



EESSI - RINA

Functional Specifications

*Administration console
Use Cases*

Architecture & Design Specifications

Contents

1	Glossary of Terms	5
2	Document Information and Audience	5
3	Business Purpose	5
4	Introduction.....	5
4.1	Context.....	5
4.2	Scope	6
4.3	Out of scope:	6
4.4	Requirements	6
5	RINA Administration Console – Functional Specifications	17
5.1	Main Modules.....	17
6	Interface Use Cases	21
6.1	Access Control Interfaces	21
6.2	Application Settings	29
6.3	Messaging Settings	52
6.4	NIE Settings	77
6.5	RINA Archiving	85
6.6	IAM	94
6.7	Authorization	114
6.8	Notification Centre.....	146
6.9	Logs	154
6.10	Technical Logs.....	161
6.11	Automatic Updates.....	165
6.12	Test Center	176
6.13	Business Exceptions	178

Document Control Information

Document Control	Value
Project Title	Electronic Exchange of Social Security Information (EESSI)
Document Title	EESSI – RINA - Functional Requirements - Administration Portal
Document Category	Architecture & Design Specifications
Revision	-
Component Version	-
Last Publication Date Project Milestone	18/12/2020 EESSI-2020
Document Status	Final
Sensitivity (TLP) Distribution terms	Traffic Light Protocol (TLP) = "GREEN"  The distribution of this document is done strictly in line with the Traffic Light Protocol (TLP) established by the European Commission's note AC 790/15 REV for the EESSI project documentation. In line with the note AC 790/15 REV, this document is labelled as TLP = "Green". Therefore, it can be circulated widely within the EESSI community. However, the document or the information herein may not be published or posted on the Internet, nor released outside of the EESSI community.
Connected/Embedded Files	None
Authors	European Commission, DG EMPL F5, EESSI BA
Revised by	European Commission, DG EMPL F5, EESSI QA
Approved by	European Commission, DG EMPL F5, EESSI PM

Document History

Released Component version	Changes/Corrections Description
EESSI 2020	Initial Document

1 Glossary of Terms

Term/Acronym	Definition
RINA	Reference Implementation of a National Applications

2 Document Information and Audience

Purpose:

This document provides a functional description of the Reference Implementation of a National Application (**RINA – Administration Console**) from a user point of view. For this purpose, the specification describes the RINA services behaviour with a set of identified use-cases.

Audience:

- All project team members
- Project Sponsor, Business Owner, and IT/Technical Owner
- All other key stakeholders

3 Business Purpose

The free movement of people is a fundamental right in Europe. Citizens of the European Union can freely travel to other countries in the EU/EFTA space and take up residence and employment there. Modern social security systems need to reflect this mobility and make sure that citizens enjoy full access to social security in cross-border settings as well.

The Reference Implementation of a National Applications (**RINA**) is a **web-based software application** for the electronic management and exchange of social security cases across competent institutions of the participant countries. RINA is developed by the Directorate-General for Employment, Social Affairs and Inclusion (DG EMPL) and evolved out of the EESSI (Electronic Exchange of Social Security Information) project.

It fulfils the business needs – the so-called business layer requirements – for national institutions participating in the EESSI cross-border message exchange. The application supports the complete range of business use cases concerning the exchange of social security data.

4 Introduction

4.1 Context

Part of the National Institutions Domain, RINA (Reference Implementation for National Applications) consists in a collection of infrastructure and communication services, foundation, repository and publishing services, business, integration and user interface services which will provide for clerks and their organisations the tools to implement the International Protocol of Data Exchange based on Structured Electronic Documents in Social Security belonging to European Community Member States and Associated States. It is based on 4 layers which are built one on top of the other:

- **Business Messaging Services (BMS)** - provide a reusable component for sending business messages to the Access Point using the technical protocol (ebMS/AS4). These services provide the translation (business message to technical message and vice versa), transformation (converting IDs to GUIDs), validation and signing of the

business messages for correct exchange with the EESSI environment, and the correct reception of messages from other institutions.

- **Case Processing Services (CPS)** – provide a state full component built on top of the Business Messaging Services that manage cases in a structured manner taking care of all the issues regarding case flow, documents, notifications, user management and provides several interfaces for external access
- **Portal** – provides an UI (user interface) built on top of the Case Processing Services having:
 - **Case Management Console and**
 - **Administration Console**
- **CAS Authentication Server** – the SSO (Single Sign On) server providing the authentication to users/clients requesting to use a service;

4.2 Scope

The scope of this document is to provide a specification document for Administration Console, part of the Case Processing Interface (UI Portal). It covers the perspective of an IT administrator and details how a RINA instance can be configured locally or adapted to the needs of a specific institution.

4.3 Out of scope:

Additional details related to the Case Processing Interface functions and use cases, service contract, data contract and relevant samples are out of scope for this specification and can be found in other RINA related specifications:

- RINA Identity and Access Management (IAM),
- RINA National Information Exchange Interface (NIE),
- RINA Archiving,
- RINA Localisation,
- RINA High Availability and High Performance

4.4 Requirements

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoScow
EESSI.NA.001	EESSI BL Conformance	The system must fully conform to the EESSI BL specifications (BUCs)	Non-Functional	General	Must have
EESSI.NA.002	Search management requirements	The system must provide tools for users to be able to search and find cases in different ways: • free-text search • structured search • predefined structured search • combination of predefined with text search	Functional	Presentation(GUI)	Must have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
		All Searches are performed against Case Metadata			
EESSI.NA.003	Search management requirements	All Searches are performed against Case Metadata	Functional	Presentation(GUI)	Must have
EESSI.NA.004	Free-text search	A user must be able to perform free-text search in fuzzy or exact manner on case metadata in order to identify a case or a group of cases.	Functional	Presentation(GUI)	Must have
EESSI.NA.005	Predefined - Structured search	The system must allow users to define structured searches using visual search expressions and allow users to persist their searches as pre-defined searches.	Functional	Presentation(GUI)	Should have
EESSI.NA.006	Predefined - Structured search	A user must be able to add a new or modify an existing predefined search.	Functional	Presentation(GUI)	Should have
EESSI.NA.007	Predefined - Structured search	A user must be able to delete an existing pre-defined search	Functional	Presentation(GUI)	Should have
EESSI.NA.008	Applying a predefined search	A user must be able to quickly select and apply a predefined search in order to minimize searching effort.	Functional	Presentation(GUI)	Should have
EESSI.NA.009	Refine predefined search results	After the system has filtered the cases based on a users predefined search request, the user can read the list of filtered cases. The user must be able to optionally use the free text search to further refine the returned results.	Functional	Presentation(GUI)	Should have
EESSI.NA.010	Configure Search Result	A user must have the possibility to configure for each case type: • the list of columns that will be returned by the search engine • the order of the columns and • the order of the results (ascending/descending sort).	Functional	Presentation(GUI)	Should have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
EESSI.NA.011	Case management requirements	The case management requirements cover all aspects of case management, including creation of case, creation of document, creation of a counterparty list, sending documents, running case specific actions, listing cases, documents, or actions	Functional	General	Must have
EESSI.NA.012	Create case	The system must allow a user to create a case through accessing a hierarchical structure of case types	Functional	Presentation(GUI)	Must have
EESSI.NA.013	Create case	The system should retain (per session) the last case type instantiated to enable to quickly creation of another case.	Functional	Presentation(GUI)	Should have
EESSI.NA.014	Determine Exchange Partners	The system must allow the user to specify the case participant(s) for each case	Functional	Presentation(GUI)	Must have
EESSI.NA.015	Determine Exchange Partners	The system must persist the case participant (s) for each case instance	Functional	Presentation(GUI)	Must have
EESSI.NA.016	Determine Exchange Partners	The system must allow the user to view the current case participant(s) and any historical changes.	Functional	Presentation(GUI)	Must have
EESSI.NA.017	Case management actions	The system must provide users with a list of available actions (tasks) related to a specific case instance depending on the state of the case.	Functional	Presentation(GUI)	Must have
EESSI.NA.018	Case management actions	Any case action executed by a user must update the case state.	Functional	Presentation(GUI)	Must have
EESSI.NA.019	Case management actions	The system must recalculate display the available action list upon the change of case state to ensure that users can only perform actions that are correct based the case state.	Functional	Presentation(GUI)	Must have
EESSI.NA.020	Case management actions	The user must have the possibility to select one action from the action list presented to him.	Functional	Presentation(GUI)	Must have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
EESSI.NA.021	Group Case Actions	The system must provide logical grouping of case actions at case level or SED level.	Functional	Presentation(GUI)	Must have
EESSI.NA.022	Group Case Actions	The system could provide further logical grouping of case actions as case level.	Functional	Presentation(GUI)	Should have
EESSI.NA.023	Group Case Actions	The system should offer the possibility to filter case actions by grouping.	Functional	Presentation(GUI)	Could have
EESSI.NA.024	Case Importance/Criticality	A user must be able to specify the level of Importance of a case.	Functional	Presentation(GUI)	Must have
EESSI.NA.025	Case Importance/Criticality	A user must be able to specify the level of Criticality of a case.	Functional	Presentation(GUI)	Must have
EESSI.NA.026	Case Importance/Criticality	A user should be able to change the importance and criticality of a case at time during the case.	Functional	Presentation(GUI)	Should have
EESSI.NA.027	Case Importance/Criticality	The system should allow a user to set the importance/criticality of more than one case at a time.	Functional	Presentation(GUI)	Could have
EESSI.NA.028	Case Alarm	A user must be able to set an alarm by which they expect an action to have occurred.	Functional	Presentation(GUI)	Must have
EESSI.NA.029	Case Alarm	A user must be able to delete the alarm.	Functional	Presentation(GUI)	Must have
EESSI.NA.030	Case Alarm	The system must notify the user when an alarm expires.	Functional	Presentation(GUI)	Must have
EESSI.NA.031	Create Documents	The system must allow the persistence of documents in multiple draft states.	Functional	Presentation(GUI)	Must have
EESSI.NA.032	Document Validation	The system must display document validation errors in a clear and logical fashion, allowing the user to navigate directly to the source of the error from the error description.	Functional	Presentation(GUI)	Must have
EESSI.NA.033	Document Validation	Document validation must fire on the sending of a document.	Functional	Presentation(GUI)	Must have
EESSI.NA.034	Document Validation	Document validation must not fire on the saving of a draft.	Functional	Presentation(GUI)	Must have
EESSI.NA.035	Manage Document Views	The system must allow users to view all major document versions	Functional	Presentation(GUI)	Must have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoScow
EESSI.NA.036	Manage Document Views	The system could allow users to view minor document versions	Functional	Presentation(GUI)	Could have
EESSI.NA.037	Manage Document Views	The system should offer multiple views for users to view sent and received documents	Functional	Presentation(GUI)	Should have
EESSI.NA.038	Manage Document Views	The system must offer the possibility to filter documents by: • Time • Direction • Partner • Type • Status	Functional	Presentation(GUI)	Must have
EESSI.NA.039	Manage Document Views	A user must be able to clearly visualise draft documents from sent/received documents.	Functional	Presentation(GUI)	Must have
EESSI.NA.040	Manage Document Views	A user should be able to clearly visualise documents that are in different document states.	Functional	Presentation(GUI)	Should have
EESSI.NA.041	Manage Document Views	The system must offer access to view all document versions.	Functional	Presentation(GUI)	Must have
EESSI.NA.042	Manage document attachments	The user must be able to manage the attachments through attaching and detaching files.	Functional	Presentation(GUI)	Must have
EESSI.NA.043	Manage document attachments	The system must allow attachments to be added at case level or at SED level.	Functional	Presentation(GUI)	Must have
EESSI.NA.044	Manage document attachments	The user must be able to manage the attachments through attaching and detaching files.	Functional	Presentation(GUI)	Must have
EESSI.NA.045	Manage document attachments	The system must allow attachments to be added at case level or at SED level.	Functional	Presentation(GUI)	Must have
EESSI.NA.046	Manage document attachments	The system should restrict the type of attachments allowed to the following types: • application/pdf • application/msword • application/xml • image/jpeg • image/png • image/tif • text/rtf	Functional	Presentation(GUI)	Should have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
		· text/xml			
EESSI.NA.047	Manage document attachments	The system must restrict the access to attachments of a certain business type where necessary.	Functional	Presentation (GUI)	Must have
EESSI.NA.048	Manage document attachments	The system must allow users the access to read/open attachments directly.	Functional	Presentation(GUI)	Must have
EESSI.NA.049	Print Documents	The system must allow a user to choose an action that will render a document as a printable form (PSSED).	Functional	Presentation(GUI)	Must have
EESSI.NA.050	Print Documents	The system should generate Portable Documents.	Functional	Presentation(GUI)	Should have
EESSI.NA.051	Manage comments	The user must be able to create, read or delete comments (case notes) at document level or case level.	Functional	Presentation(GUI)	Must have
EESSI.NA.052	Manage comments	The system must persist and display the author and time of each comment.	Functional	Presentation(GUI)	Must have
EESSI.NA.053	Manage comments	The system must ensure only the author of a comment (or a user with special permissions) can delete a comment.	Functional	Presentation(GUI)	Must have
EESSI.NA.054	Case assignment	New Cases (both created locally & received) should be automatically assigned to users using configurable case assignment rules (via the administration console). The type rules that can be set should be based on for example: • The country concerned • The case metadata (PIN, Surname, DOB) • The outstanding workload of users	Functional	Presentation(GUI)	Should have
EESSI.NA.055	Case assignment	A user (with permission) must be able to assign a case to users or groups of users that are part of the local organisation.	Functional	Presentation(GUI)	Must have
EESSI.NA.056	Case assignment	A user (with permission) must be able to unassign/reassign a case to users or groups of users that are part of the local organisation.	Functional	Presentation(GUI)	Must have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
EESSI.NA.057	Case assignment	A user (without permission) must be able to request to a user (with permission) to assign a specific case to them.	Functional	Presentation(GUI)	Must have
EESSI.NA.058	Case assignment	A user must be able to assign/unassign/reassign more than one case at a time.	Functional	Presentation(GUI)	Must have
EESSI.NA.059	Case assignment	The system must ensure that only assigned users can actively work on/progress a case.	Functional	Presentation(GUI)	Must have
EESSI.NA.060	Case assignment	The system must restrict access to certain case types where necessary (e.g., sensitive cases)	Functional	Presentation(GUI)	Must have
EESSI.NA.061	Document Translation	A user must be able to translate a received documents content (whole document of part of) into any of the EU official languages.	Functional	Presentation(GUI)	Must have
EESSI.NA.062	Generate notifications	Every time an event condition is fulfilled, the system must notify the assigned Users of the case. Examples of events are presented below: • New message arrived; • New case arrived; • Message update; • Message delivered; • Message delivery error; • New case assigned; • New counterparty case was created;	Functional	Presentation(GUI)	Must have
EESSI.NA.063	Generate notifications	Each notification must have associated a type that is either: • Error • Alert or • Information	Functional	Presentation(GUI)	Must have
EESSI.NA.064	View notifications	Users must be able to view all their notifications through a dedicated Notifications panel.	Functional	Presentation(GUI)	Must have
EESSI.NA.065	View notifications	User should be able to view case specific notifications in the case level view	Functional	Presentation(GUI)	Should have
EESSI.NA.066	Notification actions	A user should be able to take logical actions direct from the notification	Functional	Presentation(GUI)	Should have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
EESSI.NA.067	Filter notifications	The system must offer the possibility to filter notifications based on type and status	Functional	Presentation(GUI)	Must have
EESSI.NA.068	Filter notifications	The System should offer the possibility to navigate to the notifications' timeline.	Functional	Presentation(GUI)	Should have
EESSI.NA.069	Notification Summary	The system must provide count of notification by types in the notification panel and the case level views	Functional	Presentation(GUI)	Must have
EESSI.NA.070	Notification Summary	The counts be automatically re-calculated when User take actions on the notifications	Functional	Presentation(GUI)	Must have
EESSI.NA.071	Notification Summary	A user must be able to receive anytime in every module of the application the delivery of a new notification. This must be obtrusive to the user.	Functional	Presentation(GUI)	Must have
EESSI.NA.072	Suppress/Unsuppress notification	The user must be able to suppress a notification so that it is not taken into account anymore	Functional	Presentation(GUI)	Must have
EESSI.NA.073	Suppress/Unsuppress notification	The user must be able to unsuppress a previously suppressed notification so that it is taken into account anymore.	Functional	Presentation(GUI)	Must have
EESSI.NA.074	Mark notification as read/unread	The user can mark a notification as read or unread so that the next time the notifications are displayed the read/unread state is preserved.	Functional	Presentation(GUI)	Must have
EESSI.NA.075	Report requirements	TBD			
EESSI.NA.076	Administration Console	All administrator tasks must be provided through a dedicated administrator console	Functional	Presentation(GUI)	Must have
EESSI.NA.077	User Management and organization structure	An administrator must be able to define organization units, together with departments having any level of nesting.	Functional	Presentation(GUI)	Must have
EESSI.NA.078	User Management and organization structure	An administrator must be able to define users or to refer them from an external identity management repository.	Functional	Presentation(GUI)	Must have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
EESSI.NA.079	User Management and organization structure	An administrator must be able to configure the default user settings	Functional	Presentation(GUI)	Must have
EESSI.NA.080	Authorisation policies	For each case type, the administrator must be able to configure what users or groups are allowed to create, to execute, to administer or to audit new cases. These are corresponding to the regular user roles: Clerk, Supervisor and Auditor.	Functional	Presentation(GUI)	Must have
EESSI.NA.081	Audit	The administrator must be able to configure what events the system needs to audit. The audit must reflect to all main resources exposed by the functional modules, for all possible operations: create, read, update, delete and execute.	Functional	Presentation(GUI)	Must have
EESSI.NA.082	Audit	The minimum dataset the system must audit are: • Id of event • Operation (create, read, update, delete and execute) • Username • Computer name and IP • Date and time • Component which generated the event • Outcome: Success or business error • Audited object (e.g.: case) • Participants (e.g.: person or organisation)	Functional	Presentation(GUI)	Must have
EESSI.NA.083	Technical log	All the modules of system must populate a centralised log available for Administrators.	Functional	Presentation(GUI)	Must have
EESSI.NA.084	Technical log	The administrator must be able to configure the level of logging: trace, debug, info, warn, error and fatal.	Functional	Presentation(GUI)	Must have
EESSI.NA.085	Notification Management	An administrator should be able to suspend notification types	Functional	Presentation(GUI)	Should have

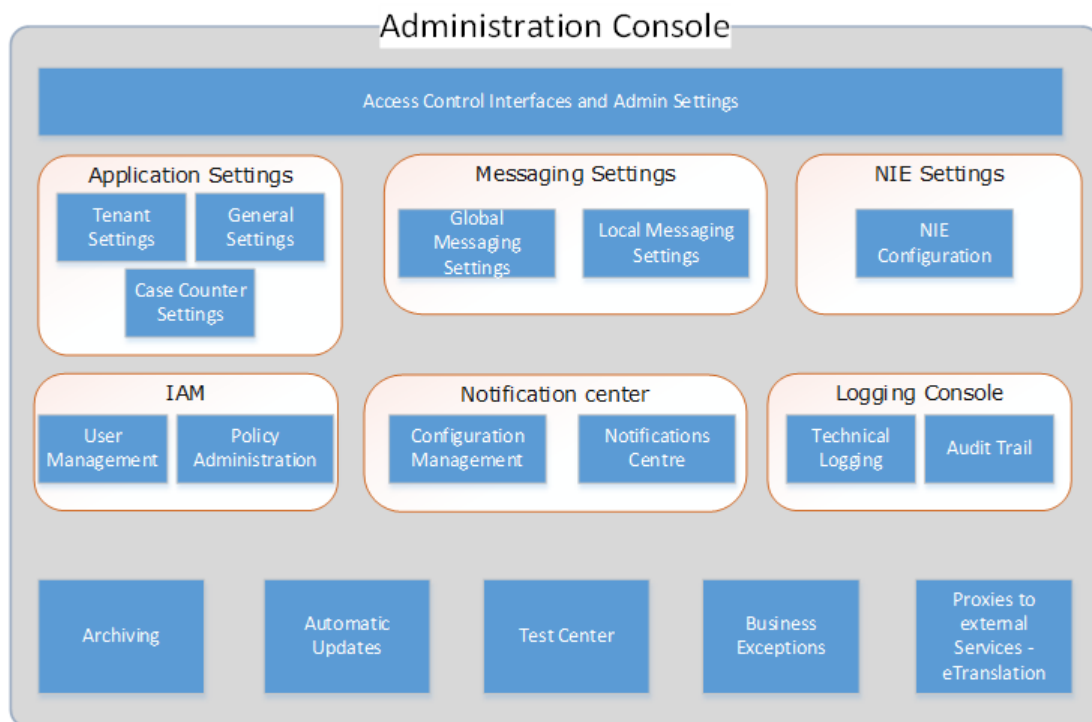
Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoScow
EESSI.NA.086	Notification Management	An administrator should be able to configure notification behaviour (i.e. how a notification is presented to a user)	Functional	Presentation(GUI)	Should have
EESSI.NA.087	System updates and versioning	The physical artefacts (forms, case behaviour, vocabularies, etc.) distributed by CSN through AP must be able to be updated by an administrator. These physical models must be accompanied with a minimum set of metadata: • Version • Date of release • Name	Functional	Presentation(GUI)	Must have
EESSI.NA.088	Messaging configuration	The messaging configurations must be fully available for administrators through the administration console	Functional	Presentation(GUI)	Must have
EESSI.NA.089	Counter management	The administrator must be able to define counters for national case ID. The policies for national case identification can be particular to a department and must have a period of availability	Functional	Presentation(GUI)	Must have
EESSI.NA.090	Retention policy (case, audit, technical log)	The system must be able to archive the closed cases, audit and technical log. The retention policy for all of this must be configurable	Functional	Presentation(GUI)	Must have
EESSI.NA.091	Dead letter Queue	The system must provide an administrator with access to received documents that it could not logically processed (i.e., unrelated documents, documents with errors)	Functional	Presentation(GUI)	Must have
EESSI.NA.092	Dead letter Queue	The system must allow the administrator to return a business exception error automatically for these documents	Functional	Presentation(GUI)	Must have
EESSI.NA.093	Dead letter Queue	The sending of business exception error could be a bulk operation	Functional	Presentation(GUI)	Could have
EESSI.NA.094	User login	Any user having the right credentials must be able to access the system. The credentials can be username and password or smartcards.	Non-Functional	Presentation(GUI)	Must have

Req. ID	Summary	Req. Statement	Req. Type	Layer(s)	MoSCoW
EESSI.NA.095	User login	The system must logout a user if the application is left idle for a pre-configurable period of time	Non-Functional	Presentation(GUI)	Must have
EESSI.NA.096	Multi-tenancy	The system must be able to host multiple institutions completely isolated between them and with independent capabilities of administration	Non-Functional	Presentation(GUI)	Must have
EESSI.NA.097	Localization	The user can decide any-time what the language of its user interface is. The user interface must act accordingly to this setting by translating all the screens together with the codified fields (vocabularies).	Non-Functional	Presentation(GUI)	Must have
EESSI.NA.098	Accessibility	The system must be WCAG 2.0 compliant to minimum AA standard.	Non-Functional	Presentation(GUI)	Must have
EESSI.NA.099	Browser Compatibility	The system must fully work in the following browsers: • Chrome (v.40 +) • Firefox (v.32+) • Internet Explorer (v.11) • MS Edge	Non-Functional	Presentation(GUI)	Must have
EESSI.NA.100	Error Handling	Application Errors must be delivered to users in an unobtrusive manner, while providing sufficient information to understand the problem	Non-Functional	Presentation(GUI)	Must have
EESSI.NA.101	Help	The system should provide context aware help for users	Non-Functional	Presentation(GUI)	Should have

5 RINA Administration Console – Functional Specifications

5.1 Main Modules

This console includes all components for administering RINA installation. The services contained are consoles used by the privileged users to administer RINA. All Tenants in the same RINA Application share the following common application configuration and administration:



Component	Description
Access Control Interfaces	The core function of Access Control Interfaces is to validate the required credentials of users, administrators or several applications accessing information or protected resources in the subsystem environment There are sub-categories that can be used: • Localization Settings: to customize the administrator portal • Change Password: to change the administrator(s)' password • Help: to receive online contextual help about the usage of the Admin Portal About RINA: to visualize the version specific information concerning the specific RINA Installation.

Component	Description
	• Login • Logout
Application Settings	The “Application Settings” component contains three major categories: • Tenant Settings: configures the Institutions/Liaison Body/etc1, that are defined as Tenants of the specific RINA Installation (via Add, Delete, Set Default and Enable/Disable actions) • General Settings: defines the general application settings • Case Counter Settings: defines the method to automatically generate the local Case ID (Case Management Identification counter)
Messaging Settings	The “Messaging Settings” component contains two major categories: • Global Messaging Settings that contain the definition of: the BMP validation method; the Authentication/Authorisation and Business Signature parameters; the transport protocol settings; the Antimalware settings; and the Clustering Nodes settings • Local Messaging Settings contains shared Local Messaging Settings that are shared between all Tenants and specific settings of each Tenant.
NIE Settings	National Information Exchange (NIE) is a RINA stateful interface that allows participating countries to exchange information with their National Legacy Applications/Systems. Additionally, NIE allows RINA to receive documents and/or be notified when configurable events occur during the lifecycle of a Case and including its documents, based on subscriptions to specific events during the case handling lifecycle at both Case and Document levels.
IAM	IAM allows configuring users and groups in RINA. The settings are distinguished and independent between each RINA Tenant. The section is split in three subsections: Users, Groups and LDAP Configuration.
Authorisation	Authorisation is the administrative screen where the Administrator configures who gets access to resources in RINA. It consists of two main sections, Assignment Policies

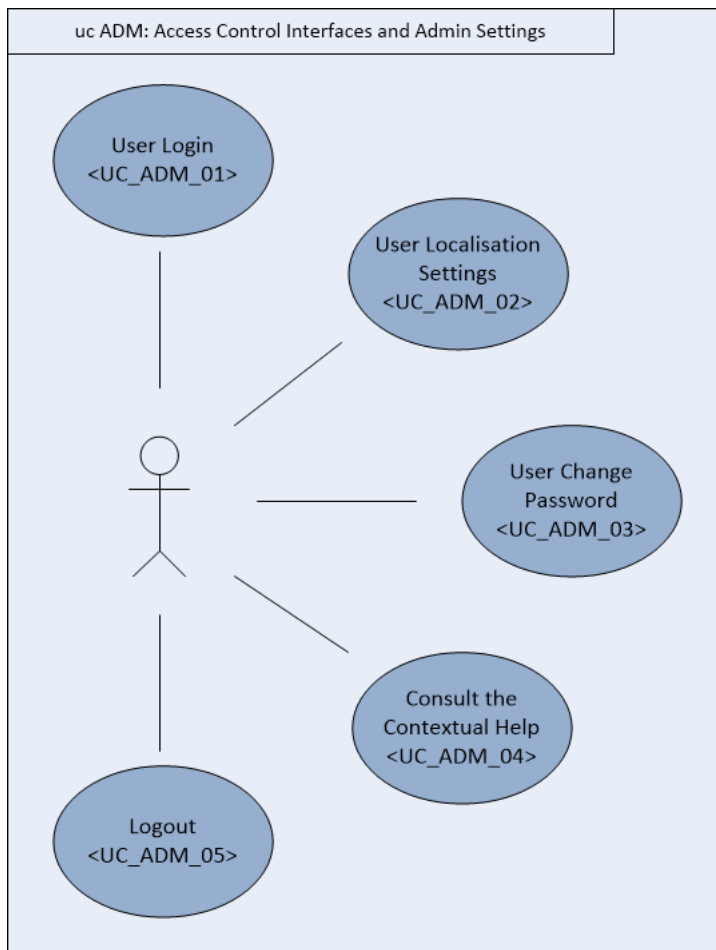
Component	Description
	and Process Assignments. Together, the policies provide the administrator with the tools required to manage and restrict control to cases in RINA
Notification Centre	The Notification Centre provides the following functions: • Configuration of the critical notifications' parameters (i.e. retention & notification periods, etc.) • List of the received Notifications with the necessary filtering and navigation tools. In general, the notifications can be filtered by severity, type, status and grouped by date. Also, the navigation functionality can be used to easily select the notification of a specific time period.
Logging Console	The logging consoles (Audit Logs & Technical Logs) package provides the detailed views on the logs created at RINA deployment level. It contains consoles to access the technical logs and audit trails.
Archiving	Data archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention. Archive data consists of: • data that is not currently used but it is still important to the organization and it has to be available for any future reference, as well as • data that must be retained for regulatory compliance. The data archives serve as a way of reducing primary storage consumption and related costs, rather than acting as a data recovery mechanism. A data archive that can be used for litigation situations or contains sensitive data, should be treated as "read-only" in order to protect it from any modification.
Automatic Updates	The Automatic Updates component is used to synchronise/configure either IR (Institution repository) or CDM (Common Data Model) retrieved from CSN, through the AP component.
Test Centre	This Test Center component allows performing basic testing of RINA's network connectivity to EESSI International Domain.
Business Exceptions	The Business Exceptions component provide access to the settings related to operations on Business Exceptions and Pending Messages, such as: • Retrieve the business exceptions details • Submit a business exception • Retrieve the business exceptions time slots

Component	Description
	• Retrieve the SED content of the business exception • Retrieve the rejection SED content of the business exception • Retrieve the pending messages details • Retrieve the pending messages time slots • Retrieve the SED content of the pending message

6 Interface Use Cases

6.1 Access Control Interfaces

Use case diagrams



Use Case View

UC_ADM_01 Login Administrator

Use Case ID:	UC_ADM_01		
Use Case Name:	Login Administrator		
Created By:	Mihaela Manolache	Last Updated By:	
Date Created:	04.03.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case (UC) describes how the Administrator can Login and get access to the functions related to the relevant role. This UC is performed in two steps: authentication (verification of the user identity using the submitted password) and authorization (granting access to the functions/data of the system according to the role of the user).		

Trigger:	The Administrator opens a Web browser and types in the RINA application URL of the institution.		
Preconditions:	N/A		
Post conditions:	The Administrator can perform any action he is authorized to in the system.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator opens a Web browser and types in the RINA application URL of the institution.	The System opens "RINA Home Page". This page contains a <i>Login</i> button
	2	The Administrator clicks "Login" button	The System opens "RINA Login Page". The System displays a notification in case a non-secure URL connection is established, in order to inform the Administrator. This page contains: • A free text field labelled "Username:" where the Administrator enters his/her username • A free text field labelled "Password:" where the Administrator enters his/her password • A Login button
	3	The Administrator enters the username and relevant password and clicks "Login" button	The System validates the provided credentials. The System redirects the Administrator to "RINA Admin Console". The System navigates the user to the home screen, which follows a certain basic structure throughout the application. The "RINA Admin Console" screen layout consists in the following menu options: 1. "Application Settings" 2. "Messaging Settings" 3. "NIE Settings" 4. "RINA archiving" 5. "IAM" 6. "Authorization" 7. "Logs" 8. "Notifications Centre" 9. "Automatic updates" 10. "Test Center" 11. "Business exceptions"

Exception Flow 1		The Administrator enters wrong credentials (username or password)	The Administrator authentication fails. The System displays the login page with the following error message: "Invalid credentials".
-------------------------	--	---	--

UC_ADM_02 Set up User Localization Settings

Use Case ID:	UC_ADM_02		
Use Case Name:	Set up User Localization Settings		
Created By:	Mihaela Manolache	Last Updated By:	
Date Created:	04.03.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how an Administrator can set up the localization settings: language, number format, data format, time format, currency, or time zone		
Trigger:	The Administrator clicks on the user icon from the main menu and then clicks on the "Localization Settings" option.		
Preconditions:	1. The Administrator is authenticated in RINA (UC_CPI_01)		
Post conditions:	The new localization settings are saved at user level and will be used for: • Language: All RINA UI messages (labels, value lists, error messages, notifications, etc) of the Admin Portal are given in the selected language • Number/Date/Time format and Time Zone: displays the Numbers, Dates and Time in the selected format and the correct Time Zone is applied • Currency: currently not used		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the user icon from the main menu.	The System displays a contextual menu with the following menu options: • "Localization Settings" • "Change Password" • "Help" • "Logout"
	2	The Administrator clicks on the "Localization Settings" option	The System displays "Localization Settings" form. This page contains: • a drop-down list field labelled "Language *" where the user can select the language of the UI. The languages used by the

			participating countries are available • a drop-down list field labelled "Number Format *" where the user can select the format of numbers. The possible options are: ○ 1.000,00 ○ 1,000.00 ○ 1 000.00 ○ 1000,00 ○ 1000.00 ○ 1 000,00 • a drop-down list field labelled "Date Format *" where the user must select the format of the date from the provided list of available date formats • a drop-down list field labelled "Time Format *" where the user must select the default time format • a drop-down list field labelled "Currency *" where the user must select the default currency from the list of available currencies • a drop-down list field labelled "Time Zone *" where the user must select the default time zone from the list of available time zones. The "*" character from all the labels of the fields mean that they are mandatory. All the fields are pre-populated with default values (as per set up of the administrator). The form also contains: - "Reset" button - "Save" button - "Back" button
	3	The user selects the desired values of the localization fields and clicks on the "Save" button	The System closes "Localization Settings" form. The System saves all values in the server. Remark:

			• "Language". The selected language is applied: - for all the labels and list of values displayed in RINA screens and for all the error messages text - for the <i>Translate</i> link inside the received SEDs • "Number/Date/Time Format" and "Time Zone": the specific values are displayed in the selected format
Alternate Scenario 1		The Administrator make changes in one or more fields and clicks "Reset" button	The value(s) on the field(s) are discarded and the fields values are reloaded from the server.
Alternate Scenario 2		The Administrator clicks "Back" button	The System closes "Localization Settings" form and returns to previous form.
Exception Flow 1		The Administrator selects the blank value for one or more fields and clicks on the "Save"	The System displays the field(s) with blank value and displays them marked in red.

UC_ADM_03 Change Administrator Password

Use Case ID:	UC_ADM_03		
Use Case Name:	Change Administrator Password		
Created By:	Mihaela Manolache	Last Updated By:	
Date Created:	04.03.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how an Administrator changes his own password		
Trigger:	The Administrator clicks on user icon and then clicks "Change Password" option.		
Preconditions:	The Administrator is authenticated in RINA		
Post conditions:	The Administrator password is changed and can be used for future logins		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the user icon from the main menu.	The System displays a contextual menu with the following options: • "Localization Settings" • "Change Password" • "Help" • "Logout"

	2	The Administrator clicks "Change Password" option	The System displays "Change Password" form. This page contains: • a free-text field labelled "Old password*:" where the Administrator must enter his current password • a free-text field labelled "New password*:" where the Administrator must enter the new password • a free-text field labelled "Confirm new password*:" where the Administrator must enter again the new password As the * from all the fields suggests, all are mandatory. The form also contains: - "Reset" button - "Save" button - "Back" button
	3	The Administrator enters the old and the new password in the dedicated fields and clicks on the "Save" button.	The System compares values entered in fields "Old password" and "New password" of the user. The System saves the new password in the server which can be used for future logins. The System closes "Change password" form.
Alternate Scenario 1	1	The Administrator make changes in one or more fields and clicks on the "Reset" button	The value(s) on the field(s) are discarded and the fields values are reloaded from the server.
Alternate Scenario 2	1	The Administrator clicks on the "Back" button	The System closes "Change Password" form and returns to previous form.
Exception Flow 1	1	The Administrator enters different values in fields "New password*:" and "Confirm new password*:" and clicks on "Save" button	The System displays the field "Confirm new password: *" marked in red and an error message is displayed under the field: "Password must match". The Administrator can re-enter the value for this field and resume the main scenario.

Exception Flow 2	1	The Administrator enters a wrong value in the "Old password: *" field and values for the new and old password and clicks on the "Save" button	The System displays the error message: "Old password of user does not match". The Administrator can re-enter the value for this field and resume the main scenario
Exception Flow 3	1	The Administrator enters a value shorter than 8 characters in the "New password: *" field and leaves the field.	The System marks the field "New password: *" in red and an error message is displayed under the field: "Password must be at least 8 characters" The Administrator can re-enter the value for this field and resume the main scenario

UC_ADM_04 Access contextual Help

Use Case ID:	UC_ADM_04		
Use Case Name:	Access contextual Help		
Created By:	Mihaela Manolache	Last Updated By:	
Date Created:	04.03.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how an Administrator accesses the Contextual Help		
Trigger:	The Administrator clicks on User icon and then clicks "Help" option.		
Preconditions:	1. The user is authenticated in RINA.		
Post conditions:	The user consulted the <i>RINA Help Manual</i> .		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the user icon from the main menu	The System displays a contextual menu with the following options: • "Localization Settings" • "Change Password" • "Help" • "Logout"
	2	The Administrator clicks on the "Help" option	The System opens in a new browser window/tab - "Rina Help Manual". The content shown is specific for the step where the user is. This window displays the content of the Administrator Manual in an easy to navigate form. This content is available only in English.

			The System displays the following fields: • A free text "Search" field where the user can enter the text and press enter to launch the search of the entered text in the content of the admin manual. The system provides/adapts the search results automatically as the Administrator types the input in the Search field • A table of content where each entry is a link that allows the Administrator to access the specific content directly
	3	The Administrator navigates via the "Search" functionality or by clicking on the topic of interest from the table on content. The Administrator has access to read the available information. Optionally the Administrator closes the browser window/tab.	The System closes "Rina Help Manual". The Administrator can also leave the "Rina Help Manual" window open and continue his/her work in RINA, and meanwhile consult needed information in the manual.

UC_ADM_05 Logout User

Use Case ID:	UC_ADM_05		
Use Case Name:	Logout User		
Created By:	Mihaela Manolache	Last Updated By:	
Date Created:	04.03.2020	Last Revision Date:	
Actors:	System administrator		
Description:	This use case describes how an Administrator can logout from the application.		
Trigger:	The Administrator clicks user icon and then clicks "Logout" option.		
Preconditions:	1. The Administrator is authenticated in RINA.		
Post conditions:	The Administrator is logged out from application.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the user icon from the main menu	The System displays a contextual menu with the following options: • "Localization Settings"

			• "Change Password" • "Help" • "Logout"
	2	The Administrator clicks on the "Logout" option	The user is logged out. The application displays the "RINA Home Page" where the user has the possibility to log in again.

Fields Details

Admin – Localisation Settings

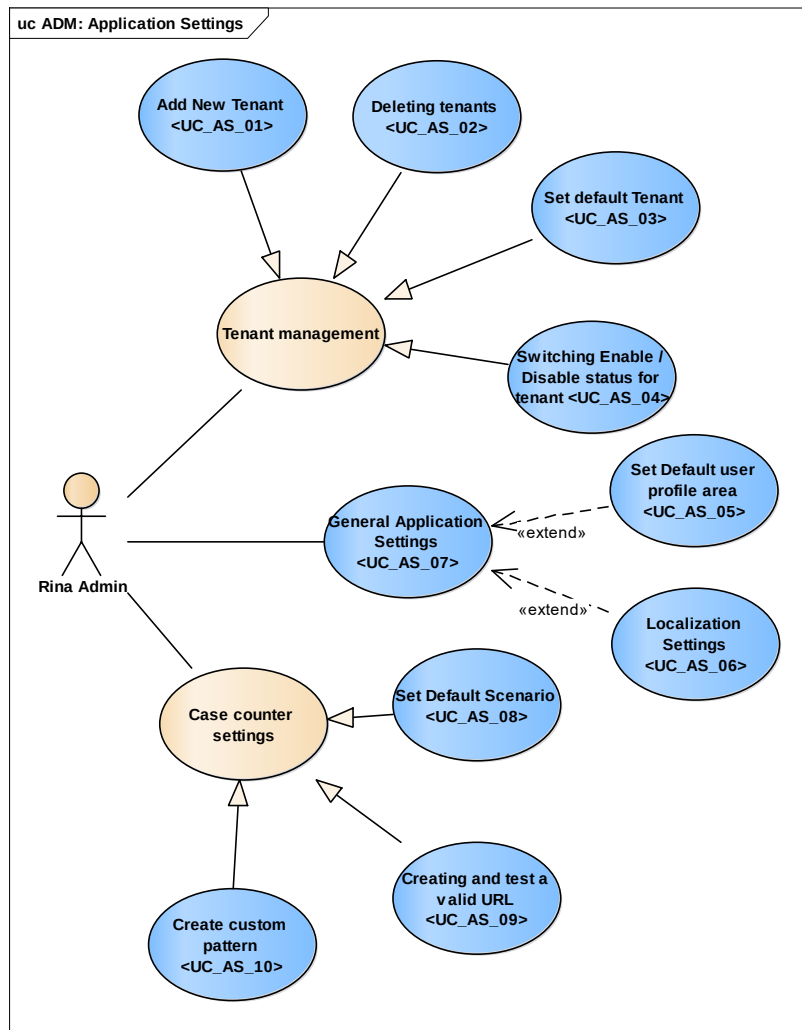
No.	Item name	Type	Validation/ business rules
1	Language	List	Mandatory, contains values chars
2	Number Format	List	Mandatory, contains numbers
3	Date Format	List	Mandatory, contains values type date
4	Time Format	List	Mandatory, contains values type time (hh:mm)
5	Currency	List	Mandatory, contains values chars
6	Time Zone	List	Mandatory, contains values type zone
7	Save	Button	
8	Reset	Button	

Admin – Change Password

No.	Item name	Type	Validation/business rules
1	Old password	Free text box field	Mandatory, use visible/invisible functionality
2	New password	Free text box field	Mandatory, use visible/invisible functionality
3	Confirm new password	Free text box field	Mandatory, use visible/invisible functionality
4	Save	Button	
5	Reset	Button	

6.2 Application Settings

Use case diagrams



Use Case View

UC_AS_01 Add new tenant

Use Case ID:	UC_AS_01		
Use Case Name:	Add new tenant		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	14.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds a new tenant (The Administrator defines and configures the Institutions that are defined as Tenants in the RINA)		
Trigger:	The Administrator clicks on "Application Settings" menu option and then "Tenant Settings" option.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system. 3. The institution to be added as Tenant belongs to the same AP as the Default Tenant and they are part to the Institution Repository (IR).		

Post conditions:	The new Tenant is added, and it is visible in the system. The list with existing tenants is updated accordingly. The simple addition of a new Tenant is not enough to have a fully functional Tenant. For a Tenant, new or existing, to be operational, all its tenant specific configurations should be successfully completed ("Valid Messaging Configuration", "IAM" and "Authorization Settings", "Case Counter Settings").		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Tenant Settings" option from "Application Settings" menu option	The System displays "Tenant Settings" form, containing: • a field labelled "Add Tenant" with Institution free text "Search" functionality enabled. Only institutions belonging to the same AP as the Default tenant are available. • a button "+" disabled • a button "x" disabled • a grid displaying the existing tenants, with the following header ◦ "Tenant": column for displaying the institution identifier ◦ "Is Default": column for displaying if tenant is the default one ◦ "Status" ◦ "Actions", with associated buttons "Set Default", "Enable", "Delete". For the default tenant, the "Actions" column is empty. • "Refresh" button
	2	The Administrator starts typing in the "Add Tenant" field.	The System display a list with institutions which meet the criteria.
	3	The Administrator selects the desired institution from the list	The System display the selected institution in "Add Tenant" field and the "+" and "x" buttons are enabled.
	4	The Administrator clicks on the "+" button.	The System displays the "Confirmation" form, which contains: • The following text field "You are about to add the tenant:" and the identification attributes of the selected institution • "Yes" button • "No" button
	5	The Administrator clicks on the "Yes" button	The System closes "Confirmation" pop-up window. The System displays the messages: "Tenant settings successfully added".

			"Please update the Local Messaging Settings of the newly added Tenant." The list with tenants is updated accordingly and the new added tenant is displayed in the grid of tenants. In the "Status" column, the new tenant has the value "Disabled". Remark: The simple addition of a new Tenant in the "Tenant Settings" form is not enough to have a fully functional tenant. The Administrator also needs to specify: • The valid messaging configuration: "Global Messaging Settings" and "Local Messaging settings" should be modified and set accordingly. ◦ Authorisation Private Key and Business Signature default certificate of the Tenant should be added in the Global Messaging Settings ◦ Next, the above elements should be paired with their passwords in the Local Messaging (Tenant) Settings • The IAM and Authorisation Settings for the new Tenant should also be modified accordingly. In more details: ◦ At least one Group and one regular User should be added for the new Tenant ◦ The user should have at least membership "Supervisor" and "Authorized" to this Group to be assigned with enough access rights in each case instance ◦ A "Case Creator" Assignment Policy and a "supervisor" Assignment Policy should be added and related to this User. Both policies could be grouped to a group policy ◦ For each sector and BUC, for this user to be automatically assigned (either in case of Case Owner or Counter Party) to case instances, the previous "creator" and "supervisor" policy (or the
--	--	--	---

			group policy) should be assigned to the relevant processes. The Case Counter Settings. The Case Counter Settings are Tenant dependent, and it is not necessary to be configured by the administrator since a default value is used.
Alternative scenario 1	1	The Administrator clicks the "No" button	The System discards all changes. The System closes "Confirmation" pop-up window
Alternative Scenario 2	1	The Administrator clicks "Refresh" button	The System redisplay the form "Tenant Settings".

UC_AS_02 Deleting tenants

Use Case ID:	UC_AS_02		
Use Case Name:	Deleting tenants		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	14.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator deletes a Tenant		
Trigger:	The Administrator clicks "Application Settings" menu option, clicks on "Tenant Settings" option and then clicks in the "Delete" button.		
Preconditions:	- The user is authenticated in RINA. - The user is authorized as an administrator of the system. - The tenant has no active cases (cases which are not closed or archived) or business Users. - The tenant is not set as a Default tenant		
Post conditions:	The system removed the tenant from the tenant's list, the tenant will no longer be visible on the list.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Application Settings" menu option, "Tenant Settings" option	The System displays "Tenant Settings" form, containing: - a field labelled "Add Tenant" with Institution free text "Search" functionality enabled. Only institutions belonging to the same AP as the Default tenant are available. - a button "+" disabled - a button "x" disabled - a grid displaying the existing tenants, with the following header

			○ "Tenant": column for displaying the institution identifier ○ "Is Default": column for displaying if tenant is the default one ○ "Status" ○ "Actions", with associated buttons "Set Default", "Enable", "Delete". For the default tenant, the "Actions" column is empty. ○ "Refresh" button
	2	The Administrator identifies the tenant to be deleted in the display grid and clicks on the "Delete" button from the "Actions" column	The System displays the "Confirmation" form. In this form, the Administrator has available: • the message: "You are about to delete the tenant" and the identification attributes of the institution to be deleted as tenant. • "Yes" button • "No" button – when clicked, it closes the "Confirmation" form, without saving the deletion.
	3	The Administrator clicks on the "Yes" button	The System deletes the existing institution as a Tenant from the RINA instance. The System closes the "Confirmation" form. The list with tenants is updated accordingly, and the deleted tenant is no longer displayed in the tenants' grid.
Alternative Scenario 1	1	The Administrator clicks "Refresh" button	The System redisplay the form "Tenant Settings".
Exception flow 1	1	The Administrator identifies for deletion a tenant that still has active cases and/or users and clicks on the "Delete" button	The System displays the error message: "Error deleting tenant: Cannot delete tenant <Institution Identifier> because it contains active cases!" The System does not delete the tenant.

UC_AS_03 Set Tenant as default

Use Case ID:	UC_AS_03
---------------------	-----------------

Use Case Name:	Set tenant as default		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	14.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator sets a Tenant as Default tenant		
Trigger:	The Administrator clicks "Application Settings" menu option, clicks on "Tenant Settings" option and then clicks "Set Default" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The System sets up the Default tenant (the Default Tenant cannot be deleted, "Set default", "Disable", "Delete" buttons are not available)		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Application Settings" menu option, "Tenant Settings" option	The System displays "Tenant Settings" form, containing: - a field labelled "Add Tenant" with Institution free text "Search" functionality enabled. Only institutions belonging to the same AP as the Default tenant are available. - a button "+" disabled - a button "x" disabled - a grid displaying the existing tenants, with the following header "Tenant": column for displaying the institution identifier "Is Default": column for displaying if tenant is the default one "Status" "Actions", with associated buttons "Set Default", "Enable", "Delete". For the default tenant, the "Actions" column is empty. "Refresh" button
	2	The Administrator identifies the tenant to be set as default in the display grid and clicks on the "Set Default" button from the "Actions" column	The System displays the "Confirmation" form. In this form, the Administrator has available: - the information message: "You are about to set as default the tenant:" and the identification attributes of the institution that was selected "Yes" button

			• "No" button
	3	The Administrator clicks "Yes" button	The System closes "Confirmation" form. In the tenants' grid, the details of the selected tenant and the old default tenant are updated accordingly: • the selected tenant is set as Default tenant • for the old default tenant, in the "Is Default" column, the values is changed to not default and in the "Actions" column the associated buttons "Set Default", "Enable", "Delete" are displayed
Alternative Scenario 1	1	The Administrator clicks "No" button	The System discards all changes. The System closes the "Confirmation" form.
Alternative Scenario 2	1	The Administrator clicks "Refresh" button	The System redisplayes the form "Tenant Settings".

UC_AS_04 Switching Enabled / Disabled status for tenant

Use Case ID:	UC_AS_04		
Use Case Name:	Switching Enable / Disable status for tenant		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	14.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator switches the "Enabled/Disabled" status for tenants by clicking on the appropriate button (for enabled status the associated icon is green, for disabled status the associated icon is red; enabled status gives the possibility to insert, change parameters)		
Trigger:	The Administrator clicks "Application Settings" menu option, then "Tenant Settings" option and clicks "Enable/Disabled" button		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access RINA Application with the Administrator role 3. The tenant should not be set up as Default tenant		
Post conditions:	The user switches between Enable/Disable tenant status		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Application Settings" menu option, "Tenant Settings" option	The System displays "Tenant Settings" form, containing: • a field labelled "Add Tenant" with Institution free text "Search" functionality enabled. Only institutions belonging to the same

			AP as the Default tenant are available. • a button "+" disabled • a button "x" disabled • a grid displaying the existing tenants, with the following header ◦ "Tenant": column for displaying the institution identifier ◦ "Is Default": column for displaying if tenant is the default one ◦ "Status" ◦ "Actions", with associated buttons "Set Default", "Enable", "Delete". For the default tenant, the "Actions" column is empty. "Refresh" button
	2	The Administrator clicks on the "Enabled/Disabled" button	The System displays the "Confirmation" form. In this form, the Administrator has available: • An information message: "You are about to disable the tenant:" and the identification attributes of the institution that was selected • "Yes" button • "No" button
	3	The Administrator clicks on the "Yes" button	The System closes the "Confirmation" form. Notes: In case the Administrator clicks on the "Disable" button, the "Status" column is updated with status "Disabled" and the "Set Default" button is disabled. (a disabled tenant cannot be set as Default). In case the Administrator clicks on the "Enable" button, the "Status" column is updated with status "Enabled" and the "Set Default" button is enabled.
Alternate Scenario 1	1	The Administrator clicks "No"	The System discards all changes. The System closes the "Confirmation" form.
Exception flow 1	1	The administrator clicks on the "Disable" button corresponding to a	The System checks opened cases related to this institution.

		tenant that has active cases	The System does not allow disabling tenants in opened cases.
	2	The Administrator clicks "Yes" for confirming the existence of opened cases related to this institution	The System display a warning message. The System disable the action.
Alternative Scenario 2	1	The Administrator clicks "No" for confirming the non-existence of opened cases related to this institution	The System discards all changes. The System closes "Confirmation" pop-up window.

UC_AS_05 Set Case Settings Default area

Use Case ID:	UC_AS_05		
Use Case Name:	Set Case Settings Default area		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	14.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator fills in and sets up the Case Settings default area.		
Trigger:	The Administrator clicks on the "Default Case Settings" option from "Application Settings" menu option.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator set up Default Case Settings area. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Default Case Settings" option, from "Application Settings" menu option	The System displays the "Default case Settings" form, with the following fields: • an area labelled "Documents", used to define the Documents preferable View and the way of sorting, with: ○ a selection field labelled "View mode"– with possible values "Classical View" and "Timeline View" ○ a selection field labelled "Sort by"– with possible values "Creation" and "Last Update" ○ a check box field labelled "Display Flags" • a dynamic area, labelled and populated based on the selection in the "View Mode" field

			• an area labelled "Alarm Settings", with: ○ a checkbox field -when clicked it enables the counter field for setting up the number of days ○ a counter field that allows the user to set up a numerical value for the number of days for the alarm. • a "Reset" button • a "Save" button
	2	The Administrator select the "Classic View" value for the "View Mode" field	The dynamic area is labelled "Classic View", and contains: ○ a checkbox field labelled "Group by Month"
	3	The Administrator chooses to check/uncheck the flag "Display Flags"	The System displays the checked/unchecked "Display Flags"
	4	The Administrator chooses to check the checkbox field "Auto set Alarm on Send Action", related to "Alarm Settings" area	The System enables the counter field where the Administrator can input the number of days.
	5	The Administrator chooses to uncheck the checkbox field "Auto set Alarm on Send Action", related to "Alarm Settings" area	The System disables the counter field.
	6	The Administrator clicks on the "Save" button.	The System displays the message "Case Settings successfully saved".
Alternative scenario 1	1	The Administrator select the "Timeline View" value for the "View Mode" field	The dynamic area is labelled "Timeline View", and contains: a selection field labelled "Display Mode" with possible values "1 Column" and "2 Columns"
Alternative Scenario 2	1	The Administrator clicks the "Reset" button	The System redisplay the form "Default Case Settings".

UC_AS_06 Set User Profile Default Area

Use Case ID:	UC_AS_06		
Use Case Name:	Set User Profile Default area		
Created By:	Madalina Alecsandrescu	Last Updated By:	

Date Created:	14.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator fills in the "Default User Profile" available options.		
Trigger:	The Administrator selects "Default User Profile" option from the "Application Settings" menu option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as RINA administrator		
Post conditions:	The Administrator set up the "Default User Profile" options. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Default User Profile" option, available from the "Application Settings" menu option.	The System displays the "Default User Profile" form with following mandatory drop-down list fields: • "Language*" – contains all European languages • "Number Format*" – 6 possible number formats are available as described in the relevant field of UC_ADM_02 • "Date Format*" – includes all types of data format • "Time Format*" – includes all types of time format • "Currency*" – includes all types of European currencies • "Time zone*" – all time zones (All the settings are applied to all RINA users as default settings. After any customisation at user level, the user does not use the default setting but the customised ones)
	2	The Administrator chooses from mandatory drop-down list fields his preferences and clicks on the "Save" button	The System displays the message "Default User Profile successfully saved". The System saves the settings related to "Localization Settings" section.
Alternative Scenario 1	1	The Administrator clicks on the "Reset" button	The System discards all value(s) from the field(s) and the fields values are reloaded from the server.

UC_AS_07 Set up main area parameters

Use Case ID:	UC_AS_07		
Use Case Name:	Set Up Main Area Parameters		
Created By:	Madalina Alecsandrescu	Last Updated By:	

Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator sets up Main Area parameters		
Trigger:	The Administrator clicks on the "General Settings" option from "Application Settings" menu option		
Preconditions:	1. The user is authenticated in RINA 2. The user is authorized as RINA administrator 3. The user is performing updates only related to the fields in the main section		
Post conditions:	The Administrator has setup main area parameters. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "General Settings" option available from "Application Settings" menu option	The System displays the "General Settings" form with the following fields: • "Use Application Id": ◦ with a checkbox field – when selected, the free text field is enabled. ◦ a free text field for entering the identifier of the application id to be used. This setting is used to identify the sending and receiving application for "Intelligent routing" on AP level. The "Intelligent Routing" function can automatically route messages depending on certain attributes. One of the attributes is the "Application Id". For example, one institution could have different RINA deployments which use the same Institution Id, but different Application Ids based on different competences; one "Application Id" can be used for Pensions and Sickness sectors (i.e., "application1") and another one for AWOD (i.e., "application2"). • "Languages*": This option allows the administrator to select the list of the languages available to all users of this application. A default language proposed to new users (along with other settings) is defined in the "Default User Profile" form. • "Max Idle Time (in minutes) *": The Administrator can configure and set the "Maximum Idle Time" for the users/clients until disconnecting them from the system. The default value is set to 15 minutes and the timer is reset by any action of the GUI. The

		duration of the connection of the users/clients to RINA depends also to the thresholds that have been set for the Session time (these timers are refreshed only when a CPI call is performed). • "Organization System Password": Sets the Organization system password (System User Password) that is the password of the BPM engine. • An area labelled SEDs where the Administrator has available: ○ a checkbox field labelled "Validate SEDs in Client" – when checked the validation is performed on the client-side (outcome is visible on User Portal level when users trigger the prepared SEDs to get saved and/or sent). Turning this option off (not recommended), the application allows the SED saving and sending without performing any validation. ○ a selection field labelled "SED Validation Mode", where the Administrator can configure how the application should validate a SED. For this, the following 3 options are available to choose from: ▪ "Continue When No Validation" – when selected, the validation is activated but the process continues even if validation criteria are not met ▪ "Exception When No Validation" – when selected the process does not continue when an exception occurs ▪ "No Validation"- when selected, no validation is performed, and the SED can be saved/submitted anyway ○ a counter field labelled "Maximum number of Child Documents in Bulk SED *" – mandatory list box, allows to setup the limit for the number of child documents (individual claims) under the bulk SEDs (containing the global claims).
--	--	--

			• An area labelled Errors, containing the following fields: ◦ a checkbox field labelled "Show Full Error Information"- when checked, the application provides more information in the stack trace in case of an error. By default, this is not enabled. ◦ a checkbox field labelled "Show Process Version" - when checked, the application shows the version of a process (BUC) along with its name. By default, this is not enabled, but it can be used for testing or other purposes. • An area labelled "Attachments" that contains: ◦ a free text field labelled "Attachment Directory Path *" ◦ a counter field labelled "Attachment Maximum File Size (in MB)" – allows the Administrator to set the maximum file size of case attachments (per attachment) that can be uploaded in RINA application. The default value is 10Mbytes and the maximum permitted value is 1.024 Mbytes. ◦ a selection field labelled "Attachment Allowed Mime Types" that: ▪ displays the allowed file types that may be attached to a case/SED ▪ allows the Administrator to delete a predefined file type from the list by clicking on [x] ▪ allows the Administrator to add other types that are not included by clicking on ADD button associated to a text field in bottom of the section. • an area labelled "Default Values (Importance – Criticality)" where the default importance and criticality levels for new cases that will be submitted can be configured. This area contains the following fields: ◦ a selection field labelled "Importance" where the
--	--	--	---

			Administrator can select from possible values "Normal" and "High" ○ a selection field labelled "Criticality" where the Administrator can select from possible values "Normal" and "High" The importance/ criticality may be changed for each case afterwards; this just sets the implicit/default values. • a "Reset" button • a "Save" button
	2	The Administrator selects the desired values and clicks on the "Save" button	The System saves the data on server. The System displays the message: "General Settings successfully saved."
Alternative scenario 1	1	The Administrator clicks on the "Reset" button	The system discards all values changed by the Administrator and displays the values saved on server.

UC_AS_08 Set Up Case Counter Settings – Default Scenario

Use Case ID:	UC_AS_08		
Use Case Name:	Set Up Case Counter Settings – Default Scenario		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator sets the method to be used when generating the local Case IDs and Business IDs as a default sequence provided by the counter engine. The "Case Counter Settings" are defined per Tenant.		
Trigger:	The Administrator clicks on the "Case Counter Settings" option from "Application Settings" menu option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system. 3. The user defined a Tenant		
Post conditions:	The Case Counter Settings have been setup as a Default type for a Tenant and the counter to be used when generating the Local Case ID/Business ID is generated by the counter engine.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Case Counter Settings" option from	The system displays the form "Case Counter Settings" with the following fields

		"Application Settings" menu option	- A drop-down list field labelled "Select Tenant" which contains the available tenants. - A selection field labelled "Type" with available values: "Default", "HTTP Call back", "Pattern"
	2	The Administrator selects the value "Default" in the "Type" field.	The system displays, under the "Type" field, the message: "Internal sequence for all cases will be used"
	3	The Administrator clicks "Save" button	The system displayed the message "Case counter settings successfully saved", changes regarding this section are saved for the tenant (<i>the Local and the Business Case IDs are set to the same integer value that automatically generated by the platform internal counter engine (the Local Case ID changes after Case archiving/unarchiving)</i>)

UC_AS_09 Creating and test a valid URL

Use Case ID:	UC_AS_09		
Use Case Name:	Creating and test a valid URL		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator sets the method to be used when generating the Business IDs as the "HTTP callback" type and tests the given URL validity. This URL is called every time a new case is created, and it is in the implementation responsibility to ensure the uniqueness of the IDs.		
Trigger:	The Administrator clicks "Case Counter Settings" option from "Application Settings" menu option		
Preconditions:	- The user is authenticated in RINA. - The user is authorized as an administrator of the system. - The user has defined a Tenant		
Post conditions:	A valid URL has been configured and the counter to be used when generating the Business Id is received through an integration with an external provider that generates IDs		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Case Counter Settings" option from "Application Settings" menu option	The system displays the form "Case Counter Settings" with the following fields

			- A drop-down list field labelled "Select Tenant" which contains the available tenants. - A selection field labelled "Type" with available values: "Default", "HTTP Call back", "Pattern"
	2	The Administrator clicks on "HTTP Call Back" type	The system displays on the new screen: - a free text field labelled "URL" where the Administrator can provide the URL of the external provider. - a "Test" button – enables the Administrator to test the provided URL to check its validity by pressing the "Test" button,
	3	The Administrator enters a value in the "URL" and clicks on "Test" button (In case the URL is correctly introduced (http:// or https://) the button "Test" is enabled)	The URL is called, and the outcome is communicated to the Administrator.
	4	The Administrator clicks "Save" button	The System saves data on server. The System displays message "Case Counter Settings Successfully Saved". (The URL is called always when a case is created, and it is the implementation responsibility to ensure the uniqueness of the IDs. RINA issues a GET request to the specified URL and use whichever string that gets received in response as the business ID parameter.)
Exception flow 1	1	The Administrator inserts a wrong URL	The system does not permit to update fields, "Test" button remains disabled

UC_AS_10 Create custom pattern

Use Case ID:	UC_AS_10		
Use Case Name:	Create custom pattern		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		

Description:	This use case describes how the Administrator sets the method to be used when generating the Business IDs as a Pattern string.		
Trigger:	The Administrator clicks "Case Counter Settings" option from "Application Settings" menu option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system. 3. The user defined a Tenant		
Post conditions:	The system has created a string Pattern for the automatically generated Business Case ID values.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Case Counter Settings" option from "Application Settings" menu option	The system displays the form "Case Counter Settings" with the following fields • A drop-down list field labelled "Select Tenant" which contains the available tenants. • A selection field labelled "Type" with available values: "Default", "HTTP Call back", "Pattern"
	2	The Administrator clicks "Pattern" type button	The system displays: • a free text field labelled "Pattern*" where: ◦ the Administrator can enter text ◦ the System adds text during the creation of the pattern, based on the Administrator selection. • an area with parameters that contains the list of main parameters that can be used to construct the required pattern: ◦ "<BUC_TYPE>", ◦ "<SECTOR>", ◦ "<SECTORSHORT>" ◦ "<SEQ (global,1000,10)>" with 3 associated field: ▪ a drop-down list field with possible values "global", "buc", "sector" ▪ 2 free-text fields that allow only numerical values (offset and minimum length) ◦ "<DATE (dd/MMM/yyyy)>" with an associated drop-down list, which contains all data formats). Each parameter has available an "Add" button.
	3	The Administrator clicks on the "Add" button of	The string "<BUC_TYPE>" is added in the "Pattern" field. This keyword

		the "<BUC_TYPE>" parameter.	means that the construction algorithm shall put the relevant BUC type (i.e., P_BUC_01) at the specific place of the Case ID string.
	4	The Administrator clicks on the "Add" button of the "<SECTOR>" parameter.	The string "<SECTOR>" appears in the Pattern field. This character sequence shall be replaced by the Case sector name (e.g., <Pensions>)
	5	The Administrator clicks on the "Add" button of the "<SECTORSHORT>" parameter.	The string "<SECTORSHORT>" appears in the Pattern field. This character sequence shall be replaced by the Case short name ID (e.g., the letter 'P' for Pensions)
	6	The Administrator selects from List of Patterns "<SEQ(NAME, OFFSET, MINIMUM_LENGTH)>" and chooses from drop-down list box a value, inputs a value from the second text box field and inputs a value in the second text box field and clicks "Add" button	The string "<SEQ(NAME, OFFSET, MINIMUM_LENGTH)>" appears in Pattern field. This character sequence shall be replaced by a sequence number in the defined format. The pattern must be defined with three parameters, which influence the look and context of the sequence number. The attributes are explained below: • NAME – name of the sequence. There are three available sequence types: ◦ <i>Global</i> – incremental number for all the cases of the tenant (institution) ◦ <i>BUC</i> – incremental number for all the cases of the given BUC type. This is evaluated when the case is created, i.e., the BUC type is known ◦ <i>Sector</i> – incremental number for all the cases of the given sector type. This is evaluated when the case is created, i.e., the sector type is known. • OFFSET – defines the offset, which will be added to the generated number. Must be an integer value. Example: if the generated number was 10 and the offset set to 1000, the final sequence number will be 1010 • MINIMUM_LENGTH – defines the minimum length of the generated sequence number. If the character length of the generated number is shorter than the minimum length, it will be padded with zeros '0'. Example: if the

			generated sequence number was 1234 and the minimum length is set to 8, the final sequence string will be 00001234.
	7	The Administrator selects from List of Patterns "<DATE(dd/MMM/yyyy)>" and chooses a format date from the associated drop-down list and clicks on green icon associated	The string "<DATE(dd/MMM/yyyy)>" is added in the "Pattern" field. This character sequence will be replaced by the date of the case creation in the given format.
	8	The Administrator clicks "Save" button	The system displayed the pop-up message "Case Counter Settings successfully saved".

Fields Details

Application Settings – Tenant Settings

No.	Item name	Type	Validation/business rules
1	Tenant	Free text field	Enabled Search - Look up to IR local repository.
2	(List of tenants)	Grid	"Tenant": column for displaying the institution identifier((format: BE:PCTNA05, PCTNA05, PCTNA05, BE represent Country: Institution, Institution, Country) - o "Is Default": column for displaying if tenant is the default one - o "Status" - o "Actions", with associated buttons "Set Default", "Enable", "Delete". For the default tenant, the "Actions" column is empty.
3	Add Tenant	Button	
4	Refresh	Button	

Application Settings – General Settings

No.	Item name	Type	Validation/business rules
1	Use Application Id	Check box	Checked/unchecked
2	Use Application Id name	Label	
3	Languages	List	Check all

			Uncheck all
4	Max Idle Time (in minutes)	List	Contains numbers Possibility to select a number from the list
5	Organization System Password	Free text box field	Visible/invisible inserted characters with role to protect the visibility of the password
6	Continue when no validation	Tab	
7	Exception when no validation	Tab	
8	No validation	Tab	
9	Validate SEDs in Client	Check box	Checked/unchecked
10	Show Full Error Information	Check box	Checked/unchecked
11	Show Process Version	Check box	Checked/unchecked
12	Attachment directory Path	Free text box field	Mandatory free text field (C:/EESSI/Share/portal/attachments/)
13	Attachment maximum File Size (in MB)	List	Numeric values, mandatory
14	Attachment Allowed Mime Type	Area contains attachments	
15	Importance	Area	
16	Normal	Button	
17	High	Button	
18	Criticality	Area	
19	Normal	Button	
20	High	Button	
21	Reset	Button	
22	Save	Button	

Application Settings – Default Case Settings

No.	Item name	Type	Validation/business rules
1	View mode	Area	
2	Classic view	Button	When clicked change colour in blue
3	Timeline view	Button	When clicked change colour in blue
4	Sort by	Area	
5	Creation		When clicked change colour in blue
6	Last Update		When clicked change colour in blue
7	Display Flags	Check box	
8	Group By Month	Check box	
9	Auto Set Alarm on Send Action	List	Contains numeric values (Number of days)
10	Reset	Button	
11	Save	Button	

Application Settings – Default User Profile

No.	Item name	Type	Validation/business rules
1	Language	List	Mandatory, contains language's list
2	Number Format	List	Mandatory, contains format numbers
3	Date Format	List	Mandatory, contains date formats
4	Time Format	List	Mandatory, contains time formats

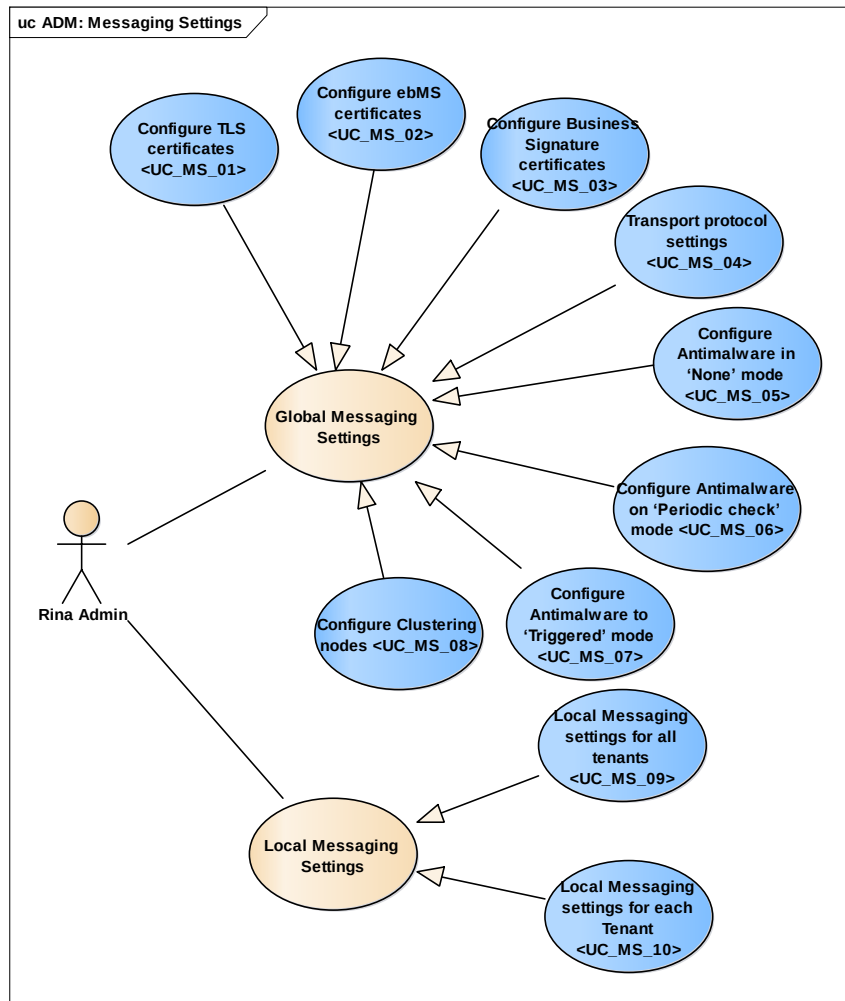
5	Currency	List	Mandatory, contains currencies format
6	Time Zone	List	Mandatory, contain time zone formats
7	Reset	Button	
8	Save	Button	

Application Settings – Case Counter Settings

No.	Item name	Type	Validation/business rules
1	Select tenant:	List box	Contains all Tenant, attached explanatory notes
2	Editing the tenant	Label	Displays the selected tenant (in format Country: Institution)
3	Default	Tab	Displays label 'Internal sequence for all cases will be used'
4	HTTP Callback	Tab	Displays following fields:
5	URL	Free text box field	Proposed format http://test.com Enabled, mandatory
6	Test	Button	
7	Pattern	Tab	Displays following fields:
8	Pattern	Free text box field	Enabled, mandatory
9	List of Patterns, contains explanatory notes for following parameters: <BUC_TYPE> <SECTOR> <SECTORSHORT> <SEQ(global,1000,10)> With associated: Global list box; Free text box, enabled (proposed format number 1000); Free text box, enabled (proposed format number 10) <DATE(dd/MMM/yyyy)> list contains all dates format	Grid	Possibility to select a parameter and add it to Pattern free text field
10	Save	Button	

6.3 Messaging Settings

Use case diagrams



Use Case View

UC_MS_01 View TLS certificates

Use Case ID:	UC_MS_01		
Use Case Name:	View and delete TLS certificates		
Created By:	Madalina Alecsandre scu	Last Updated By:	
Date Created:	18.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator can read details about the certificates for Authentication (TLS) against the AP		
Trigger:	The Administrator clicks on the "Messaging Systems" menu option, selects option "Certificates" and clicks on the "Authentication (TLS)" button from "Certificates" form.		

Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system.		
Post conditions:	The Administrator viewed the TLS certificates for Authentication against the AP.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option and clicks on the "Certificates" button	The "Certificates" form is displayed to the Administrator. with the following fields: • a "Refresh" button • a "+ New TLS Private Certificate" • a "v" expand button – when clicked it displays to the user the available options: ○ "New TLS Public Certificate" ○ "New MSG Private Certificate" ○ "New MSG Public Certificate" ○ "New Business Private Certificate" • a display area, where the displayed content is changed using the 3 available buttons: ○ "Authentication (TLS)" – default selected, when clicked displays information about certificates for authorization against the AP ○ "Authorization (Signature)" – when clicked displays information about certificates for signing messages ○ "Business Signature" – when clicked displays information about certificates for signing SEDs. The default display corresponds to the "Authentication (TLS)" button and contains the following fields: • the warning message: "Warning: please restart MSH after any add/remove of TLS certificates!" (red label) • an area labelled "TLS Keystore (<path to the private certificates>)" (i.e., "TLS Keystore (C:/EESSI/Share/repository/certs/tlskeystore.jks)") where the RINA TLS (private) certificate (National Domain) is displayed. For this area, the Administrator has available:

			○ a free text field labelled "Password" ○ a "Save" button ○ a grid with the columns: ○ "Alias" ○ "Actions" – for each displayed value in the grid, a "Delete" button is available • an area labelled "TLS Truststore (<path to public certificates>)" where the AP (public) certificate (National Domain) is displayed. For this area, the Administrator has available: ○ a free text field labelled "Password" ○ a "Save" button ○ a grid with the columns: ○ "Alias" ○ "Actions" – for each displayed value in the grid, a "Delete" button is available.
Alternate Scenario 1	1	The Administrator clicks "Refresh" button	The System redisplay the form "Certificates"

UC_MS_02 Add New TLS Private Certificate

Use Case ID:	UC_MS_03		
Use Case Name:	Add New TLS Private Certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds new TLS private certificates		
Trigger:	The Administrator accesses "Messaging Systems" menu option, selects option "Certificates" and clicks on the "+New TLS Private Certificate" button from "Certificates" form.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		

Post conditions:	The Administrator added a new TLS private certificate.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button and then clicks on "+ New TLS Private Certificate" button.	The System displays the "TLS Private Certificate Form" which contains: • "Keystore Password" – free-text field • "Certificate File *" - field where the imported certificate file id displayed • "+Import certificate" button – when clicked it enables the Administrator to upload the certificate file • "Certificate Alias *" - mandatory free-text field • "Certificate Password *" – mandatory free-text field • "Back" button • "Reset" button • "Save" button
	2	The Administrator fills in the fields, imports the certificate and clicks on the "Save" button	The System saves the data on server. The System closes the "TLS Private Certificate Form" and navigates back to the "Certificates" form, where the new certificate is displayed in the corresponding display grid.
Alternate Scenario 1	1	The Administrator clicks on the "Reset" button	The value(s) on the field(s) are discarded and the fields values are reloaded from the server.
Alternative Scenario 2	1	The Administrator clicks on "Back" button	The present form closes, and the system navigates the Administrator to the previous form "Certificates"

UC_MS_03 Add New TLS Public Certificate

Use Case ID:	UC_MS_03		
Use Case Name:	Add New TLS Public Certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds new TLS public certificates		

Trigger:	The Administrator accesses "Messaging Systems" menu option, selects option "Certificates" and clicks list box with option "New TLS Public Certificate" from "Certificates" form.		
Precondition s:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator added new TLS public certificates		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button, clicks on the "v" expand button, and, from the available options, clicks on the then clicks on "New TLS Public Certificate".	The system displays the "TLS Public Certificate Form" which contains: • "Keystore Password" – free-text field • "Certificate File *" - field where the imported certificate file id displayed • "+Import certificate" button – when clicked it enables the Administrator to upload the certificate file • "Certificate Alias *" - mandatory free-text field • "Back" button • "Reset" button • "Save" button
	2	The Administrator fills in the fields, imports the certificate and clicks on the "Save" button	The System saves the data on server. The System closes the "TLS Public Certificate Form" and navigates back to the "Certificates" form, where the new certificate is displayed in the corresponding display grid.
Alternate Scenario 1	1	The Administrator clicks on the "Reset" button	The value(s) on the field(s) are discarded and the fields values are reloaded from the server.
Alternative Scenario 2	1	The Administrator clicks on "Back" button	The present form closes, and the system navigates the Administrator to the previous form "Certificates"

UC_MS_04 Delete TLS certificates

Use Case ID:	UC_MS_04		
Use Case Name:	Delete TLS certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.05.2020	Last Revision Date:	

Actors:	System, Administrator		
Description:	This use case describes how the Administrator delete certificates for Authentication (TLS) against the AP		
Trigger:	The Administrator accesses "Messaging Systems" menu option, selects option "Certificates".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system.		
Post conditions:	The Administrator deleted TLS certificates for Authentication against the AP.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option and clicks on the "Certificates" button	The system displays the "Certificates" form
	2	The Administrator identifies in the display grids the certificate to be deleted and clicks on the corresponding "Delete" button	The System displays confirmation pop-up with the message "You are about to delete the certificate: <detail of certificate>" with buttons "Yes" and "No".
	3	The Administrator clicks on "Yes" button	The System deletes the TLS certificate from the associated row from the view.
Alternate Scenario 1	1	The Administrator clicks "No" button	The System discards the action to delete the TLS certificate. The System closes the confirmation pop-up message.

UC_MS_05 View ebMS certificates

Use Case ID:	UC_MS_05		
Use Case Name:	View ebMS certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator can read details about certificates for signing Messages (ebMS)		
Trigger:	The Administrator accesses "Messaging Systems" menu option, selects option "Certificates" and clicks tab "Authorization (Signatures)" from "Certificates" form.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		

Post conditions:	The Administrator viewed ebMS certificates		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button	The system displays the "Certificates" form
	2	The Administrator clicks on the "Authorization (Signature)" button	In the display area the following information is displayed: - an area labelled "MSG Keystore (<path to the private certificates>)" where the (private) ebMS signing National Domain certificate(s) of every Tenant hosted by RINA is displayed. For this area, the Administrator has available: - a free text field labelled "Password" - a "Save" button - a grid with the columns: "Alias" "Actions" – for each displayed value in the grid, a "Delete" button is available - an area labelled "MSG Truststore (<path to public certificates>)" where the (public) ebMS International Domain (TESTA) certificate of the AP is displayed. For this area, the Administrator has available: - a free text field labelled "Password" - a "Save" button - a grid with the columns: "Alias" "Actions" – for each displayed value in the grid, a "Delete" button is available

UC_MS_06 Add New MSG Private Certificate

Use Case ID:	UC_MS_06		
Use Case Name:	Add New MSG Private Certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	

Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds new MSG private certificates		
Trigger:	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button, and in the "Certificate" form clicks on the "v" expand button, and, from the available options, clicks on the "New MSG Private Certificate".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator added new MSG private certificates		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button, and in the "Certificate" form clicks on the "v" expand button, and, from the available options, clicks on the "New MSG Private Certificate".	The system displays the "MSG Private Certificate Form" which contains: • "Keystore Password" – free-text field • "Certificate File *" - field where the imported certificate file id displayed • "+Import certificate" button – when clicked it enables the Administrator to upload the certificate file • "Certificate Alias *" - mandatory free-text field • "Certificate Password *" – mandatory free-text field • "Back" button • "Reset" button • "Save" button
	2	The Administrator fills in the fields, imports the certificate and clicks on the "Save" button	The System saves the data on server. The System closes the "TLS Public Certificate Form" and navigates back to the "Certificates" form, where the new certificate is displayed in the corresponding display grid.
	1	The Administrator clicks on "Reset" button	The value(s) on the field(s) are discarded and the fields values are reloaded from the server.
Alternate Scenario 1	1	The Administrator clicks on "Reset" button	The value(s) on the field(s) are discarded and the fields values are reloaded from the server.
Alternative Scenario 2	1	The Administrator clicks on "Back" button	The present form closes, and the system navigates the Administrator to the previous form "Certificates"

UC_MS_07 Add New MSG Public Certificate

Use Case ID:	UC_MS_07
---------------------	-----------------

Use Case Name:	Add New MSG Public Certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds new MSG private certificates		
Trigger:	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button, and in the "Certificate" form clicks on the "v" expand button, and, from the available options, clicks on the "New MSG Public Certificate".		
Precondition s:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator added new MSG private certificates		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button, and in the "Certificate" form clicks on the "v" expand button, and, from the available options, clicks on the "New MSG Public Certificate".	The system displays the "MSG Public Certificate Form" which contains: • "Keystore Password" – free-text field • "Certificate File *" - field where the imported certificate file id displayed • "+Import certificate" button – when clicked it enables the Administrator to upload the certificate file • "Certificate Alias *" - mandatory free-text field • "Back" button • "Reset" button • "Save" button
	2	The Administrator fills in the fields, imports the certificate and clicks on the "Save" button	The System saves the data on server. The System closes the "MSG Public Certificate Form" and navigates back to the "Certificates" form, where the new certificate is displayed in the corresponding display grid.
Alternate Scenario 1	1	The Administrator clicks on "Reset" button	The value(s) on the field(s) are discarded and the fields values are reloaded from the server.
Alternative Scenario 2	1	The Administrator clicks on "Back" button	The present form closes, and the system navigates the Administrator to the previous form "Certificates"

UC_MS_08 Delete ebMS certificates

Use Case ID:	UC_MS_08		
Use Case Name:	Delete ebMS certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator delete certificates for signing Messages (ebMS)		
Trigger:	The Administrator accesses "Messaging Systems" menu option, clicks on the "Certificates" button, and, in the "Certificates" form, clicks on the "Authorization (Signature)" button		
Precondition s:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system.		
Post conditions:	The Administrator deleted the ebMS certificate.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Messaging Systems" menu option, clicks on the "Certificates" button, and, in the "Certificates" form, clicks on the "Authorization (Signature)" button	The system displays the "Certificates" form. In the display area, information about certificates for signing messages are shown.
	2	The Administrator identifies in the display grids the certificate to be deleted and clicks on the corresponding "Delete" button	The System displays confirmation pop-up with the message "You are about to delete the certificate:<detail of certificate>" with buttons "Yes" and "No".
	3	The Administrator clicks on "Yes" button	The System deletes the TLS certificate from the associated row from the view.
Alternate Scenario 1	1	The Administrator clicks "No" button	The System discards the action to delete the TLS certificate. The System closes the confirmation pop-up message.

UC_MS_09 View Business Signature certificates

Use Case ID:	UC_MS_09		
Use Case Name:	View Business Signature certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	

Actors:	System, Administrator		
Description:	This use case describes how the Administrator can read details about certificates used for signing the SEDs		
Trigger:	The Administrator accesses "Messaging Systems" menu option, selects option "Certificates" and clicks on the "Business Signatures" button from "Certificates" form.		
Preconditions :	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator viewed ebMS certificates		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button	The system displays the "Certificates" form
	2	The Administrator clicks on the "Business Signature" button	In the display area the following information is displayed: - an area labelled "Business Keystore (<path to the private certificates>)" (i.e., "MSG Keystore (C:/EESSI/Share/repository/certs/businessSignatureKeystore.jks)") where the certificates used to sign SEDs are displayed. For this area, the Administrator has available: - a free text field labelled "Password" - a "Save" button - a grid with the columns: "Alias" "Actions" – for each displayed value in the grid, a "Delete" button is available

UC_MS_10 Add New Business Private Certificate

Use Case ID:	UC_MS_10		
Use Case Name:	Add New Business Private Certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds a new Business private certificate.		

	Each Tenant can use its own Business signature certificate that can be added.		
Trigger:	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button, and in the "Certificate" form clicks on the "v" expand button, and, from the available options, clicks on the "New Business Private Certificate".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator added a new business private certificate		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, clicks on the "Certificates" button, and in the "Certificate" form clicks on the "v" expand button, and, from the available options, clicks on the "New Business Private Certificate".	The system displays the "MSG Private Certificate Form" which contains: • "Keystore Password" – free-text field • "Certificate File *- field where the imported certificate file id displayed • "+Import certificate" button – when clicked it enables the Administrator to upload the certificate file • "Certificate Alias *" - mandatory free-text field • "Certificate Password *" – mandatory free-text field • "Back" button • "Reset" button • "Save" button
	2	The Administrator fills in the fields, imports the certificate and clicks on the "Save" button	The System saves the data on server. The System closes the "TLS Public Certificate Form" and navigates back to the "Certificates" form, where the new certificate is displayed in the corresponding display grid.
Alternate Scenario 1	1	The Administrator clicks on "Reset" button	The value(s) of the field(s) are discarded, and the fields values are reloaded from the server.
Alternative Scenario 2	1	The Administrator clicks on "Back" button	The present form closes, and the system navigates the Administrator to the previous form "Certificates"

UC_MS_11 Delete Business Signature certificates

Use Case ID:	UC_MS_11		
Use Case Name:	Delete ebMS certificates		
Created By:	Madalina Alecsandrescu	Last Updated By:	

Date Created:	18.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator deletes a certificate for signing SEDs		
Trigger:	The Administrator accesses "Messaging Systems" menu option, clicks on the "Certificates" button, and, in the "Certificates" form, clicks on the "Business Signature" button		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system.		
Post conditions:	The Administrator deleted the business certificate.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Messaging Systems" menu option, clicks on the "Certificates" button, and, in the "Certificates" form, clicks on the "Business Signature" button	The system displays the "Certificates" form. In the display area, information about certificates for signing SEDs are shown.
	2	The Administrator identifies in the display grid the certificate to be deleted and clicks on the corresponding "Delete" button	The System displays confirmation pop-up with the message "You are about to delete the certificate: <detail of certificate>" with buttons "Yes" and "No".
	3	The Administrator clicks on "Yes" button	The System deletes the TLS certificate from the associated row from the view.
Alternate Scenario 1	1	The Administrator clicks "No" button	The System discards the action to delete the TLS certificate. The System closes the confirmation pop-up message.

UC_MS_12 Change password for certificate store

Use Case ID:	UC_MS_12		
Use Case Name:	Change password for certificate store		
Created By:	Madalina Alecsandre scu	Last Updated By:	
Date Created:	18.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator can change the password for the certificates store. The default password is supervisor . The password can be also changed in the file:		

	"RINA_Root_Folder\HolodeckB2B\bin\startServer.bat"		
Trigger:	The Administrator clicks on the "Messaging Systems" menu option, selects option "Certificates".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized as an administrator of the system.		
Post conditions:	The Administrator changed the password for the certificates store		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option and clicks on the "Certificates" button	The "Certificates" form is displayed to the Administrator. In the display area, the authentication private and public certificated are displayed
	2	The Administrator fills in the desired value in the "Password" corresponding to the "TLS Keystore" store and clicks on the "Save" button.	The password for the TLS Private Certificates store is changed.
Alternative flow 2	1	At step 2, the Administrator fills in the desired value in the "Password" corresponding to the "TLS Truststore" store and clicks on the "Save" button.	The password for the TLS Public Certificates store is changed.
Alternative flow 2	1	After step 1, the Administrator clicks on the "Authorisation (Signatures)" button	In the display area, the authorisation private and public certificated are displayed
	2	At step 2, the Administrator fills in the desired value in the "Password" corresponding to the "MSG Keystore" store and clicks on the "Save" button.	The password for the MSG Private Certificates store is changed.
Alternative flow 3	1	After step 1, the Administrator clicks on the "Authorisation (Signatures)" button	In the display area, the authorisation private and public certificated are displayed
	2	At step 2, the Administrator fills in the desired value in the "Password" corresponding to the "MSG Truststore"	The password for the MSG Public Certificates store is changed.

		store and clicks on the "Save" button.	
Alternative flow 4	1	After step 1, the Administrator clicks on the "Business Signatures" button	In the display area, the business certificated are displayed
	2	At step 2, the Administrator fills in the desired value in the "Password" corresponding to the "Business Keystore" store and clicks on the "Save" button.	The password for the Business Certificates store is changed.

UC_MS_13 Set Transport protocol parameters

Use Case ID:	UC_MS_13		
Use Case Name:	Set Transport protocol parameters		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the system allows the Administrator to configure the settings for receiving messages from the APs (transportation method), maximum message size, retry interval and maximum number of retries, in parallel with the interval of pulling request (in case this communication pattern has been selected while receiving from the AP).		
Trigger:	The Administrator accesses "Messaging Systems" menu option and clicks on the "Global Messaging Systems" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application 3. The user has filled in one area related to certificates		
Post conditions:	The Administrator configured settings for receiving messages depending on Transport mode.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Messaging Systems" menu option and clicks on the "Global Messaging Systems" button.	The system displays the "Global Messaging Settings" form with the following fields: • a selection field labelled "BPM Validation Mode", that allows the Administrator to configure the validation against the local XSD files, at the business message services level– by ApClient microservice (at BMS layer), with possible values: ○ "Exception When No Validation" ○ "No Validation" ○ "Continue When No Validation"

		• a selection field labelled "Transport Mode", with possible values: ○ "Pull" ○ "Push" Remark: The terminology "PULL" and "PUSH" refers to the way the messages are retrieved, at the receiving side, by the MSH (Holodeck) "PULL": the message is "pulled" by RINA (ebMS/AS4 client) from the AP queue "PUSH": the message is "pushed" from AP to RINA • a counter field labelled "Max Message Size (KB) *", mandatory integer value. This attribute sets the message maximum permitted size that can be sent from RINA application. This parameter configures the size limitation of the entire exchanged message including the SOAP ebMS envelope, the SED and the attachments. The maximum limit is set to 2GB. The default value is 51200Kbytes. • a counter field labelled "Retry interval (sec) *", mandatory integer field. This attribute sets the message re-sending retry interval (in secs). This defines the interval for which RINA waits for the acknowledgement receipt before starts a re-transmission. The default value is 237600 (secs) • a counter field labelled "Maximum retries *", mandatory integer field. This attribute sets the maximum number of retries to send a message. The default value is 1. • a counter field labelled "Default pull request interval (sec) *", mandatory integer field. This attribute configures the frequency of checking for new data from AP when the Transport Mode is set to PULL.
--	--	--

	2	The Administrator fills in the fields and clicks on the "Save" button	The System saves all parameters concerning the Transport Protocol.
Alternative Scenario 1	1	The Administrator clicks "Reset" button	The System returns all field(s) value(s) to previous value(s) on server.

UC_MS_14 Disable Antimalware

Use Case ID:	UC_MS_14		
Use Case Name:	Disable Antimalware		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator configures the settings to disable the Antimalware control. The default value for Antimalware Mode is 'None'.		
Trigger:	The Administrator accesses "Messaging Systems" menu option, and clicks on the "Global Messaging Systems" button		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as Admin user 3. The Antimalware Mode is set to a value different than "None"		
Post conditions:	The Administrator configured Antimalware section related to 'None' section (no antimalware control)		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Messaging Systems" menu option and clicks on the "Global Messaging Systems" button.	The "Global Messaging Settings" is displayed. In this form, the Administrator has available the selection field labelled "Antimalware Mode" with possible values: • "None" • "Periodic check" • "Triggered" The value retrieved from the server is different than "None".
	2	In the selection field "Antimalware Mode", the Administrator selects the value "None"	The System displays the "None" value highlighted.
	3	The Administrator clicks on the "Save" button	The System displays pop-up window with message "Global Messaging Settings successfully saved". Remark: No antimalware control is applied.

Alternative Scenario 1	1	The Administrator clicks on the "Reset" button	The System returns all field(s) value(s) to previous value(s) on server.
-------------------------------	---	--	--

UC_MS_15 Set Antimalware on 'Periodic check' mode

Use Case ID:	UC_MS_15		
Use Case Name:	Set Antimalware on 'Periodic check' mode		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator configures the settings regarding antimalware control in periodic check mode, which means that antimalware is applied periodically.		
Trigger:	The Administrator accesses "Messaging Systems" menu option, and clicks "Global Messaging Systems" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as Admin user 3. The Antimalware Mode is set to a value different than "Periodic check"		
Post conditions:	The Administrator configured Antimalware mode applied periodically		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Messaging Systems" menu option and clicks on the "Global Messaging Systems" button.	The "Global Messaging Settings" is displayed. In this form, the Administrator has available the selection field labelled "Antimalware Mode" with possible values: • "None" • "Periodic check" • "Triggered" The value retrieved from the server is different than "Periodic check".
	2	In the selection field "Antimalware Mode", the Administrator selects the value "Periodic check"	The System displays the "Periodic check" value highlighted. A counter field labelled "Timeframe Settings *" is enabled. In this field the Administrator must enter the number of seconds between checks. Remark: it is recommended to not set high value for antimalware period, preferred value for timeframe less than 45 secs.

	3	The Administrator fills in the "Timeframe Settings *" field and clicks on the "Save" button	The System displays pop-up window with: "Global Messaging Settings successfully saved". The System has been configured to be periodically checked.
Alternative Scenario 1	1	The Administrator clicks "Reset" button	The System returns all field(s) value(s) to previous value(s) on server.

UC_MS_16 Set Antimalware to 'Triggered' mode

Use Case ID:	UC_MS_16		
Use Case Name:	Set Antimalware to 'Triggered' mode		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator configures the settings regarding antimalware control, as triggered check, which means that antimalware starts when the Administrator 'calls' it.		
Trigger:	N/A		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as Admin User 3. The Antimalware Mode is set to a value different than "Triggered"		
Post conditions:	The Administrator configured Antimalware as triggered check mode.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Messaging Systems" menu option and clicks on the "Global Messaging Systems" button.	The "Global Messaging Settings" is displayed. In this form, the Administrator has available the selection field labelled "Antimalware Mode" with possible values: • "None" • "Periodic check" • "Triggered" The value retrieved from the server is different than "Triggered".
	2	In the selection field "Antimalware Mode", the Administrator selects the value "Triggered"	The System displays the "Triggered" value highlighted. Two additional fields are enabled:

			- free-text field, labelled "Antimalware Scan Command *", mandatory - free-text field, labelled "Antimalware inf code *", mandatory
	2	The Administrator fills in data related to Antimalware section, and clicks on the "Save" button	The System displays pop-up window with: "Global Messaging Settings successfully saved". Remark: The Antimalware control is activated triggered by the Administrator.
Alternative Scenario 1	1	The Administrator clicks "Reset" button	The System returns all field(s) value(s) to previous value(s) on server.

UC_MS_17 Set Local Messaging settings

Use Case ID:	UC_MS_17		
Use Case Name:	Set Local Messaging settings		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.03.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator configures the Local Messaging Settings		
Trigger:	N/A		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The user configured local messaging settings.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Messaging Systems" menu option, and then clicks on the "Local Messaging Systems" button.	The System displays the "Local Messaging Settings" form: "Access Point FQDN Address" section, as defined through the RINA Installation and Configuration process, which includes "Protocol *" - mandatory drop-down list to select the http protocol (includes the possible values "http" and "https"). Default value is "https" "IP *" - free text field for introducing the IP address (in terms of the Fully Qualified Domain Name - FQDN)

		• "Port *" – free text field for introducing the relevant connection port. The AP FQDN must be the same as the one defined in the CN (Common Name) of the public certificates provided by the AP "Business Endpoint" section used for SED exchange – content depends on the selected "Transport Mode" • For "Pull" - "Inbox" (Business) - text box field. The AP application context related service where messages are being retrieved from (only used when the Transport Mode is set to 'Pull' mode); this is configured in CSN/AP and defined through installation scripts in RINA application "/eessi/BusinessMessaging/v1.0/Inbox/Service.svc" • For "Push" - "Outbox" (Business) - text box field: the AP application context related service where the messages are being sent to; this is configured in CSN/AP and defined through installation scripts in RINA application "/eessi/BusinessMessaging/v1.0/Outbox/Service.svc" "System Endpoint" section used for synchronization activities- content depends on the selected "Transport Mode" • "Inbox" (System) - text box field. The AP application context related service where messages are being retrieved from (only used when the Transport Mode is set to 'Pull' mode); this is configured in CSN/AP and defined through installation scripts in RINA application "/eessi/SystemMessaging/v1.0/Inbox/Service.svc" • "Outbox" (Systems) - text box field: the AP application context related service where the messages are being sent to; this is configured in CSN/AP and defined through installation scripts in RINA application.
--	--	--

			"/eessi/SystemMessaging/v1.0/Outbox/Service.svc" - Grid with columns: "Institution" "Default business signature alias" "Endpoint" "MPC" "Pulling interval" "Alias" "Password" (editable field) "Reset" button "Save" button
	2	The Administrator makes the desired changes and clicks on the "Save" button	The System saves the changes and displays pop-up message "Messaging Settings successfully saved"
Alternative scenario 1	1	The Administrator clicks "Reset" button	The System discards all changes included on the fields from the form and restore previous values from server.

Fields Details

Messaging Settings – Global Messaging Settings

No.	Item name	Type	Validation/business rules
1	BPM Validation Mode	Label	
2	Exception When No Validation	Tab	When clicked changes the colour in blue
3	No Validation	Tab	When clicked changes the colour in blue
4	Continue When No Validation	Tab	When clicked changes the colour in blue
5	Authentication (TLS)	Tab	By selecting this tab is displayed next fields:
6	Transport mode	Label	
7	Pull	Tab	When clicked changes the colour in blue
8	Push	Tab	When clicked changes the colour in blue
8	Max Message Size (KB)	List	Contains numerical values, mandatory
9	Retry Interval (sec)	List	Mandatory, contains numerical values
10	Maximum retries	List	Mandatory, contains numerical values

11	Default Pull Request Interval(sec)	List	Mandatory, contains numerical values
12	Antimalware Mode	Label	
13	None	Button	When clicked changes the colour in blue
14	Periodic check	Button	When clicked changes the colour in blue
15	Timeframe settings	List	Mandatory
16	Triggered	Button	When clicked changes the colour in blue
17	Antimalware Scan command	Free text field	Mandatory
18	Antimalware inf Code	Free text field	Mandatory
19	Reset	Button	
20	Save	Button	

Messaging Settings – Certificates

No.	Item name	Type	Validation/business rules
1	Refresh	Button	
2	New TLS Public Certificate		
3	Authentication TLS	Button	When clicked the system displays
4	TLS Keystore (C:/EESSI/Share/repository/certs/tlskeystore.jks)	Label	
5	Password	Free text box field	
6	Save	Button	
7	Alias	Grid	Contains columns: Alias Action Delete button, associated to every row
8	TLS Truststore (C:/EESSI/Share/repository/certs/tlstruststore.jks)	Label	
9	Password	Free text box field	
10	Save	Button	
11	Alias	Grid	Contains columns: Alias Action Delete button, associated to every row
12	Authorization (Signatures)	Button	When clicked the system displays:
13	MSG Keystore (C:/EESSI/Share/repository/certs/privatekeys.jks)	Label	
14	Password	Free text box field	

15	Save	Button	
16	Alias	Grid	Contains columns: Alias Action Delete button, associated to every row
17	MSG Truststore (C:/EESSI/Share/repository/certs/publickeys.jks)	Label	
18	Password	Free text box field	
19	Save	Button	
20	Alias	Grid	Contains columns: Alias Action Delete button, associated to every row
21	Business Signatures	Button	When clicked displays:
22	Business Keystore (C:/EESSI/Share/repository/certs/businessSignatureKeystore.jks)		
23	Password	Free text box field	
24	Save	Button	
25	Alias	Grid	Contains columns: Alias Action Delete button, associated to every row
26	New TLS Public Certificate		
27	Keystore password	Free text box field	
28	Certificate File	Free text box field	Mandatory with associated
29	Import Certificate	Button	Open window that offers possibility to choose a file
30	Certificate Alias	Free text box field	Mandatory
31	Reset	Button	
32	Save	Button	
33	Back	Button	
34	New MSG Private certificate		
35	Keystore password	Free text box field	
36	Certificate File	Free text box field	Mandatory with associated
37	Import Certificate	Button	Open window that offers possibility to choose a file

38	Certificate Alias	Free text box field	Mandatory
39	Certificate Password	Free text box field	Mandatory
40	Reset	Button	
41	Save	Button	
42	Back	Button	
43	New MSG Public Certificate		
44	Keystore password	Free text box field	
45	Certificate File	Free text box field	Mandatory with associated
46	Import Certificate	Button	Open window that offers possibility to choose a file
46	Certificate Alias	Free text box field	Mandatory
48	Reset	Button	
49	Save	Button	
50	Back	Button	
51	New Business Private Certificate		
52	Keystore password	Free text box field	
53	Certificate File	Free text box field	Mandatory with associated
54	Import Certificate	Button	Open window that offers possibility to choose a file
55	Certificate Alias	Free text box field	Mandatory
56	Certificate Password	Free text box field	Mandatory
57	Reset	Button	
58	Save	Button	
59	Back	Button	

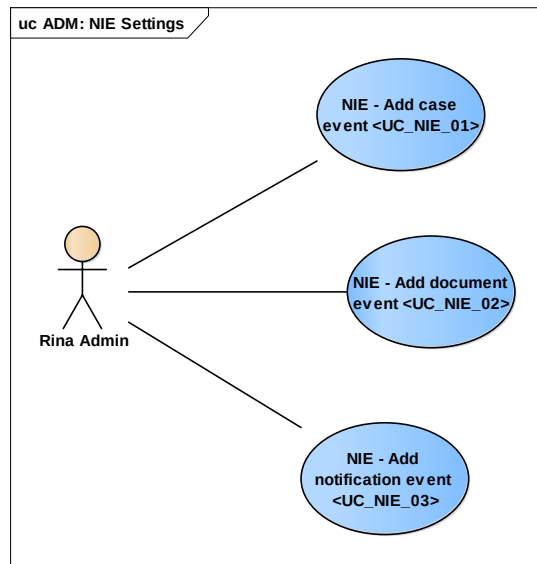
Messaging Settings - Local Messaging Settings

No.	Item name	Type	Validation/business rules
1	Protocol	List	Mandatory, contains http, https values
2	IP	Free text box	Mandatory
3	Port	Free text box	Mandatory
4	Business Endpoint	Label	
5	Outbox /eessi/BusinessMessaging/v1.0/Outbox/Service.svc	Label	
6	System Endpoint	Label	
7	Outbox /eessi/SystemMessaging/v1.0/Outbox/Service.svc	Label	
8	Local Message	Grid	Contains columns:

			Institution (ex: RO:RONA06, RO:RONA06, RO:RONA06, RO) Default Business Signature Alias, has attached list with values Endpoint Alias Password
9	Reset	Button	
10	Save	Button	

6.4 NIE Settings

Use case diagrams



Use Case View

UC_NIE_01 NIE - Add case event

Use Case ID:	UC_NIE_01		
Use Case Name:	NIE - Add case event		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.03.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds a new case event in RINA.		
Trigger:	The Administrator clicks on the "NIE Settings" menu option and clicks on the "Add Case Event" button.		

Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin 3. By default, no cases are defined following a new RINA deployment		
Post conditions:	The Administrator added a new case event to NIE.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "NIE Settings" menu option and clicks on the "Add Case Event" button.	The System displays the "Add Case Event" form, which includes: • "Subscription name *", mandatory, free-text field • an area labelled "Subscribers" where the Administrator has available: ○ a free-text field "BUC *", ○ a free-text field "Version *" ○ an "Add" button for repeating the above fields ○ a "Delete" button corresponding to each pair of "BUC *" and "Version *" fields • an area labelled "Listeners" that contains field for introducing URLs for specific events: ○ "Open Case", free-text field ○ "Receive Case", free-text field ○ "Remove Case", free-text field ○ "Close Case", free-text field ○ "Delete Case", free-text field ○ "Forward Case", free-text field ○ "Reopen Case", free-text field ○ an information label: "Reference implementation URI: http://ip:port/rinieRest/CasesEvents" - is the URL for relevant cases event • "Save" button • "Reset" button The NIE listener for cases runs under the location mentioned on the form. (As an example, the settings could be populated in the form with the following data: "http://10.1.2.35:8080/eessi-rina-nie/CasesEvents", "Pension ", "P_BUC_01", "1.0".
	2	The Administrator clicks "Add" button	The System displays in the "Subscribers" area a new row with "BUC" and "Version" fields and corresponding "Delete" button.
	3	The Administrator fills in the fields and clicks "Save" button	The system saves the inserted data.
Alternative scenario 1	1	The Administrator	The System discard all changes made on the field(s) of this form and restores value(s) from server.

		clicks "Reset" button	
Exception flow 1	1	The Administrator does not fill in any of the URL dedicated fields in the "Listeners" area and clicks the "Save" button	The System displays the message 'At least one of the listeners should be filled'

UC_NIE_02 NIE - Add document event

Use Case ID:	UC_NIE_02		
Use Case Name:	NIE - Add document event		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.03.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator adds a new document event in RINA.		
Trigger:	The Administrator clicks on the "NIE Settings" menu option and clicks on the "Add Document Event" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin		
Post conditions:	The Administrator added a new document event.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "NIE Settings" menu option and clicks on the "Add Document Event".	The System displays the "Add Document Event" form, which includes: "Subscription name *", mandatory, free-text field - an area labelled "Subscribers" where the Administrator has available: - a free-text field "Document *", - an "Add" button for repeating the above field - a "Delete" button corresponding to each "Document *" field - an area labelled "Listeners" that contains field for introducing URLs for specific events: "Initialise Document" - free-text field "New Document" - free-text field "Update Document" - free-text field "Send Document" - free-text field "Delete Document" - free-text field "Cancel Document" - free-text field

			○ "Receive Document" - free-text field ○ "Initialise Subdocument" - free-text field ○ "New Subdocument" - free-text field ○ "Update Subdocument" - free-text field ○ "Delete Subdocument" - free-text field ○ "New Document Batch" - free-text field ○ "Receive Document Batch" - free-text field ○ an information label: "Reference implementation URI: http://ip:port/rinieRest/CasesEvents" ● "Save" button ● "Reset" button
	2	The Administrator clicks on the "Add" button	The System displays in Subscribers section a new row with "Document" field and corresponding "Delete" button.
	3	The Administrator clicks on "Save" button	The System displays the message 'At least one of the listeners should be filled' in case there is no listeners inserted in the list of listeners. The system saves inserted data and display the message 'NIE setting successfully saved'
Alternate Scenario 1	1	The Administrator clicks on "Reset" button	The System discards all the changes made on the fields of the form and restores previous values from the server.

UC_NIE_03 NIE - Add notification event

Use Case ID:	UC_NIE_03		
Use Case Name:	NIE - Add notification event		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.03.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the System allows the Administrator to add a new notification event in RINA and how NIE interface (owned by RINA) allows participant countries to exchange information with their National Applications/Systems.		

	RINA uses the NIE client to connect to a listener at National level. This listener will be notified by RINA when a specific Notification event happens.		
Trigger:	The Administrator accesses "NIE Settings" menu option and clicks "Add Notification Event".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin		
Post conditions:	The Administrator added a new notification event.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "NIE Settings" menu option and select "Add Notification Event" option	The System displays "Add Notification Event" form, which contains: - "Subscription Name *", mandatory, free-text field - "Reference implementation URI: http://ip:port/rinieRest/NotificationsEvents " (this is the URL of the listener, where the URL defines the location where the notification's templates should be saved) - "Generate Notifications *", free-text field, mandatory - "Save" button - "Reset" button
	3	The Administrator fills in the fields and clicks "Save" button	The system saves the inserted data.
Alternative scenario 1	1	The Administrator clicks "Reset" button	The System discard all changes made on the field(s) of this form and restores value(s) from server.
Exception flow 1	1	The Administrator does not fill in any of the URL dedicated fields in the "Listeners" area and clicks the "Save" button	The System displays the message 'At least one of the listeners should be filled'

UC_NIE_04 NIE - Consult NIE events

Use Case ID:	UC_NIE_04
Use Case Name:	Consult NIE Events

Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.03.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator consults details about all the NIE events.		
Trigger:	The Administrator accesses "NIE Settings" menu option and clicks "NIE Events".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin		
Post conditions:	The Administrator consulted the list with NIE events		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "NIE Settings" menu option and clicks on "NIE Events" button.	The System displays the "NIE Events" form with the following information: - A header area that enables the Administrator to sort and search the displayed NIE events using: - a drop-down list field with possible values: "Newest First", "Oldest First", "Event name" – when a value is selected, the events displayed are sorted accordingly - a free text field for entering text to be searched in the event name - A display area where the existing events are displayed. For each displayed event, the Administrator has available a "Delete" button.

UC_NIE_05 NIE - Delete NIE events

Use Case ID:	UC_NIE_04		
Use Case Name:	Manage NIE Events		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.03.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator deletes a NIE event.		
Trigger:	The Administrator accesses "NIE Settings" menu option and clicks "NIE Events".		
Preconditions:	1. The user is authenticated in RINA.		

	2. The user is authorized to access Application as RINA Admin		
Post conditions:	The Administrator consulted the list with NIE events		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "NIE Settings" menu option and clicks on "NIE Events" button.	The System displays the "NIE Events" form
	2	The Administrator identifies the NIE event to be deleted and clicks on the corresponding "Delete" button.	The System displays confirmation pop-up with buttons "Yes" and "No".
	3	The Administrator clicks on "Yes" button	The System deletes the event.

UC_NIE_05 NIE - Configures policy decision Nie Client Implementation

Use Case ID:	UC_NIE_05		
Use Case Name:	Configure policy decision NIE – Client Implementation		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	18.03.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator configures the policy decision point implementation class		
Trigger:	The Administrator accesses "NIE Settings" menu option and clicks "NIE Client Implementation" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin		
Post conditions:	The Administrator configures the policy decision point implementation class		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator access "NIE Settings" menu and clicks on "NIE Client Implementation" button.	The System displays the "Nie Client Implementation" form with: "Policy Decision Point Implementation Class (Fully qualified name) *" – mandatory free-text field - "Save" button - "Reset" button
	2	The Administrator enter the needed value in the "Policy Decision Point Implementation	The System saves data on server.

		Class (Fully qualified name) "*" field and clicks on the "Save" button	The System displays message "Nie Client Implementation successfully saved".
Alternative scenario 1	1	The Administrator clicks "Reset" button	The System discards all changes made on the field(s) of the form and restores the value(s) from the server.

Fields Details

NIE Events

No.	Item name	Type	Validation/business rules
1	Sort By	List	Contains: Newest First, Oldest First, Event Name
2	Search by element name	Search element	Enabled

NIE Client Implementation

No.	Item name	Type	Validation/business rules
1	Policy Decision Point Implementation Class (Fully Qualified Name)	Free text box	Mandatory
2	Reset	Button	
3	Save	Button	

NIE – ADD Case Event

No.	Item name	Type	Validation/business rules
1	Subscription name*	Free text box	Mandatory
2	BUC	Free text box	Mandatory
3	Version	Free text box	Mandatory
4	Add	Button	
5	Delete	Button	
6	Listeners	Label	
7	Open Case	Free text box	
8	Receive Case	Free text box	
9	Remove Case	Free text box	
10	Close Case	Free text box	
11	Delete Case	Free text box	
12	Forward Case	Free text box	
13	Reopen Case	Free text box	
14	Reset	Button	
15	Save	Button	

NIE – ADD Document Event

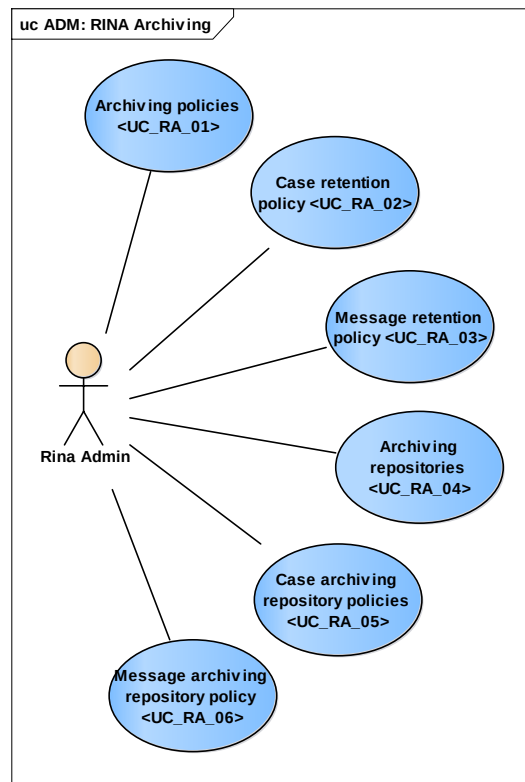
No.	Item name	Type	Validation/business rules
1	Subscription name*	Free text box	Mandatory
2	Document	Free text box	Mandatory
4	Add	Button	
5	Delete	Button	
6	Listeners	Label	
7	Initialise Document	Free text box	
8	New Document	Free text box	
9	Update Document	Free text box	
10	Send Document	Free text box	
11	Delete Document	Free text box	
12	Cancel Document	Free text box	
13	Receive Document	Free text box	
14	Initialise Subdocument	Free text box	
15	New Subdocument	Free text box	
16	Update Subdocument	Free text box	
17	Delete Subdocument	Free text box	
18	New Document Batch	Free text box	
19	Receive Document Batch	Free text box	
20	Reset	Button	
21	Save	Button	

NIE – ADD Notification Event

No.	Item name	Type	Validation/business rules
1	Subscription name*	Free text box	Mandatory
2	Generate Notifications	Free text box	Mandatory
3	Reset	Button	
4	Save	Button	

6.5 RINA Archiving

Use case diagrams



Use Case View

UC_RA_01 Set up archiving policies

Use Case ID:	UC_RA_01		
Use Case Name:	Set up archiving policies		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	06.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator can define the archiving policies for the cases and the enablement of the messages archiving procedure (archiving of cases is automatically enabled). The archiving policies are defined per Sector and BUC.		
Trigger:	The Administrator clicks on the "RINA Archiving" button from main menu, then clicks on the "Archiving Policies" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin		
Post conditions:	The user created/set up policy for archived messages related to a business case.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "RINA Archiving" menu option, then on the "Archiving Policies" button	The System displays the form "Archiving Policies", which includes: • "+Add Policies", button • "Settings", button

			• Grid displaying the existing archiving policies, with following columns ◦ "Sector" ◦ "Process" – for displaying the BUC type of the archiving policy ◦ "Role" ◦ "Days" ◦ "Actions" where, for each displayed policy, the Administrator has available: ◦ "Edit" button ◦ "Delete" button • "Refresh" button
	2	The Administrator clicks on the "+Add Policies" button	The System displays the "Archiving Policy" Form, with following fields: - "Process Owner" - check box - "Counter Party" - check box The Administrator must check at least one of the above checkbox fields. - "Archiving Period(days)" – counter field with the default value 90 days, where the Administrator must select the archive period. This is the period of time during which a closed case is retained at such state, prior to automatically getting to archived state. The archived state can be reverted, only if the case is not deleted. For a case in archive state only case metadata are available to the user - the "Sector" drop-down field that allows the Administrator to select the relevant business sector (AWOD, Pensions, Family benefits, Horizontal, Legislation applicable, Miscellaneous, Recovery, Sickness, Unemployment). - the "BUC": based on the selected Sector, the System displays all the BUCs of that Sector. Each BUC has a corresponding checkbox field for the administrator to select one or more BUCs to be included in the

			archiving policy by clicking on the check box - "Save" button - "Reset" button - "Back" button
	3	The Administrator fills in the fields and clicks on "Save" button	The System saves data and displays message "Archiving policies successfully saved". The System closes the form "Archiving Policy" and displays "Archiving Policies" form. In the display grid, the new added policy is visible.
	4	The Administrator clicks on the "Edit" button corresponding to a displayed archiving policy	The System: • Enables for changes the "Days" field of the archiving policy: • In the "Action" the "Edit" and "Delete" buttons are replaced with : - "Save" button - "Cancel" button
	5	The Administrator fills in the "Days" field and clicks "Save" button	The System save the updated value and display message 'Archiving policies successfully saved'.
Alternate Flow 1	1	At step 5, The Administrator fills in the field and clicks on the "Cancel" button	The System discards the changes made on the fields and the previous data is kept on the server.
Alternate Flow 2	1	After step, the Administrator clicks on the "Delete" button	The System displays pop-up message 'You are about to delete the archiving policy: <BUC>' with two buttons "Yes" and "No"
	2	The Administrator clicks "Yes" button	The System deletes a Case archiving policy, and it is not visible on the archiving policies list.
Alternate Flow 3	1	The Administrator clicks "No" button	The System discards delete action which means the case archiving policy continues to be visible on archiving policies case's list.
Alternate Flow 4	1	The Administrator clicks "Reset" button	The System discards all values from the fields on the form and return to previous values on server.
Alternate Flow 5	1	The Administrator clicks "Refresh" button	The System redisplay the form.
Alternate Flow 6	1	The Administrator clicks "Back" button	The System closes present form and returns to previous form.

Alternate Flow 7	1	The Administrator clicks on "Settings" button	The System display "Archiving Policies Settings" form, which contains: - a checkbox field "Archive Messages" – when clicked indicates that the messages are to be archived - "Default Period (Days) *" – mandatory list which contains values type integer, indicating number of days - "Reset" button - "Save" button
	2	The Administrator fills the fields and clicks "Save" button	The System saves data, closes "Archiving Policies Settings" form, and returns to the previous form.
Alternate Flow 8	1	The Administrator clicks on the "Reset" button	The System discard all changes made on the fields from this form and restore previous values from the server.

UC_RA_02 Configure location and messages repositories

Use Case ID:	UC_RA_02		
Use Case Name:	Configure location and messages repositories		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator configures the cases and messages repositories parameters (i.e., name, location, minimum size)		
Trigger:	The Administrator accesses "RINA Archiving" and then select "Archiving Repositories".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin		
Post conditions:	The Administrator configured the location of the cases and messages repositories, set up volumes		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Archiving Repositories" option from "Rina Archiving" menu option	The System displays "Archiving Repositories" form which contains: • "Refresh" button • "Add Repository" button • a grid for displaying the existing repositories, which contains columns:

			○ "Volume Name" ○ "Min Threshold (MB)" - (Once the minimum threshold (MB) is reached -the disk space used by archives exceeds this value, the administrator receives a notification to check the disk space availability on the respective volume) ○ "Path" ○ "Actions", for each displayed repository, the Administrator has available : ○ "Edit" button ○ "Delete" button
	2	The Administrator clicks on the "Add Repository" button	The System displays the "Archiving Repository form" which includes: • "Volume Name *" - free-text field, mandatory • "Min Threshold (MB) *" – counter field, mandatory • An area labelled "Locations" with following fields ○ "Path*" – mandatory, free-text field and corresponding "Delete" button ○ "Add" button – when clicked, it repeats the "Path*" field • "Save" button • "Reset" button • "Back" button
	3	The Administrator clicks the "Add" button	The System display a new "Path *" - mandatory free-text field and a new corresponding "Delete" button
	4	The Administrator clicks on the "Delete" button	The system deletes the row with the field "Path *" and the "Delete" button
	5	The Administrator fills in the fields and clicks "Save" button	The System saves the data and displays pop-up message 'Archiving Repository successfully saved'. The System closes the form and returns to the form "Archiving Repositories" with the new repository item displayed in the grid.

	6	The Administrator clicks on the "Delete" button corresponding to a repository entry from the display grid.	The System displays pop-up window with the message "You are about to delete the archiving repository: <Volume name>" - "Yes" button - "No" button.
	7	The Administrator clicks on the "Yes" button	The System deletes selected archiving repository and displays pop-up message "Archiving repository successfully saved".
Alternative Scenario 1	1	At step 7, the Administrator clicks "No" button	The System displays the item in the grid.
Alternative Scenario 2	1	After step 5, the Administrator clicks on the "Edit" button corresponding to a repository entry from the display grid.	The System enables for edit all the values displayed in the grid corresponding to the repository.
	2	The Administrator fills in the fields on the grid and clicks on the "Save" button	The System saves data and displays pop-up message 'Archiving repository successfully saved'. The System displays the row line with the data changed in view mode.
Alternative Scenario 3	1	At step 2 of Alternative Scenario 2, the Administrator clicks "Cancel" button	The System discards all changes and displays the line item with previous values before being edited.

UC_RA_03 Set up message archiving repository policy

Use Case ID:	UC_RA_03		
Use Case Name:	Set up message archiving repository policy		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator configures the volumes(repositories) where the messages are to be stored for archiving purposes.		
Trigger:	The Administrator accesses "RINA Archiving" and then select "Message Archiving Repository Policy".		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user has defined archiving policies and volumes		
Post conditions:	The Administrator has configured the volume where the messages are to be stored for archiving purposes		

Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Message Archiving Repository Policy" option from "RINA Archiving" menu option	The System displays the screen which contains: "Volume *" – mandatory, drop-down list field with possible values the list of volumes defined by the Administrator by performing UC_RA_02 ("Min Threshold (MB)") associated to selected volume, free-text field, disabled for editing – the System populates the corresponding value after a selection is made in the "Volume*" field. - "Reset" button - "Save" button
	2	The Administrator fills in "Volume*" field and clicks "Save" button	The System saves data on server. The System displays pop-up window with message "Message archiving repository policy successfully saved"
Alternative Scenario 1	3	The Administrator clicks "Reset" button	The System discards all changes and return to previous values on server.

UC_RA_04 Set up message retention policies

Use Case ID:	UC_RA_01		
Use Case Name:	Set up message retention policies		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	06.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator can set up the default message retention period prior to messages getting removed.		
Trigger:	The Administrator clicks on the "RINA Archiving" button from main menu, then clicks on the "Message Retention Policies" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin		
Post conditions:	The user set up the policy for retaining messages		
Main Scenario:	#	Step actions	Expected Result

	1	The Administrator clicks on the "RINA Archiving" menu option, then on the "Message Retention Policies" button	The System displays the form "Message Retention Policies", which includes: • A counter field labelled "Default Period (Days) *" – default value 90 days • "Save" button • "Reset" button – when clicked, the System discards all the changes done by the user and displays the values retrieved from the server.
	2	The Administrator changes the value of the "Default Period (Days) *" field and clicks on the "Save" field.	The System saves the default message retention period and displays the message: "Message retention policies successfully saved"

Fields Details

RINA archiving – Archiving Policies

No.	Item name	Type	Validation/business rules
1	Refresh	Button	
2	Policies	Grid	Contains columns: Sector Process Role Days Actions
3	Add Policies	Button	When clicked the system displays:
4	Process Owner	Check box	
5	Counterparty	Check box	
6	Archiving Period (days)	List	Contains numerical values
7	Sector	List	Possibility to choose, by clicking on associated check box
8	BUC	List	Possibility to choose, by clicking on associated check box
9	Back	Button	
10	Reset	Button	
11	Save	Button	

RINA Archiving - Archiving repositories

No.	Item name	Type	Validation/business rules
1	Add Repository	Button	At click is displayed form which contains:
2	Volume Name*	Free text box field	Mandatory
3	Min. Threshold (MB)*	List	Mandatory
4	Path	Free text box field	Mandatory
5	Back	Button	
6	Reset	Button	
7	Save	Button	
8	Archiving Repositories	Grid	Contains columns: Volume name Min. Threshold (MB) Path Actions Has associated buttons: Edit button Pressing on Edit button, the system displays Save and Cancel buttons Delete button

RINA Archiving - Message Retention Policy

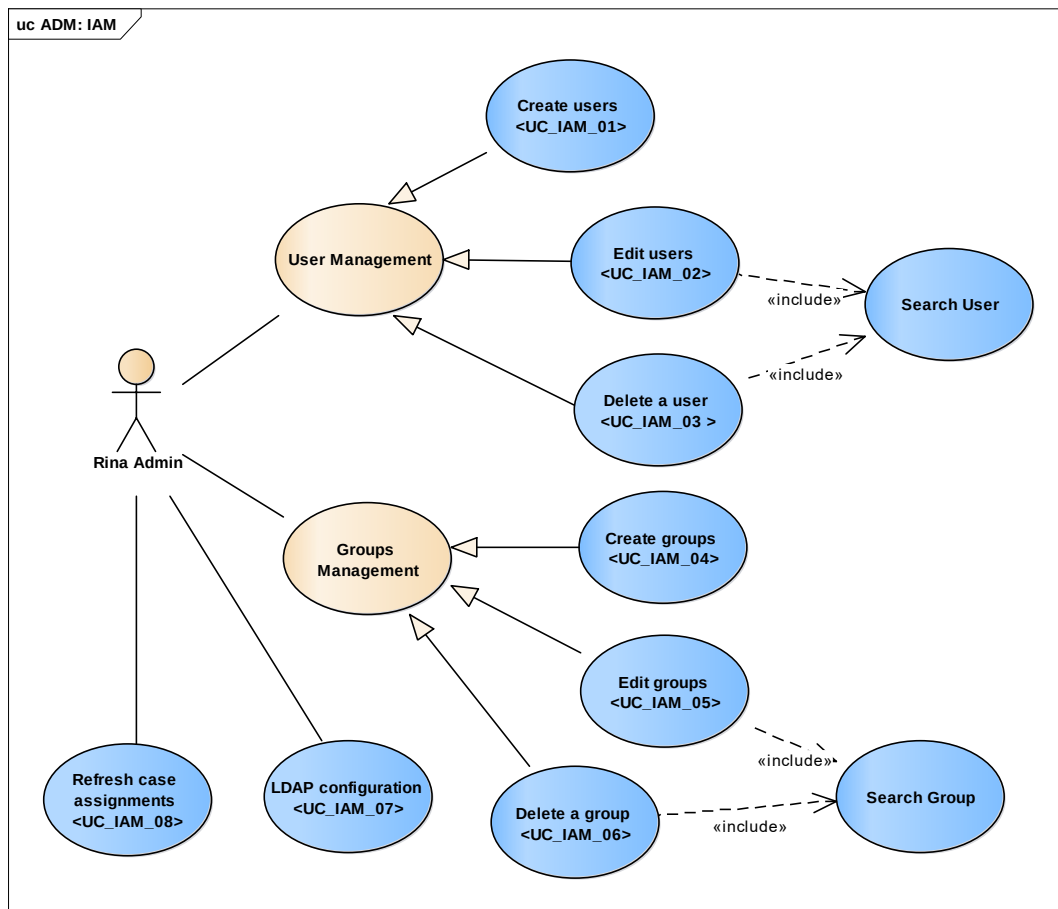
No.	Item name	Type	Validation/business rules
1	Default period days	List	Contains volumes, mandatory
2	Reset	Button	
3	Save	Button	

RINA Archiving - Message archiving repository policy

No.	Item name	Type	Validation/business rules
1	Default period days	List	Contains volumes, mandatory
2	Reset	Button	
3	Save	Button	

6.6 IAM

Use case diagrams



Use Case View

UC_IAM_01 Create users

Use Case ID:	UC_IAM_01		
Use Case Name:	Create users		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to configure users in RINA, create new users (every user belongs to a group and have defined multiples roles) and deletes users. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator accesses "IAM" menu option and clicks "Users" option.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application (with Admin role)		

	3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value) 4. The user's group is already created		
Post conditions:	The Administrator has been created and deleted the user, defined the group and roles associated to the user. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "IAM" menu option, "Users" option	The System displays: - "Search" - bar element, which offers the possibility to write and search users from the list. This element has associated "x" red icon, used to delete the characters written for the search. - "Add Users" button - "Refresh" button Grid which contains the following columns: • "Username" - (The length of Username should be equal to or less than 15 characters and the space char (" ") is not permitted). • "First name" • "Last name" • "Email" • "Enabled" – check box that describe whether the account is <i>Enabled</i> or not (the user can be provisioned for a later phase but may not be currently active). • "Actions" with: • "Edit" button (appear in case there is at least one user defined)"Delete" Button (appear in case there is at least one user defined)
	2	The Administrator clicks "Add User" button	The System displays "User Form", with the following sections: "New User" section contains: • "Username" - mandatory, free-text field, case sensitive (The length of Username should be equal to or less than 15 characters and the space char (" ") is not permitted). • "Password" – free-text field (use functionality visible/invisible mode) (Standard, the minimum length of the Users Passwords, is

			8 and the recommended length is 10 characters), case sensitive • "Confirm Password" - free-text field (use functionality visible/invisible mode) (Standard, the minimum length of the Users Passwords, is 8 and the recommended length is 10 characters), case sensitive • "First Name" - mandatory, free-text field • "Last Name" - mandatory, free-text field • "Email" - mandatory, free-text field • "Mobile Number" - free-text field • "Business Keystore Certificate Alias" - drop-down list • "Enabled" - check box (whether the account is <i>Enabled</i> or not (the user can be provisioned for a later date but may not be currently active)). Section "Memberships" - the Administrator adds the relevant groups and roles. Membership is the link between the user, the group and the user's role in the group). (A User/Clerk can have multiple roles. A user with multiple roles can perform any action permitted by all the assigned roles. As an example, an authorised clerk that is also a medical user can send SEDs (permitted by the authorised clerk role) and also access classified medical attachments (permitted by the medical user role) - "Add" button - the user adds roles to the group. - "Clear" button - the user deletes an associated role to the group. ("Medical" and "VIP" roles have limited permissions and can be considered as supplementary roles that are assigned to specific users when access to critical data is required.
--	--	--	---

			"VIP" users are able to select/unselect the "Sensitive" flag in the "Case Metadata" pop-up. "VIP" user may set "Sensitive Case" flag BUT in order to create/edit documents must be also "authorised" / "non authorised" clerk. In order to send documents, the clerk must have the "authorised" clerk role. In order to view case documents, the clerk must be "authorised"/"non authorised", "supervisor" and/or "viewer". "Medical" user can tag/un-tag an attachment as medical. In order to <u>add must be also "authorised"/"non authorised" clerk. In order to view it, the user must be "authorised"/"non authorised", "supervisor" and/or "Viewer"</u> "Supervisors", "Authorised" clerks and "non-authorised" clerks are able to change the "Criticality" and "Importance" properties (Case Assignments) Some groups can be labelled with the "Organisational Unit" flag (the equivalent of the OU in LDAP). This is used in order to represent the branches. - "Reset" button - "Save" button
	3	The Administrator click "Add" button on the membership section	The System adds a role/group to the user.
	4	The Administrator fills in "New user" section and click "Save" button	The System creates a new user, which is included and displayed as a line item in the users list. The System displays the message pop-up window 'User successfully saved'

Alternative scenario 1	1	The Administrator fill in the new user section and Membership section and clicks "Add" button	The System displays a message 'Please first select a group', in case that the Administrator has not selected a group.
	2	The Administrator select a group and a role and click on "Save" button	The System saves all data fields on the server. The System closes the "User Form" and return to "Users" form.
Alternative Scenario 2	1	The Administrator choose a group/role and click "Clear" button	The System discards all changes.
	2	The Administrator fills the new user sections, adds a group, and click on "Save" button	The System saves the data and display pop-up message 'User successfully saved'. The System closes "User Form" and returns to "Users" Form.
Alternative Scenario 3	1	The Administrator click "Edit" button on form "Users"	The System displays "User Form" filled with the data about the User in the line selected, with the following sections: "New User" section contains: • "Username" - mandatory, free-text field, case sensitive (The length of Username should be equal to or less than 15 characters and the space char (" ") is not permitted). • "Password" – free-text field (use functionality visible/invisible mode) (Standard, the minimum length of the Users Passwords, is 8 and the recommended length is 10 characters), case sensitive • "Confirm Password" - free-text field (use functionality visible/invisible mode) (Standard, the minimum length of the Users Passwords, is 8 and the recommended length is 10 characters), case sensitive • "First Name" - mandatory, free-text field • "Last Name" - mandatory, free-text field • "Email" - mandatory, free-text field • "Mobile Number" – free-text field • "Business Keystore Certificate Alias" – drop-down list

		• “Enabled” – check box (whether the account is Enabled or not (the user can be provisioned for a later date but may not be currently active). Section “Memberships” - the Administrator adds the relevant groups and roles. Membership is the link between the user, the group and the user’s role in the group). (A User/Clerk can have multiple roles. A user with multiple roles can perform any action permitted by all the assigned roles. As an example, an authorised clerk that is also a medical user can send SEDs (permitted by the authorised clerk role) and also access classified medical attachments (permitted by the medical user role) - “Add” button - the user adds roles to the group. - “Clear” button – the user deletes an associated role to the group. (“Medical” and “VIP” roles have limited permissions and can be considered as supplementary roles that are assigned to specific users when access to critical data is required. “VIP” users are able to select/unselect the “Sensitive” flag in the “Case Metadata” pop-up. “VIP” user may set “Sensitive Case” flag BUT in order to create/edit documents must be also “authorised” / “non authorised” clerk. In order to send documents, the clerk must have the “authorised” clerk role. In order to view case documents, the clerk must be “authorised”/“non authorised”, “supervisor” and/or “viewer”.
--	--	--

			"Medical" user can tag/un-tag an attachment as medical. In order to add must be also "authorised"/"non authorised" clerk. In order to view it, the user must be "authorised"/"non authorised", "supervisor" and/or "Viewer" "Supervisors", "Authorised" clerks and "non-authorised" clerks are able to change the "Criticality" and "Importance" properties (Case Assignments) Some groups can be labelled with the "Organisational Unit" flag (the equivalent of the OU in LDAP). This is used in order to represent the branches. - "Reset" button - "Save" button
	2	The Administrator click "Save" button	The System save the data and display pop-up message 'User successfully saved'. The System close "User Form" and returns to "Users" Form.
Alternate Scenario 4	1	The Administrator click "Delete" button on form "Users"	The System opens a pop-up box with the message "You are about to delete the user: xxxxx". - "Yes" button - "No" button (A user/clerk <u>cannot</u> be deleted by the Administrator if an Open Case is assigned directly to the User or if a direct Case assignment is established through the application of a policy rule (i.e., when a rule applies an assignment to a Group and not to a User, any member of that Group can be deleted if the member is not directly assigned to an Open Case). (A user/clerk can be deleted by the Administrator only if the user does not have assigned open cases (may have cases closed or archived))

	2	The Administrator click "Yes" button	The System deletes the respective data from the server and from the list of users.
Alternate Scenario 5	1	The Administrator click "No" button	The System discards all changes made and display the respective user on the list of users.
Alternate Scenario 6	1	The Administrator click the "Reset" button	The System discards all changes of values in the fields of the form and return to previous values on server. The System closes "User Form" and return to "Users" form.
Alternate Scenario 7	1	The Administrator click the "Back" button	The System closes "User Form" and return to "Users" form.
Exception 1	1	The Administrator fills in the name of an existing user	The System indicate the creation of a new user was failed and display an error message like "The Name of the User should be unique for every RINA installation. The rule is applied at the tenant level, i.e., the existence of 2 or more users with the same name under the same tenant is not permitted.

UC_IAM_02 Search user

Use Case ID:	UC_IAM_02		
Use Case Name:	Search users		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to search data related to user. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "IAM" menu option, then "User"		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value)		
Post conditions:	The Administrator has updated the user parameters. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "IAM" component, subsection "Users", and search a user, on 'Search' bar	The System executes a search in the list of users for the written text included in "Search" element.

		element, situated left-hand side of the screen	The System display the user in the grid if it is found on the search.
--	--	--	---

UC_IAM_04 Create groups

Use Case ID:	UC_IAM_04		
Use Case Name:	Create groups		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to create a new group (it is advisable to use groups in order to assign permissions, instead of assigning rights individually to users). The system allows the Administrator to assign users to groups and then assign authorization policies to groups and resources		
Trigger:	N/A		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application (with Admin role) 3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value) The system allows the Administrator to assign users to groups and then assign authorization policies to groups and resources		
Post conditions:	The Administrator created a new group. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "IAM" menu option, "Groups" option	The System displays the "Groups" form which contains: - "Refresh" button - "Search" element - "Add Group" button Group grid, which contains: - "Name" - "Description" - "Organization Unit" - ("Organisation Unit" (OU). An OU is intended to be a 'super-group'; for instance, it may be used to represent/cover a branch (in a multi-branch environment)- "Created" - "Actions" with: - "Edit" button - "Delete" button

	2	The Administrator clicks on "Add Group" button	The System displays "Groups" form which contains: - "Name *" – mandatory, free-text field - "Description" – free-text field - "Organization Unit" - check box - "Parent Group" - list that contains the list with groups and associated groups to the parent group. - "Clear" - used to unselect the group - "Save" button - "Reset" button - "Back" button The Administrator needs to decide its position/location in the group hierarchy, which means it is needed to decide first which will be its parent group. Each group needs to have a parent group, except for the root group.
	3	The Administrator fills in the fields and clicks on the "Save" button	The System saves the data, creates the new group (following the provided group structure by the administrator) The system displays a pop-up message 'Group successfully created'.
Alternative scenario 1	1	The Administrator clicks "Reset" button	The System discards all values from the form.
Alternative Scenario 2		The Administrator click on "Back" button	The System closes "Group Form" and return to step 1 of the Main scenario
Exception 1	1	The Administrator fills in the name of an existing group	The System don't create a new group and display the error message The Name of the Groups should be unique for every RINA installation. The rule is applied at the tenant level, i.e. the existence of 2 or more groups with the same name under the same tenant is not permitted.

UC_IAM_05 Search groups

Use Case ID:	UC_IAM_05		
Use Case Name:	Search groups		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to search groups		
Trigger:	The Administrator selects "IAM" menu option, then "Groups" option and clicks "Search" element.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application (with Admin role) 3. The user selects the relevant tenant (top left- hand side of the screen – if there is only 1 tenant, the system displays the default value)		
Post conditions:	The Administrator searched group in a list of groups		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "IAM" menu option, "Groups" option	The System display the "Groups" form which contains: - "Refresh" button - "Search" element - "Add Group" button Group grid, which contains: - "Name" - "Description" - "Organization Unit" - ("Organisation Unit" (OU). An OU is intended to be a 'super-group'; for instance, it may be used to represent/cover a branch (in a multi-branch environment) - "Created" - "Actions" with: - "Edit" button - "Delete" button
	2	The Administrator search a group, on 'Search' bar element, situated left-hand side of the screen with a name or part of the name of the group that exists in the grid.	The System executes a search in the list of groups for the written text included in "Search" element. The System display the group in the grid in case it is found on the search.

Alternative Flow 1	1 The Administrator search a group, on 'Search' bar element, situated left-hand side of the screen with a name or part of the name of the group that do not exist in the grid	The System executes a search in the list of groups for the written text included in "Search" element. The System display the grid without any result.
---------------------------	---	--

UC_IAM_05 Modify groups

Use Case ID:	UC_IAM_05		
Use Case Name:	Modify groups		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to modify(edit) groups		
Trigger:	The Administrator selects "IAM" menu option, then "Groups" option and clicks "Edit" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application (with Admin role) 3. The user selects the relevant tenant (top left- hand side of the screen – if there is only 1 tenant, the system displays the default value)		
Post conditions:	The Administrator modified group parameters. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator access "IAM" menu option, "Groups" option	The System displays "Groups" form which contains: - "Refresh" button - "Search" element - "Add Group" button Group grid, which contains: - "Name" - "Description" - "Organization Unit" - ("Organisation Unit" (OU). An OU is intended to be a 'super-group'; for instance, it may be used to represent/cover a branch (in a multi-branch environment)- "Created" - "Actions" with: - "Edit" button

			- "Delete" button
	2	The Administrator clicks on "Edit" button	The System shows the following fields edited in the line item where the "Edit" button is located: - "Name" - "Description" - "Organization Unit" - "Save" button - "Cancel" button
	3	The Administrator fills in the fields on the grid and click "Save" button	The System saves data and modifies the group parameters accordingly. The System displays message 'The group has been successfully updated'. Remark: It should not be possible to modify the name of group to an existing group name - name of the group is unique.
Alternative Scenario 1	4	The Administrator click "Cancel" button	The System discards all changes and return to previous data on server The System returns to step 1 from Main Scenario.
Alternative Scenario 2	5	The Administrator click "Refresh" button	The System redisplayes the form.

UC_IAM_06 Delete a group

Use Case ID:	UC_IAM_06		
Use Case Name:	Delete a group		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to delete group(s)		
Trigger:	The Administrator selects "IAM" menu option, then "Groups" option and clicks "Delete" button.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application (with Admin role) 3. The user selected the relevant tenant (top left- hand side of the screen – if there is only 1 tenant, the system displays only the default value)		

Post conditions:	The Administrator deleted a group. An audit event is raised into Audit Log.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "IAM" menu option, "Groups" option	The System display the "Groups" form which contains: - "Refresh" button - "Search" element - "Add Group" button Group grid, which contains: - "Name" - "Description" - "Organization Unit" - ("Organisation Unit" (OU). An OU is intended to be a 'super-group'; for instance, it may be used to represent/cover a branch (in a multi-branch environment)- - "Created" - "Actions" with: - "Edit" button - "Delete" button The System display several lines of groups previously created on the Use Case "Create groups"
	2	The Administrator clicks on "Yes" button	The System deletes the line item with the group data. The System displays message "Group successfully deleted". The System return to step 1 of Main Scenario.
Alternate Scenario 1	1	The Administrator click "No" button	The System discard all changes and fields value return to previous on server. The System return to step 1 of Main Scenario.
Alternate Scenario 2	1	The Administrator clicks "Refresh" button	The System redisplay the form.
Exception Flow 1	1	The Administrator select a particular group (which has active users assigned) and chooses to delete it	The system does not delete a group, once a case has been sent for that group OR if active users are still available

UC_IAM_07 Setting up LDAP configuration

Use Case ID:	UC_IAM_07		
Use Case Name:	Setting up LDAP configuration		
Created By:	Madalina Alecsandre scu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description :	This use case describes how the system allows the Administrator to add the configuration for synchronizing RINA users and groups (for a specific Tenant) with the structure residing at an LDAP server		
Trigger:	The Administrator selects "IAM" menu option and clicks "LDAP Configuration" option.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application (with Admin role) 3. The user selects the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays the default value)		
Post conditions:	The Administrator configures the relevant parameters and proceeds with the necessary user/group information mapping before the synchronization of the Users/Groups between RINA and the LDAP server		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "IAM" menu option, "LDAP Configuration" option	The System displays 3 subsections, in which the Administrator configures the LDAP sync process. The Group & User Mapping between RINA internal authentication DB and the external LDAP provider follows the LDAP communication parameters configuration. Analytically, the administrator can configure the following parameters' subsections: "Configuration" subsection (RINA/LDAP communication parameters) which contains: • "User *" - mandatory, free-text field (the user account used to authenticate to the LDAP server (for example, "cn=install,ou=people,dc=test domain ,dc=com")) • "Password *" - free-text field case sensitive, mandatory (the password for <i>auth_user_dn</i> <i>auth_ssl</i> – define whether SSL is used for authentication. Accepted values: <i>true</i> or <i>false</i>) • "Url *" - mandatory, free-text field (FQDN/ IP Address and port of the LDAP server to synchronise from) • "Security Authentication *" - mandatory, free-text field (simple (specifies the authentication mechanism to use. Possible values "simple", "none", "sasl_mech", etc)) • "LDAP User Search Base *" - mandatory, free-text field (users_provider_dn for example, "OU=people, DC=testdomain, DC=com"))

		• "LDAP Group Search Base *" - free-text field (users_provider_dn, for example, "OU=people, DC=testdomain, DC=com") • "User Search String" - free-text field (LDAP query to filter user. For example: "(&(objectClass=inetOrgPerson)(!(uid=install)))") • "Group Search String" - free-text field (Group filtering. For example, "(objectclass=posixGroup)" <i>groups_mapping</i> - Mapping of the groups "group_name=cn description=description") "Group Mappings" subsection, which contains the following group attributes/fields: • "LDAP Unique Identifier *" - mandatory, free-text field (LDAP attribute, which is unique and used to identify the group, in most LDAP implementations is "distinguishedName" or "sAMAccountName") • "Group name *" - mandatory, free-text field (the full qualified name of the group) • "Display Name *" - mandatory, free-text field (the short name of the group) • "Description" - free-text field (the description of group from LDAP) • "Is group Organisation Unit" - free-text field (Boolean to declare if the given entity is an organisation unit) • "Is group reassigned" - free-text field (Boolean to check if the given entity needs reassignment) • "Parent group Id" - free-text field (the id of the parent Group) • "Group's path" - free-text field (the full path of the Group to root unit) • "Creation Date" - free-text field (the Group creation date) • "Last Update" - free-text field (the last update of the Group) • "Groups members" - free-text field (Attribute of a group which maps members of this group (users). If it is set, members of this group will be synchronized, even if they are not looked up by user search string) "User Mappings" subsection, which contains the following User attributes/fields: • "LDAP Unique Identifier *" - mandatory, free-text field (LDAP attribute, which is unique and used to identify the group, in most LDAP implementations is "distinguishedName" or "sAMAccountName") • "Username *" - mandatory, free-text field (the full qualified Username)
--	--	---

			• "First Name *" - mandatory, free-text field (the User's first name) • "Last Name *" - mandatory, free-text field (the User's last name) • "Email *" - mandatory, free-text field (the User's email) • "Phone Number" - free-text field (the User's phone number) • "Is enabled" - free-text field (Boolean to declare if the User is enabled or not) • "Is administrator" - free-text field (Boolean to declare if the User is the administrator or not) • "Creation Date" - free-text field (the User creation date in the system) • "Last Update" - free-text field (the last update of the User info) • "User's Groups" - free-text field (the property mapping to LDAP Groups to which the User belongs) • "User's Role" - free-text field (the appropriate selection from a User's roles list) - "Save" button - "Reset" button - "Synchronize LDAP"
	2	The Administrator fill in the fields and clicks "Save" button	The system validates the inserted data and displays the messages 'LDAP Configuration settings successfully saved', 'LDAP user mappings successfully saved', 'LDAP group mapping settings successfully saved' (After successful synchronization with LDAP server, it is possible to log in to system with LDAP credentials)
Alternative Scenario 1	1	The Administrator clicks on "Synchronize LDAP", after setting up the parameters	The System synchronizes the RINA content with one LDAP server each time The System allows the Administrator to define the most appropriate mapping for the selected institution (Tenant).
Alternative Scenario 2	1	The Administrator clicks "Reset" button	The System discards all changes and return to previous values from server.

Fields Details

IAM - Users

No.	Item name	Type	Validation/business rules
1	Select tenant (with explanatory notes associated)	List	(a value is selected by default)
2	Search bar element		Delete
3	Refresh	Button	Refresh screen

4	Add user	Button	At click displays User form, which contains:
4.1	Username	Free text box field	Mandatory
4.2	Password	Free text box field	Mandatory
4.3	Confirm password	Free text box field	Mandatory
4.4	First Name	Free text box field	Mandatory
4.5	Last Name	Free text box field	Mandatory
4.6	Email	Free text box field	Mandatory, suggested format admin@example.com
4.7	Mobile number	Free text box field	Suggested format +00-00000000
4.8	Business Keystore Certificate Alias	List	
4.9	Enabled	Check box	
4.10	Memberships	Label	
4.11	Group	List	With associated Clear button
4.12	Role	List	
4.13	Add	Button	
5	Users	Grid	Contains columns: Username First Name Last Name Email Enabled Actions Every row has associates for Actions column 2 buttons
5.1	Edit	Button	The system displays User form (step 4)
5.1	Delete	Button	

IAM – Groups

No.	Item name	Type	Validation/business rules
1	Select tenant (with explanatory notes associated)	List (a value is selected by default)	
2	Search bar element		Search Delete
3	Refresh	Button	Refresh screen
4	Add Group	Button	At click displays Group Form, which contains fields:
4.1	Name	Free text field	Mandatory
4.2	Description	Free text field	
4.3	Organization Unit	Check box	
4.4	Parent Group	Free text box	Has associated Clear button
4.5	Back	Button	
4.6	Reset	Button	
4.7	Save	Button	
5	Groups	Grid	Contains columns:

			Name Description Organization unit Created Actions Every row has 2 buttons:
5.1	Edit	Button	When click the system displays: Save and Cancel Buttons
5.2	Delete	Button	

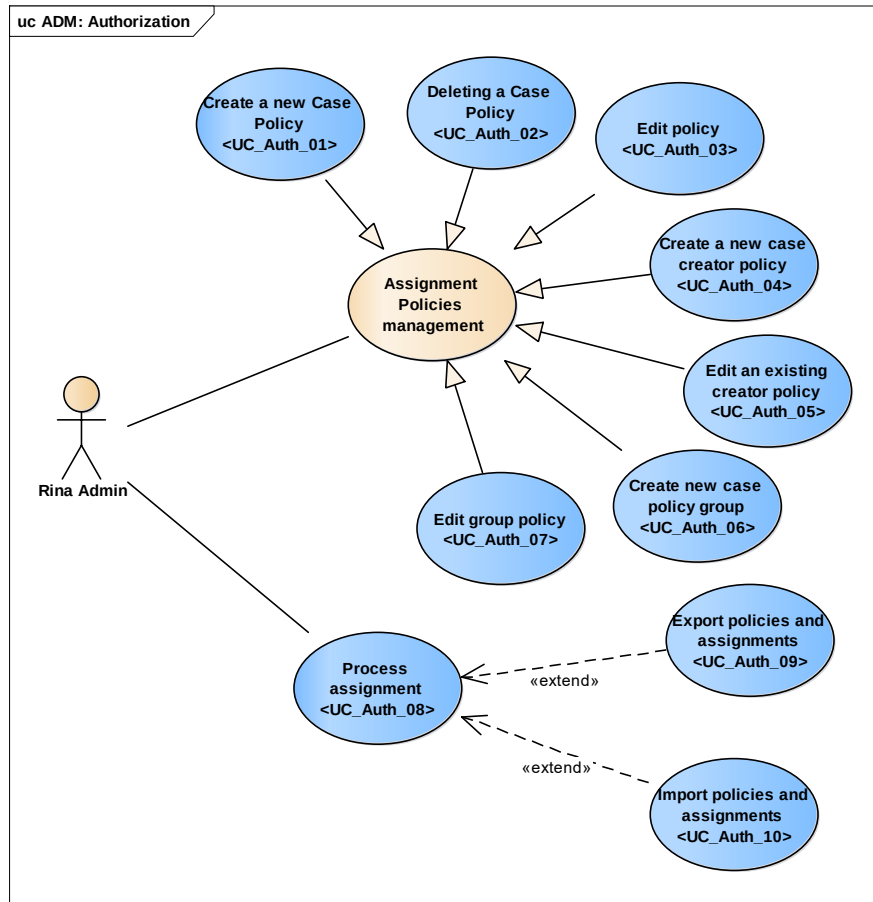
IAM – LDAP Configuration

No.	Item name	Type	Validation/business rules
1	Select tenant (with explanatory notes associated)	List	(a value is selected by default)
2	LDAP configuration for Tenant Name	Label	
3	Configuration section	Label	
4	User:	Free text box field	Mandatory, suggested format user@user.lab
5	Password	Free text box field	Visible/invisible mandatory
6	URL	Free text box field	mandatory, suggested format ldap://123.123.123.54:389
7	Security Authentication	Free text box field	Mandatory
8	LDAP User Search Base	Free text box field	Mandatory, suggested format OU=example1, DC=example2, DC=example3
9	LDAP Group Search Base	Free text box field	Mandatory, suggested format OU=example1, DC=example2, DC=example3
10	User Search String	Free text box field	
11	Group Search String	Free text box field	
12	Group Mappings	Label	
13	LDAP Unique Identifier	Free text box field	Mandatory
14	Group name	Free text box field	Mandatory
15	Display name	Free text box field	Mandatory
16	Description	Free text box field	
17	Is group Organization unit	Free text box field	
18	Is group reassigned	Free text box field	
19	Parent group id	Free text box field	

20	Group's path	Free text box field	
21	Creation date	Free text box field	
22	Last update	Free text box field	
23	Group's members	Free text box field	
24	User Mappings (<i>section</i>)	Label	
25	LDAP Unique Identifier	Free text box field,	Mandatory
26	Username	Free text box field	Mandatory
27	First name	Free text box field	Mandatory
28	Last name	Free text box field	Mandatory
29	Email	Free text box field	Mandatory, suggested format admin@example.com
30	Phone number	Free text box field	
31	Is enabled	Free text box field	
32	Is administrator	Free text box field	
33	Creation date	Free text box field	
34	Last update:	Free text box field	
35	User's groups	Free text box field	
36	User's Role	List	Contains list with groups
37	Reset	Button	
38	Save	Button	
39	Synchronize LDAP	Button	

6.7 Authorization

Use case diagrams



Use Case View

UC_Auth_01 Create a new Case Policy

Use Case ID:	UC_Auth_01		
Use Case Name:	Create a new Case Policy		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	09.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the system allows the Administrator to configure who gets access to RINA resources by creating and configuring a new policy (the policies provide the Administrator with the tools required to manage and restrict access to cases in RINA). The case assignment policies control the permissions and the access to cases. All settings are independent and distinguished between RINA Tenants.		
Trigger:	The Administrator selects "Authorization" menu option, then "Assignment Policies" and clicks list box "New Policy"		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin		

	3. The user selects the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays the default value)		
Post conditions:	The Administrator has created a new case policy.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator selects "Authorization" menu option, then clicks on the "Assignment Policies" button	The System displays the "Assignment Policies" form, with the following fields: • "Refresh" button • "Search" free text field - enables the Administrator to search within the list of existing policies based on entered text. This field has associated "x" red icon, used to delete the text to be searched and a magnifying glass icon to launch the search. • "New Policy" button. This button has associated an expand "v" button – when clicked, it provides two additional buttons: "New Creator Policy" and "New Policy Group". • a grid for displaying all existing policies, with columns: ○ "Name" ○ "Description" ○ "Type" ○ "Actions", for each displayed policy, the Administrator has available in this column: - "Edit" button - "Delete" button
	2	The Administrator clicks on the "New Policy" button	The System displays the "Policy Form", which contains: • "Name *" - mandatory, free-text field • "Description" - free-text field • "Color" –drop down list - (to be associated to a policy, which may provide visual indications in the section Process assign) • Subsection labelled "Rule X" ("X" from 1...n) with the following fields: ○ "Add" button – when clicked, it adds a new subsection of type "Rule X" ○ Information label - "When these conditions are met:"

		○ selection field "Application Role in" – with possible values: - "Process Owner" button - "Counter Party" button - "Any" button Based on the selection done by the Administrator in the "Application Role in" field, the System enables different fields in the "Rule x" subsection, as follows • with "Process Owner" button selected the System display: ○ "Sector In" – drop-down list, which contains all the EESSI sectors, i.e., "FB", "Pensions", etc. ○ "Process Type In" – drop-down list which contains all the available BUC types of the selected Sector. ○ "Case Creator In" – display field populated by the System based on selection of the Administrator for users and or groups, in the dedicated fields. This field has associated two buttons: ○ "Clear" button – when clicked, all selection of the Administrator for users and or groups is cleared ○ "Add" button ○ "Assign To Actors" – drop-down list, contains all roles ○ "These Users and Groups *" – with: ○ "Creator User" – checkbox ○ "Creator Branch" – checkbox ○ "Select Group" – drop down list that contain all groups ○ "Clear" button ○ "Add" button ○ "Select User" • with "Counter Party" button selected the System display: ○ "Sector In" – drop-down list, which contains all the EESSI sectors, i.e., "FB", "Pensions", etc. ○ "Process Type In" – drop-down list which contains all the available BUC types of the selected Sector.
--	--	--

			○ "Subject Address like" – free text field ○ "Owner Country In" – drop-down list contains participating countries ○ "Owner Organization In" – search element ○ "Assign To Actors" – drop-down list, contains all roles ○ "These Users and Groups *" – with: ○ "Select Group" – drop down list that contain all groups ○ "Clear" button ○ "Add" button ○ "Select User" • with "Any" button selected the System display: ○ "Sector In" – drop-down list, which contains all the EESSI sectors, i.e., "FB", "Pensions", etc. ○ "Process Type In" – drop-down list which contains all the available BUC types of the selected Sector. ○ "Assign To Actors" – drop-down list, contains all roles ○ "These Users and Groups *" – with: ○ "Select Group" – drop down list that contain all groups ○ "Clear" button ○ "Add" button ○ "Select User" The form also contains: • "Save" button • "Reset" button • "Back" button
	3	The Administrator clicks "Add" button in the subsection "Rule X"	The System creates a new subsection (named "Rule 1") above the one (named "Rule 2") already displayed in the form (renumbering the number on each of the rules) even if the previous one is not filled because the rule who apply first concerns the order of priority from top to down (from the most recent to the oldest unless it is used the button "Move Down" or "Move Up" to change the order of priority between rules although the order of

		the rules keep being the same on the screen (from top to the bottom of the screen) The System display: - "Rule 1" - "Move Down" button - "Delete" button - "Add" button - "When these conditions are met:" The System display by default the "Any" button clicked from the field "Application Role In" and the fields: - "Sector In" - "Process Type In" - "Assign to Actors" - "These Users And Groups *" - "Select Group" - "Clear" button - "Add" button - "Select User" - "Please select group first" - "And stop processing more rules" - "Rule 2" - "Move Down" button - "Delete" button - "Add" button - "When these conditions are met:" The System displays by default the "Any" button clicked from the field "Application Role In" and the fields: - "Sector In" - "Process Type In" - "Assign to Actors" - "These Users And Groups *" - "Select Group" - "Clear" button - "Add" button - "Select User" - "Please select group first"
--	--	--

			- "And stop processing more rules" - "Save" button - "Reset" button - "Back" button
	4	The Administrator fills the fields before the subsection "Rule 1" and click in "Process Owner" button from the field "Application Role In"	The System displays the fields: - "Sector In" – drop-down list, which contains all the EESSI sectors, i.e., "FB", "Pensions", etc. - "Process Type In" – drop-down list which contains all the available BUC types of the selected Sector. - "Case Creator In" – list with: - "Clear" button - "Add" button - "Assign To Actors" – drop-down list, contains all roles - "These Users and Groups *" – with: - "Creator Use" – check box, mandatory - "Creator's Branch" – check box, mandatory - "Select Group" – drop down list that contain all groups - "Clear" button - "Add" button - "Select User" - "Please select group first" - "Save" button - "Reset" button - "Back" button (The System apply these rules sequentially until the first successful rule completely fulfils the defined criteria and conditions. Therefore, the order of the rules in the provided list defines the priority in which the system processes the rules. The Administrator can enforce a specific rule by changing its order on the list. The change of the priority order can be done by using the selections (<i>Move rule Up</i>) and (<i>Move rule down</i>) links. The checked legend "And stop processing more rules", has been located at the end of each rule to clearly indicate that the system

			stops processing the rules queue sequentially if the specific rule fulfils completely the conditions. Eventually the Administrator removes any rule by clicking on the appropriate button "Remove Rule")
	5	The Administrator selects one value from the list on "Case Creator In" and click on "Add" button	The System displays: - a non-editable field with the value selected in the previously mentioned list - "Delete" button
	6	The Administrator clicks "Delete" button from the field "Case Creator In"	The System hides: - a non-editable field with the value selected in the previously mentioned list - "Delete" button The System return to step 4 in case the Administrator need to create more values for the field "Case Creator In".
	7	The Administrator clicks "Clear" button from the field "Case Creator In"	The System clear the selection of the value in the list of the field "Case Creator In" The System return to step 4 of the Main Scenario in case the Administrator need to create more values for the field "Case Creator In".
	8	The Administrator fills the fields, select a value from the list of the field "Select Group" and click "Add" button	The System displays in the same line as the field "Select User": - a non-editable field with the role(s) available for this group selected previously in the mentioned list - "Add" button
	9	The Administrator clicks "Add" button from the line of the field "Select User"	The System displays a new line before the field "Select Group" with: - a non-editable field with the role available for this group selected previously in the mentioned list - "Delete" button
	10	The Administrator clicks "Delete" button from the new line above the "Select Group" field	The System hides: - a non-editable field with the role value from the previously mentioned list - "Delete" button

			The System return to step 8 of the Main Scenario in case the Administrator want to add more roles for the same or other group
	1 1	The Administrator clicks on "Save" button	The System creates a new policy, which is listed in policies' list. The system displays a pop-up message "Assignment policy successfully saved" The System return to "Assignment Policy" form with the new case policy added and visible on the grid.
Alternative Scenario 1	1	The Administrator clicks "Delete" button from "Rule 1"	The System displays the following fields as previously fill: - "Name *" - "Description" - "Color" The System renumber "Rule 2" to "Rule 1" and delete all fields from previous "Rule 1". The System display only the 1st or more "Rule X" not deleted so far. The System return to step 2 of the Main Scenario.
Alternative Scenario 2	1	The Administrator clicks "Move Down" button from "Rule X"	The System deletes values from "Rule X" from the screen and from the server. The System display fields and their values from "Rule X+1" into the position of "Rule X" The System renumber the rules number from the top of screen to bottom. The System return to step 2 of the Main Scenario.
Alternative Scenario 3	1	The Administrator clicks "Move Up" button from "Rule X+1"	The System exchanges the values from the position of the "Rule X+1" into the position of "Rule X". The System renumber the rules number from the top of screen to bottom. The System return to step 2 of the Main Scenario.
Alternative Scenario 4	1	The Administrator fills the fields before the	The System displays the fields:

		subsection "Rule 1" and click in "Counter Party" button from the field "Application Role In"	- "Sector In" – drop-down list, which contains all the EESSI sectors, i.e., "FB", "Pensions", etc. - "Process Type In" – drop-down list which contains all the available BUC types of the selected Sector. - "Subject Address Like" – free-text field - "Owner Country In" – drop-down list, contains all European countries - "Owner Organization In" – search component - "Assign To Actors" – drop-down list, contains all roles - "These Users and Groups *" – with: - "Select Group" – drop down list that contain all groups - "Clear" button - "Add" button - "Select User" - "Please select group first" - "Save" button - "Reset" button - "Back" button (The System apply these rules sequentially until the first successful rule completely fulfils the defined criteria and conditions. Therefore, the order of the rules in the provided list defines the priority in which the system processes the rules. The Administrator can enforce a specific rule by changing its order on the list. The change of the priority order can be done by using the selections (<i>Move rule Up</i>) and (<i>Move rule down</i>) links. The checked legend "And stop processing more rules", has been located at the end of each rule to clearly indicate that the system stops processing the rules queue sequentially if the specific rule fulfils completely the conditions. Eventually the Administrator removes any rule by clicking on the appropriate button "Remove Rule")
Alternative Scenario 5	1	The Administrator fill the fields before the subsection "Rule 1" and	The System display the fields: - "Sector In" – drop-down list, which contains all the

		click in "Any" button from the field "Application Role In"	EESSI sectors, i.e., "FB", "Pensions", etc. - "Process Type In" – drop-down list which contains all the available BUC types of the selected Sector. - "Assign To Actors" – drop-down list, contains all roles - "These Users and Groups *" – with: - "Select Group" – drop down list that contain all groups- - "Clear" button - "Add" button - "Select User" - "Please select group first" - "Save" button - "Reset" button - "Back" button (The System apply these rules sequentially until the first successful rule completely fulfils the defined criteria and conditions. Therefore, the order of the rules in the provided list defines the priority in which the system processes the rules. The Administrator can enforce a specific rule by changing its order on the list. The change of the priority order can be done by using the selections (<i>Move rule Up</i>) and (<i>Move rule down</i>) links. The checked legend "And stop processing more rules", has been located at the end of each rule to clearly indicate that the system stops processing the rules queue sequentially if the specific rule fulfils completely the conditions. Eventually the Administrator removes any rule by clicking on the appropriate button "Remove Rule")
Alternative Scenario 6	1	The Administrator click "Reset" button	The System discard all data from the form and return to previous values on server.
Alternative Scenario 7	1	The Administrator click "Back"	The System close "Policy Form" and return to "Assignment Policies" form.

UC_Auth_02 Deleting a Case Policy

Use Case ID:	UC_Auth_02
---------------------	-------------------

Use Case Name:	Deleting a Case Policy		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	09.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to delete a policy (General – non-Creator, Creator or Policy Group). All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Assignment Policies" option and selects "Delete" button (for a Type "POLICE")		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin 3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays the default value)		
Post conditions:	The Administrator has deleted a policy.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Assignment Policies" menu from "Authorization" menu option	The System displays: - "Refresh" button - "Search" element - offer the possibility to search for policies from the list). This element has associated "x" red icon, used to delete the text to be searched. - "New Policy" button Assignment policies grid, with columns: - "Name" - "Description" - "Type" - "Actions" with: - "Edit" button (visible in case there is at least one policy created) - "Delete" button (visible in case there is at least one policy created)
	2	The Administrator clicks "Delete" button from one of the policies on the column "Actions"	The system displays a pop-up window <i>Confirmation</i> with the message "You are about to delete the policy: supervisor policy" - "Yes" button - "No" button
	3	The Administrator clicks on "Yes" button	The System close confirmation pop-up window The System delete the assignment policy and display message

			"Assignment policy successfully deleted" The System delete policy from the server and the same is no more visible in the grid. The System return to step 1 of the Main Scenario.
Alternative Scenario 1	1	The Administrator click on "No" button	The System discards any changes. The System return to step 1 of the Main Scenario.

UC_Auth_03 Edit policy

Use Case ID:	UC_Auth_03		
Use Case Name:	Edit policy		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	09.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to edit/modify a policy selected from list of policies. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Assignment Policies" option and clicks "Edit" button		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin 3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays the default value)		
Post conditions:	The Administrator has modified a general policy.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Assignment Policies" option, from "Authorization" menu option	The System displays: - "Refresh" button - "Search" element - offer the possibility to search for policies from the list). This element has associated "x" red icon, used to delete the text to be searched. - "New Policy" button Assignment policies grid, with columns: - "Name" - "Description"

			- "Type" - "Actions" with: - "Edit" button (visible in case there is at least one policy created) - "Delete" button (visible in case there is at least one policy created)
	2	The Administrator click "Edit" button from one of the policies on the column "Actions"	The System open "Policy Form" with the values previously introduced on the server and make all fields editable.
	3	The Administrator change one or more value(s) of the field(s) and/or "Add"/"Delete"/"Move Up"/"Move Down" any of the rule(s) and click "Save" button	The System update values on server. The System close "Police Form" and return to "Assignment Policies" Form. The System display the message "Assignment policy successfully saved".
Alternative Scenario 1	4	The System click "Reset" button	The System discard all changes made and return to previous values on server. The System close "Policy Form" and return back to "Assignment Policies" form.
Alternate Scenario 2	5	The Administrator click "Back" button	The System close "Policy Form" and return back to "Assignment Policies" form.

UC_Auth_04 Create a new case creator policy

Use Case ID:	UC_Auth_04		
Use Case Name:	Create a new case creator policy		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	09.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to define the policy that determines the users that are authorized to create new cases, users of a specific group, or a specific user which has assigned appropriate roles. All Settings are distinguished and independent between each RINA Tenant.		

Trigger:	The Administrator selects "Authorization" menu option, then "Assignment Policies" option and clicks list box with "New Creator Policy" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin 3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value)		
Post conditions:	The Administrator completes the configuration of the new creator policy that determines the authorized to create new cases. ("Creator policy" type is used to enrol users or groups to roles (supervisor, authorized clerk, VIP, etc.) for the newly created cases based on a set of rules defined inside the configured policies)		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Assignment Policies" option, "Authorization" menu option	The System displays: - "Refresh" button - "Search" element - offer the possibility to search for policies from the list). This element has associated "x" red icon, used to delete the text to be searched. - "New Policy" button Assignment policies grid, with columns: - "Name" - "Description" - "Type" - "Actions" with: - "Edit" button (visible in case there is at least one policy created) - "Delete" button (visible in case there is at least one policy created)
	2	The Administrator click on the drop-down list "New Policy" and select the option "Creator New Policy" of this button	The System displays "Creator Policy Form", which contains: - "Name *" - mandatory, free-text field - "Description" - free-text field - "Color" – list - (to be associated to a policy, which may provide visual indications in the section Process assign) Subsection labelled "Rule X" ("X" from 1...n) with the following: - "Add" button – to add a rule - "When these conditions are met:" - "Application Role in" – with: - "Process Owner" button - "Counter Party" button - "Any" button

			- with "Process Owner" button selected (by default) the System display: - "Sector In" – drop-down list, which contains all the EESSI sectors, i.e. "FB", "Pensions", etc. - "Process Type In" – drop-down list which contains all the available BUC types of the selected Sector. - "Case Creator In" – list with: - "Clear" button - "Add" button - "Auto stop processing more rules" - "Save" button - "Reset" button - "Back" button
	3	The Administrator clicks "Add" button in the subsection "Rule X"	The System creates a new subsection (named "Rule 1") above the one (named "Rule 2") already displayed in the form (renumbering the number on each of the rules) even if the previous one is not filled because the rule who apply first concerns the order of priority from top to down (from the most recent to the oldest unless it is used the button "Move Down" or "Move Up" to change the order of priority between rules although the order of the rules keep being the same on the screen (from top to the bottom of the screen)) The System display: - "Rule 1" - "Move Down" button - "Delete" button - "Add" button

			- "When these conditions are met:" The System display by default the "Process Owner" button clicked from the field "Application Role In" and the fields: - "Sector In" - "Process Type In" - "Assign to Actors" - "These Users And Groups *" - "Select Group" - "Clear" button - "Add" button - "Select User" - "Please select group first" - "Rule 2" - "Move Down" button - "Delete" button - "Add" button - "When these conditions are met:" The System display by default the "Process Owner" button clicked from the field "Application Role In" and the fields: - "Sector In" - "Process Type In" - "Assign to Actors" - "These Users And Groups *" - "Select Group" - "Clear" button - "Add" button - "Select User" - "Please select group first" - "And stop processing more rules" - "Save" button - "Reset" button
--	--	--	---

			- "Back" button The system applies these rules sequentially until the first successful rule completely fulfils the criteria and conditions that have been set. Therefore, the order of the rules in the provided list defines the priority in which the system processes the rules. The Administrator can enforce a specific rule by changing their order on the list. The order change can be done by using the selections (<i>Move rule Up</i>) and (<i>Move rule down</i>) links. The checked legend <i>AND STOP PROCESSING MORE RULES</i>, has been located at the end of each rule to clearly indicate that the system stops processing the rules queue sequentially if the specific rule fulfils completely the conditions. Eventually the Administrator removes any rule by clicking on the <i>REMOVE RULE</i> link
	4	The Administrator fills the fields, select a value from the list of the field "Select Group" and click "Add" button	The System displays in the same line as the field "Select User": - a non-editable field with the role available for this group selected previously in the mentioned list - "Add" button
	5	The Administrator clicks "Add" button from the line of the field "Select User"	The System displays a new line before the field "Select Group" with: - a non-editable field with the role available for this group selected previously in the mentioned list - "Delete" button
	6	The Administrator clicks "Delete" button from the new line above the "Select Group" field	The System hides: - a non-editable field with the role value from the previously mentioned list - "Delete" button The System return to step 8 of the Main Scenario in case the Administrator want to add more roles for the same or other group
	7	The Administrator clicks on "Save" button	The System creates a new policy, which is listed in policies' list.

			The System displays a pop-up message "Assignment policy successfully saved" The System returns to "Assignment Policy" form with the new case policy added and visible on the grid. ('Creator policy' type is used to enrol users and (or) groups to roles i.e., supervisor, authorised clerk, VIP, etc. for the newly created cases based on a set of rules defined inside the available creator's policies).
Alternative Scenario 1	1	The Administrator clicks "Delete" button from "Rule 1"	The System displays the following fields as previously fill: - "Name *" - "Description" - "Color" The System renumber "Rule 2" to "Rule 1" and delete all fields from previous "Rule 1". The System display only the 1 or more "Rule X" not deleted so far. The System return to step 2 of the Main Scenario.
Alternative Scenario 2	1	The Administrator clicks "Move Down" button from "Rule X"	The System deletes values from "Rule X" from the screen and from the server. The System displays fields and their values from "Rule X+1" into the position of "Rule X" The System renumber the rules number from the top of screen to bottom. The System returns to step 2 of the Main Scenario.
Alternative Scenario 3	1	The Administrator clicks "Move Up" button from "Rule X+1"	The System exchanges the values from the position of the "Rule X+1" into the position of "Rule X". The System renumber the rules number from the top of screen to bottom. The System returns to step 2 of the Main Scenario.
Alternative Scenario 6	1	The Administrator clicks "Reset" button	The System discards all data from the form and return to previous values on server.

Alternate Scenario 7	1	The Administrator clicks "Back"	The System closes "Policy Form" and return to "Assignment Policies" form.
-----------------------------	---	---------------------------------	---

UC_Auth_05 Edit an existing creator policy

Use Case ID:	UC_Auth_05		
Use Case Name:	Edit an existing creator policy		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	11.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to edit/modify the creator policy, selected from list of policies. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Assignment Policies" option and clicks "Edit" button (for a Type "CREATOR")		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin 3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays the default value)		
Post conditions:	The Administrator edited the creator policy		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator access "Assignment Policies" option, from "Authorization" menu option	The System display: - "Refresh" button - "Search" element - offer the possibility to search for policies from the list). This element has associated "x" red icon, used to delete the text to be searched. - "New Policy" button Assignment policies grid, with columns: - "Name" - "Description" - "Type" - "Actions" with: - "Edit" button (visible in case there is at least one policy created)

			- "Delete" button (visible in case there is at least one policy created)
	2	The Administrator click "Edit" button from one of the policies on the column "Actions"	The System open "Creator Policy Form" with the values previously introduced on the server and make all fields editable. The System show for every rule (including new added) the button "Process Owner" locked and disabled as this is the one allowed for a "Creator Policy"
	3	The Administrator change one or more value(s) of the field(s) and/or "Add"/"Delete"/"Move Up"/"Move Down" any of the rule(s) and click "Save" button	The System update values on server. The System close "Creator Policy Form" and return to "Assignment Policies" Form. The System display the message "Assignment policy successfully saved".
Alternative Scenario 1	1	The System click "Reset" button	The System discard all changes made and return to previous values on server. The System close "Creator Policy Form" and return back to "Assignment Policies" form.
Alternative Scenario 2	1	The Administrator click "Back" button	The System close "Creator Policy Form" and return back to "Assignment Policies" form.

UC_Auth_06 Create new case policy group

Use Case ID:	UC_Auth_06		
Use Case Name:	Create new case policy group		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	11.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the system allows the Administrator to configure policies for groups. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Assignment Policies" option and clicks list box with "New Policy Group" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin		

	3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value)		
Post conditions:	The Administrator has configured the group policies		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Assignment Policies" option, "Authorization" menu option	The System displays: - "Refresh" button - "Search" element - offer the possibility to search for policies from the list). This element has associated "x" red icon, used to delete the text to be searched. - "New Policy" button Assignment policies grid, with columns: - "Name" - "Description" - "Type" - "Actions" with: - "Edit" button (visible in case there is at least one policy created) - "Delete" button (visible in case there is at least one policy created)
	2	The Administrator clicks on the drop-down list "New Policy" and select the option "New Policy Group" of this button	The System displays "Policy Group Form", which contains: - "Name *" - mandatory, free-text field - "Description" - free-text field - "Color" – list - (to be associated to a policy, which may provide visual indications in the section Process assign) - "Existing Policy *" – list box - "Save" button - "Reset" button - "Back" button
	3	The Administrator clicks "Save" button	The System creates a new policy, which is listed in policies' list. The System displays a pop-up message "Assignment policy successfully saved" The System returns to "Assignment Policy" form with the new case policy group added and visible on the grid.

Alternative Scenario 1	1	The Administrator clicks "Reset" button	The System discards all data from the form and return to previous values on server.
Alternate Scenario 2	1	The Administrator clicks "Back"	The System closes "Policy Form" and return to "Assignment Policies" form.

UC_Auth_07 Edit group policy

Use Case ID:	UC_Auth_07		
Use Case Name:	Edit group policy		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	11.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to edit/modify a group policy selected from list of policies. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Assignment Policies" option and clicks "Edit" button (for a Type "GROUP")		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user selects a relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value)		
Post conditions:	The Administrator has modified a group policy		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses <i>Assignment Policies</i> option from "Authorization" menu option	The System displays: - "Refresh" button - "Search" element - offer the possibility to search for policies from the list). This element has associated "x" red icon, used to delete the text to be searched. - "New Policy" button Assignment policies grid, with columns: - "Name" - "Description" - "Type" - "Actions" with: - "Edit" button (visible in case there is at least one policy created)

			- "Delete" button (visible in case there is at least one policy created)
	2	The Administrator clicks "Edit" button from one of the policies on the column "Actions"	The System opens "Policy Group Form" with the values previously introduced on the server and make all fields editable.
	3	The Administrator changes one or more value(s) of the field(s) click "Save" button	The System updates values on server. The System closes "Police Group Form" and return to "Assignment Policies" Form. The System displays the message "Assignment policy successfully saved".
Alternative Scenario 1	1	The System clicks "Reset" button	The System discards all changes made and return to previous values on server. The System closes "Policy Group Form" and return back to "Assignment Policies" form.
Alternative Scenario 2	2	The System clicks "Back" button	The System closes "Policy Group Form" and return back to "Assignment Policies" form.

UC_Auth_08 Process assignment

Use Case ID:	UC_Auth_08		
Use Case Name:	Process assignment		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator assign more than one policy to a sector or to a process. The Administrator performs the process manually or automatically. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Process Assignments" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user selects the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value)		
Post conditions:	The Administrator has assigned more than one policy to a sector or to a process.		
Main Scenario:	#	Step actions	Expected Result

	1	The Administrator accesses "Authorization" menu option, "Process Assignments" option	The system displays "<i>Process Assignments</i>" form which contains: - "Refresh" button - "Export Policies and Assignments" button - "Import Policies and Assignments" button - A view of all the EESSI "Sectors", the Business "Processes" (BUCs), the "Application Roles", "Actors" and all policies assigned at each level. Next to each Sector/Process/Application Role/Actors the Administrator may notice the colour-code of the policies (or policy groups) linked to each. A Sector where there is at least one Process that has no policy assigned, has an icon next to it (top right side of the screen). The Administrator assigns more than one policy to a Sector or Process, manually or automatically.
	2	The Administrator clicks on right side coloured icon related to "Sectors"	The System displays the pop-up window "Assigned Policies", which contains: - "Name of the Sector" - "All policies from this list are evaluated and their results are cumulated." - "Existing Policy *" – List box with all policies with ability to search - - "Save" button
	3	The Administrator selects one or more policies and clicks "Save" button	The System saves data on server. The System close pop-up window. The System display message "Assignment Policies successfully saved".
Alternative Scenario 1	1	The Administrator click on right side coloured icon related to "Processes"	The System displays the pop-up window "Assigned Policies", which contains: - "Name of the BUC Process"

			- "All policies from this list are evaluated and their results are cumulated." - "Existing Policy *" - List box with all policies with ability to search - - "Save" button
	2	The Administrator selects one or more policies and click "Save" button	The System saves data on server. The System closes pop-up window. The System displays message "Assignment Policies successfully saved".
Alternative Scenario 2	1	The Administrator clicks on right side coloured icon related to "Processes"	The System displays the pop-up window "Assigned Policies", which contains: - "Name of the Sector > Name of the BUC Process - "All policies from this list are evaluated and their results are cumulated." - "Existing Policy *" - List box with all policies with ability to search - - "Save" button
Alternative Scenario 3	1	The Administrator click on right side coloured icon related to "Application Roles"	The System displays the pop-up window "Assigned Policies", which contains: - "Name of the Sector > Name of the BUC Process > Name of the Role" - "All policies from this list are evaluated and their results are cumulated." - "Existing Policy *" - List box with all policies with ability to search - - "Save" button
	2	The Administrator selects one or more policies and click "Save" button	The System saves data on server. The System closes pop-up window. The System displays message "Assignment Policies successfully saved".

Alternative Scenario 4	1	The Administrator clicks on right side coloured icon related to "Actors"	The System displays the pop-up window "Assigned Policies", which contains: - "Name of the Sector > Name of the BUC Process > Name of the Role > Name of the Actor" - "All policies from this list are evaluated and their results are cumulated." - "Existing Policy *" – List box with all policies with ability to search - - "Save" button
	2	The Administrator selects one or more policies and click "Save" button	The System saves data on server. The System closes pop-up window. The System displays message "Assignment Policies successfully saved".

UC_Auth_09 Export policies and assignments

Use Case ID:	UC_Auth_09		
Use Case Name:	Export policies and assignments		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to export policies and assignments. The Administrator does it automatically. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Process Assignments" option and clicks "Export Policies and Assignments" button		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user selected the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value) 4. Process Assignment and access policies are configured		
Post conditions:	The Administrator exported policies and assignments, which holds the policies and process assignments		
	#	Step actions	Expected Result

Main Scenario:	1	The Administrator access "Authorization" menu option, "Process Assignments" option	The system displays "Process Assignments" form which contains: - "Refresh" button - "Export Policies and Assignments" button - "Import Policies and Assignments" button - A view of all the EESSI "Sectors", the Business "Processes" (BUCs), the "Application Roles", "Actors" and all policies assigned at each level. Next to each Sector/Process/Application Role/Actors the Administrator may notice the colour-code of the policies (or policy groups) linked to each. A Sector where there is at least one Process that has no policy assigned, has an icon next to it (top right side of the screen). The Administrator assigns more than one policy to a Sector or Process, manually or automatically.
	2	The Administrator clicks "Export Policies and Assignments" button	The System export the configuration file for backup purposes or for new RINA deployments (on the same or different servers that use the same Process Assignment and policies structure). The exported filenames "ProcessDefinitionAssignments.json", which holds the policies and process assignments. This file can be opened by the Administrator or/and is saved locally.

UC_Auth_10 Import policies and assignments

Use Case ID:	UC_Auth_10		
Use Case Name:	Import policies and assignments		
Created By:	Madalina Alecsandrescu	Last Updated By:	

Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to import policies and assignments. All Settings are distinguished and independent between each RINA Tenant.		
Trigger:	The Administrator selects "Authorization" menu option, then "Process Assignments" option and clicks "Import Policies and Assignments" button		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user selects the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value) 4. Process Assignment and access policies are configured		
Post conditions:	The Administrator imports policies and assignments successfully		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator access "Authorization" menu option, "Process Assignments" option	The system displays "Process Assignments" <i>form</i> which contains: - "Refresh" button - "Export Policies and Assignments" button - "Import Policies and Assignments" button - A view of all the EESSI "Sectors", the Business "Processes" (BUCs), the "Application Roles", "Actors" and all policies assigned at each level. Next to each Sector/Process/Application Role/Actors the Administrator may notice the colour-code of the policies (or policy groups) linked to each. A Sector where there is at least one Process that has no policy assigned, has an icon next to it (top right side of the screen). The Administrator assigns more than one policy to a Sector or Process, manually or automatically.
		The Administrator click "Import Policies and Assignments" button	The System open "File Explorer" from Operating System. The Administrator select the JSON file that was successfully exported during the export procedure.

		A small progress bar appears. It is important to notice that once the import process is complete, the existing (if any) process assignments are replaced by the configuration imported from the selected JSON file. (After importing the "Exported" policies and Assignments are not automatically activated the Administrator has to EDIT and SAVE the Policies and Assignments in order to obtain a new valid ID in the new system and be applied)
--	--	--

UC_Auth_11 Implement policy decision class

Use Case ID:	UC_Auth_11		
Use Case Name:	PDP Implementation Class		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to implement policy decision class.		
Trigger:	The Administrator "Authorization" menu option and clicks "PDP Implementation Class" option.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user selects the relevant tenant (top left-hand side of the screen – if there is only 1 tenant, the system displays only the default value) 4. Process Assignment and access policies are configured		
Post conditions:	The Administrator imports policies and assignments successfully		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Authorization" menu option, "PDP Implementation Class" option	The System displays "Automatic Case Assignments Policies" form, which contains: - "Policy decision point implementation class *" - (fully qualified name)- mandatory, free-text field - "Reset" – button - "Save" - button
	2	The Administrator fills in the field and click "Save" button	The System saves data on server. The System displays message "Policy Decision Point"

			Implementation Class successfully saved".
Alternative scenario 1	1	The Administrator clicks "Reset" button	The System discards all changes.

Fields Details

Authorization - Assignment Policies

No.	Item name	Type	Validation/business rules
1	Select tenant (with explanatory notes associated)	List	(a value is selected by default)
2	Search element		Search Delete
3	Refresh	Button	Refresh screen
4	New Policy	Button	
4.1	Assignment Policies	Grid	Contains columns: Name Description Type Actions Every row has associated 2 buttons:
4.2	Edit	Button	When click on this button, Creator Policy Form is displayed, which contains:
4.2.1	Name	Free text field	Mandatory
4.2.2	Description	Free text field	
	Color	List	Contains colours: (red, yellow, green, blue, violet)
4.2.3	Rule 1	Section	
4.2.4	Add	Button	
4.2.5	Process Owner	Tab	Enabled
4.2.6	Counterparty	Tab	Disabled
4.2.7	Any	Tab	Disabled
4.2.8	Sector in	List	
4.2.9	Process Type in	List	
4.2.10	Assign to actors	List	Disabled
4.2.11	These Users And Groups	Free text box field	
4.2.12	Select Groups	Free text box field	
4.2.13	Clear	Button	
4.2.14	Add	Button	
4.2.15	Select user	Free text box field	
4.2.16	Add	Button	
4.2.17	Back	Button	
4.2.18	Reset	Button	
4.2.19	Save	Button	
4.3	Delete	Button	

5	New Creator Policy	Area	The system displays Creator Policy Form, see 4.2.1 – 4.219
6	New Policy Group	Area	The system displays Policy Group Form, which contains:
6.1	Name	Free text field	Mandatory
6.2	Description	Free text field	
6.3	Color	List	Contains colours: (red, yellow, green, blue, violet)
6.4	Existing Policy	List	
6.5	Back	Button	
6.6	Reset	Button	
6.7	Save	Button	

Authorization – Process Assignment

No.	Item name	Type	Validation/business rules
1	Select tenant (with explanatory notes associated)	List	(a value is selected by default)
2	Export Policies and Assignments	Button	The system downloads the file with policies
3	Import Policies and Assignments	Button	The system displays the directories, gives the possibility to choose the file
4	Refresh	Button	Refresh screen
5	Sectors	Grid	Contains list with all sectors: AWOD Family Benefits Horizontal Legislation Applicable Miscellaneous Pension Recovery Sickness Unemployment Every sector has associated ration button and imagine. At click of imagine, the system displays Assigned Policy form, which contains:
5.1	'Sector name' and 'All policies from this list are evaluated and their results are cumulated'	Label	
5.2	Existing Policy	List	
5.3	Save	Button	
6	Processes	List	Contains list with Processes associated

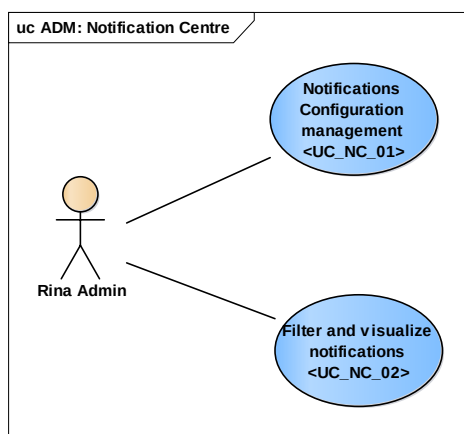
			to a sector. The list has associated ration buttons and image. At click on image is displayed Assigned Policies Form
7	Application roles	List	Contains values Process Owner and Counter Party with associated ration button and image. At click on image is displayed Assigned Policies form
8	Actors	List	Contains the Actors list with associated ratio button and image. At click on image is displayed Assigned Policies form.

Authorization – PDP Implementation Class

No.	Item name	Type	Validation/business rules
1	Policy Decision Point Implementation Class (Fully Qualified Name)	Free-text field	Mandatory
2	Reset	Button	
3	Save	Button	

6.8 Notification Centre

Use case diagrams



Use Case View

UC_NC_01 Set Notifications

Use Case ID:	UC_NC_01		
Use Case Name:	Set Notifications		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the system allows the Administrator to configure: - the notifications to be shown to the users (Clerks) - the notifications to be shown to the administrators - the retention and notification periods for the Business exceptions - the generation of the NIE events per Notification type.		
Trigger:	The Administrator clicks on the "Notifications Centre" menu option and clicks "Notifications Settings" button		
Preconditions:	- The user is authenticated in RINA. - The user is authorized to access Application as RINA Admin		
Post conditions:	The Administrator sets up the rules related to what types of notifications are visible for end users and Administrator, configures the retention period and notification periods for the Business Exceptions, and sets up the Business Exception to be automatically sent by RINA without any manual intervention.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Notifications Centre" menu option, and then clicks on the "Notification Settings" button	The System displays the "Notification Settings" form. This form contains a grid displaying all the possible types of notification with the following columns: "Notification Type" : in this column all the types of notifications are displayed: "Notification Centre for Clerk" – for each displayed notification, the Administrator has available in this column a checkbox field for selecting if the type of notification is to be displayed to clerks or not. Exception, for the types of notifications "Business Exception - Unknown Cause " and "Business Exception - Case Missing", this option is not available "Notification Centre for Admin" - for each displayed notification, the Administrator has available in this column a checkbox field for selecting if the type of notification is to be displayed to the Administrator or not. This option is available only for the types of notifications: - Archiving Case Exception

		○ Case Assignment Exception ○ Business Exception - Attachment failed antimalware checking ○ Business Exception - Case Forwarded ○ Business Exception - Case Closed ○ Business Exception - Unknown Cause ○ Business Exception - Invalid Business Signature ○ Business Exception - SED in Wrong Sequence ○ Business Exception - SED update without Create • "Retention period (in days) *" and "Notification period (in days *)" columns, related only to "Business Exceptions" notifications where the Administrator has available a counter field for setting up the number of days: ○ Business Exception - Attachment failed antimalware checking ○ Business Exception - Case Forwarded ○ Business Exception - Case Closed ○ Business Exception - Unknown Cause ○ Business Exception - Invalid Business Signature ○ Business Exception - SED in Wrong Sequence ○ Business Exception - SED update without Create "Retention period (in days)"- is the period of time that needs to elapse since the appearance of the relevant messages under the "Business Exceptions: Pending Message" form. Upon the expiration of the retention period, the System automatically generates Business Exceptions for the respective incoming Pending Messages and the exception is moved from Pending Messages to Business Exceptions. "Notification period (in days)" is the period of time that needs to elapse since the appearance of the relevant messages under the "Business Exceptions: Pending Message" form.
--	--	---

			Upon this expiration of notification period, the System automatically generates the respective notification) The "Retention period" parameter should be greater or equal to the "Notification Period". According to approved business specifications the default values for "Retention Period" and "Notification Period" for the Business Exceptions are: ○ "Attachment failed antimalware checking": Retention Period = 0; Notification Period = 0 (in days) ○ "Case Forwarded: Retention Period = 1; Notification Period = 0 (in days) ○ "Case Closed": Retention Period = 1; Notification Period = 0 (in days) ○ "Unknown Cause": Retention Period = 1; Notification Period = 0 (in days) ○ "Invalid Business Signature": Retention Period = 0; Notification Period = 0 (in days) ○ "SED in Wrong Sequence": Retention Period = 1; Notification Period = 0 (in days) ○ "SED update without Create": Retention Period = 1; Notification Period = 0 (in days) ○ "Case Removed": Retention Period = 1; Notification Period = 0 (in days) ○ "Case Missing": Retention Period = 1; Notification Period = 0 (in days) • "Generate a NIE event" - for each displayed notification, the Administrator has available in this column a checkbox field for selecting if the type of notification should generate a NIE event - • "Reset" - Button • "Save" - Button • "Refresh" - Button
	2	The Administrator selects the relevant	The system saves data on server

		Notification types and configures the appropriate Retention & Notifications periods, the NIE event generation and clicks on "Save" button	The System display the message "Notifications settings successfully saved".
	3	The Administrator clicks "Refresh" button	The System redisplay the form with data from server.
Alternative scenario 1	1	The Administrator clicks on <i>Reset</i>	The System discards all changes on the form.

UC_NC_02 Filter and visualize notifications

Use Case ID:	UC_NC_02		
Use Case Name:	Filter and visualize notifications		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the System allows the Administrator to access the notifications. The System automatically generates notifications to inform about updates and changes within the existing and new cases.		
Trigger:	The Administrator selects "Notifications Centre" menu option and clicks "Notifications" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin		
Post conditions:	The Administrator consulted the notifications about updates and changes within the existing and about new cases.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Notifications Center" menu option, "Notifications" option	The System displays the "Notifications" form. This form has 2 areas: 1. <u>The Display area</u> The notifications are displayed in a grid with the following header: • Checkbox field – when selected all displayed notifications are selected. For each displayed notification, the checkbox field is also available. Clicking on the checkbox field at notification level/ all notification level) activates 2 buttons in the header: ○ a button labelled "Mark as Unread" ○ a button labelled "Mark as Read"

		• (show details column)- for each displayed notification, in this column the Administrator has available the ">" button for displaying the details of the notification • (more info column) – for each displayed notification, in this column the Administrator has available two icons: ◦ An info "!" icon- to indicate the type of notification colored in blue for information notification, yellow for warning notification and red for error notification ◦ The criticality and severity matrix icon of the case • "Date" – the date when notification was generated • "Type" – type of notification • "Description" • "Actions" – for each displayed notification, an "Action" button-when clicked displays available actions for that type of notification Under the header, all the relevant notifications are displayed ordered descending by the notification date. The types of notifications generated by the system are: • Warning notifications: ◦ "A New Case Arrived"; ◦ "A New SED Arrived"; ◦ "An Updated SED Arrived"; • Information notifications: ◦ "Request to Assign Case"; ◦ "Request to Assign Case Rejected"; ◦ "Request to Assign Case Accepted"; ◦ "Case Unassigned"; ◦ "Case Assigned"; ◦ "Your Alarm Expired"; ◦ "Approval for Sending Required for SED"; ◦ "Case Automatically Closed"; ◦ "SED Delivered"; ◦ "Case SEDs Automatically Sent to New Participant"; • Error notifications: ◦ "Archiving Case Problem"; ◦ "SED Not Matching Case"; ◦ "Case Missing"; ◦ "Case Assignment Exception";
--	--	---

			- o "Attachment failed antimalware checking"; - o "Archiving Case Exception"; - o "SED Update without Create"; - o "SED Failed to be Delivered"; - o "SED in a wrong Sequence"; - o "Case Forwarded"; - o "Invalid Business Signature"; - o "Case Removed"; - o "Unknown Cause"; - o "Case Closed"; 2. <u>The Search area</u> In the Search area the Administrator has available: - o A search button – when clicked refreshes the list of displayed notifications. - o A free text field "Enter case id" for searching notifications related to a case id - o A "filter icon" button
	3	The Administrator enters a case id in the "Enter case id" free text and clicks the magnifying glass icon	In the display area, only notifications linked to the search case id are displayed.
	4	The Administrator clicks the filter icon button and selects needed filters. The filters are checkbox fields, grouped by type. Each grouping has a descriptive label and an x icon to remove the criterion from filter. The groups and criteria are: • "Severity" group with: - o "Warning" - o "Information" - o "Error" • "Recent" group with: - o "Unread" - o "Read" • "Type group" with available values the types of notifications.	Only the notifications complying the selected criteria are displayed.
	5	The Administrator clicks the Search button	The System redisplay the list of notifications, and all applied filters are removed.

Alternate Scenario 1	1	The Administrator clicks on an individual notification from the list (related to the main section)	The system opens a detailed view and provides information about the case ID, the case type, and a list of assignees. For alerts that require a reaction within a specified time frame, the detail view also shows by which date an action is required. The actual detail views differ for each notification severity category type.
Alternative Scenario 2	1	The Administrator selects a bulk of notifications (multiple notifications selected once)	The system automatically selects all notifications from that date (bulk operation) Once the Administrator selects a notification (or more as a bulk) the links <i>Mark as Read</i> or <i>Mark as Unread</i> will be visible
	2	The Administrator clicks "Mark as Read" or "Mark as Unread"	The system sets a notification to read state (if link <i>Mark as Read</i> was clicked). The state can be reset to unread (if <i>Mark as Unread</i> link was clicked)

Fields Details

Notification Centre – Notification Settings

No.	Item name	Type	Validation/business rules
1	Notifications	Grid	Contains columns: Notification Type Notification Center for Admin Notification Center for Clerk Retention Period (in days) Notification Period (In days) Generate a NIE event
2	Refresh	Button	
3	Reset	Button	
4	Save	Button	

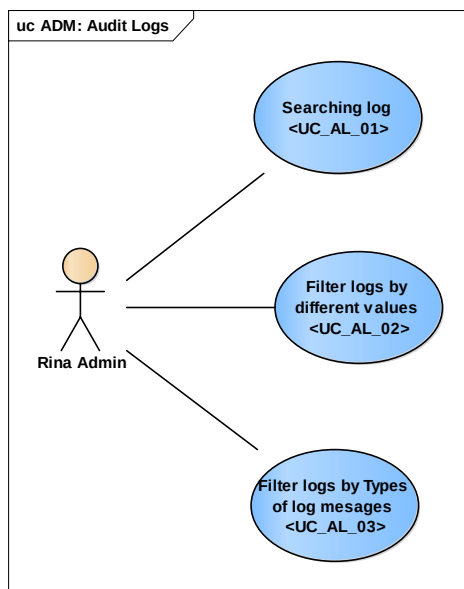
Notification Centre – Notifications

No.	Item name	Type	Validation/business rules
1	Search	Element	Has associated - X Button, used to cancel the search - Filter icon.

			At click on Filter, the system displays:
1.1	Severity	Check boxes	Associated values: Error, Information, Warning
1.2	Recent	Check boxes	Associated values: Read, Unread
1.3	Type	Check boxes	Associated values: A new Case Arrived, A new SED Arrived, etc
2	Notification	Grid	Contains columns: Date Type Description

6.9 Logs

Use case diagrams



Use Case View

UC_AL_01 Searching logs

Use Case ID:	UC_AL_01		
Use Case Name:	Searching logs		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		

Description:	This use case describes how the system allows the Administrator to search and visualize Audit Logs, related to a time interval or related to a search for a Case ID		
Trigger:	The Administrator selects "Logs" menu option and selects "Audit Logs" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The system displayed Audit Logs for a search related to a time interval or for a Case ID		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Audit Logs" menu option from "Logs" option	The System displays: - "From" - component for writing or searching dates - "To " - "1" button - "2" button - "3" button - "days(s) ahead" (these buttons are used to set up the dates). The list can be filtered in a granular form by year, month, date, and hour and page number - "Search" element, where the Administrator search for a record by defining the appropriate <i>Keyword</i>. The <i>Keyword</i> is typed in the edit box of the searching window in the right part of the top row and the searching algorithm searches for the specific <i>Keyword</i> against the entire logs content. The search is not Case Sensitive. The search algorithm uses only the first given <i>Keyword</i> regardless the number of the keywords provided in the Search edit box. As Keyword can be used: the participant code (i.e., bgna01), the case number (i.e. 20673), the message return by the object (i.e. error), - "Navigate" panel, the Administrator filter for a time period by setting the specific time period at the Navigate panel at the top-right section of the screen. - grid with the following fields": - "Date" - "Event Time" - "Username"

			- "Action Type" - "Description"
	2	The Administrator performs a search using "Calendar" element	The System displays the list with Audits logs grouped per day and time on main area: - "Date" - "Event Type" - "Username" - "Action Type" - "Description" - "Total records" – the current number of audit logs displayed per page - section (arrow icon on the left side of the grid) with all retrieved cases. The section may be expanded, and the System displays other more information as: - "Outcome" - "User" - "Action" - "Location" - "Source" - "Objects" - "Subdocument" - "Document" - "Participants" The free text search functionality is not case sensitive
		The Administrator perform a search using "Search Bar" element	The System display the list with Audits logs grouped per day and time on main area: - "Date" - "Event Type" - "Username" - "Action Type" - "Description" - "Total records" – the current number of audit logs displayed per page - section (arrow icon on the left side of the grid) with all retrieved cases. The section may be expanded, and the System displays other more information as: - "Outcome" - "User" - "Action" - "Location"

		- "Source" - "Objects" - "Subdocument" - "Document" - "Participants" The free text search functionality is not case sensitive
--	--	--

UC_AL_02 Filter logs by different values

Use Case ID:	UC_AL_02		
Use Case Name:	Filter by different values		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows to the Administrator to filter and visualize Audit Logs (filter based on different values: <i>Action type, Component type, Object type, Participant Type, Participant Role, Category Type, Event Type</i>)		
Trigger:	The Administrator selects "Logs" menu option and selects "Audit Logs" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The system displayed the filtered options.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Audit Logs" component, "Filter By" subsection	The System displays subsection <i>Filter by</i>, which contains different areas: <u>"All Log Types":</u> - "Success" - "Error" - "Unauthorized" <u>"Action Type" area:</u> - "Read" - "Create" - "Update" - "Delete" - "Execute" <u>"Component Type" area:</u> - "Security" - "Notifications" - "Search Definitions" - "Business Messaging" - "Cases"

		- "Administration" - "Documents" - "Attachments" - "Comments" - "Technical Messaging" <u>"Participant Type" area:</u> - "Organization" - "Person" <u>"Participant Role" area:</u> - "Receiver" - "Sender" - "Subject" <u>"Object Type" area:</u> - "Notification" - "Credential" - "Business Error" - "Business Acknowledge" - "Alarm" - "Comment" - "Attachment" - "Subdocument" - "Search Definition" - "Business Message" - "Case" - "User Profile" - "Policy" - "Document" - "Technical Message" - "Application Profile" - "User Group" <u>"Category Type" area:</u> - "Security" - "Business" - "Messaging" <u>"Event Type" area:</u> - "Retrieve Case Id By International Id" - "Submit Attachment On Document" - "Create Document" - "Import Subdocument Batch" - "Create Search Definition" - "Logout" - "Delete Attachment On Document" - "Export Subdocument Batch" - "Application Start" - "Submit Document" - "Receive Technical Message" - "Change Authorization Policy" - "Retrieve Notifications Consolidated" - "Summary" - "Update Document"
--	--	---

			"Update Search Definition" "Send Document" "Retrieve Initial Document" "Set Alarm" "Delete Attachment on Case" "Create User Or Group" "Retrieve Case By Id" "Send Business Message" "Retrieve Attachment On Document" "Retrieve Case By International Id" "Submit Attachment on Case" "Retrieve Case Hash Code By Id" "Delete Comment On Document" "Retrieve Notification Time Slots" >Login" "Retrieve Case Assignments" "Submit Comment On Document" "Update User Profile" "Retrieve Attachment on Case" "Clear Alarm" "Delete Document" "Update Application Profile" "Retrieve Notification Summary" "Retrieve Document" "Delete Comment On Case" "Submit Comment On Case" "Notify About Received Business Message" "Assign Case" "Send Technical Message" "Retrieve Notification Details" "Create New Case" "Delete User Or Group" "Notify About Status Update" "Retrieve Thumbnail" "Application End" "Search Cases By Search Definition And Or Free-Text" "Delete Search Definition" "Update Notification"
	2	The Administrator select the filters	The System displays the list with Audits logs per day and for each daily list, the following info is displayed on a header: Date - "Date" - "Event Type" - "Username" - "Action Type" - "Description"

			- current number of the display page - section with all retrieved cases.
	3	The Administrator selects a log from log's list, in main area	The System displays data related to the selected search like: - "Outcome" - "User" - "Action" - "Location" - "Source" - "Objects" - "Participants with more information"

Fields Details

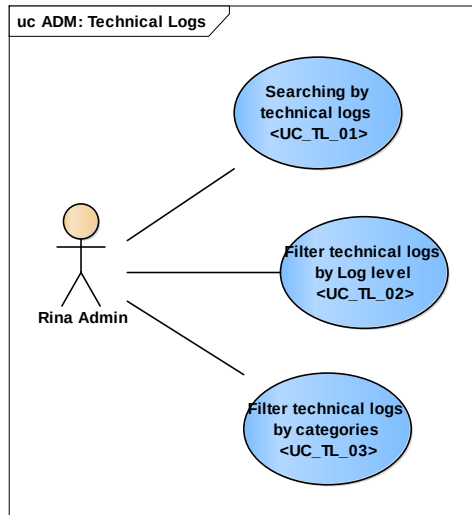
Audit Logs

No.	Item name	Type	Validation/business rules
1	Calendar	Date element	Insert date From...
2	Days (ahead)	Buttons	At click displays 3 tabs: 1 Day, 2Days, 3Days
3	Search	Search element	Search Delete (search)
4	Filter	Imagine	At click of this imagine, the system displays:
4.1	Filter by All Logs types	Check box	Values: Success, Error, Unauthorized
4.2	Filter by Action type	Check box	Values: Read, Create, Update, Delete, Execute
4.3	Filter by Component type	Check box	Values: Administration Attachments Business Messaging Cases Comments Documents Notifications Search Definitions Security Technical Messaging
4.4	Filter by Participant type	Check box	Values: Organization Person
4.5	Filter by Participant role	Check box	Values: Receiver Sender Subject
4.6	Filter by Object type	Check box	Values: Action

			Alarm Application Profile Attachment Business Acknowledge Business Error Business Message Case Comment Credential Document Notification Policy Search Definition Subdocument Technical Message User Group User Profile
4.7	Filter by Category type	Check box	Values: Security Business Messaging
4.8	Filter by Event type	Check box	Values: Application End Application Start Archive / Unarchive Case Assign Case Change Authorization Policy Clear Alarm Create Document Create New Case Create Search Definition Create User Or Group, etc
5	Total Records:	Label	The system displays the number of audit logs records
6	Audit logs	Grid	Contains columns: Date Event type Username Action Type Description

6.10 Technical Logs

Use case diagrams



Use Case View

UC_TL_01 Searching technical logs

Use Case ID:	UC_TL_01		
Use Case Name:	Searching technical logs		
Created By:	A Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to visualize basic troubleshooting information directly in the RINA portal. The Administrator perform very granular searches to pinpoint to the dates, type of information and area of interest.		
Trigger:	The Administrator selects "Logs" menu option and selects "Technical Logs" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin		
Post conditions:	The Administrator performed granular search and the system displayed troubleshooting information list.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Technical Logs" option from "Logs" menu option	The system displays the "Technical Logs" form. This form contains: • A search area where the Administrator can search for specific logs based on: ○ the date of the log ○ using free text search functionality ○ filter based on predefined filters

			In the case, the Administrator is interested in monitoring the logs of a specific period (of 1, 2 or 3 days) then the starting date is defined by using the calendar and the number of days is defined making the appropriate selection on the menu appeared beside the calendar <i>Keyword:</i> The Administrator search for a specific term/keyword. The icon (x), at the right side of the text box, resets the searching, clears the edit box and refreshes the search. The <i>Keyword</i> is typed in the edit box of the searching window given in the right part of the top row and the searching algorithm searches for the specific <i>Keyword</i> against the entire logs content. The search is not Case Sensitive. The search algorithm uses only the first given <i>Keyword</i> regardless the number of the keywords provided in the Search edit box. The algorithm searches for the given keyword in the fields: date and time, component name (i.e. Bonita), in the message content and message Id, in the log level, etc.
	2	The Administrator search using search bar element	The system displays the list with troubleshooting per day and for each daily list the following info is displayed on a header: Date Type Level Description the current number of the display page section with all retrieved cases, with related attributes: Source Level Logger name Thread Message

UC_TL_02 Filter technical logs by Log level

Use Case ID:	UC_TL_02
Use Case Name:	Filter technical logs by Log level

Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to visualize Technical logs filtered by log level		
Trigger:	The Administrator selects "Logs" menu option and selects "Technical Logs" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The system displayed Technical Logs filtered by log level		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Technical Logs" option, "Filtered by" subsection	The system displays the following categories and the Administrator toggle between one or more of the following categories "Trace", "Error", "Info", "Fatal", "Debug" and "Warn".
	2	The Administrator filters by log level	The system displays the list with Technical logs related to this filter. The list can be expanded for every technical log, the system displays section with all retrieved cases, with related attributes: Source Level Logger name Thread Message

UC_TL_03 Filter technical logs by categories

Use Case ID:	UC_TL_03		
Use Case Name:	Filter technical logs by categories		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to visualize Technical Logs related to a particular category		
Trigger:	The Administrator selects "Logs" menu option and selects "Technical Logs" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The system displayed Technical Logs based on a search by category		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses <i>Technical Logs</i>	The logging level can be filtered for each component (Bonita, AP Client, REST)

		component, and accesses filter icon	
	2	The Administrator selects the specific category to be listed by clicking on the information type square icon related to categories	The system displays the advanced troubleshooting, the technical logs are located in Elastic Search, in the relevant node files: bonita_rina.log (for BONITA), rest-api.log (for REST-API) and apclient.log (for AP Client) within the application system.
	3	The Administrator clicks on "X" icon, top left	The system undoes all the category selections

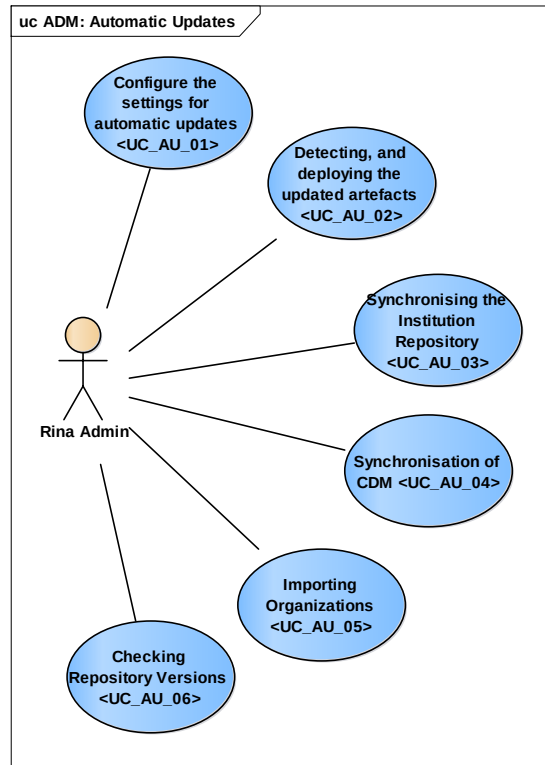
Fields Details

Technical Logs

No.	Item name	Type	Validation/business rules
1	Calendar	Date element	Insert date From...
2	Days (ahead)	Buttons	At click displays 3 tabs: 1 Day, 2Days, 3Days
3	Search	Search element	Search Delete (search)
4	Filter	Imagine	At click of this imagine, the system displays:
4.1	Filter by All Logs types	Check box	Values: AP Client REST
4.2	Filter by Log Level	Check box	Values: TRACE ERROR INFO DEBUG FATAL WARN
5	Total Records:	Label	The system displays the number of audit logs records
6	Technical logs	Grid	Contains columns: Date Event type Username Action Type Description

6.11 Automatic Updates

Use case diagrams



Use Case View

UC_AU_01 Configure the settings for automatic updates

Use Case ID:	UC_AU_01		
Use Case Name:	Configure the settings for automatic updates		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to configure the settings for automatic updates		
Trigger:	The Administrator clicks on the "Automatic Updates" button form main menu		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator has configured the settings for automatic updates		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Automatic Updates" button form main menu	The System displays the "Automatic Updates" form that contains: "Refresh" button "Sync" button with associated ">" button – when clicked, the "Sync Institutions" and "Sync CDM" become available

			• "Install <number>" button • "Import Organizations" button • "Search" free-text field with associated "x" button and magnifying glass icon • "Settings" button • filter icon button. • grid labelled "To Install (<number>)" – for displaying the performed automatic updates, with following structure: • header of the sub-section labelled based on the type of resource (i.e., "Organizations", "SEDs", "Transactions") with associated checkbox field for selected all resources displayed and "+/-" icon – when clicked expands/hides the content of the grid. • for each displayed sub-section, the following columns are available: ○ "Type" ○ "Status" ○ "Disk Version" ○ "Disk Date" ○ "Server Version" ○ "Server Date"
	2	The Administrator click on the "Settings" button	The System displays "Automatic Updates Settings" form, which contains: • "Disk Resources Path on Server *" - free text field, mandatory - the path where the content is downloaded from CSN (through AP). • "Shared Configuration Path *" - free text field, mandatory • "Shared BMP Repository Path *" - free text field • "Form Templates Repository Path *" - free text field • "Office Templates Repository Path *" - free text field • "Localization Resources Repository Path *" - free text field

			• "Save" button • "Reset" button
	3	The Administrator fills in the fields and clicks on the "Save" button	The System saves the data into the server. The System closes the "Automatic Updates Settings" form and returns to "Automatic Updates" form.
Alternative scenario 1	1	The Administrator fills in the fields and click on the "Reset" button	The System discards values from the fields and return values from server. The main scenario can be resumed at step 3.

UC_AU_02 Synchronising the Institution Repository

Use Case ID:	UC_AU_02		
Use Case Name:	Synchronising the Institution Repository		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to synchronize of the Institution Repository (IR)		
Trigger:	The Administrator selects "Automatic Updates" menu option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA admin 3. The user configured the settings for automatic updates		
Post conditions:	The system has synchronized the Institution Repository (IR)		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Automatic Updates" button form main menu	The System displays the "Automatic Updates"
	2	The Administrator clicks on the ">" button associated to the "Sync" button and then clicks on the "Sync Institutions" button	The System displays "SYN002 - Request for IR Sync" form, which contains: "Current version" – mandatory, free-text field - parameter is used for the IR request sent to the AP "Save" button "Reset" button "Back" button

	3	The Administrator fills in the field and clicks on the "Save" button	The System sends the IR synchronisation request to the AP. (Upon finalisation of this operation, the RINA application sends a <i>system</i> message to the AP to request the latest IR version (SYN002 message). The AP responds in an asynchronous manner with the new version file (in case there is any), or without any file (if Current Version of RINA sent request has the latest available version). The referred file is provided as attachment onto the received SYN001 system (sync) message. Any new files are persisted under the defined (via the configuration) disk resource path of the application system) The System closes "SYN002 – Request For IR Sync" form and displays message "Success. Request for IR Sync." (Recommendations: The Automatic Updates (CDM & IR Synchronisation) are time consuming operations and cannot be instantly completed (this is also depending on the volume as it is described above). Therefore, the administrator should monitor the operation progress: ○ related to receiving the files by checking their existence at the level of the system (Holodeck component) ○ related to the deployment by pressing the refresh button periodically (with the period varying on the list of deployed files per operation, i.e., the more files, the longer the period).
Alternative Scenario 1	1	The Administrator clicks on "Reset" button	The system reset any parameter modified during editing regarding "Current Version".

UC_AU_03 Synchronisation of CDM

Use Case ID:	UC_AU_03
---------------------	-----------------

Use Case Name:	Synchronisation of CDM		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to request the synchronization of the Common Data Model (CDM)		
Trigger:	The Administrator clicks on the "Automatic Updates" button form main menu		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application 3. The user configured the settings for automatic updates		
Post conditions:	The system allows synchronization of the Common Data Model (CDM)		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Automatic Updates" button form main menu	The System displays the "Automatic Updates"
	2	The Administrator clicks on the ">" button associated to the "Sync" button and then clicks on the "Sync CDM" button	The System displays "SYN005 – CDM Sync Status" form, which contains: • "CMD Sync Status" section • 4 "Artefact Request" subsections, each containing ○ "Artefact Group" -mandatory radio button selection filed . The available choices for requests are: ▪ -"BMP" for Business processes ▪ -"RINA_BL" for the artefacts concerning RINA Business Layer ▪ -"RINA_PL" for the corresponding artefacts of the RINA Protocol Layer ▪ -"AP" (Access Point) Artefacts. Each of the 4 subsections has selected a distinct value for this field ○ Time Sync Up To - mandatory, calendar field ○ Add button – add subsection Artefact Request ○ Delete button The Administrator provides information about which artefact group(s) need(s) to be synchronized with the AP.

			The number of groups to be synchronised can be customised along with the date of the latest synchronisation date in RINA to the CDM request from the AP. The Administrator can add/remove a request by simple clicking on "Add" button or Delete button. - "Save" button - "Reset" button
	2	The Administrator fills in the fields and clicks "Save" button	The Administrator sends the request. The system (RINA application) sends a system message to the AP to request the latest CDM content based on the related requested artefact groups (SYN005 message). The AP responds in an asynchronous manner with the new file (in case there is any newer related content), or an empty file (if RINA has the latest data content). Any new files are persisted under the defined (via the configuration) disk resource path of the application system. (Recommendation: The "Automatic Updates: CDM sync" feature is used when the CDM artefacts are not installed during the installation procedure but the new CDM artefacts are published from CSN)
Alternative scenario 1	1	The Administrator clicks "Reset" button	The System discards all values modified during editing.

UC_AU_04 Detecting and deploying the updated artefacts

Use Case ID:	UC_AU_04		
Use Case Name:	Detecting and deploying the updated artefacts		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to perform the actions in order to complete the synchronisation processes and update all the corresponding artefacts (select the relevant "Resource Type" category(ies), refresh the displayed information, Install artefacts)		

Trigger:	The Administrator clicks on the "Automatic Updates" button from main menu.		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application and configured the settings options. 3. The user has performed UC_AU_02 or UC_AU_03 for synchronising.		
Post conditions:	The Administrator has filtered the artefacts, refreshed the displayed information, and initiated the installation process (started the deployment of the artefacts).		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Automatic Updates" button from main menu.	The System displays the "Automatic Updates" form.
	2	The Administrator clicks on the filter icon button	The System displays the "Filter by" subsection which contains: • area for selecting the resource type labelled "Resource Type" with associated "x" button for clearing the current selections. In this area, the available fields are: ○ "Localization" checkbox field ○ "Vocabularies" checkbox field ○ "SEDs" checkbox field ○ "Form Templates" checkbox field ○ "SBDHs" checkbox field ○ "Organizations" checkbox field ○ "Transactions" checkbox field ○ "Initial Documents" checkbox field • area for selecting the status labelled "Status" with associated "x" button for clearing the current selections. In this area, the available fields are: ○ "Same Version Everywhere" ○ "Older Version On Disk" ○ "On Disk Only" ○ "Installed Only" ○ "Newer Version on Disk"
	3	The Administrator selects the desired filters and clicks on "Refresh" icon.	The System hides the "Filter by" subsection and refreshes the displaying grid by displaying only the selected resources types.
	4	The Administrator selects the exact resources that should be installed by clicking on	The System launches the installation process (start the deployment of the artefacts). On the successful completion of the deployment

		the checkbox field of the resources group and clicks on the "Install" button to trigger the deployment process of the corresponding artefacts.	operation, the red rectangle icons are converted to green colour to indicate that the resource type has been updated, meaning that there is no new relevant update available. (Recommendations: In case of a large update, where the number of generated artefacts to be synchronized is huge (i.e., hundreds or thousands of artefacts), it is strongly recommended to install ONLY one artefacts resource type at a time and to repeat the procedure until all the necessary artefacts are correctly installed. If an artefact type contains many updates to get deployed, it is also recommended to get this operation performed over multiple steps by selecting a file subset of such long lists at a time)
--	--	--	--

UC_AU_05 Importing Organizations

Use Case ID:	UC_AU_05		
Use Case Name:	Importing Organizations		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator the manual import of the IR from a local file		
Trigger:	The Administrator selects "Automatic Updates" menu option and clicks on the "Import Organizations" button		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application 3. The user configured the settings for Automatic Updates		
Post conditions:	The system allowed the manual import of the IR from a local file.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Automatic Updates" button form main menu	The System displays the "Automatic Updates" form.
	2	The Administrator clicks on the "Import Organization" button	The system opens "File Explorer" from operating system. The Administrator has the option to import an organization structure directly through local files, this action allows the manual import of the IR from a local file.

UC_AU_06 Checking Repository Versions

Use Case ID:	UC_AU_06		
Use Case Name:	Checking Repository Versions		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to check the available repository file versions		
Trigger:	The Administrator selects "Automatic Updates" menu option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application 3. The user configured the settings for automatic updates		
Post conditions:	The system allowed the Administrator to check the available repository file versions		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Automatic Updates" button from main menu.	The System displays the "Automatic Updates" form.
	2	The Administrator accesses "Automatic Updates" menu option, then main area (ex: "Organizations (2) +")	The System display the full (expanded) detail list via clicking the "+" icon next to the relevant entry. This can be reverted by clicking the relevant "-" icon which has replaced the "-" icon following the content expansion.

Fields Details

Automatic Updates

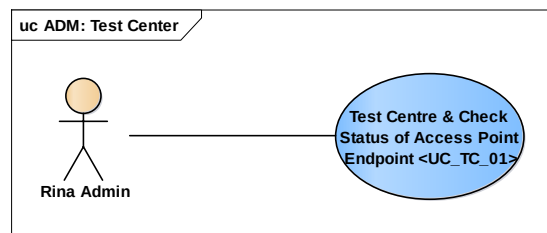
No.	Item name	Type	Validation/business rules
1	Search	Search element	Search with associated X, Delete (search)
2	Filter	Imagine	At click of this imagine, the system displays:
2.1	Filter by All Resource Type	Check box	Values: Localization Vocabularies SEDs Form Templates SBDHs Organizations

			Transactions Initial Documents
2.2	Filter by Status	Check box	Values: Same Version Everywhere Older Version On Disk On Disk Only Installed Only Newer Version on Disk
3	Setting	Imagine	The system displays Automatic Updates Settings, which contains:
3.1	Disk Resources Path On Server	Free text box fields	Mandatory, (C:/EESSI/Share/cdm/)
3.2	Shared Configuration Path	Free text box fields	Mandatory, (C:/EESSI/Share/)
3.3	Shared BMP Repository Path	Free text box fields	Mandatory, (C:/EESSI/Share/repository/bmp/)
3.4	Form Templates Repository Path	Free text box fields	Mandatory, (C:/EESSI/Share/portal/templates/)
3.5	Office Templates Repository Path	Free text box fields	Mandatory, (C:/EESSI/Share/portal/office_templates/)
3.6	Localization Resources Repository Path	Free text box fields	Mandatory, (C:/EESSI/Share/portal/localization/)
3.7	Back	Button	
3.8	Reset	Button	
3.9	Save	Button	
4	Import organizations	Button	At click open directory window, offers the possibility to choose a file from directory
5	Install 0	Button	Disabled
6	Refresh	Button	
7	To Install (0)	Label	Has associated imagine used to expand or contract grid
8	Organization	Grid	Contains columns: Type Status Disk version Disk date Server version Server date

9	Sync Institution	List	The system displays SYN002 - Request For IR Sync form, which contains:
9.1	Request For IR Sync	Label	
9.2	1.1 Current Version	Free text box field	Mandatory
9.3	Back	Button	
9.4	Reset	Button	
9.5	Save	Button	
10	Sync CMD	List	The system displays SYN005 - CDM Sync Status form, which contains:
10.1	CDM Sync Status	Label	
10.2	1.1[1]. Artefact Request	Section	
10.2.1	1.1.1. Artefact Group	Radio buttons	Mandatory Values: [01] BMP [02] RINA_BL [03] RINA_PL [04] AP
10.2.2	1.1.2. Time Sync Up To	Calendar	
10.2.3	Add	Button	
10.2.4	Delete	Button	
10.3	Back	Button	
10.4	Reset	Button	
10.5	Save	Button	

6.12 Test Center

Use case diagrams



Use Case View

UC_TC_01 Test Center & Check Status of Access Point Endpoint (Network)

Use Case ID:	UC_TC_01		
Use Case Name:	Test Center & Check Status of Access Point Endpoint (Network)		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	

Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to perform some basic testing of RINA's network connectivity to EESSI International Domain.		
Trigger:	The Administrator selects "Test Center" from main menu		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application as RINA Admin		
Post conditions:	The system allowed testing Rina network connectivity to EESSI International Domain		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Test Center" button from main menu	The system displays the "Test Center" form, where the Administrator has available: • "Refresh" Button • "Check Status of Access Point Endpoint" button • a grid where performed tests are displayed. The grid has a dynamic label – "Total <number> Successful: <number> Failed: <number>" and the following columns: ○ "Date" ○ "Message" ○ "Status"
	2	The Administrator clicks "Check Status of Access Point Endpoint (Network)" button	The System performs a "Sanity test". This test that can be used to test mainly the status of the Access Point (AP) at which RINA is connected. The System displays the performed test in the display grid.
	1	The Administrator clicks on "Refresh" button	The System redisplay the form.

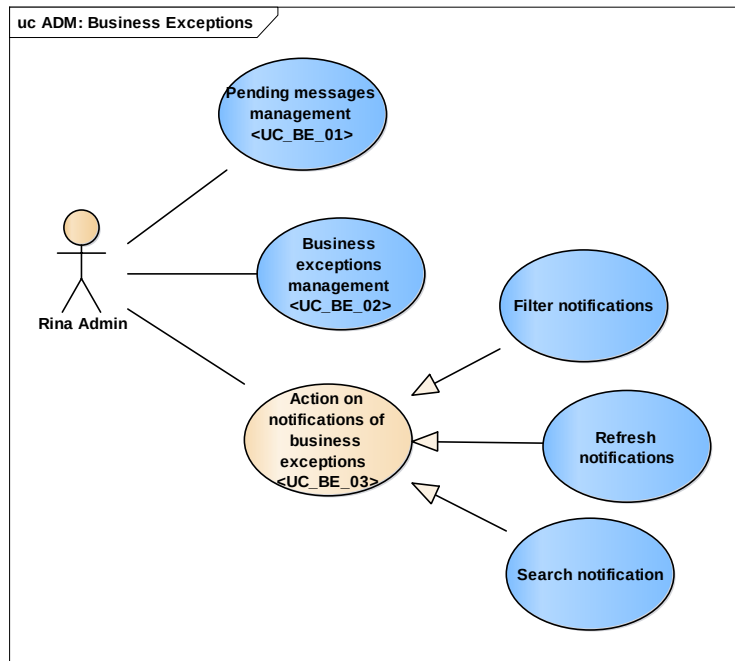
Fields Details

Test Center

No.	Item name	Type	Validation/business rules
1	Check Status of Access Point Endpoint (Network)	Button	
2	Refresh	Button	Refresh screen
3	Total: Successful: Failed:	Label	
4	(tests grid)	Grid	Contains columns: Date Message Status

6.13 Business Exceptions

Use case diagrams



Use Case View

UC_BE_01 Pending messages

Use Case ID:	UC_BE_01		
Use Case Name:	Pending messages		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	07.05.2020	Last Revision Date:	
Actors:	System, Administrator		
Description:	This use case describes how the Administrator can consult the list of pending messages and manually intervene for generating a business exception for the pending message.		
Trigger:	The Administrator selects "Business Exceptions" menu option and clicks "Pending Messages" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator had the possibility to consult list of pending messages and to manually send back to the SED originator a business exception (X050 SED) message.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Business Exceptions" menu	The system displays "Pending Messages" form which contains:

		option and then "Pending Messages" option	- "Search" button - (search) free text field - filter icon button - grid displaying the pending messages with columns: - "Date" - "Type" - "Description" - "Actions" – for each displayed pending message, the Administrator has available - "View SED" button - "Reject" button The list with pending messages contains received SEDs for which the System identified an issue that requires a waiting period before automatically generating a business exception (this issue could be solved by receiving another SED). Additional information about these exceptions may be found in the document "EESSI Business Use Case AD_BUC_11". For each displayed SED, the Administrator also has available a ">" icon button.
	2	The Administrator selects a pending message from the grid and clicks on the ">" icon button.	The System expands the display area for the selected pending message with the following fields: "Problem" "Date" "SED type" "BUC type" "International Case Id" "Sender" "Participants" (list with tenants)
Alternative Scenario 1	1	The Administrator identifies the pending message and clicks on the corresponding "Reject" button	The System displays the "Reject Messages" form, where the Administrator has available : - "Reason*" – free text field for providing the rejection reason - "Yes" button - "No" button
	2	The Administrator fills in the "Reason*" field and	The System sends back to the SED originator a business exception (X050 SED) message.

		clicks on the "Yes" button	The System close the "Reject Messages" form. The System delete the pending message from the grid.
Alternative Scenario 2	1	The Administrator clicks "View SED" button	The System displays the "SED Form" of the selected SED.

UC_BE_02 Business exceptions

Use Case ID:	UC_BE_02		
Use Case Name:	Business exceptions		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	08.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the Administrator can consult the list of the SED that caused the business exception or even see the Rejection SED generated for this SED		
Trigger:	The Administrator selects "Business Exceptions" menu option and clicks "Business Exceptions" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator consulted the list of the SED that caused the business exception.		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator accesses "Business Exceptions" main menu and then "Business Exceptions" option	The system displays "Business Exceptions" form which contains: - "Search" button - (search) free text field - filter icon button - grid displaying the SEDs that caused a business exception, with the following columns: - "Date" - "Type" - "Description" - "Actions" – for each displayed SED, in this column, the Administrator has available the following buttons: - "View SED" - "View Rejection SED" For each displayed SED, the Administrator also has available a ">" icon button.

	2	The Administrator selects a SED from the grid and clicks on the corresponding ">" icon button.	The System expands the display area for the selected SED with the following fields: - "Rejection Date" - "Rejection reason" - "Problem" - "Date" - "SED type" - "BUC type" - "Local Case Id" - "International Case Id" - "Sender" - "Participants" (list with tenants)
	3	The Administrator clicks on the "View Rejection SED" button	The System displays the "SED Form" related to the business exception - X050 SED.
	4	The Administrator clicks "View SED" button	The System displays "SED Form" related to the original SED previously appearing as a pending message.

UC_BE_03 Filter, refresh, and search notification of business exceptions

Use Case ID:	UC_BE_03		
Use Case Name:	Filter, refresh, and search notification of business exceptions		
Created By:	Madalina Alecsandrescu	Last Updated By:	
Date Created:	14.05.2020	Last Revision Date:	
Actors:	System Administrator		
Description:	This use case describes how the system allows the Administrator to filter, refresh list and search elements in order to display and treat business exceptions, grouped by year (displayed in Navigate section)		
Trigger:	The Administrator selects "Business Exceptions" menu option and clicks on the "Business Exceptions" option		
Preconditions:	1. The user is authenticated in RINA. 2. The user is authorized to access Application		
Post conditions:	The Administrator has performed search, refresh, and filtered business exceptions		
Main Scenario:	#	Step actions	Expected Result
	1	The Administrator clicks on the "Business exceptions" button from main menu, then clicks on the "Business exceptions" button.	The system display "Business Exceptions" form which contains: - "Search" button - (search) free text field - filter icon button - Grid with: - "Date"

			- "Type" - "Actions"
	2	The Administrator clicks "Filter" element	The System displays "Filter by" subsection which contains: • "Business Exception" label with x icon button to clear all selections • "Case Missing" checkbox field • "SED Update without Create" checkbox field • "Case Forwarded" checkbox field • "Case Removed" checkbox field • "SED in Wrong Sequence" checkbox field • "Case Closed" checkbox field • "Invalid Business Signature" checkbox field • "Attachment failed antimalware checking" checkbox field
	3	The Administrator selects the desired filters and clicks outside the "Filter by" subsection	The System displays only the business exceptions related to the selected filters.
	4	The Administrator enters the keywords to search by the free text search field and clicks on the "Search" button	The System displays only the business exceptions containing the keyword provided by the Administrator.
Alternative Scenario 2	1	The Administrator clicks "Refresh" button	The system redisplay the form.

Fields Details

Business Exceptions – Pending messages

No.	Item name	Type	Validation/business rules
1	Search	Search element	Search Delete
2	Filter by – Business exceptions	Check boxes	Values: Case Missing SED Update without Create Case Forwarded Case Removed SED in Wrong Sequence Case Closed Invalid Business Signature Attachment failed antimalware checking
3	Total Records:	Label	
4	Pending messages	Grid	Contains columns: Date

		Type Description Actions
--	--	--------------------------------

Business Exceptions – Business Exceptions

No.	Item name	Type	Validation/business rules
1	Search	Search element	Search Delete
2	Filter by – Business exceptions	Check boxes	Values: Case Missing SED Update without Create Case Forwarded Case Removed SED in Wrong Sequence Case Closed Invalid Business Signature Attachment failed antimalware checking
3	Total Records:	Label	
4	Pending messages	Grid	Contains columns: Date Type Description Actions