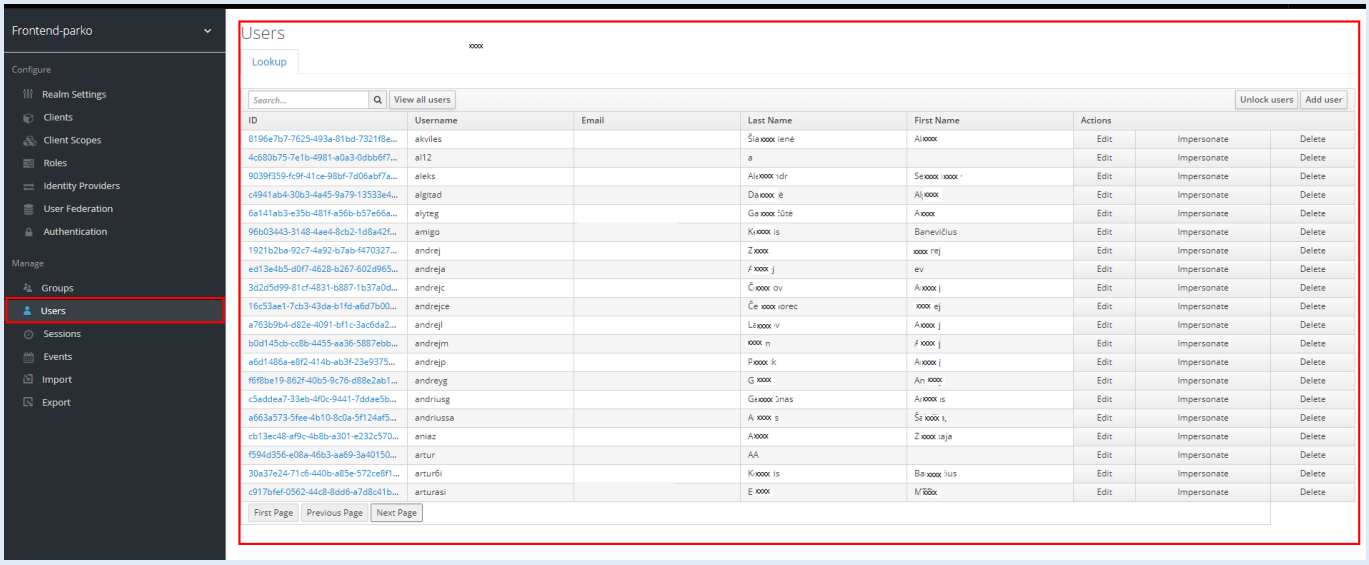
Yes, reference manuals and parameterization are in the IPS database, we adhere to the principle of data centralization in one DB.

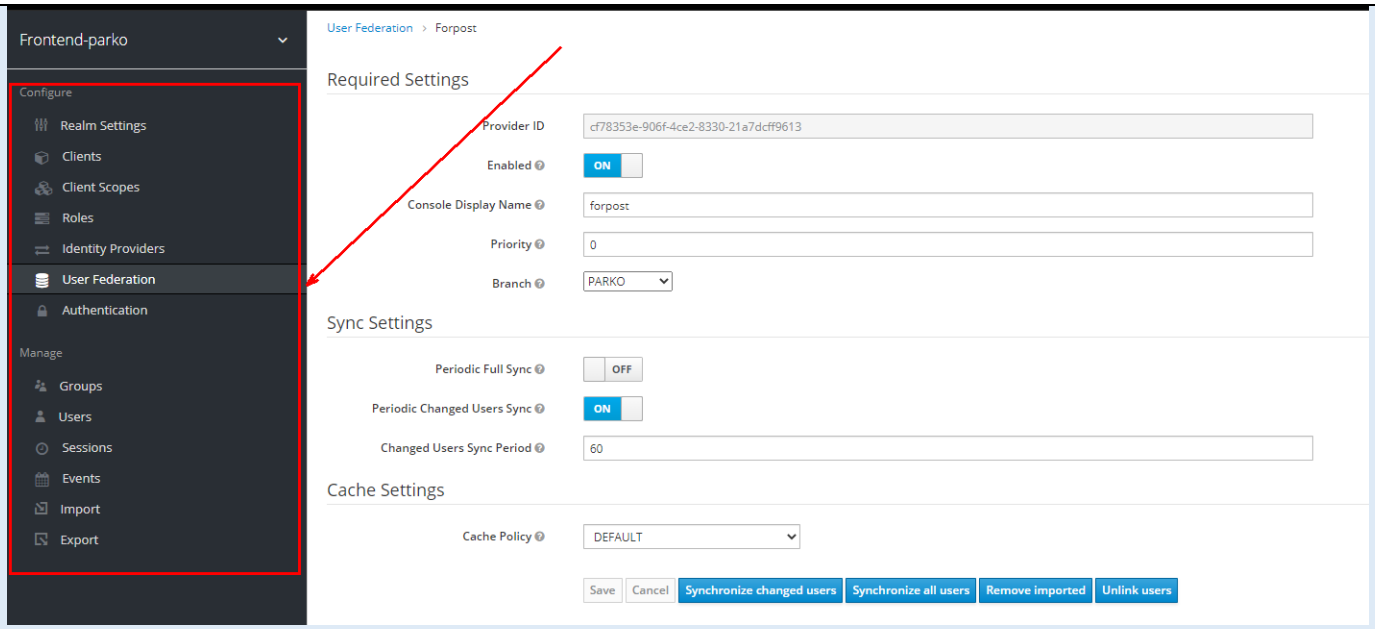
NF. 26	The solution must provide friendly GUI interfaces for administrators to allow the customization/configuration activities, where most operations can be performed by click and drag-and-drop.	Mandatory

- A separate IPS MENU item with the clearly divided main system administration functions:

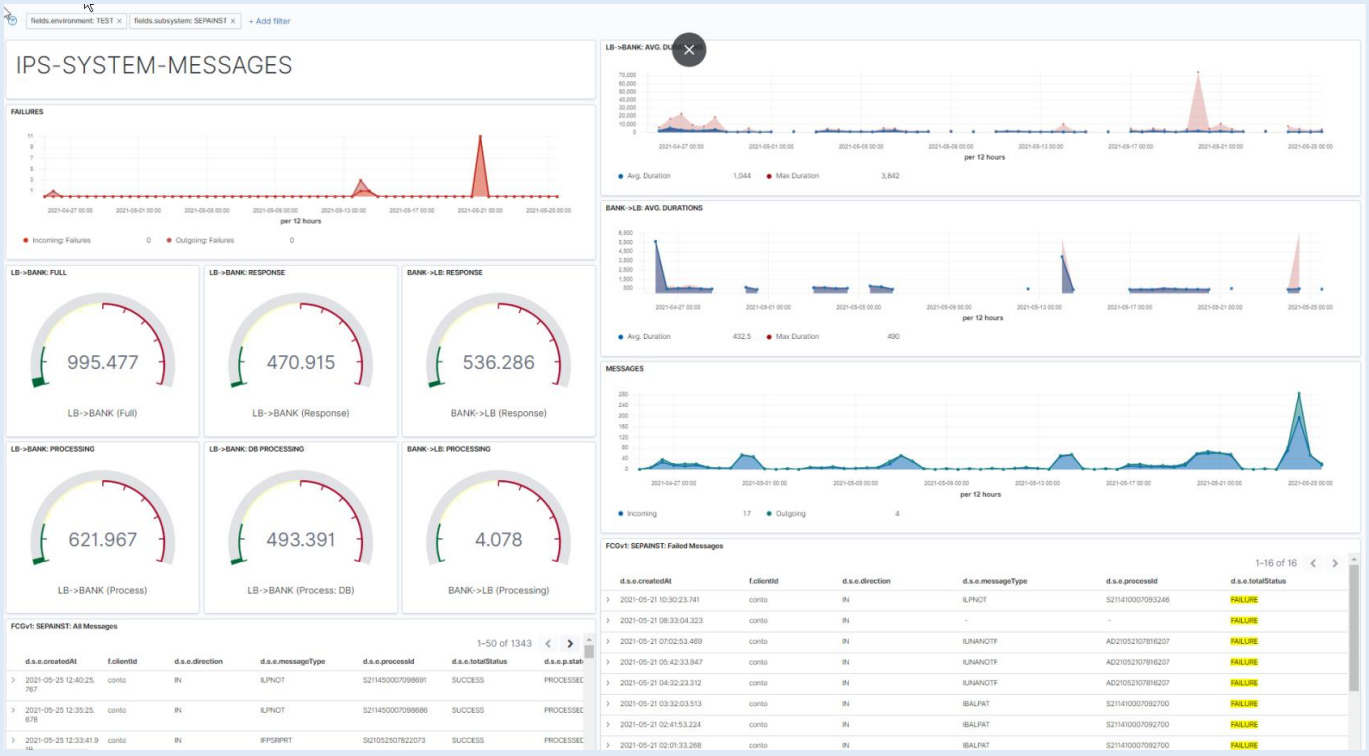


- Authentication and management of the system users, employing the functionality of the Keycloak authorisations' server:

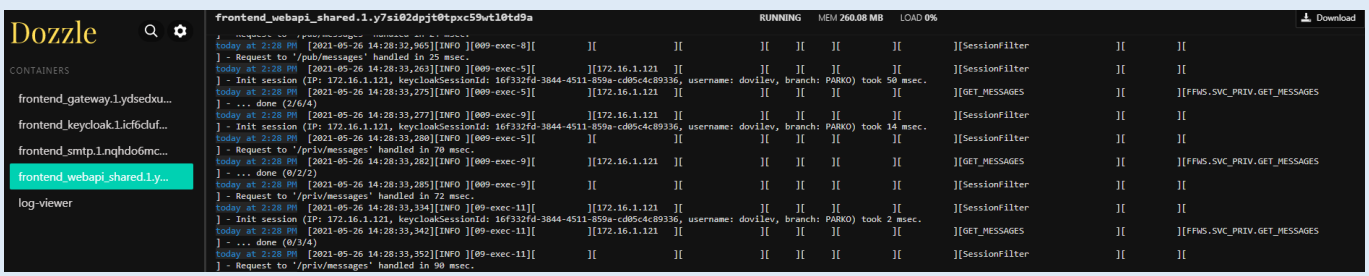




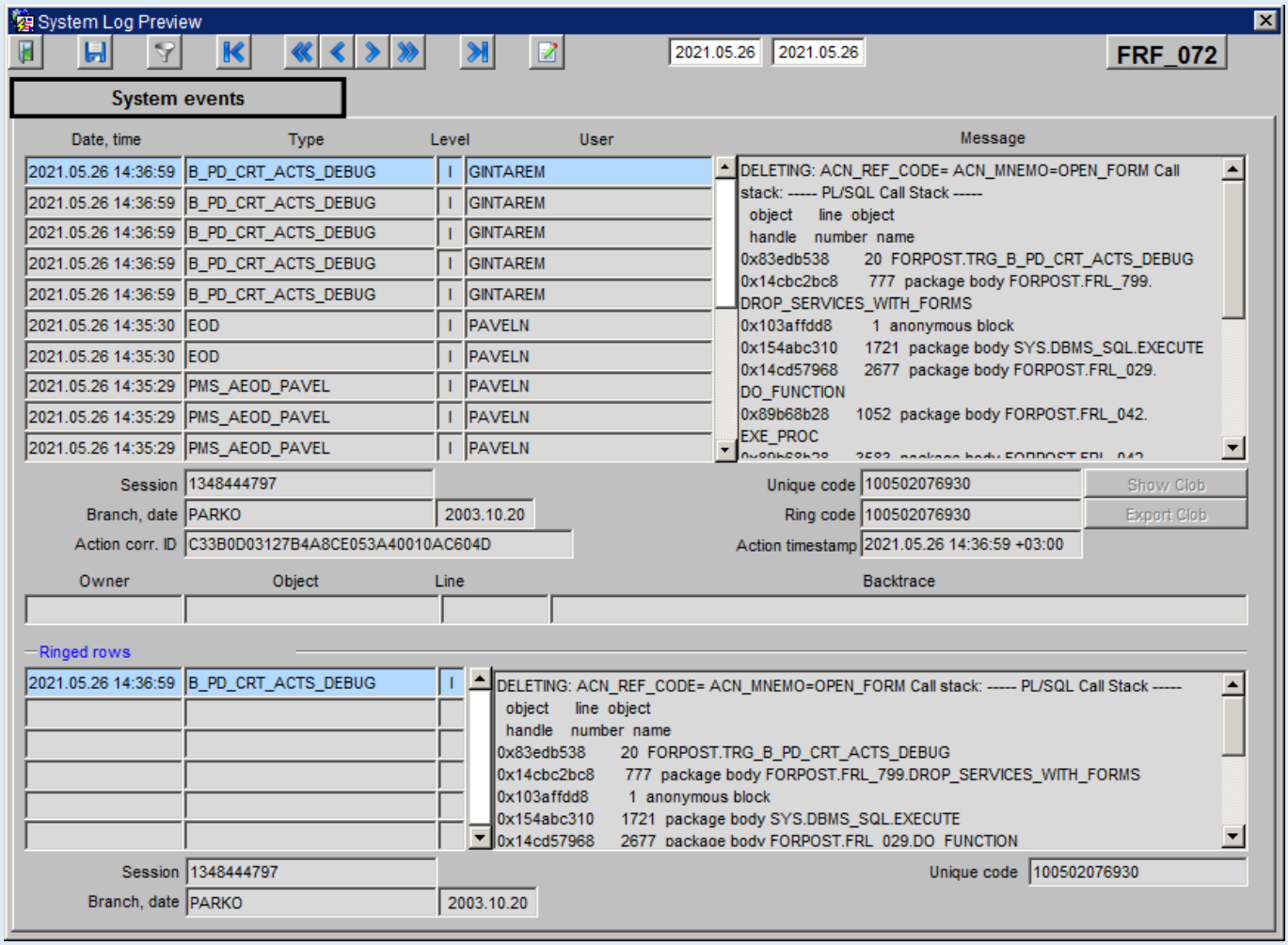
- Broad selection of the monitoring tools with the possibility to customize the screens in accordance with the required information.
  - Monitoring of the data exchange with the external system:



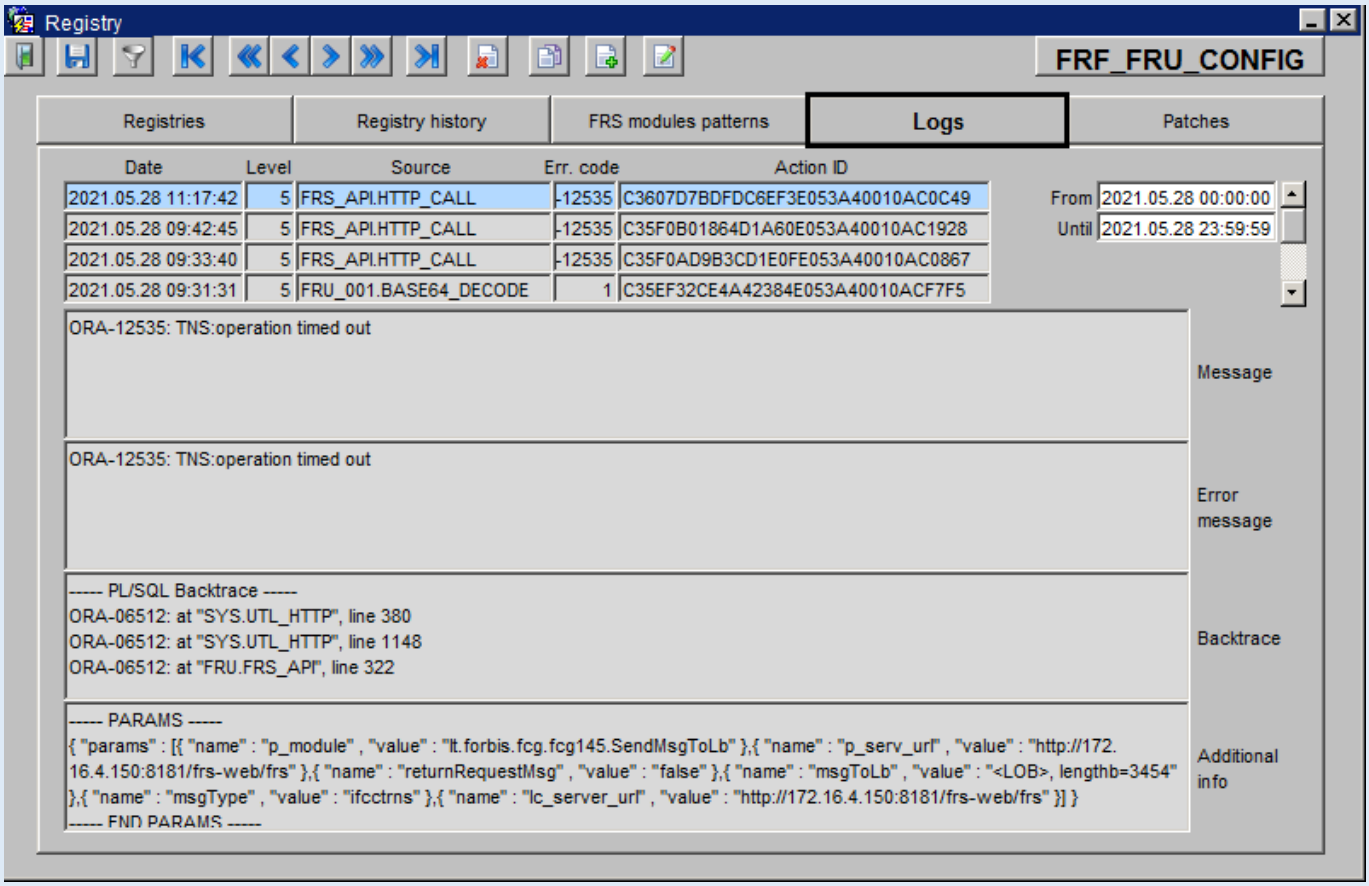
  - Docker containers logs:



- IPS kernel logs:

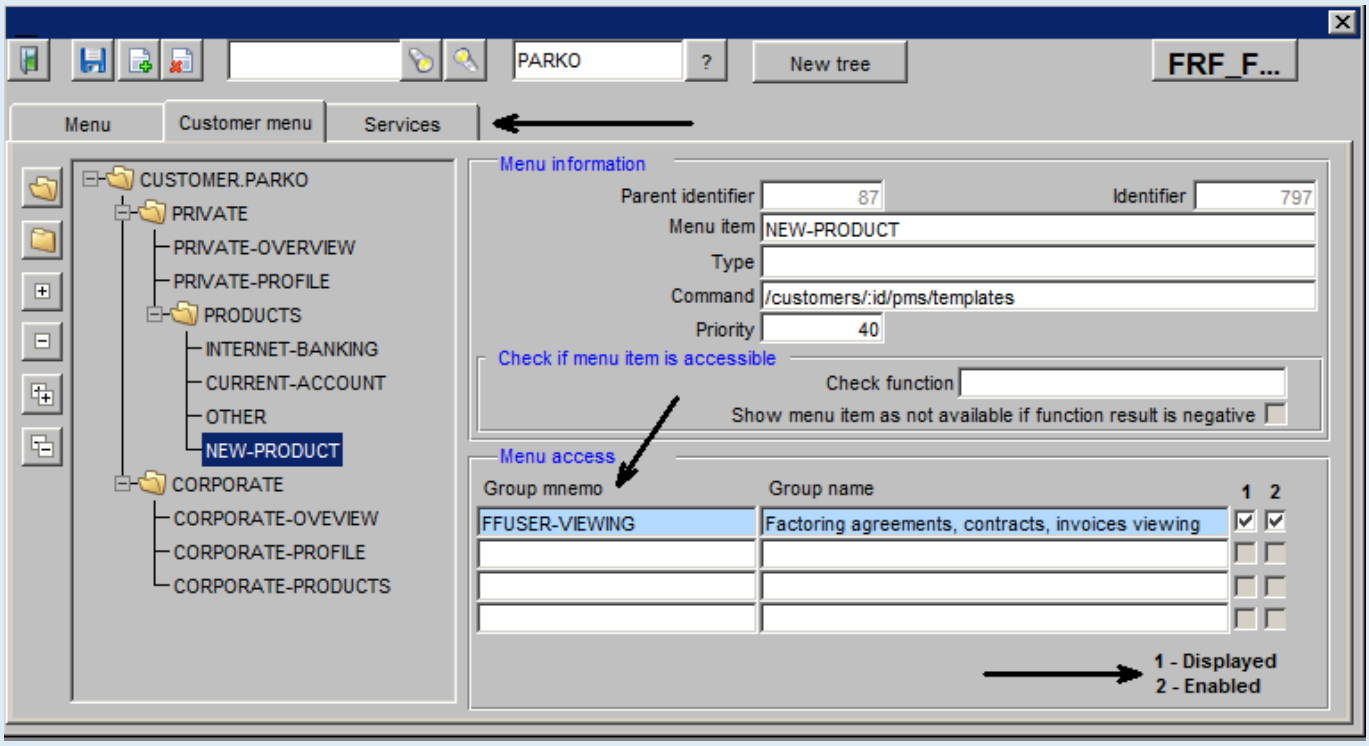


- Logs of data exchange (DB layer) with external systems:



NF. 27	The application will allow the definition and customization of external interfaces of the application (e.g. setting available business function, setting the format of input/output data, setting communication protocols, access control settings, etc.).	Recommended
API functions can be enabled and disabled. If there are more than one input/output formats, the communication protocol is available – it is possible to configure, which one is to be used. IP whitelists are used to limit the accessibility.		

From the GUI part, the IPS has a possibility to manage the user's available services and interface elements by user groups, or additionally, by custom function:



2.4. Requirements for usability

NF. 28	All business functions available to users of application must be accessible through web interfaces.	Mandatory

The IPS is based on:

- Oracle web FORMS for back-end.

JAVA SCRIPT-based Web interface for other applications. Once the Keycloak server has authorized/authenticated the users, they will be redirected to our front-end application (FFE), which handles our business functions by the given user roles/grants.

NF. 29	All user interfaces must be in English language. *It is recommended the user interfaces to be available also in Romanian language*.	Mandatory

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

NF. 30	Application will have user-friendly interfaces that are intuitive and convenient to use for business users and users with administrative roles.	Mandatory

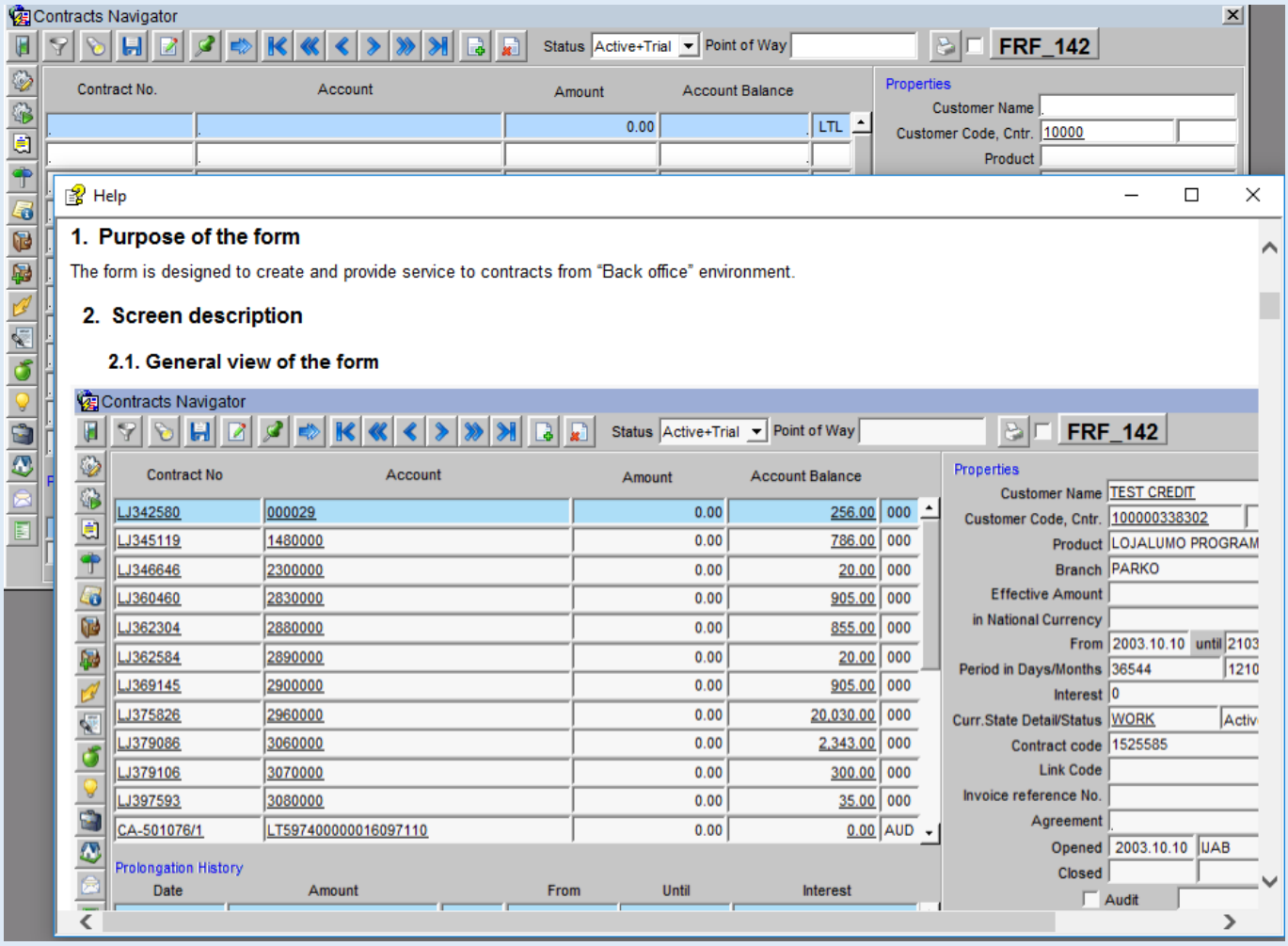
The IPS GUI solutions have been developed under a design concept, the implementation of which is based on the Google Material design system.

Therefore, at creating the design solutions that meet our needs, we can save up time and focus on the functional part.

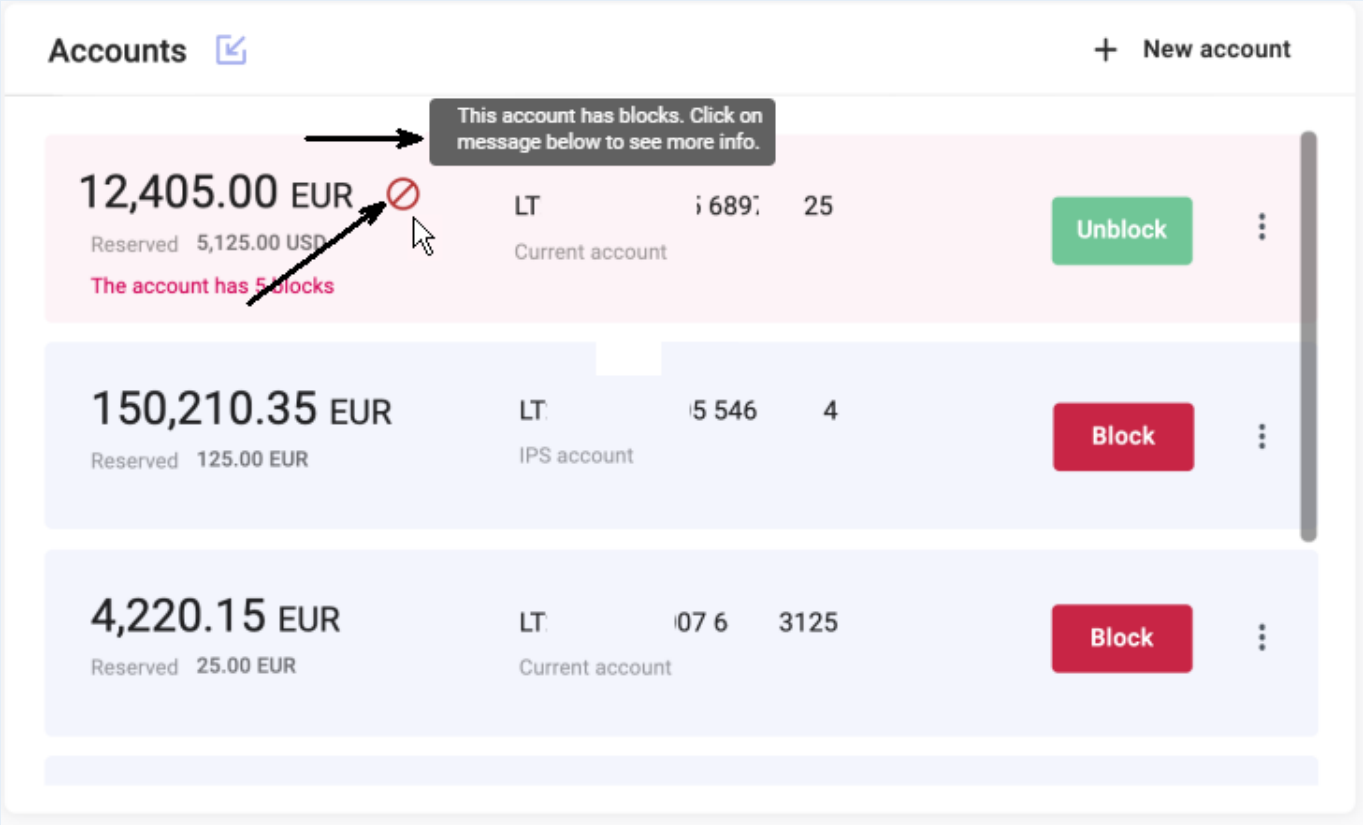
Although the template base is available, the majority of the design components are developed according to individual needs, for specific situations, with regard to the role of the user working with a particular solution. This allows offering the system users a user-friendly and intuitive interface.

NF. 31	The system shall be intuitively clear for the users so that it will allow the use of the system with a minimal training.	Mandatory
Being aware of the basic needs of the system user, we have adapted the application so that the user could perform his/her tasks as quickly as possible, and have justified our UI/UX design by qualitative testing. Thus, we managed to avoid negative user experience and improve the usability of the application by employing the solutions based on the user practices.		
NF. 32	Documentation related to the solution shall contain complete guides, detailed and updated for all groups of users.	Mandatory
Yes, it is available. For future developments, it will come as part of deliverables and access to Documentation portal (wiki) will be provided too.		
NF. 33	Users shall have access to context-sensitive help.	Recommended

- The IPS users have access to system descriptions on different levels, depending on the system role assigned to them:
  - User manuals (intended for the client's employees working with the IPS system, accessible in the external application).
  - Administrator guides (intended for the client's administrators who manage the IPS System on the client's side, accessible in the external application).
  - User help files (accessible directly in the IPS system). These are descriptions of the system operation and user interface. For example:

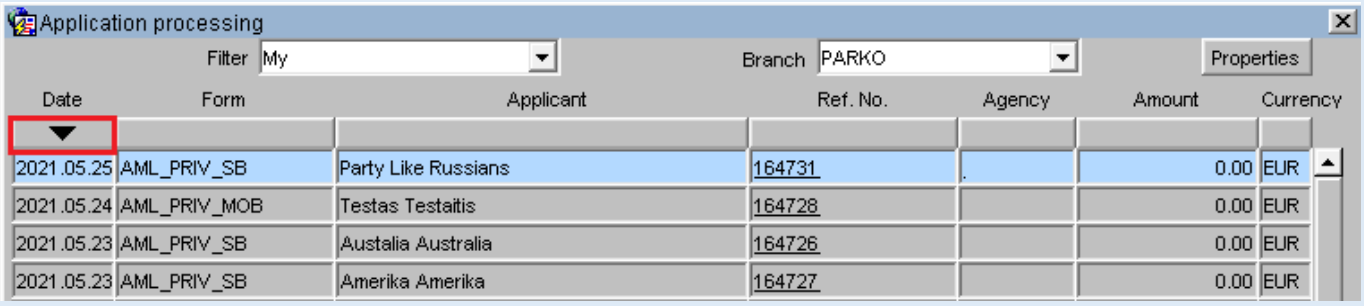


- The front-end application has tooltips which are common user interface elements to display important data or as act as assistants:

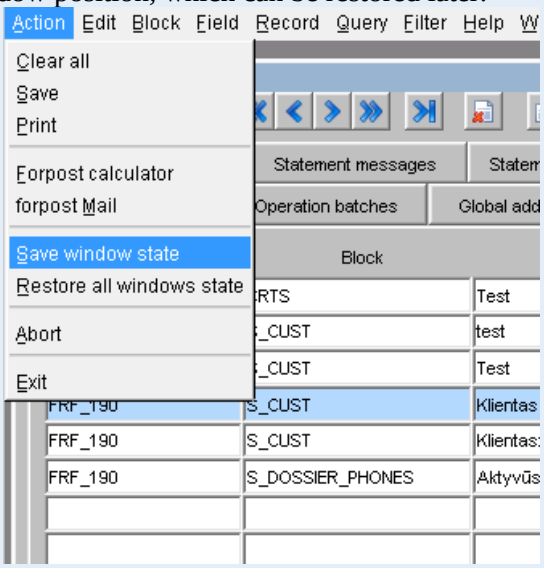


NF. 34	The solution shall allow saving intermediate work and operations initiated by the user (automatically or at user request).	Recommended
Partially, in those places where thereit is enabled. Until it is set, editing is performed in several stages.		
NF. 35	The solution shall allow users to customize its own workspace (e.g., adding menu items to favorites, displaying the latest hits, save searches, save templates, etc.).	Recommended

- The IPS display multi-record blocks, it is allowed to use the user-defined sorting:

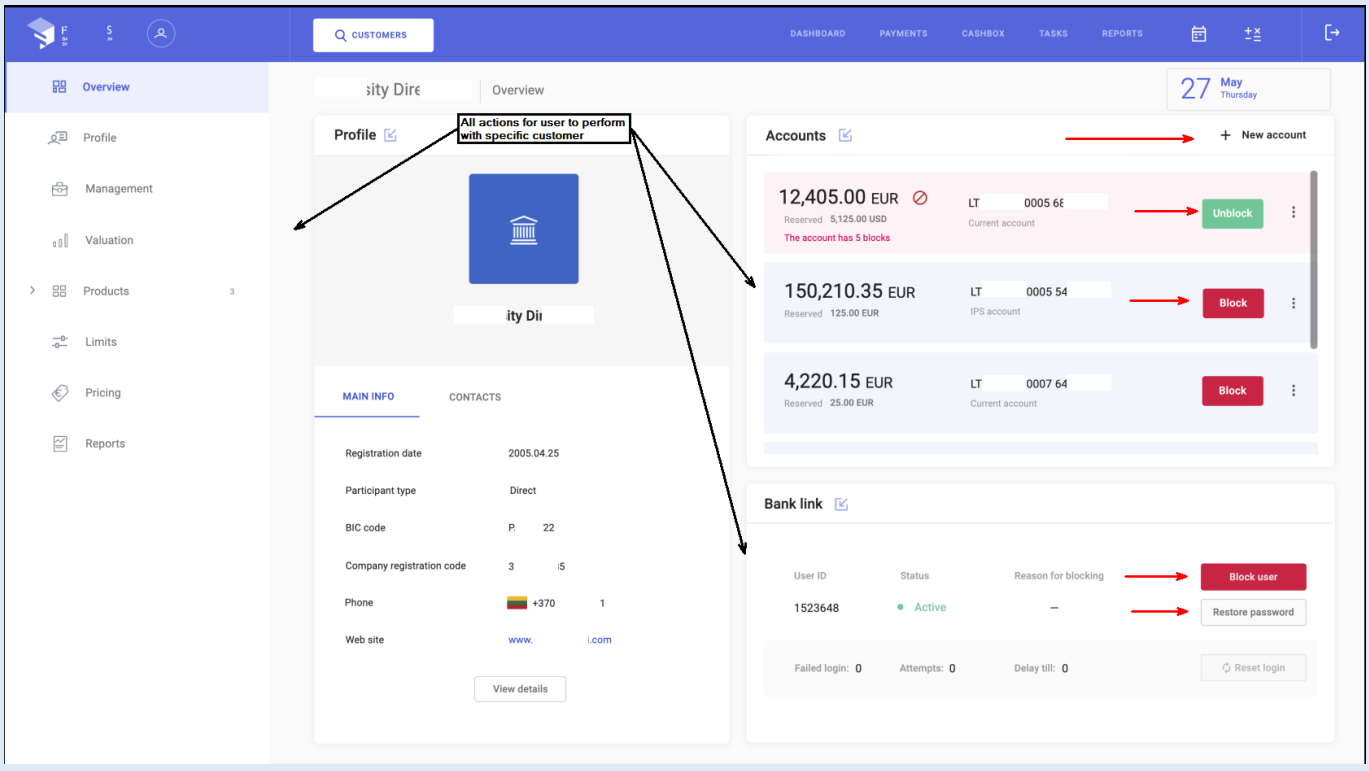


- Users can save/delete their own filters (searches), which later can be applied to the form‘s data. Besides, users can save their preferred window position, which can be restored later:

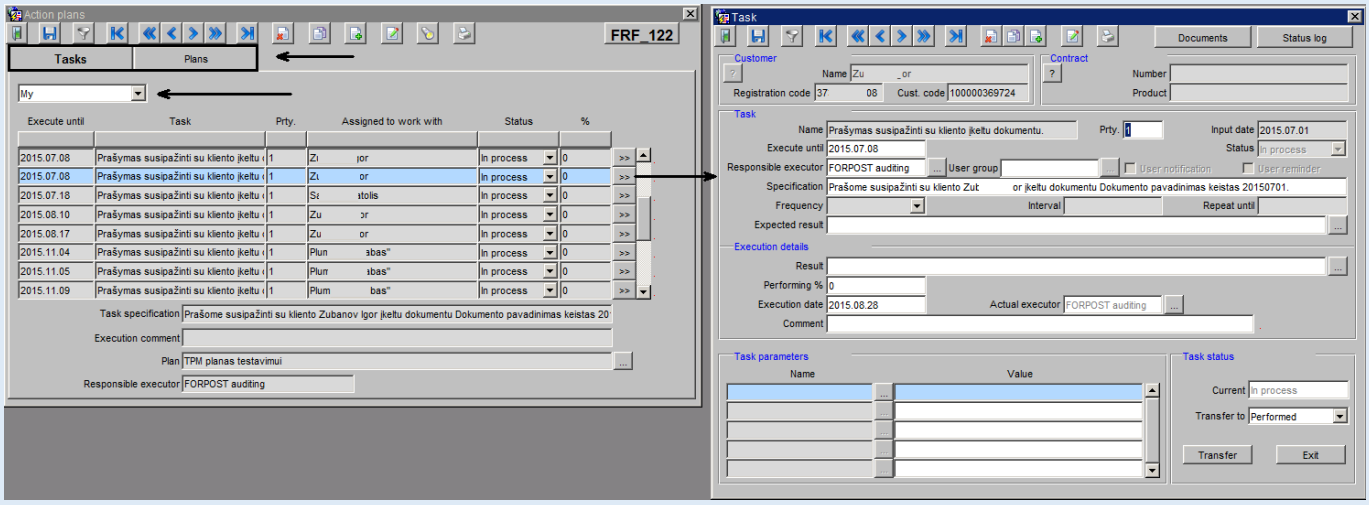


NF. 36	User interfaces shall allow easy navigation through solution forms, by using complementary mechanisms (e.g., mouse and/or keyboard and/or special functions).	Mandatory
Yes, it is so, WEB GUI interface.		
NF. 37	The application must provide a mechanism for centralized displaying (e.g. dashboard) of all actions that user has to perform within the application.	Recommended

- The IPS provides a dashboard with clearly arranged actions to work with the customer:



- A dashboard for centralized user's tasks and plans:



2.5. Requirements for security

2.5.1. Security architecture

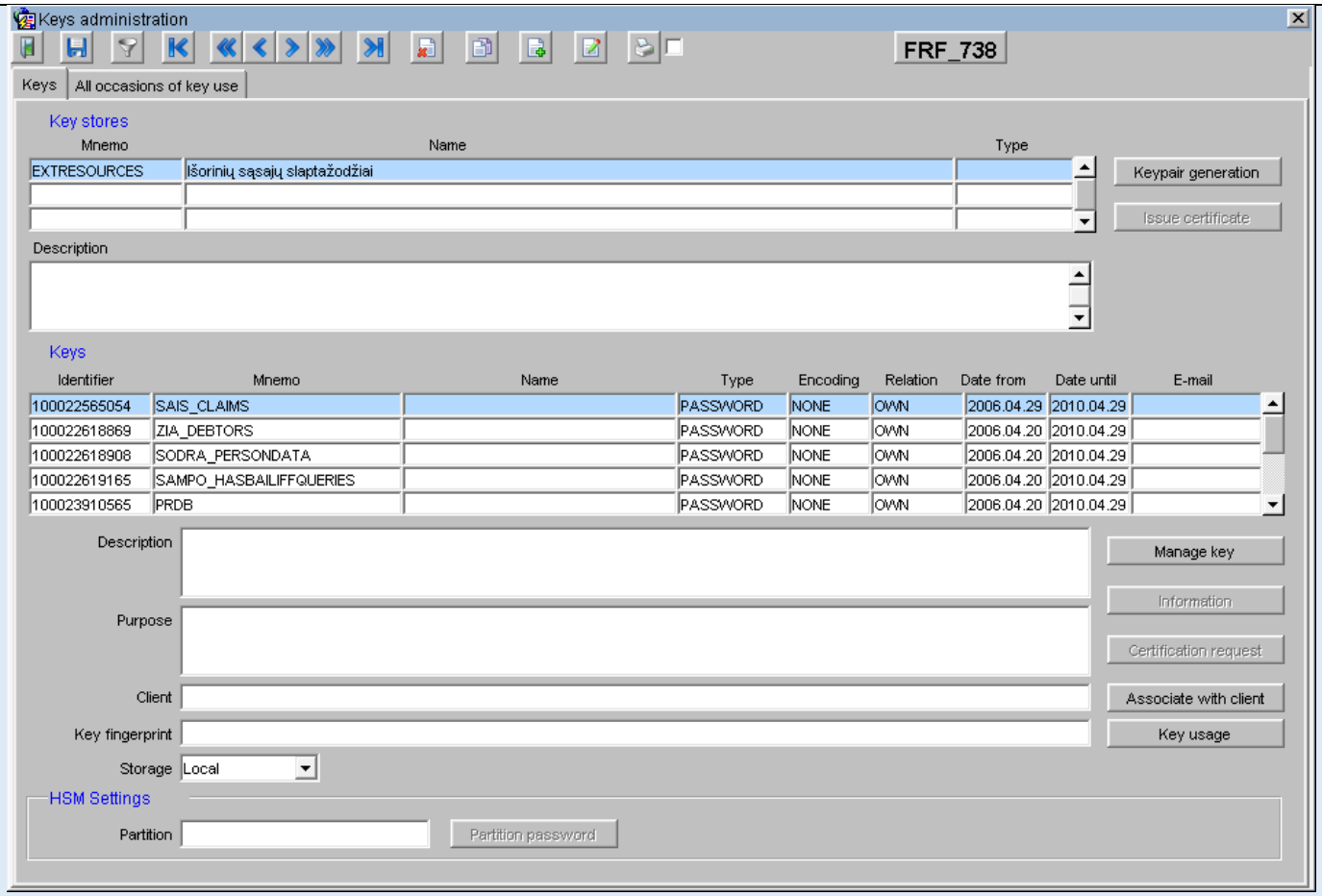
NF. 38	The solution must implement a Multi-layered security approach at the application level and have the ability to integrate into institutional model of NBM (further into institutional model of CSD) for information security management (based on ISO 27000 family of standards).	Mandatory

The system has multi-layered security approach. Inside IPS Core data integrity and confidentiality is ensured by access control:

- Access to the database tables and API is controlled using password-protected database roles.
- Access to specific IPS Core entities (participiants, accounts, etc.) and operations (create participiant, open account, view balance, close account etc) is controlled using IPS Core user groups and object groups.
- Additionally changes of the data can be tracked using customizeable audit mechanism. Audit tables are protected.

NF. 39	All access credentials used by the application shall be configurable in the administrative interface. Applications shall not contain hardcoded credentials for access.	Mandatory

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.



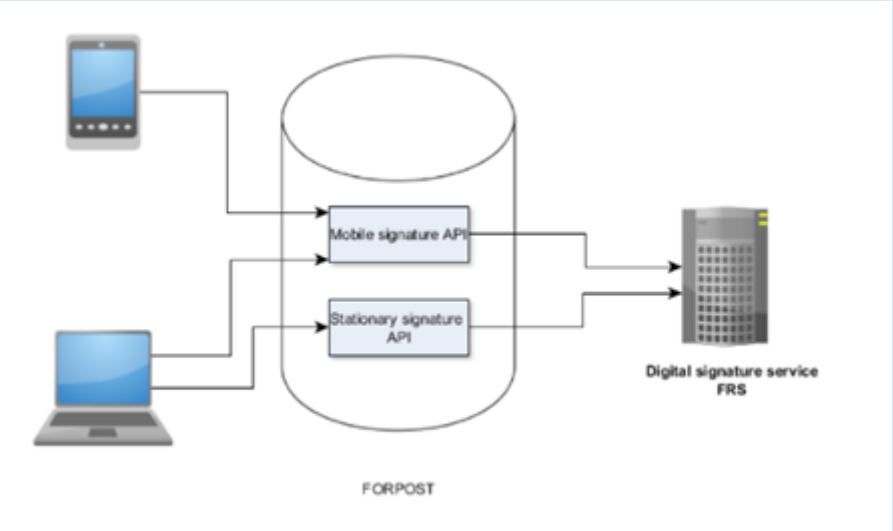
NF. 40	None of the solution components shall contain stored access credentials in open form (in databases, configuration files).	Mandatory
None of the user passwords are stored as a plain text in the database or other external applications that are configured on the server; the sensitive information is encrypted.		
NF. 41	All solution related system processes shall run with minimum privileges needed to execute the tasks assigned.	Mandatory
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.		
NF. 42	All external interfaces of application will be accessed by using secure authentication methods (e.g. X.509 certificate-based authentication).	Mandatory
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.		
NF. 43	The solution will be able to encrypt sensible data stored in the database.	Recommended
By means of Oracle Advanced Security Option, Transparent database Encryption, or by our developed means.		

2.5.2. Authentication

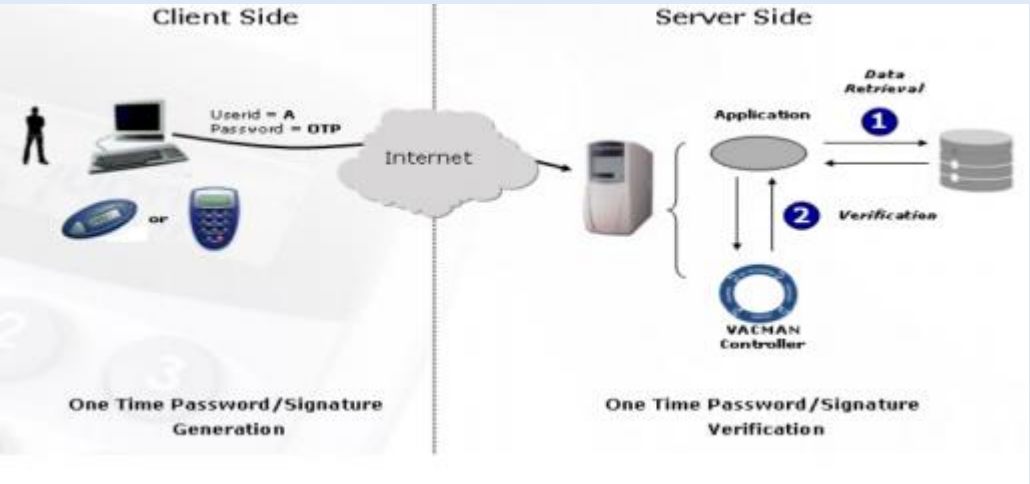
NF. 44	Application will permit registration of users and their profile information (e.g. ID, password, first name, surname, email, etc.).	Mandatory
Keycloak allows additional logins flows (optional user self-registration, recover password, verify email, require password update, etc.), adding other fields to login, registration flows.		
NF. 45	Application should support strong authentication mechanisms, including two factor authentication. *Vendor will describe all supported mechanisms for user authentication.*	Mandatory

- Authentication and authorisation is performed via the authorisation server.
- Authentication is performed by the username and password alongside with the acknowledged third-party secure devices:

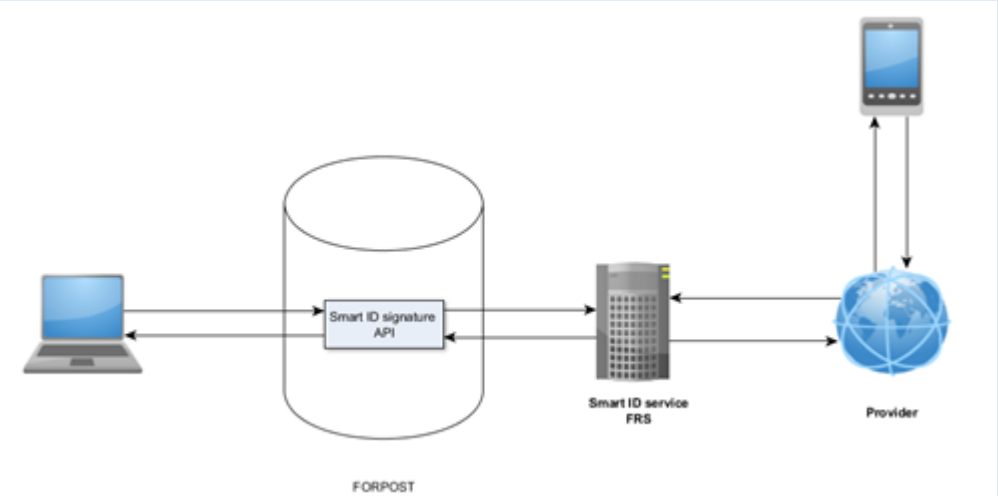
Mobile signature/stationary signature:

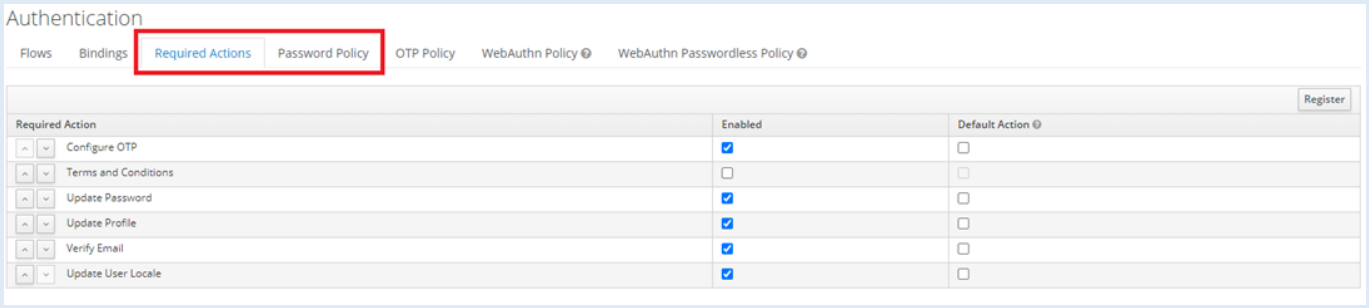


Vasco Digipass:

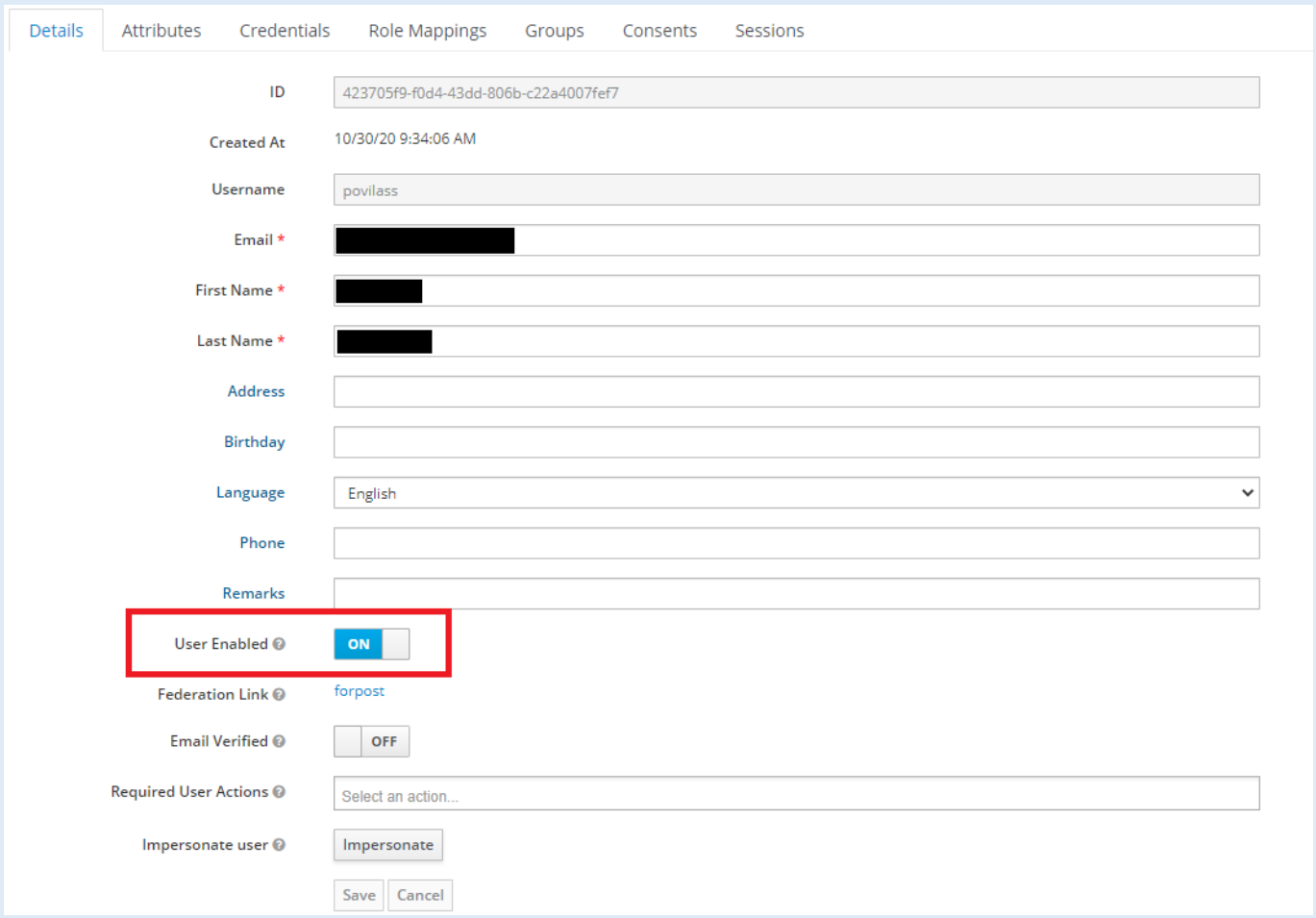


Smart ID:



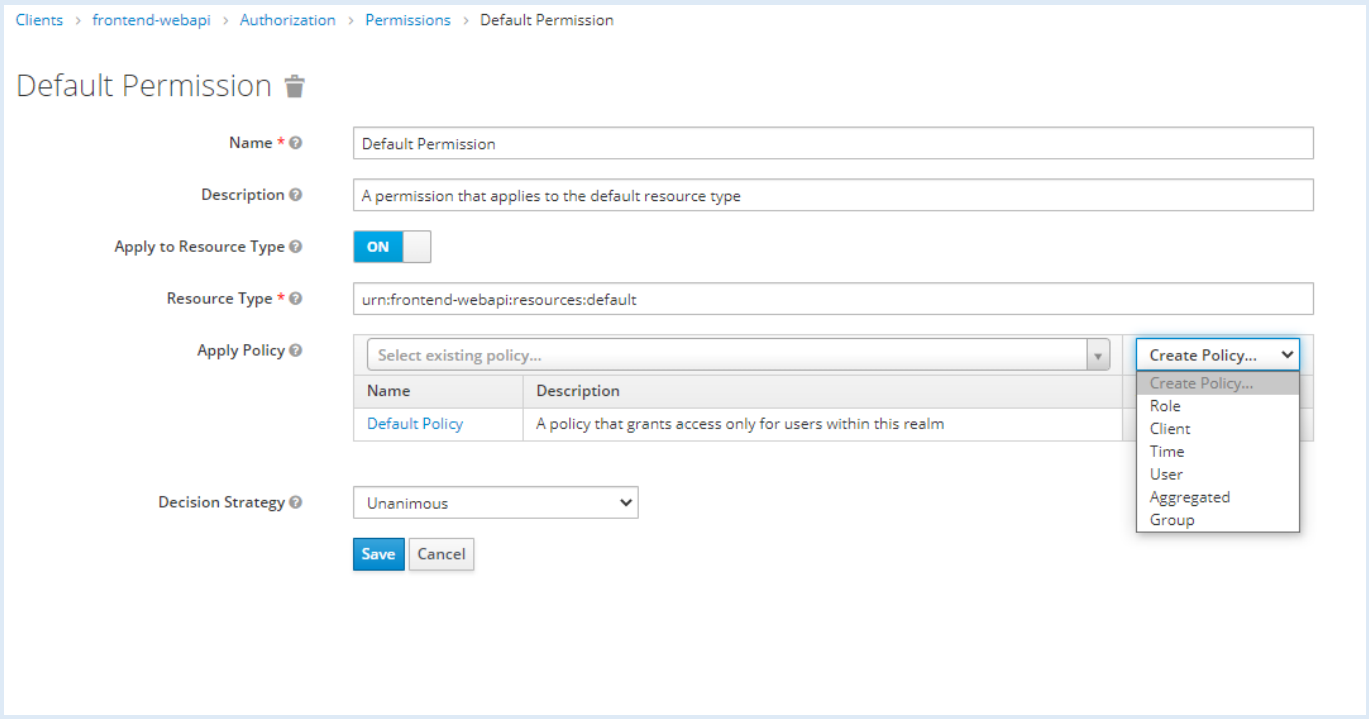
NF. 46	User passwords must be protected within the application. The method of protecting passwords must ensure the impossibility of their interception, deduction or retrieval.	Mandatory
User passwords are not stored in an open form. All passwords are salted and hashed which prevents deduction and retrieval. Only up to date secure hashing algorithms are used, such as: SHA-2, SHA-3. Passwords are always transmitted via a secure channel (TLS), which prevents interceptions.		
NF. 47	Application will allow: a. Setting password policy requirements for at least: the complexity of password, password change requirement, password lifetime, repeated use of passwords, the number of failed login attempts and dictionary of prohibited passwords. In this case, the application will timely provide the user with information regarding the use of password usage policies (e.g. a message about password expiring in n days). b. Application will allow segregated use of password usage policies for different user groups. c. Application will enable their users to change the password via user interface.	Mandatory
• Keycloak allows adding different policies, required actions for each case, for individual users, or globally.  • Keycloak allows extending functionality and adding new functions, like per-group password policy.		
NF. 48	Application will allow to block, disable or suspend user accounts at the application level.	Mandatory

Keycloak allows disabling individual users:



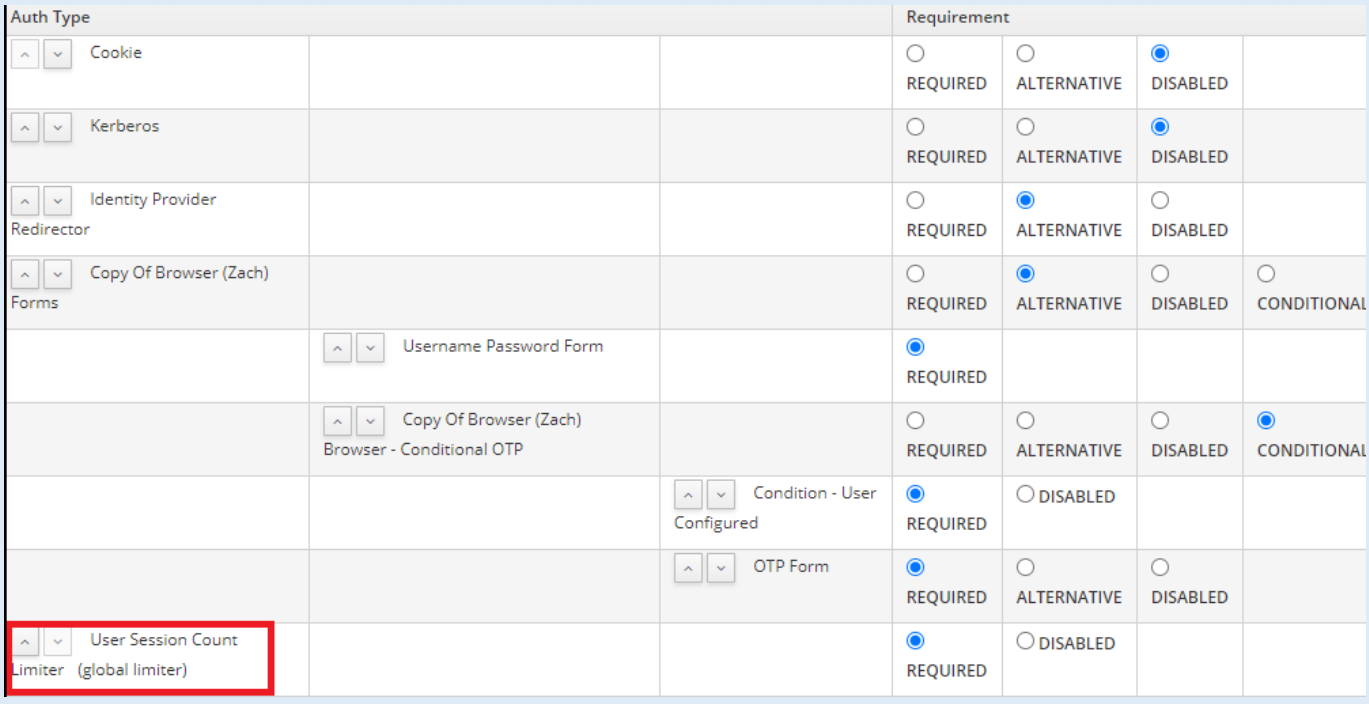
NF. 49	Application will allow users to access application only through an authentication procedure.	Mandatory
The user can access the IPS only by the authentication procedure. For back-end, a standard Oracle authentication procedure is used, for front-end, the Keycloak functionality for authentication is used. Both of them support Multi-Factor Authentication.		
NF. 50	Application will allow differentiated use of authentication methods, depending on different categories of users.	Recommended

It is possible to create new policies for users or their groups:



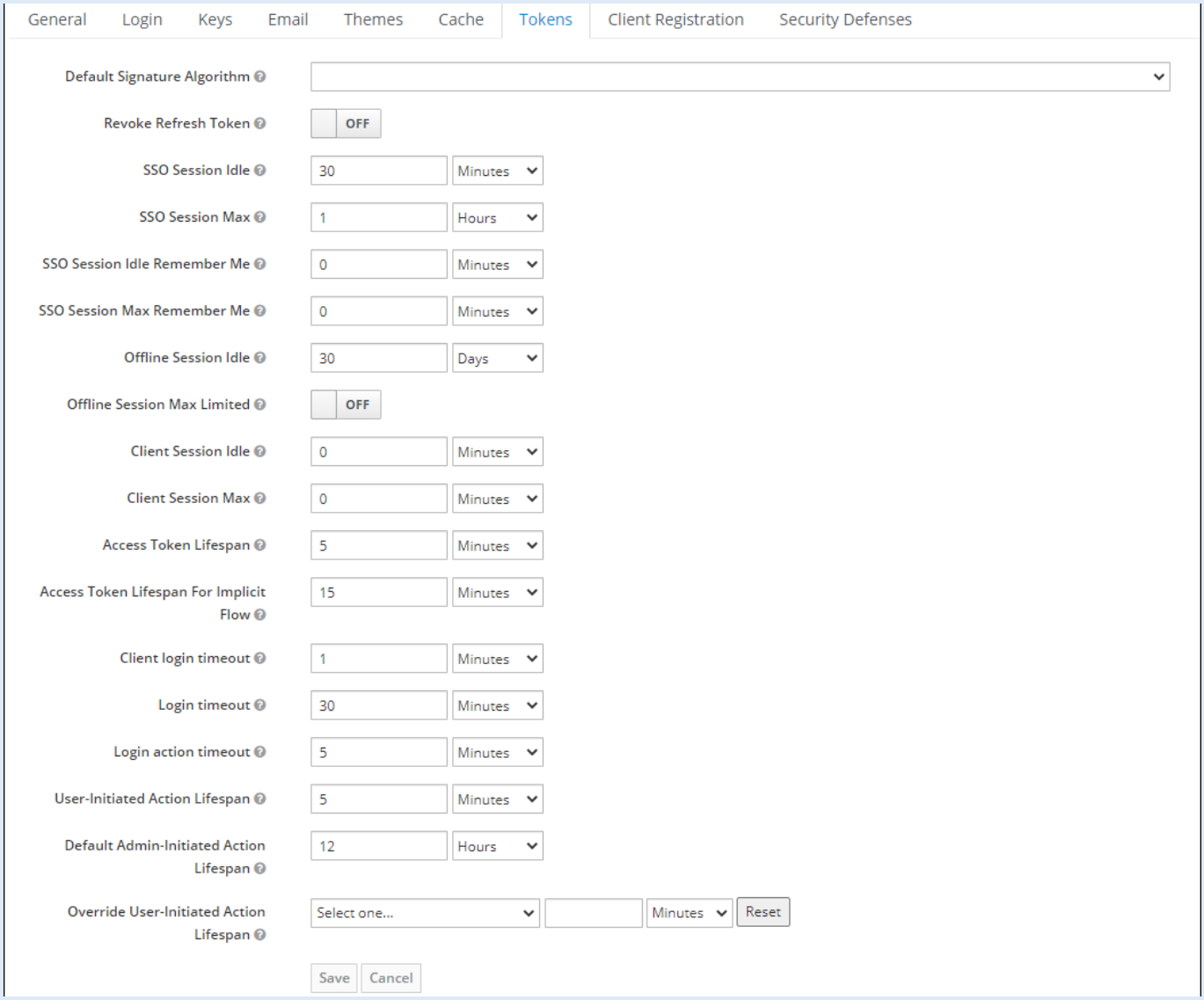
NF. 51	Application will permit to set the number of simultaneous connections that can be initiated by a user. In case this feature is not supported, the solution will not allow more than one connection per user.	Mandatory

Keycloak allows configuring the user session count limiter/restrictor for all users globally:



NF. 52	Application will permit to set user session timeout in case of inactivity.	Mandatory

Keycloak allows configuring the session timeouts as lifespans by the realms:

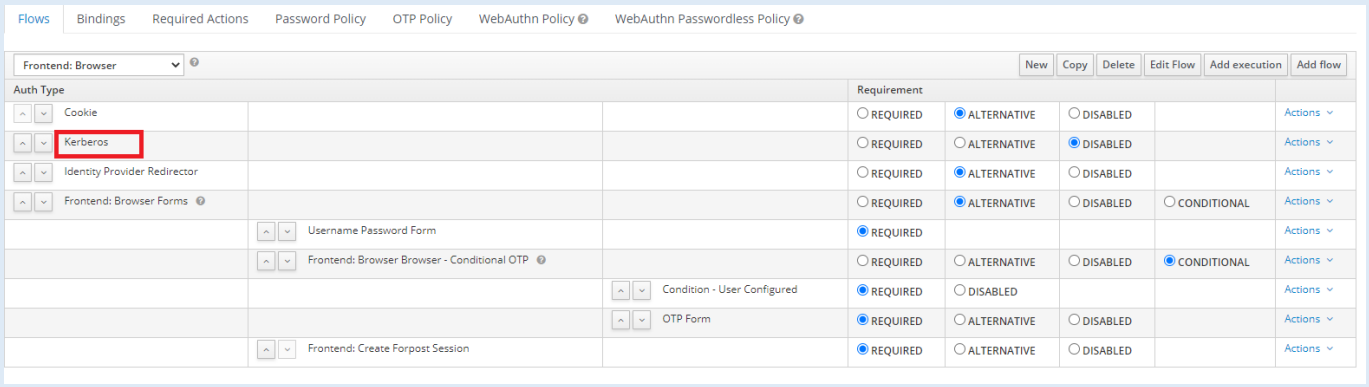


NF. 53	Application will provide mechanisms to prevent unauthorized take-over of active sessions initiated by legitimate users.	Mandatory

Keycloak had this issue in the older version (6.0.0), but it is fixed now by Keycloak, and it is not possible to hijack other user sessions in later versions.
The IPS is based on the higher Keycloak version.

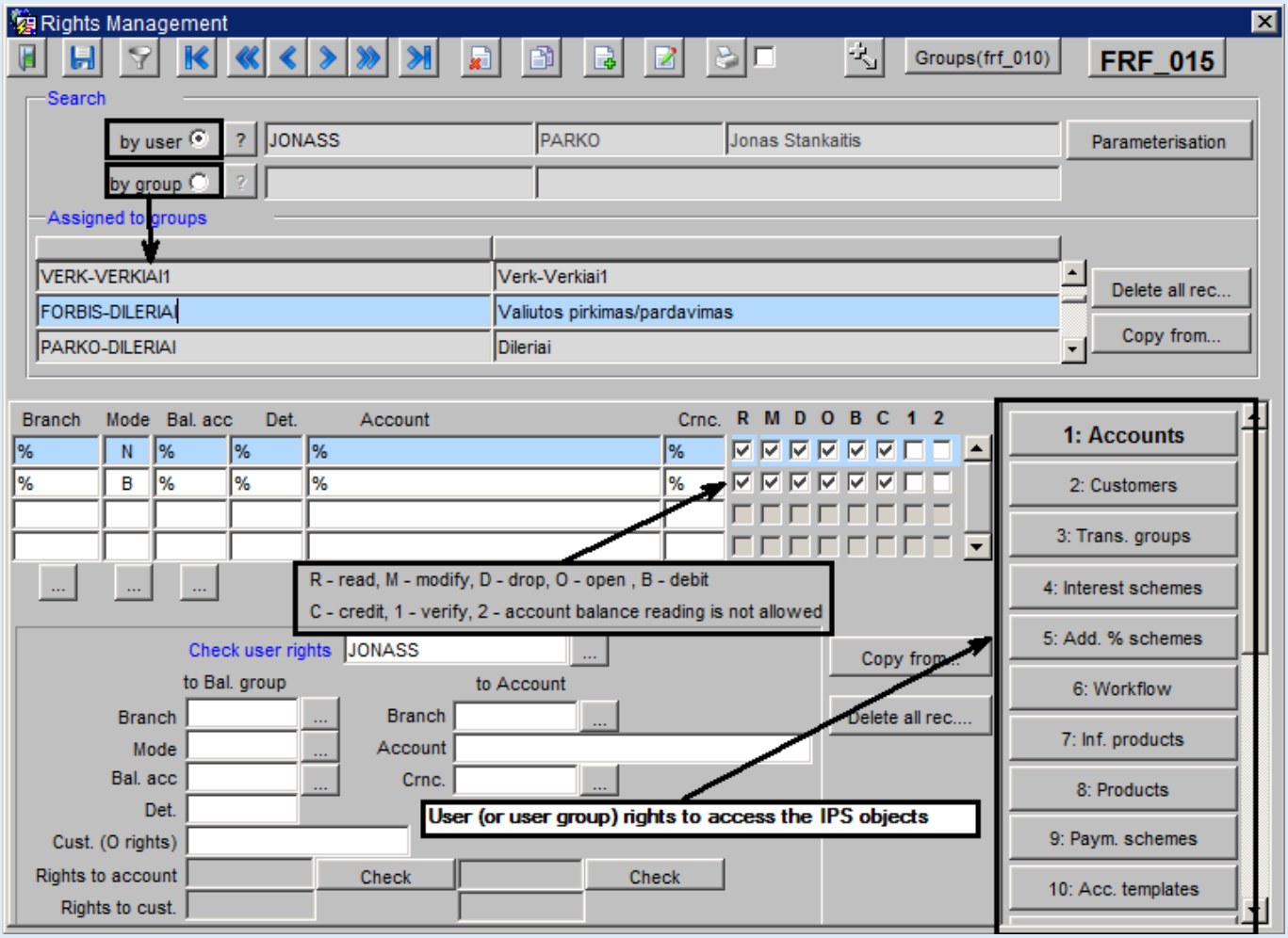
NF. 54	Application will provide the necessary mechanisms for implementation of Single Sign-On (e.g. Kerberos).	Mandatory

Keycloak allows adding extra Auth types like Kerberos:



2.5.3. Authorization

NF. 55	Authorization method in the application will be based on the principle "everything not expressly permitted is forbidden".	Mandatory
Yes, it is so. After user creation, possible connect only without any rights		
NF. 56	Application will allow definition of user groups and roles within the application, and association of users of the application with these groups and roles.	Mandatory

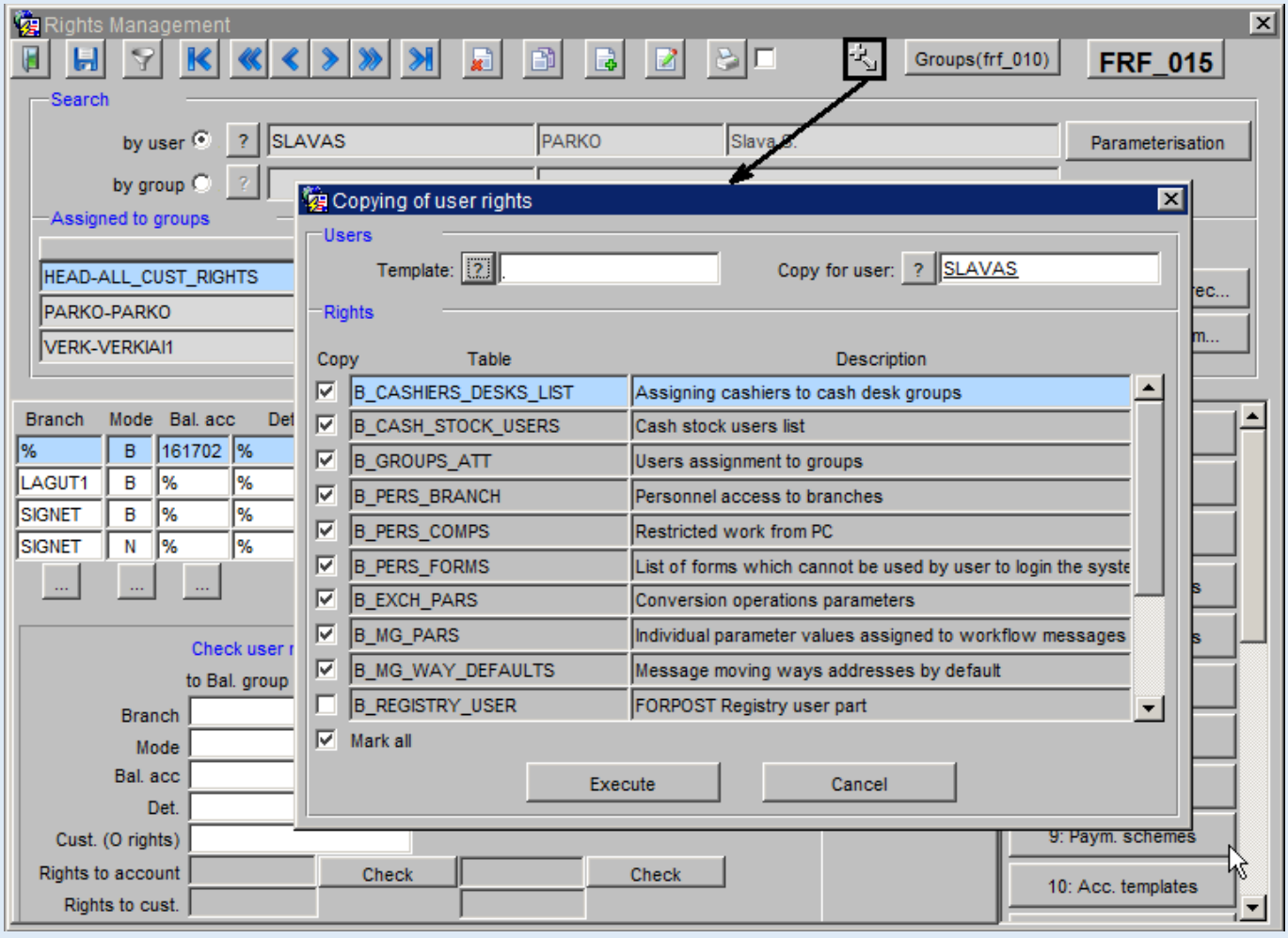


The IPS system is optimized for operating with a large number of users. That is why instead of setting rights and roles for each particular user, the rights and roles are defined for groups of users. The IPS system supports unlimited number of user groups, and the groups are created according to the business needs. In fact, a user group is a set of users having the same business role. A user group may have different access rights to various groups of the IPS objects (accounts, customers, products, payment messages, etc.). Once the user has been included into the group,

he/she obtains all the privileges the group provides.		
NF. 57	Application will allow the granting of access rights for user, user groups and user roles. A group can contain multiple subgroups / roles. A user can be assigned to one or more groups or roles, access rights being determined cumulatively.	Mandatory
The access rights to various IPS system objects are granted to user groups. A user may be included to several user groups; in such a case, the user obtains the cumulative privileges of all the groups it belongs to. The number of groups the user can be belong to is not limited.		
NF. 58	Application will allow temporary delegation of rights held by one user to another user. The delegation will be made with keeping or suspending of rights owned by the user to whom these rights are being delegated.	Mandatory

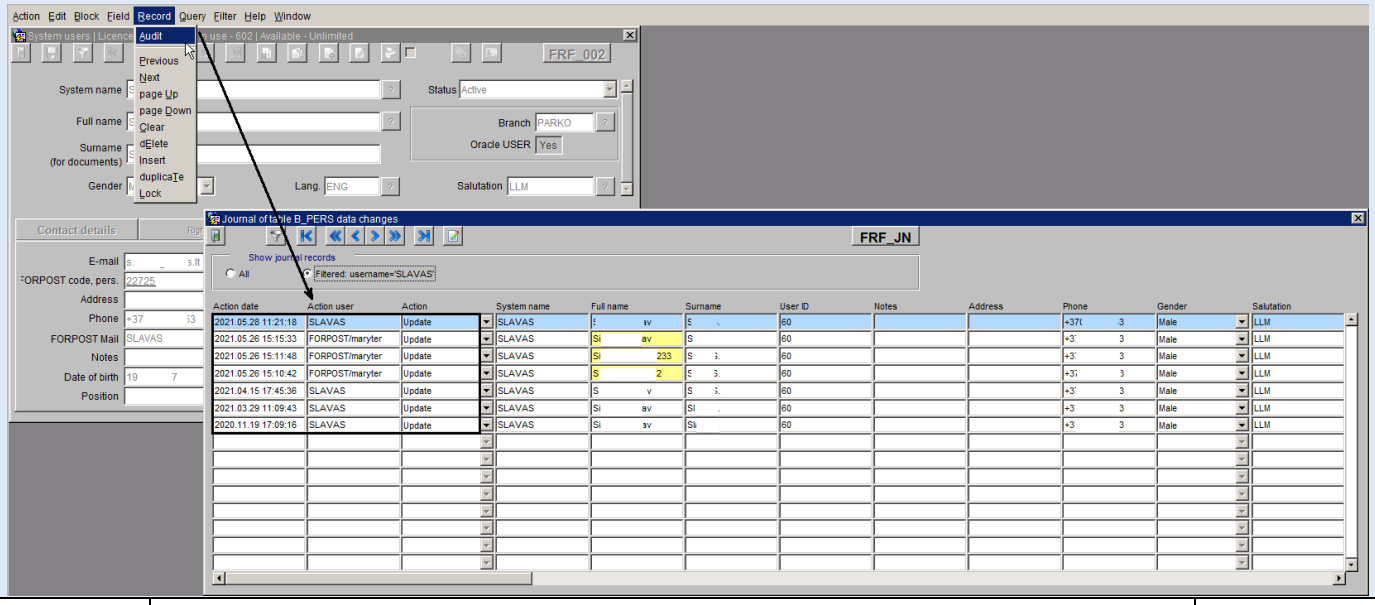
Since the rights in the IPS system are managed via the user groups, the delegation of rights is quite easy. One user is removed from a certain group, while another user is added. Accordingly, all the rights are instantly revoked from removed user, and instantly granted to the added user. The ISP system logs the fact and the basis (reason) of such a change.

Alternatively, a dialog for copying user rights from one person to another may be used:



NF. 59	Application will provide views and reports regarding existing access rights within the application. They can be parameterized by at least the following parameters: user group / role within the applications, user ID, business entity, property related to business entity, permitted operations.	Mandatory

All the rights-related changes in the IPS are logged. The system records the previous state, the new state, which user and when initiated the change, the type of the change (insert, update, or delete), and the updated information can be put in even in a more detailed way in each particular database field. The log is accessible to the authorized users via a GUI form or various reports. Since all the information is recorded in the log, the reports' output can be filtered by any criteria.



NF. 60	The solution must support multi-level authorization framework for verifications and approvals, based on configurable business workflows. At least three levels must be available by default.	Mandatory

Keycloak Authorization Services can help you improve the 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.

2.5.4. Input and output validation

NF. 61	Application will provide appropriate mechanisms to prevent manipulation of the input data (user inputs, inputs from external applications).	Mandatory

All data that comes from the User Interface (e.g. WEB application) or external applications (suppliers, partners, vendors, regulators, etc.) is considered unsafe and validated on both syntactical and semantic level.

OWASP Input Validation Cheat Sheet is used as guidance for Input Validation.

Syntactic validation checks the correct syntax of the structured fields (e.g. IBAN, currency, amount, etc.).
Semantic validation checks the correctness of their values in the specific business context (e.g. the start date is before the end date, the price is within the expected range).
When the input format is XML, then input validated against the XML schema, if any.
To ensure data integrity, the MAC, hash, or digital signature is validated.

2.5.5. PKI

NF. 62	IPS infrastructure must ensure the protection of the integrity of messages exchanged between IPS system participants and the operator. *Integrity protection should be ensured using PKI and digital signatures for sender*	Mandatory

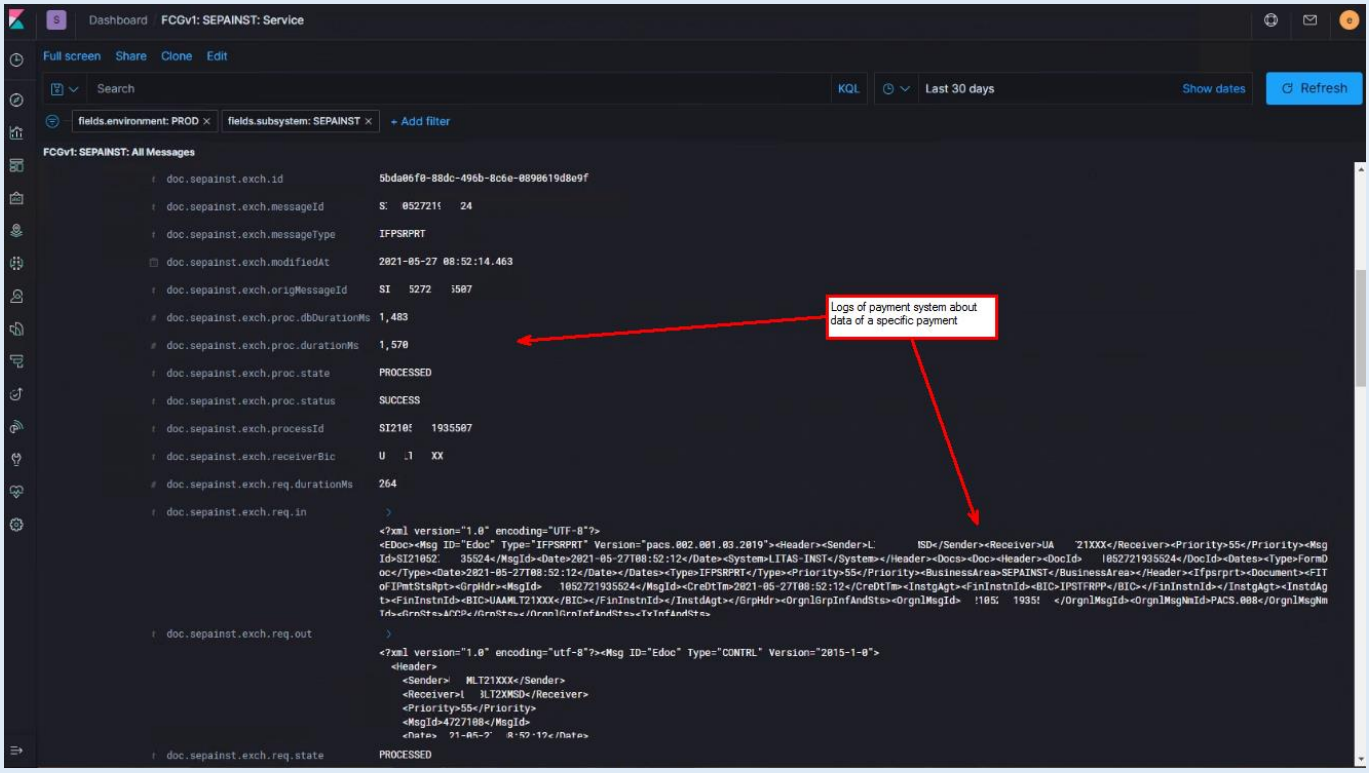
	messages as well as the validation of the digital signature by the recipient.	
The messages are signed with an electronic signature. The cryptographic certificate is on the HSM. Both communicating parties (IPS and Participant's IS) will be authenticated using cryptographic keys (X.509 certificates and TLS Mutual authentication protocol).		
NF. 63	The IPS infrastructure must ensure the protection of confidentiality of data exchanged between IPS system participants and the operator. *Confidentiality protection is provided by using PKI and traffic encryption between system participants and the operator at application level.*	Mandatory
All communication is done via a secure TLS channel. The technologies used are: TLS1.2, TLS1.3, and up to date encryption algorithms. There is also a possibility of additional encryption by encrypting the message itself (XML, JSON...), which is later transmitted via a secure channel.		
NF. 64	Client application modules need to be ensured that enable the integration of participants into the PKI of the IPS system. *Adequate software support should be ensured for each of the proposed methods for connecting participants to the IPS system.*	Mandatory
The client's applications can be easily integrated with our system, owing to the used industry-wide standards. It does not matter which programming language or tools are employed by the client's applications as long as they follow the common practices. If the client has not yet upgraded the system to the newest TLS version or encryption algorithms, then it is possible for the IPS to allow communication using the older version for a limited transition period. The use of X. certificates issued by Certificate Authorities provide means of standard based certificate revocation checking, such as OCSP and CRL.		
NF. 65	The solution for the electronic signature and PKI will meet the following technical requirements: • Centralized management of public key certificates, based on a widely-adopted protocol (e.g. LDAP), with possibilities for scaling up and integration with other solutions. • Acceptance of third-party certificates as Root of Trust (RoT). • Acceptance of certificates with RSA public key of length up to 4096 bit, SHA-256 as signature/hash algorithm and up to 4 levels of certification path. • Private key and private key's password / PIN will be protected against being tampered with or eavesdropped during the creation of electronic signatures. • Modern and commonly used standards and specifications will be used for creation of signature, such as RSA of minimum 2048 bit for end user keys, SHA-256, AES-256. • Possibility for integration with Hardware Secure Modules (HSM) and other electronic signature creation means by using PKCS#11 (v.2.20+) standard. • Addressing the requirements of security standards in the field of digital payment protection, such as PCI SSC, will be considered as an important advantage.	Mandatory
Part of our PKI solution is based on Java technologies, which are kept up to date when it comes to security concerns. Root of Trust is definitely supported, as well as at least 4 levels of certification path. RSA Keys of length 4096, SHA-256, AES-256 are already in use, as well as other algorithms such as DSA, ECDSA. Private Keys can be stored in HSM, for which we already have experience with multiple vendors. Most of which are based on PKCS#11. PIN is stored encrypted, and the encryption key may be provided at application start-up.		
2.5.6. Auditing and security monitoring		
NF. 66	For auditing and security monitoring, the following requirements are applicable: a. The proposed solution will have audit components that will centrally collect and manage audit records at each component level. b. Audit component shall allow granular configuration of audit policies. c. The proposed solution shall allow determining the specific characteristics of events that must be registered (e.g. products in a certain period, certain events, facts).	Mandatory

	d. Application shall allow auditing of any event within the application. e. Each audit record shall contain at least: i. Moment in time of the event; ii. Subject of the event (User ID); iii. Categories of affected data/parameters; iv. Event that happened; v. IP address of the source that initiated the event, or any other information permitting to identify the source; f. Audit records will not include confidential business information (e.g. inserted passwords at failed attempts). g. The application will allow to fix historical versions of the data, which will be considered extremely sensitive. h. The application will be able to automatically generate the notifications to those responsible for the production of certain security events, according to set up configurations. i. Audit component shall use the system clock set to the operating system that runs the audit component. j. The proposed solution shall have secure mechanisms to protect the integrity of audit information recorded.	

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:

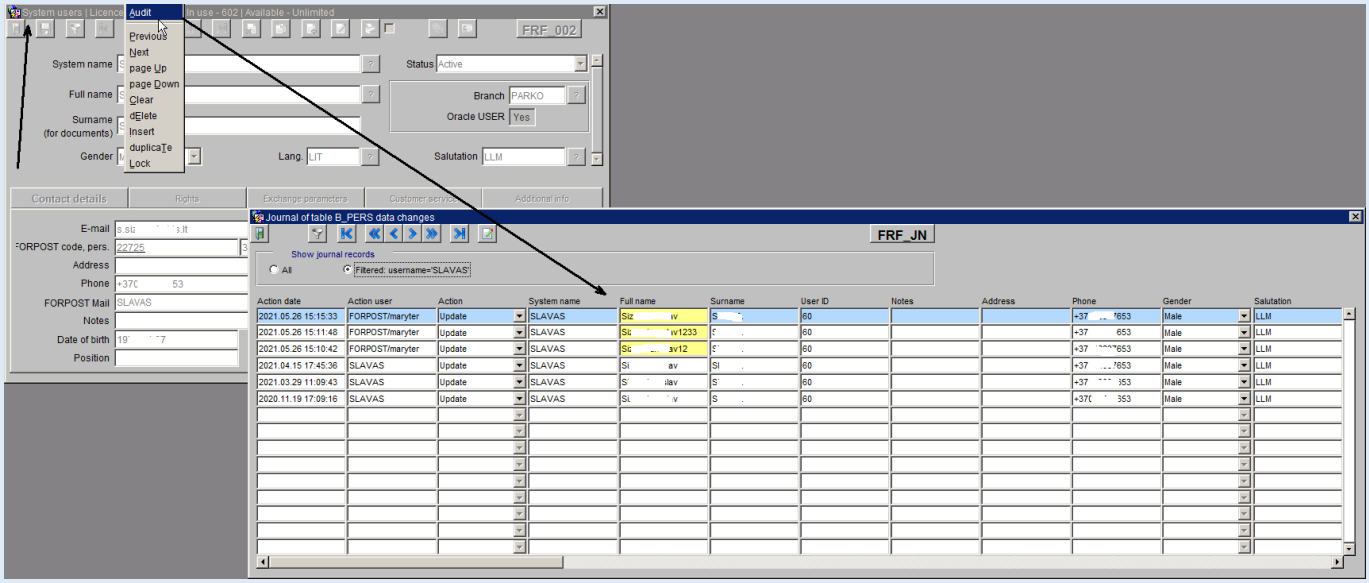


FCGv1: SEPAINST: All Messages

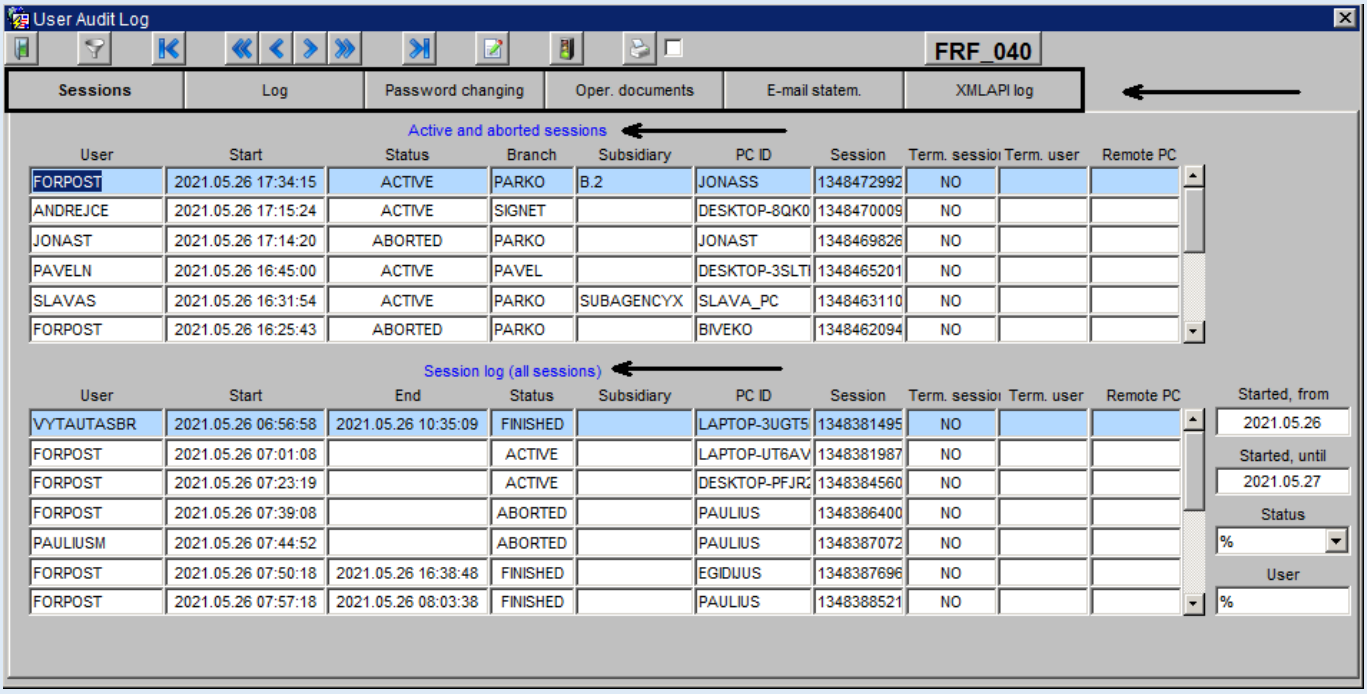
1–50 of 1458

d.s.e.createdAt	f.clientId	d.s.e.direction	d.s.e.messageType	d.s.e.processId	d.s.e.totalStatus	d.s.e.p.state
2021-05-26 15:35:36.067	conto	IN	ILPNOT	S211460007102126	SUCCESS	PROCESSED
2021-05-26 15:30:35.934	conto	IN	ILPNOT	S211460007102122	SUCCESS	PROCESSED
2021-05-26 15:25:35.872	conto	IN	ILPNOT	S211460007102115	SUCCESS	PROCESSED
2021-05-26 15:20:35.787	conto	IN	ILPNOT	S211460007102110	SUCCESS	PROCESSED
2021-05-26 15:15:35.758	conto	IN	ILPNOT	S211460007102105	SUCCESS	PROCESSED
2021-05-26 15:10:35.664	conto	IN	ILPNOT	S211460007102086	SUCCESS	PROCESSED
2021-05-26 15:05:36.228	conto	IN	ILPNOT	S211460007102061	SUCCESS	PROCESSED
2021-05-26 15:00:35.480	conto	IN	ILPNOT	S211460007102042	SUCCESS	PROCESSED

- 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:

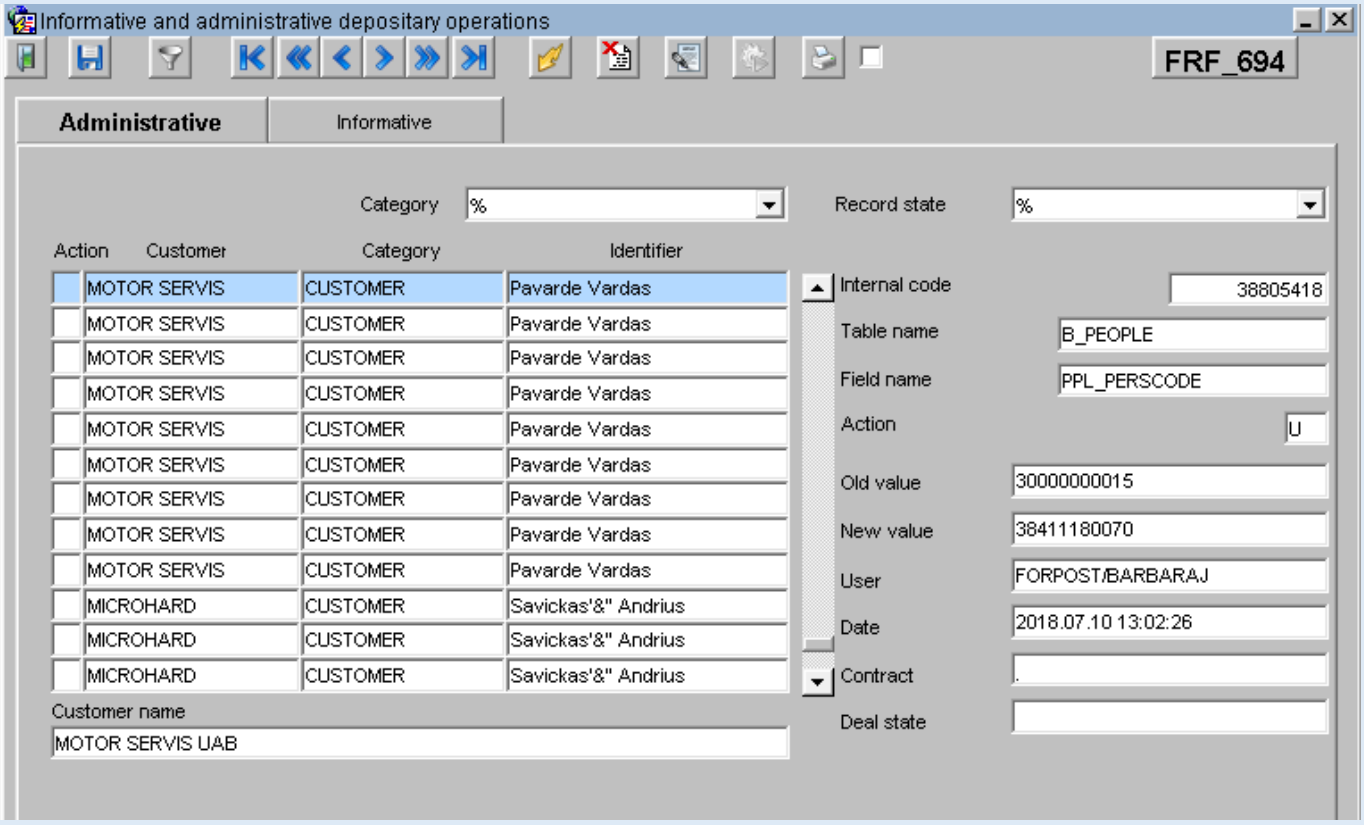


- Important tables with sensitive data have journaling tables for all actions with records. These tables store the exact copy of the record at the moment of change. Thus, it is possible to see, how records have changed over time.
- Reports logs. The IPS keeps track of launching reports: who, when launched 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.

NF. 67	The solution shall have also its own user interfaces for accessing and processing recorded log events, including filtering of audit records by any field owned and their export in the usual format.	Mandatory

Various IPS subsystems have their own interfaces for recorded log events. For example:

- Logged events of the customer data change:

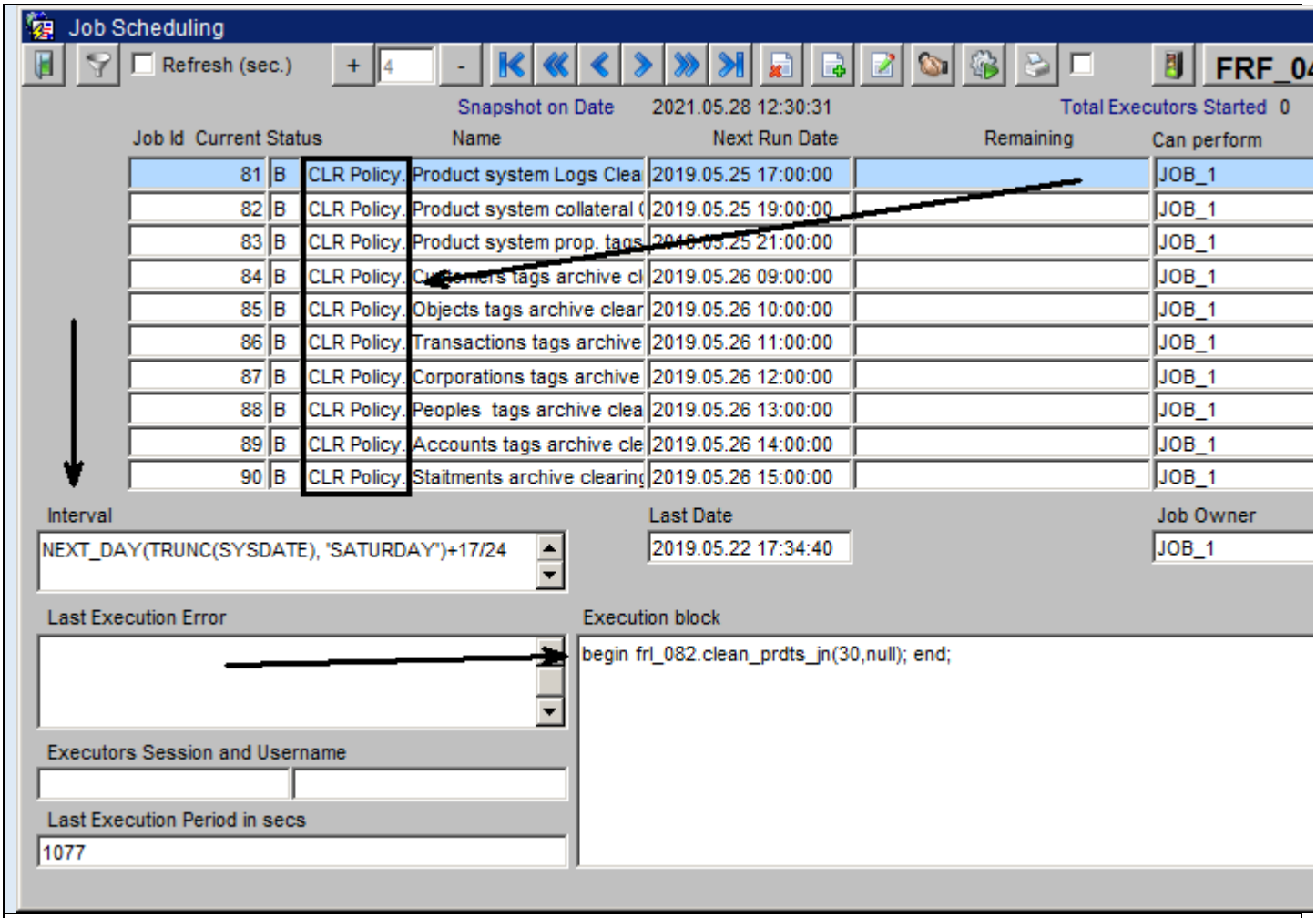


NF. 68	Audit component shall be able to be integrated with solutions based on open standards, such as SIEM (Security Incident and Event Management) to take over the audit records produced in the solution by SIEM.	Recommended

Currently, there is no such integration implemented but there are the possibilities to integrate.

NF. 69	The audit component will own a mechanism for historical audit records archiving. The archiving process can also be parameterized by (frequency, data seniority, archiving format, destination, etc.).	Mandatory

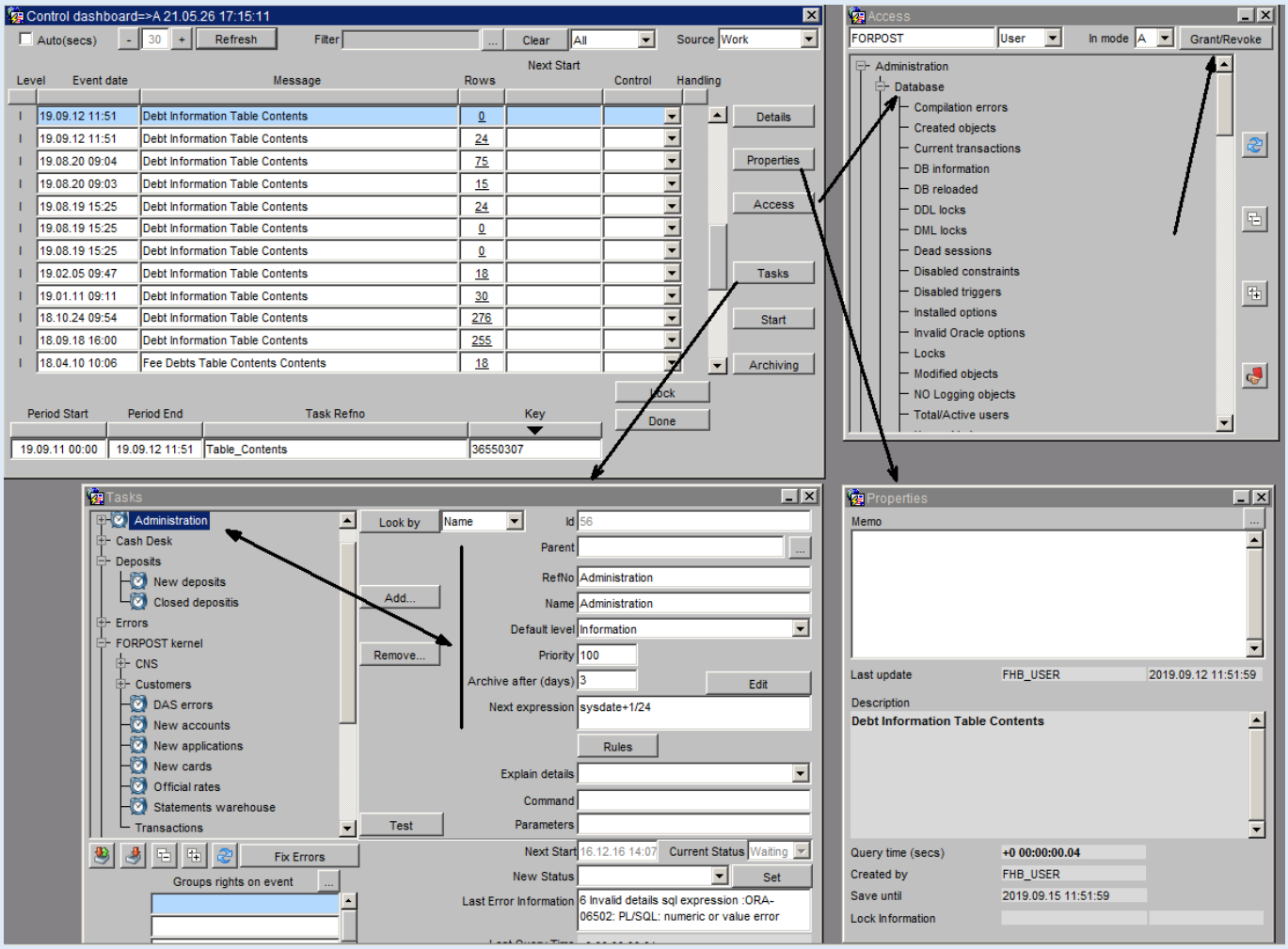
The mechanism for historical audit records' archiving is available in the IPS system. The information from audit records is transferred to the long-term storage tables where it is accessible in the read-only mode. When there is no more need to keep this information, it can be deleted, or it can be exported in various formats. The frequency and other settings of archiving are configurable.



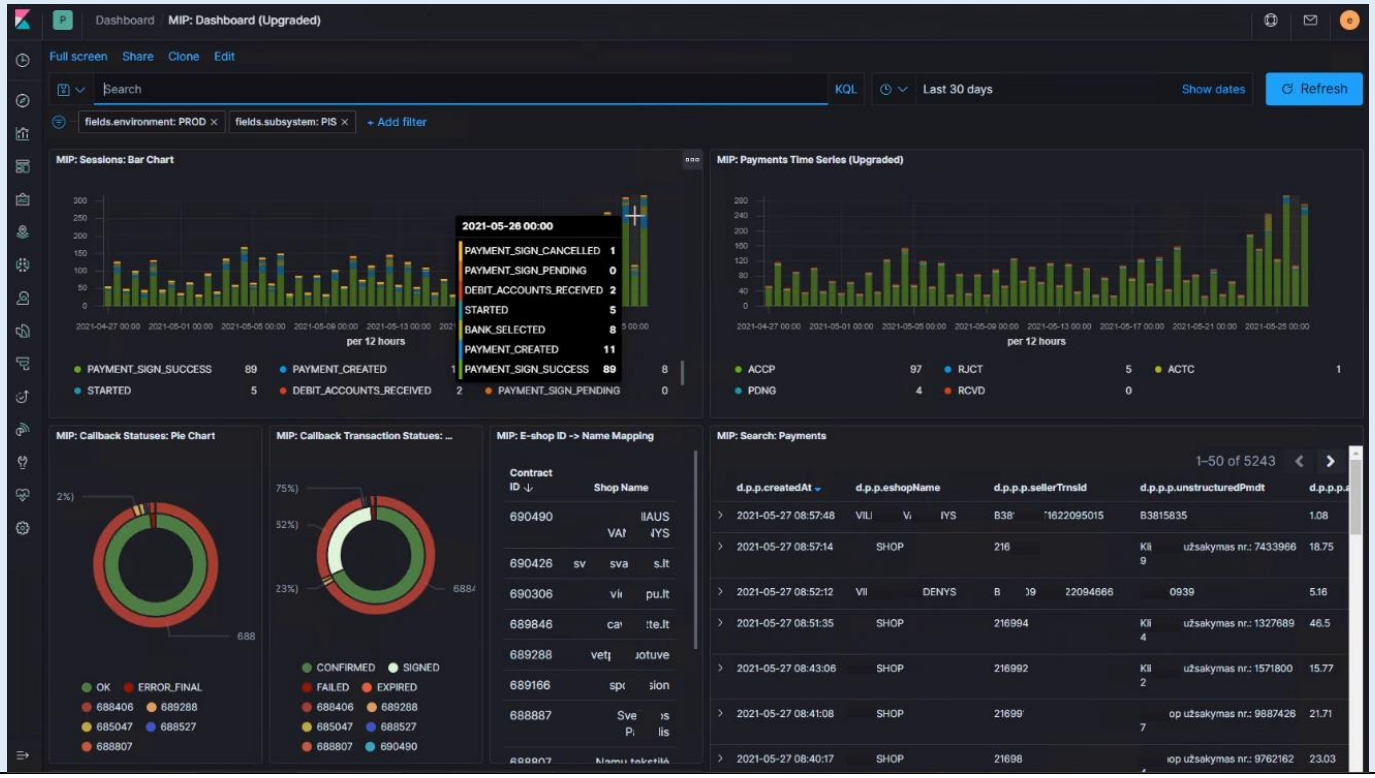
2.6. Requirements for Maintainability

NF. 70	The offered solution should be easily maintainable and meet the following basic characteristics: a. Unified technology platform (a single database management system, a single hardware/software infrastructure); b. A single vendor for software modules that are part of the offered solution; c. A minimum number of development environments used for the development of application which is part of the offered solution; d. Effective mechanisms to identify and monitor problems appeared during the exploration of the solution.	Mandatory
As the basis, we mainly use the technological stack from Oracle (DB, Forms, Java, Linux). Since the critical threshold metrics have not been indicated, we assume that the answer is Yes.		
NF. 71	For application to be available and accessible to business users at agreed level, they must be continuously monitored and maintained. Application must enable proactive problem identification and prevention by facile going of operational maintenance activities across all application components.	Mandatory

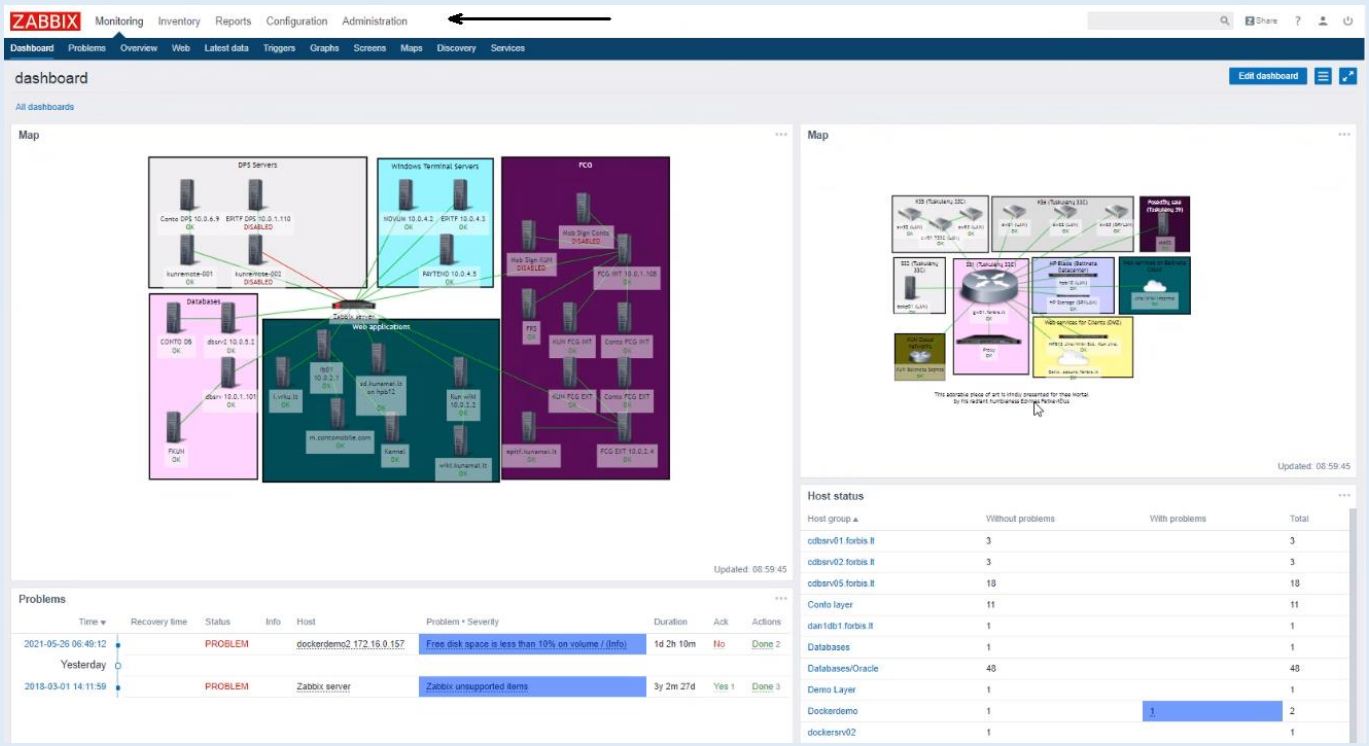
The IPS has its own built-in Dashboard and Monitor. It is also open to such systems as Zabbix and ELK.
A Built-in dashboard for the internal IPS processes:



- A dashboard for the external IPS processes.



- A dashboard for the IPS infrastructure components:



NF. 72	The solution will allow to monitor its own business-related parameters: the processing time for input/output messages, transaction processing time, etc. and generate appropriate notifications when certain parameters exceed critical thresholds.	Recommended
The system has its own built-in Dashboard and Monitor, but it is also open to such systems as Zabbix and ELK.		

2.7. Requirements for performance, continuity and resilience

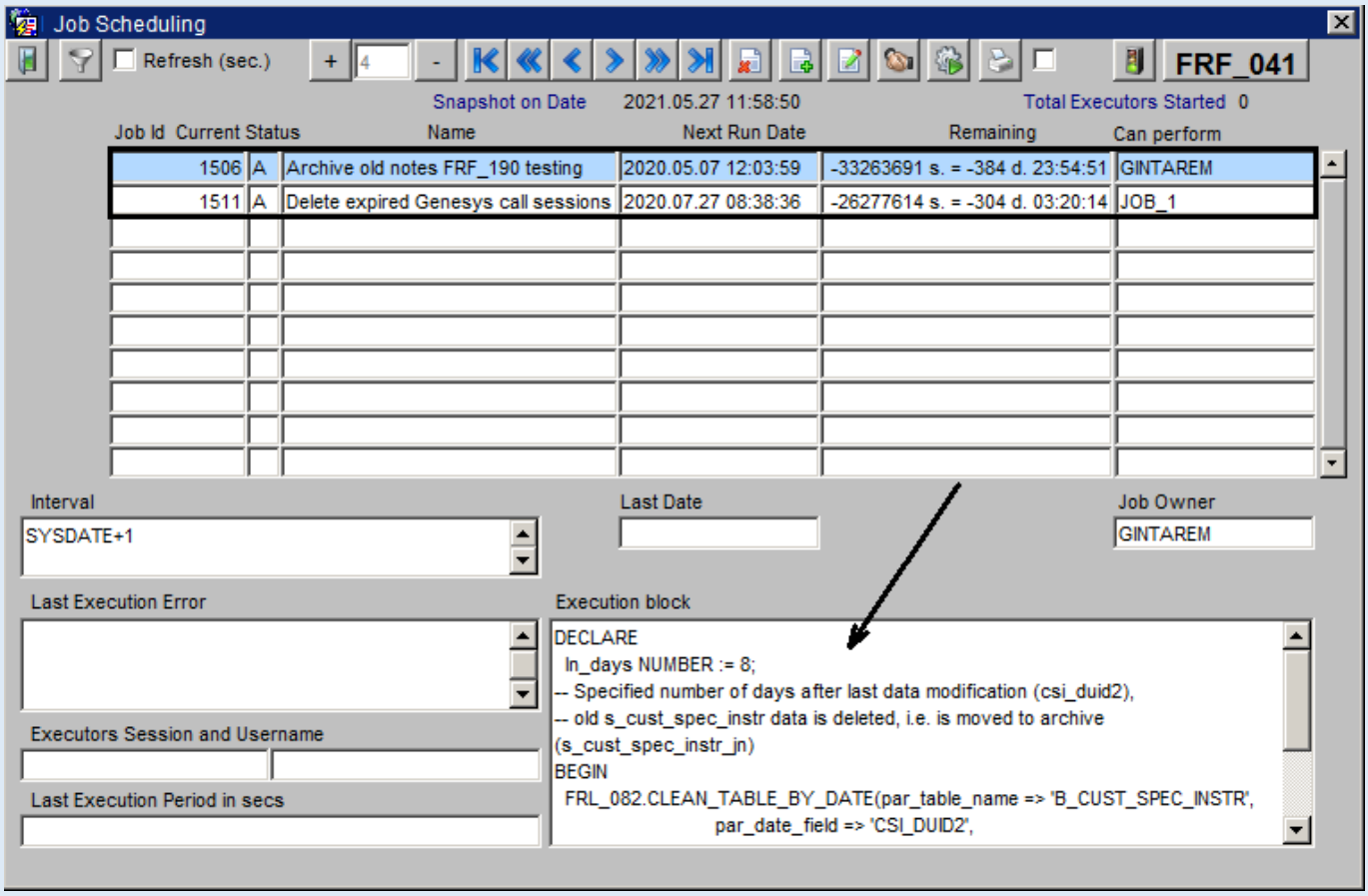
NF. 73	The solution must have the ability to process in a timely manner the transactions performed by IPS, according to volumes resulting from its activity. Technology platform architecture proposed by the Tenderer must provide the following minimum performance levels for application: a. IPS must be designed to enable the execution of 5,000,000 transactions (transfer orders) in A2A mode; b. IPS must be designed to enable the execution of about 100 transactions (transfer orders) in A2A mode per second in the peak times; c. IPS will complete the established tasks in the transfer order execution in less than 1 second. The established tasks executed by IPS within the defined deadline entail: Validation of the received message and forwarding it to the Recipient; Validation of the inbound Recipient's response, execution (in case of a transfer order) and forwarding the response (network delays and recipient's response delays are not accounted for this purpose). *The Vendor shall indicate in his offer the guaranteed minimum values of performance characteristics of the application, taking into account the technology platform recommended by Tenderer.*	Mandatory

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, which we cannot affect, we can only parallelize calls to several HSMs.		
NF. 74	IPS must support a configuration to operate on a 24/7 basis. *IPS must be configured in such a way as to enable operations in 24/7 mode with the availability higher than 99.99% per month. All the system components must function in active-active mode.* *Vendor shall describe continuous availability options and proposed technologies for disaster recovery supported by the solution. Recovery times for different options have to be described.*	Mandatory
The IPS system is fully ready to operate 24h a day. Its core is the OTLP system, and it has been designed to function 24/7 from the very start. Continuous availability is ensured by RAC/DATAGUARD at the Oracle level, and by clustering and load balancing on the level of the application/service.		
NF. 75	IPS must enable changes to the configuration on-the-fly with near to zero downtime. *IPS should be designed to enable the upgrade process on-the-fly, including changes to the set of messages and processes in the system as well as addition of new functionalities. The system should have the possibility to operate with multiple message versions simultaneously.*	Mandatory
The configuration of the IPS system is carried out in real-time and does not require downtime. Once the configuration is changed, and the rights are granted to certain groups of users/automated system services, the updated setup starts functioning. Multiple versions of messages may be operated simultaneously, the IPS system support such operation mode. Downtime may be required to upgrade software components' versions during the version release (2-4 hours annually).		
NF. 76	IPS must ensure that changes to hardware configuration meet the new capacity requirements. *IPS should be designed to enable acceleration of message processing only by adding the hardware.*	Mandatory
At the Oracle level, this is implemented by RAC. At the application and service level – by cluster and load balancing.		
NF. 77	IPS must ensure a RPO (Recovery point objective) value of zero. *In case of a system failure, IPS must not lose a single transaction executed.*	Mandatory
This is possible by the Oracle means (RAC/DATAGARD).		
NF. 78	IPS must ensure a RTO (Recovery time objective) not longer than 15 minutes. *In case of a system failure, maximum recovery time must not be longer than 15 minutes.*	Mandatory
This is possible by the Oracle means (RAC/DATAGARD).		
NF. 79	The IPS system will have suitable instruments for executing backup procedures and the management of the historical backup copies.	Mandatory
Yes, it is based on standard Oracle tools, load balancing, Docker.		
NF. 80	The IPS system will have defined operational recovery procedures, to ensure the availability and accessibility of the solution in case of major incidents.	Mandatory
Yes, it is based on standard Oracle tools, load balancing, Docker.		
2.8. Requirements for scalability		
NF. 81	During the use of the IPS system, it is possible that the number of processed transactions to increase or decrease significantly from time to time. To make a rational use of processing resources the solution required by NBM should be easily scalable (up and down).	Mandatory

At the DB level, this must be done in advance, the resources must be added, or RAC nodes must be reloaded. At the level of applications and services, this happens quite quickly, due to starting of new nodes.		
NF. 82	Solution will allow to increase the processing capacity without disrupting the business activity. To this end, application will support horizontal expansion of processing capacity (e.g. hardware infrastructure upgrade, adding new servers for application servers and performing load balancing).	Mandatory
At the database level, this can be done using RAC. At the level of applications, services - by cluster nodes, clusters or Dockers. The means of Virtual Machines are used. Balancing is done at the http load balancer level.		
NF. 83	Application can be configured for automatic load distribution and automatic scaling at the level of key components (lag sensitive applications). Scaling of the application will take place both up and down.	Recommended
Docker based solutions allow us to easily scale up and down the required services, control how many instances (system processes) of each service are run. It is also possible to control how many hardware resources are available for a service. Automatic scaling can be triggered when a particular threshold is hit. For system parts that cannot be easily scaled due to licensing costs, we can provide a stand-in, which simplifies the handling of the load for the time being. Our expertise with the virtualization technologies makes it easy when it comes to deploying applications to a cloud-based infrastructure.		
2.9. The technological and infrastructure requirements		
NF. 84	The technological and infrastructure architecture represents all software and hardware components necessary to ensure the operating environment in which all solution components shall run. The technological platform includes development platforms, database management systems, operating systems that can run solution components, specific system software required to be installed for correct run of the solution, hardware platform that can run solution components, etc. In order to be scalable, flexible and easily maintainable, it is recommended that all solution components have a minimum level of dependence on the technological platform on which it runs.	Recommended
We are tightly connected to Oracle and Java, and the solution would not function without them. Anything below the Oracle and Java level is possible only if properly certified. All IPS applications based on Oracle and Java are designed using independent layers of solutions.		
NF. 85	Platform technologies presented in the solution architecture shall be open technologies or widely used technologies.	Mandatory
Our products are developed on: • Oracle, • Java, • JavaScript, • Linux, • Docker platforms, • XML, • XSL, • JSON, • MS Windows.		
NF. 86	To run the application it will require only standard equipment, available to be purchased by NBM freely on the market.	Mandatory
We promote x86 by HP, but our clients also use IBM and DELL.		
NF. 87	The application must support the creation, modification, processing, storage and access for text data in Unicode format.	Mandatory
Yes, everything is stored and processed in the Unicode. Oracle and Java support Unicode format, and we use it.		
NF. 88	The IPS system must include clearly defined system administration procedures, which should be automated as far as possible.	Mandatory
Yes, it is so and will be available in the documentation portal upon signing of the agreement.		
NF. 89	The IPS system must include clearly defined system maintenance procedures.	Mandatory

	Vendor shall describe required maintenance procedures and periodicity of those procedures.	
Yes, it is so and will be available in the documentation portal upon signing of the agreement.		
NF. 90	The proposed solution will meet the minimal infrastructure requirements stated in ***Chapter 8.2. Additional information related to non-functional requirements***, ***Table 2 – Minimal infrastructure requirements.*** *Vendor shall include in his offer detailed information on the recommended technology platform, taking into account the needs of NBM defined in this tender specification. If the case of the winning bid, this will be taken as basis for determination of technology platform related to the application.*	Mandatory
Yes, we meet the specified minimum requirements. Our DB is ORACLE 19, it is the system's core. We use LINUXx86 everywhere, both for DB and for application servers, we promote ORACLE UNBREAKABLE LINUX. Our solution functions on both XEN and VMWare (however, we stopped supporting them ourselves, and take virtual resources from the Data Center). We support the specified encryption algorithms. We support the specified browsers. We do not use VDI+Citrix on our side, but we know that it works, since our client provides us with the remote access in this way. Note, for optimal licensing and performance, Oracle products are best used on physical rather than on virtual hosts. Additionally we are using DOCKER, SERVICEMIX , TOMCAT, ACTIVE MQ products.		
2.10. Data Retention and Archiving		
NF. 91	IPS must be able to store all operational data for a minimum of two years, without affecting its performance.	Mandatory
The IPS is designed and developed to comply with the General Data Protection Regulation (BDAR), 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 architects responsibly design all system nodes, 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). During the development of the IPS, the software developers (programmers) use a profiling tool to identify potential speed of operation issues in the system, review SQL explain query plans, and assess whether database queries are efficient enough in terms of data volume and flows. The Quality Assurance Department initiates manual and automated tests to verify how the system interacts, and performs speed of operation tests to identify problem areas. 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 repots for some long past periods.		
NF. 92	IPS must ensure that the system operator is able to retrieve transaction data and data on participants in the system up to 10 years. *Different access methods should be implemented for "recent" and "old" transactions.*	
Yes, we have no depth restrictions. *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 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 tablespace separately form the operational data. This data is not editable (read-only). The operational archive data is accessed using 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 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 specific 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 API manually or auto-scheduling jobs.		
NF. 93	The IPS system must support the efficient data archiving procedures. *Vendor has to describe archiving approach and automated/manual procedures*	Mandatory
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.		
NF. 94	The IPS system must maintain sufficient information for audit purposes for a period of at least seven (7) years.	Mandatory
The IPS allows collecting all the historical data, including the system audit records and logs. However, such accumulation is not advisable; in accordance with the client's needs, in the system, it is possible to configure which data structures should be audited additionally, thus increasing the traceability of the information changes. In analogy, the IPS allows configuring automatic users, who launch and process the data at a scheduled time according to the rules set out to them, i.e. who perform data transfer, deletion of obsolete data, clearing of obsolete system logs, etc.		



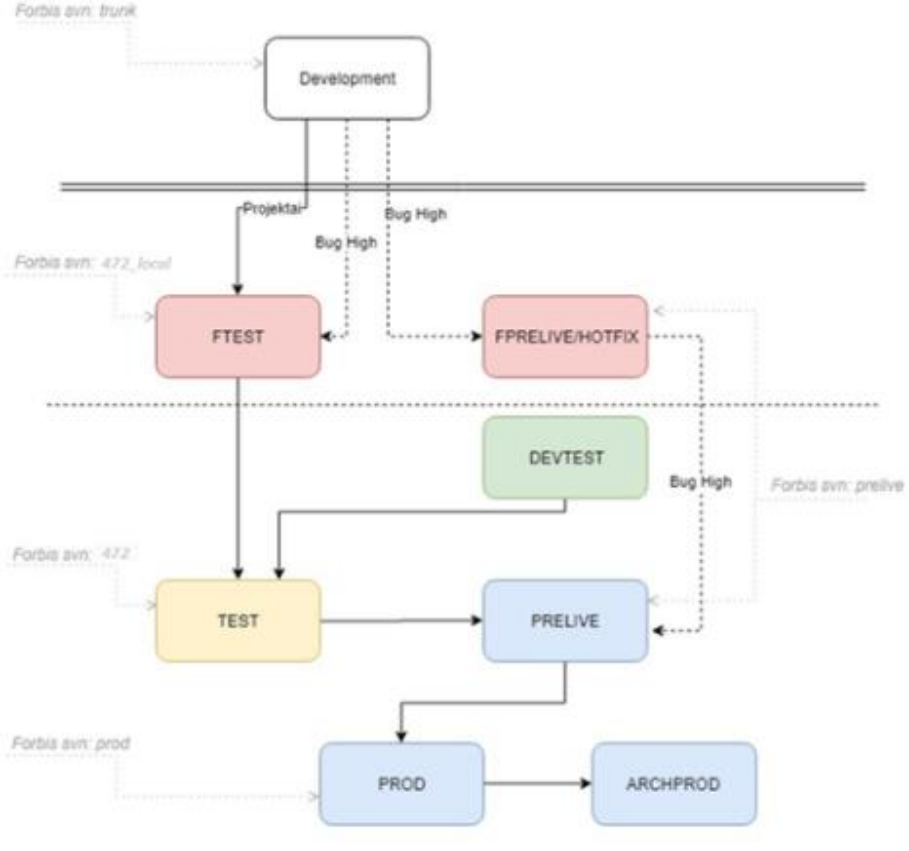
NF. 95	The IPS system must provide an efficient data archiving solution for data protection based on flexible backup-restore approach.	Mandatory
As data archiving solution Oracle means are used.		

2.11. Requirements for environments

NF. 96	IPS will operate at least the following environments for the tendered solution: • Production – This will be the main environment to deploy the solution for production; • Testing and Developments – IPS will maintain the development and the test environments even after going into production, for development and testing purposes;	Mandatory

	• Back-up – For resilience and back-up purposes IPS intends to implement an active/ active failover node architecture. In this regard, the Tenderer will consider these facts, when calculating the number of licenses.	

The concept of environments is applied to the development, maintenance, and transfer of the IPS system:



1. Development – the main development environment of the IPS developer.
2. CI (code inspection) – a dedicated environment layer, where the quality of the code in a fully automated process is checked.
3. FTEST and FPRELIVE environment dedicated to the IPS quality assurance before the components are delivered to the client (QA).
4. DEVTEST – client development environment (not necessary in the general concept of environments).
5. TEST and PRELIVE environments available in the client's infrastructure to ensure the IPS quality.
6. PROD – the client's production environment.
7. ARCHPROD – the client's back-up PROD environment.

NF. 97	The solution will have in place mechanisms to assure the transfer of data between different environments.	Mandatory

Yes, we have regulations on how to do this.
The IPS has the internal tools to transfer data between different environments:

- Transfer all system parameters and data,
- Depersonalisation process.

NF. 98	The solution shall have in place some mechanisms to assure puzzling or depersonalization of the data when copied from production to test environment.	Recommended

Yes, we have our own tools for depersonalizing data when creating test environments. IPS supports independently rules for depersonalization for each business data area.

2.12. Source Codes

NF. 99	The Tenderer undertakes to provide for the application that is part of the offered solution (including third parties) guarantees regarding the transmission of source codes in cases where for some reason the software supplier will not be able to	Mandatory

	maintain it (e.g. liquidation, bankruptcy, reorganization etc.). In the event that the source code can not be transmitted, it is necessary to provide an escrow commitment.	
We use the escrow deposit service with a number of our clients (provided by NCC group).		

8.2. Additional information related to non-functional requirements

Table 2: Minimal infrastructure requirements

Client side:	HW requirements	Requirements for HW should be as minimal as possible. It must run on VDI infrastructure of NBM without any visible impact on the performance of the virtual desktop machine.
	Operating environments	Windows 10/ VDI Citrix XenDesktop 7.5 and newer operating systems
	Software type:	Recommended: Thin client running on standard Web browser (IE, Chrome, Mozilla)
Server side:	Supported HW platform	x86 platform
	Supported operating systems	Linux or Windows Server family
	Supported versions for operating systems	OS must be maintained by their manufacturers and to be one of the last two major versions
	Supported database systems	Oracle 19c or MS SQL 2019, or newer versions
	Requirements for virtualization	Must support virtualized infrastructures based on Xen or VMware hypervisors
	The minimal accepted requirements for cryptographic algorithms in NBM	a. AES-256 for encryption of electronic data; b. SHA-2 for message digest; c. RSA 2048bit for end-point private keys.
Detailed recommended infrastructure with hardware and software configuration in provided in the document "IPS technical offer", chapters "3.4 IPS environments, 3.5 Technical architecture, 3.6 Integration platform, 3.7 Technical characteristics of the IPS environments (For One Node), 3.8 3rd party software specification, 3.9 Technical solution and characteristics of the environment for IPS Participants".		