Project number: 653454
H2020-DS-2014-1

Project start: October 1, 2015
Project duration: 3 years

D2.1

Scenarios and Use-Cases

Document Identification	
Due date	June 30, 2016
Submission date	June 30, 2016
Revision	1.0

Related WP	WP2	Dissemination Level	PU
Lead Participant	FOKUS	Lead Author	Florian Thiemer (FOKUS)
Contributing Beneficiaries	AIT, ATOS, LISPA, FOKUS, OTE, KGH, ICERT, TUG	Related Deliverables	

Abstract: This document gives formal specifications and descriptions of the use cases that have been identified for the different pilots considered within CREDENTIAL. It describes all involved stakeholders, actors, and their interactions with the Cloud Identity Wallet.

This document is issued within the CREDENTIAL project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 653454.

Executive Summary

In traditional Identity and Access Management as a Service (IDMaaS) systems an Identity Provider (IdP) has full access to the user's identity data. The shift of such services into the cloud discloses sensible user data to the cloud provider. Thus, the user's privacy is compromised, and legal issues and challenges for service providers may arise. With the invention of proxy-re-encryption and redactable signature algorithms it is possible to outsource an Identity Provider into a cloud environment without disclosing the processed data to the cloud provider. While these novel cryptographic technologies are mature from a scientific research perspective they are not yet included in market-ready products. In this document actors and use cases will be elaborated, and explain how to integrate those technologies into an IDMaaS environment. We call this IDMaaS environment the CREDENTIAL Wallet.

The purpose of this document is to have a clear understanding of applicable business use cases and the identification of all actors involved in a CREDENTIAL Wallet. These generic artifacts form modularized basic blocks for a CREDENTIAL Wallet. Furthermore, this document shows how to apply these building blocks in three different application domains: eGovernment, eHealth, and eBusiness.

This document contains the collection of all generic business use cases for the CREDENTIAL Wallet. These use cases fully describe its functionality. Since business use cases tend to be abstract, we additionally specify logical use cases describing each step in the business use cases in more detail. Starting from these use cases, further development of the CREDENTIAL Wallet can proceed and requirements, architecture, and technology can be elaborated.

In order to show practical relevance of the proposed use cases, three pilots in the domains mentioned above adapted them and developed scenarios and storyboards. Thus we show how we can enhance existing applications and service by integrating a CREDENTIAL Wallet and its functionality. This document contains multiple scenarios for each domain and a list of business use cases describing on a high level how to use a CREDENTIAL Wallet in the domains.

Document information

Contributors

Name	Partner
Andreas Abraham	TUG
Pasquale Chiaro	ICERT
Sara Facchinetti	LISPA
Felix Hörandner	TUG
Stephan Krenn	AIT
Andrea Migliavacca	LISPA
Nicola Notario-McDonnel	ATOS
Anna Schmaus-Klughammer	KGH
Evangelos Sfakianakis	OTE
Florian Thiemer	FOKUS
Alberto Zanini	LISPA

Reviewers

Name	Partner
Pasquale Chiaro	ICERT
Stephan Krenn	AIT
Andrea Migliavacca	LISPA

History

0.1	2016-02-04	Florian Thiemer	Initial draft and ToC
0.2	2016-02-15	Florian Thiemer	Added use case Template definition
0.3	2016-02-25	Nicola Notario-McDonnel	Added Scope section
0.4	2016-03-29	Florian Thiemer	Added Draft Content for Executive Summary, Introduction and Methodology
0.5	2016-04-06	Sara Facchinetti Andrea Migliavacca	Added eGovernment section
0.6	2016-05-12	Pasquale Chiaro	Added eBusiness section
0.7	2016-05-31	Florian Thiemer Evangelos Sfakianakis	Added eHealth section Finalized eBusiness section
0.8	2016-05-31	Florian Thiemer	Added generic actors, business use cases and logical use cases
0.9	2016-06-15	Stephan Krenn	Added review comments and suggestions for improvements
0.10	2016-06-20	Florian Thiemer	Started working on reviewer comments
0.11	2016-06-27	Pasquale Chiaro	Added review comments
0.12	2016-06-28	Stephan Krenn	Extensive restructuring; moved generic LUCs and BUCs into Appendix and introduced overview tables; reformatting to new template
0.13	2016-06-29	Stephan Krenn	Restructured domain specific use cases
0.14	2016-06-30	Florian Thiemer Stephan Krenn	Added goals subsection Copy-editing and finalization
1.0	2016-06-30	Florian Thiemer	Final version

Table of Contents

List of Figures

List of Tables

List of Acronyms

BUC	Business Use Case
BMI	Body Mass Index
CNS	Carta Nationale dei Servizi (National Authentication Card)
CRS	Carta Regionale dei Servizi (Regional Authentication Card)
DPP	Diabetes Prevention Program
eID	Electronic Identity
EMR	Electronic Medical Record
HPO	Health Professional Organisation
HW	Hard Ware
IAM	digital Identity and Access Management
IDMaaS	Identity Management as a Service
IdP	Identity Provider
IdPC	Identity Provider Cittadino
LAN	Local Area Network
LUC	Logical Use Case
NIF	Numero de Identificacion Fiscal
OTP	One Time Password
PAN	Personal Area Network
PHR	Personal Health Record
UML	Unified Modeling Language

1 Introduction

One of the fundamental techniques in requirements engineering is the use case analysis. It describes how actors interact with a system in order to achieve an overlying goal. Use cases are usually described in a text form but can also be visualized using formal notations like UML[1]. Various use case templates have been developed over time. The most common used templates are the ones defined by A. Cockburn[2] and the ones defined by M. Fowler[3].

In this document use cases and actors are divided into three categories. They are organized from a top-down approach.

- The **business** category is the first one and describes use cases and actors at the highest abstraction level. In this category no connections to specific technologies are drawn. Instead it explains how actors can achieve a desired goal by using the CREDENTIAL system without describing the concrete steps.
- The **logical** category is the second one and refines the artifacts from the business category. Here the logical use cases are used to describe the individual steps the actors need to perform in the business use cases. If new actors are involved in order to fulfill the steps, they are assigned to the logical category of actors.
- The **technical** category is third. It draws the connection between concrete technologies and the logical use cases. They are out of scope for this document.

1.1 Goal of CREDENTIAL

The idea of the CREDENTIAL Wallet is to create a data-sharing and identity and access management platform in the cloud, which increases the security and privacy level compared to already existing solutions by using cryptographic primitives like proxy-re-encryption[4] or malleable signatures[5]. The Wallet itself acts as the safe data store where the participants' personal data is kept. The main features offered by the CREDENTIAL Wallet to participants are:

- Store and view personal data in the wallet
- Share personal data with other participants
- Using CREDENTIAL Wallet as IAM system for accessing other services
- Hide Information in documents to other participants while still guaranteeing the authenticity of the revealed data

[1] http://www.uml.org/
[2] http://alistair.cockburn.us/Basic+use+case+template
[3] Writing Effective Use Cases – A. Fowler ISBN: 0201702258
[4] R. Johnson, D. Molnar, D. Song, and D. Wagner, "Homomorphic Signature Schemes," in Topics in Cryptology - CT-RSA 2002, vol. 28913, 2002, pp. 244–262
[5] R. Johnson, D. Molnar, D. Song, and D. Wagner, "Homomorphic Signature Schemes," in Topics in Cryptology - CT-RSA 2002, vol. 28913, 2002, pp. 244–262

The main benefit provided by these features is:

- Reduced trust assumption to the cloud provider are required
- Increased flexibility
- High security guarantees
- Strong authenticity guarantees

Most traditional cloud services providers have access to the plaintext data stored by their users, and thus users have to take care of encryption and the associated overhead (such as, e.g., key management) themselves. Recently, encrypted cloud storage providers entered the market, which relieve the users from these tasks. However, so far all fully cloudified IAM systems require access to plain data; in particular, currently every identity provider requires access to the users personal data in order to deliver its service. In CREDENTIAL, this shall be overcome by the use of cryptography.

Our solution offers an increased flexibility for a participant by offer a solution that is completely available in the cloud. Participants can store and share their data from anywhere and using different devices like smartphone, tablet or computer. The data is highly protected by novel cryptographic mechanisms in the cloud. At any processing stage the data is always encrypted in an end-to-end way. As soon the data leaves the participant's device it is never available in plaintext in the cloud by design.

We offer strong authenticity guarantees for service provider. The identity information of participants can and will be used for Identity Management in the cloud by the CREDENTIAL Wallet provider. The CREDENTIAL mechanisms guarantees strong hardware-based multi-factor authentication mechanisms and the provided identity information in corresponding assertions are safely transmitted to the service provider.

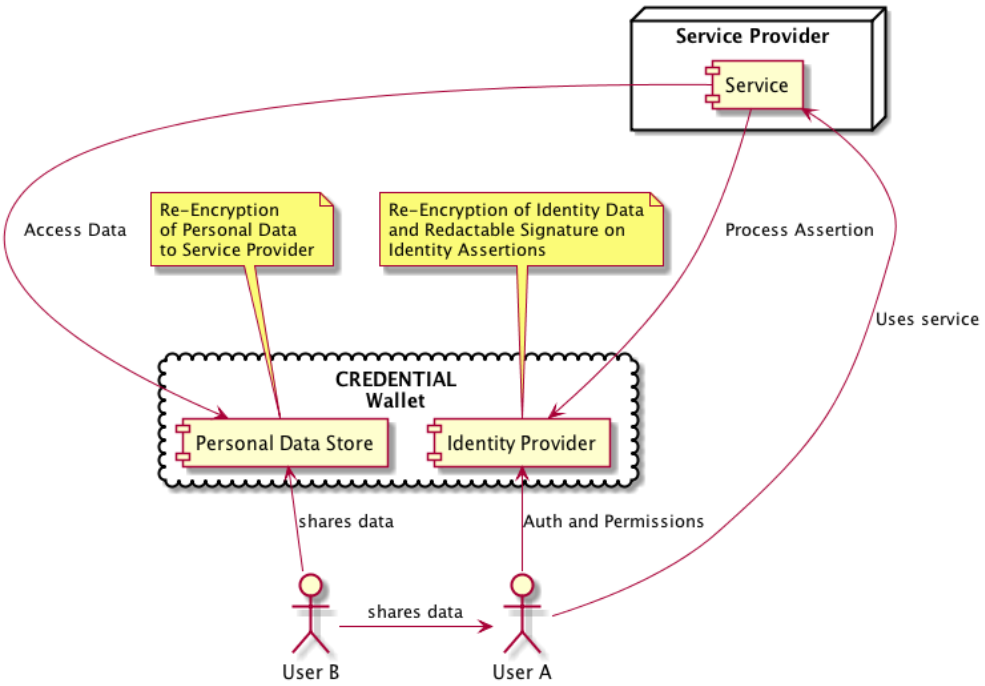


Figure 1: High Level Overview of CREDENTIAL Wallet

Figure 1 describes the main features of the CREDENTIAL Wallet. Firstly, it serves as a personal data store. Each participant can store any personal information safely in the cloud. A user can decide to share such information with other users by providing a forward rule in the CREDENTIAL Wallet. Now the other user is able to read the data without any more user interaction from the owner of the data because the wallet can process the forward rule. Since the data is encrypted, the wallet has to re-encrypt the data for the other user. In this whole process, the data is never disclosed for the wallet provider by design. Users cannot only share their data among each other, but also with service providers. The same mechanisms are used for this process. Access to the data is secured by the IAM system of the CREDENTIAL Wallet. The authentication process requires strong authentication mechanisms which will be enforced by the CREDENTIAL Wallet's Identity Provider. This Identity Provider issues identity assertions which are necessary to access any service or resource within the CREDENTIAL Wallet or using the wallet as the IAM in the cloud. It is protected by the novel cryptographic mechanisms like proxy-re-encryption or redactable signature. Thus we are able to provide user information stored in the wallet inside these assertions without the CREDENTIAL Wallet learning anything about the users' personal data revealed to the service provider.

1.2 Scope and Relation to Other Documents

The purpose of this document is twofold.
On the one hand, it documents the state of the art of secure cloud provider solutions and the requirements of various stakeholders. It analyzes, for the specific application domains of CREDENTIAL, the currently used technologies, and how they could be improved – in particular with respect to (data) privacy, authenticity, or usability – using CREDENTIAL technologies.
On the other hand, this document identifies concrete scenarios where CREDENTIAL could improve over the state of the art. From those scenarios, the main actors and their roles (with which they interact with the CREDENTIAL Wallet) are to be defined. These high-level use cases should then be decomposed into lower-level technical use cases in order to identify common functionalities across the domains, and provide inputs for the CREDENTIAL Wallet architecture. For this purpose, all identified use cases will be fully formalized.

Deliverable **"D2.1 Scenarios and use-cases"** does not depend on any other deliverable but on the work performed by most of the partners involved in the project. However, and given the pilot-centric approach of the project, the following deliverables will directly depend, at least partially, on this deliverable and/or in the work performed for its development:

- **"D2.3 Cloud identity wallet requirements"**: the requirement elicitation process will be driven by the functionalities required according to the use cases identified in this deliverable.
- **"D2.5 System security requirements, risk and threat analysis –2nd iteration"**: the analysis depends on the reference use cases identified in this deliverable.
- **"D2.6 User centric privacy and usability requirements"**: the requirement elicitation process will be driven by the functionalities required according to the use cases identified in this deliverable.
- **"D6.1 Pilot use case specification":** a more detailed analysis of the use cases identified in this deliverable, taking into account CREDENTIAL's building blocks will be conducted.

Many other deliverables indirectly depend or are influenced by this deliverable but do not rely in this deliverable as an input. For instance, **"D3.2 UI Prototypes V2 and HCI Patterns"** will provide UI mockups for functionality that has been identified in the use cases identified in this deliverable.

This deliverable describes the results of multiple activities that have been conducted by CREDENTIAL's partners:

Deliverable activity	Work Package Objective
Identify and define, in close collaboration with end-user partners, scenarios where the interaction with the Cloud Identity Wallet can add extra value to their services Identify in this scenarios who are the different actors and stakeholders that are part of scenarios;	O.2.1 Identify strong scenarios and use cases for the Cloud Identity Wallet.
Develop formalized business use cases where business and end-user 's functionalities required are represented	O.2.3 Identify end-user and business user needs for the Cloud Identity Wallet.
Find the commonalities of the different business Use cases on the different domains and formalize them in generic business use cases Move the generic use cases from a business level to a logical one enabling a deeper understanding of the Cloud Identity Wallet components and its functionalities	O.2.5 Define detailed use cases for the Cloud Identity Wallet acting as (i) Identity Provider, (ii) Attribute Provider, (iii) Personal Data Store, (iv) Credential Manager (e.g., passwords, certificates, assertions, etc.)

Table 1: Deliverable activities and WP objectives

Deliverable D2.1 is part of a bigger effort which is to design a Cloud Identity Wallet addressing end-users and businesses' needs. Figure 2 shows the positioning of this deliverable in such global picture. This deliverable will identify pilot-specific business use cases which will be generalized and derived into generic logical use cases. The design efforts will be responsible of designing the collaboration among all the logical actors and components and how they will be technically implemented to fulfill the use cases. Pilots will be specified to demonstrate the relevant domain-specific use cases and in accordance to the specified functional design.

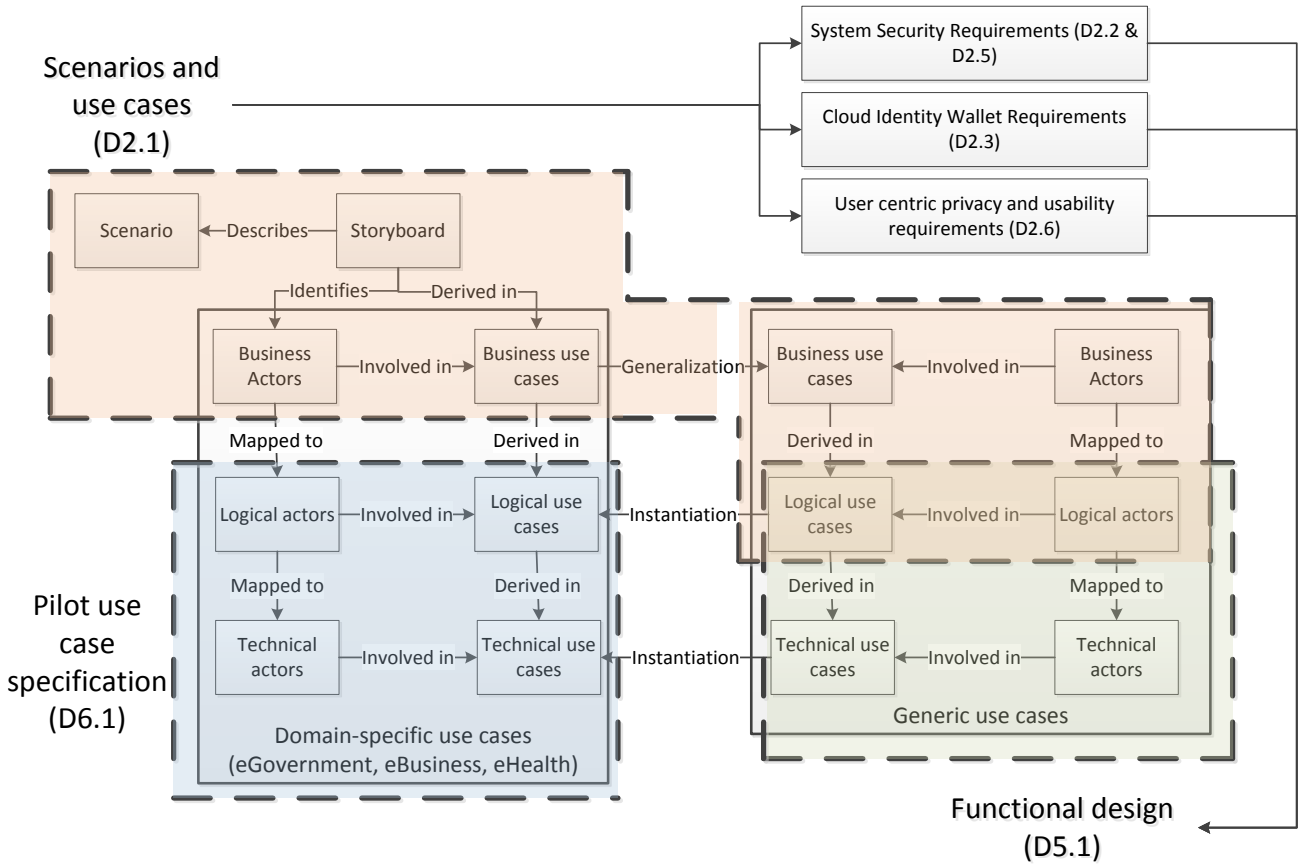


Figure 2: D2.1 as part of a broader mission

1.3 Document Outline

This document is structured as follows.

Section 2 describes the methodology which is used in order to derive the generic use cases and actors and how this work is included in the whole development process of the CREDENTIAL system.

In Section 3, the **generic use cases** for a CREDENTIAL system are described. It includes a detailed description of business actors and supporting logical actors from a generic point of view. The use cases for the business and logical category are described in this section.

In Section 4, the generic use cases are then applied in three different domains as **specific business use cases**. Each domain explains in form of a storyboard how the generic use cases can be used in their specific context. Furthermore, it explains the state of the art per domain and how a CREDENTIAL system can enhance products and solutions.

Finally, Section 5 gives a conclusion about the work done in this document and outlines the future work based on these results.

For readability, the main body of this document presents the use cases on a very high level only. The formal specifications of all use cases can be found in Appendix 1A.11A.1 (generic business use cases),

Appendix 1A.2 (generic logical use cases), and Appendix 1A.3 (domain specific business use cases), respectively.

2 Methodology

This section defines the terminology used in this document as well the description of the approach in order to create use cases for a CREDENTIAL system.

The documentation and creation of the use cases was made using a Redmine[6] wiki instance using the Requirements Engineering[7] plugin. The plugin has a built-in support for common requirement engineering frameworks. Mainly it supports the creation of use cases based on the templates introduced by A. Cockburn. In addition, it allows to create actors and requirements as own artifacts. Since it is a shared knowledge base we are able to keep track of relations between storyboards, use cases, and actors. The artifacts in this repository build the base for all upcoming development of the CREDENTIAL Wallet. Moreover, a graphical UML representation is provided for each storyboard and use case. UML diagrams are generated using the open source tool PlantUML[8].

This report represents the current stable status of the generic business and logical use cases, as well as the domain specific business use cases. Due to the status of the project, minor modifications or extensions may become necessary during the implementation process and the pilot use case specification in D6.1.

Figure 3 shows an example use case and its relation to other artifacts.

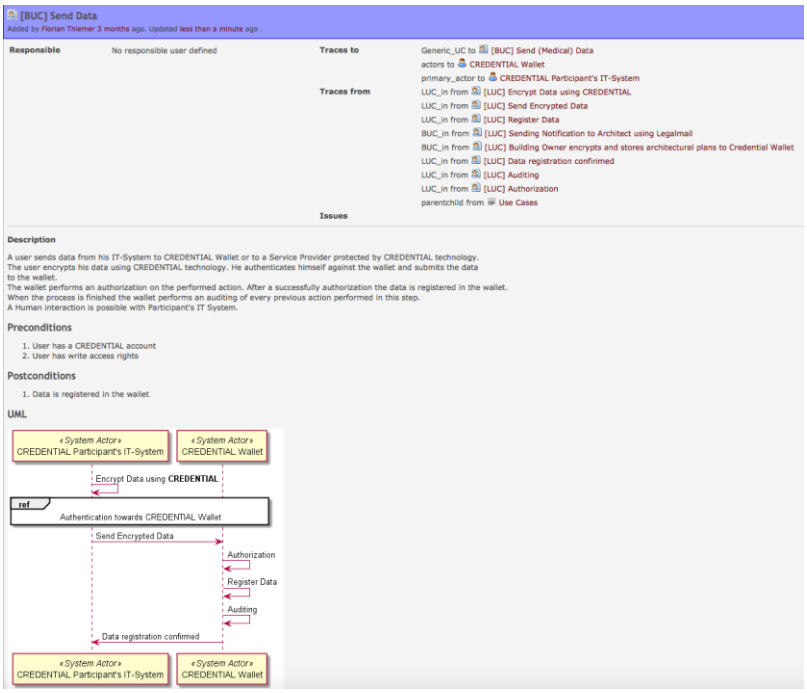


Figure 3: Business use case representation in Redmine

[6] http://www.redmine.org/
[7] https://github.com/tmerten/redmine_re
[8] http://plantuml.com/

2.1 Terminology

To avoid confusion, we will next fix some terminology that we will use throughout this document.

2.1.1 Storyboards

Story boards are a central tool for describing the high-level functionality of the CREDENTIAL Wallet.

Storyboard – A storyboard describes at a high level, using the terms of a specific domain, from a user point of view what functionality a system offers to him. It contains all of the structured information to explain a story. It contains a purpose, actors, pre-conditions, scenario, post-conditions, and a UML diagram.

Precondition – The precondition contains one or multiple statements about what need to be fulfilled before a use case.

Postcondition – The postcondition describes in one or multiple statements what is the effect of the use case.

Scenario – This is the central piece in a storyboard. It describes at a very high level what actors can do with existing technologies and how CREDENTIAL technology can improve the user experience.

2.1.2 Use Cases

We use use cases for a more fine granular specifications of the functionality of the CREDENTIAL Wallet. We distinguish the following four types:

Generic Use Case – A generic use case describes one or more general functionalities of the CREDENTIAL Wallet. It abstracts from any domain and focusing on the CREDENTIAL Wallet itself.

Pilot Use Case – A Pilot use case describes one or more functionalities of the CREDENTIAL Wallet inside a specific domain. It can be a specialization of a generic use case but can also stands for its own and thus enhance the CREDENTIAL Wallet with optional features.

Business Use Case – A business use case is an activity in a storyboard where actors are involved. A business use case is derived from a storyboard.

Logical Use Case – A logical use case is a single step in a business use case. It describes how two actors interact with each other.

2.1.3 Actors

Actors are natural or technical entities that are participating in use cases and story boards. We distinguish the following types of actors:

Business Actor – This is an actor in a business use case. Business actors can be humans, systems, or legal actors.

Logical Actor – This is an actor in a logical use case. Logical actors can be humans, systems, or legal actors.

Human Actor – This is a natural persons involved in the scenario.

System Actors – This is a technical entity involved in the scenario.

Legal Actors – This is a legal party involved in the scenario.

Persona – This is an actor in a storyboard which has some characteristics in order to describe specific use cases for different types of people. Usually personas are used for developing the use cases in a way that most of the possible imaginary user types are covered in the use cases.

2.2 Approach

In order to derive generic use cases that describe the general functionality of the CREDENTIAL system we follow a bottom up approach. Each pilot is challenged with the task to identify current business issues in their domain which can be solved or better handled by using proxy-re-encryption[9] and redactable[10] signature algorithms in the context of their domain, IAM and cloud service providers. We include pilots from three different domains – namely eGovernment, eHealth and eBusiness. Each pilot describes multiple storyboards including existing applications and services.

The storyboards describe at a high level how a CREDENTIAL system can be integrated and used in the context of the domain. The heart of a storyboard is the scenario. It uses personas and a textual description of what these personas do in a scenario. Mainly it describes the interaction between humans and systems in a coherent story. These scenarios do not necessarily introduce specific CREDENTIAL components but are designed in a way that features of a CREDENTIAL Wallet can enhance the user experience or even develop new functionalities.

All actors involved in a scenario are extracted and assigned to a different type. The types are human actor, system actor, and legal actor.

From the storyboards we identify business use cases. For each activity initiated by an actor in a storyboard we create an own business use case. Each storyboard can contain multiple business use cases and some of them can occur in multiple storyboards. To keep track of such relationships we are using custom relationships in the Redmine wiki. The following table describes all relationships, where they occur and to which artifact type they can link.

Relationship	Occurs in	Links to	Description
BUC_in	Business use cases	Storyboards, business use case	Indicates that a business use case is referenced in another business use case or Storyboard.
LUC_in	Logical use cases	Business use case, logical use case	Indicates that a logical use case is referenced in another logical use case or business use case.
Actor_in	Human Actor,	Storyboards,	Indicates that an Actor is referenced

[9] M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” in In EUROCRYPT. Springer-Verlag, 1998, pp. 127–144.

[10] R. Johnson, D. Molnar, D. Song, and D. Wagner, “Homomorphic Signature Schemes,” in Topics in Cryptology - CT-RSA 2002, vol. 28913, 2002, pp. 244–262

Relationship	Occurs in	Links to	Description
	system actor, legal actor	business use case, logical use case	in another Storyboard, business use case or logical use case.
Generic Actor	Human Actor, system actor, legal actor	Human Actor, system actor, legal actor	Indicates that an actor is a generic actor and derived from the referenced actor.
Generic UC	Business use case, logical use case	Business use case, logical use case	Indicates that a use case is a generic use case and derived from the referenced use case.

Table 2: Custom relationships defined in Redmine

After describing the business use cases they will be further subdivided into multiple logical use cases. Each logical use case represents an individual step in the corresponding business use case between two actors. Additional actors may be introduced in this process. These newly created actors will be tagged as Logical Actors.

We describe business use cases and logical use cases according to the following structure:

Use Case Name	Name of the Use Case
ID	Unique ID of the use case. The ID follows the pattern: [DOMAIN]-[TYPE]-[UNIQUENAME], where: • DOMAIN is either "G" for generic use cases, or "E-GOV", "E-HEA", or "E-BUS" for domain-specific use cases from the eGovernment, eHealth, or eBusiness pilots, respectively; • TYPE indicates whether it is a business use case ("BUC") or a logical use case ("LUC"); • UNIQUENAME is unique and describes what is included in the use case.
Main Actor	According to A. Cockburn[11], the main actor of a use case is defined as follows: "[The] primary actor of a use case is the stakeholder that calls on the system to deliver one of its services. It has a goal with respect to the system – one that can be satisfied by its operation. The primary actor is often, but not always, the actor who triggers the use case."
Secondary Actors	Again following A. Cockburn, secondary actors are defined as "actors that the system needs assistance from to achieve the primary actor's goal." A use case can have one or multiple secondary actors.
Pre-conditions	One or multiple pre-conditions, i.e., conditions that need to be satisfied before the use case can be executed.
Post-conditions	One or multiple post-conditions, i.e., guarantees that are satisfied after a successful execution of the use case.
Description	A detailed description for this use case.
Image	A UML representation of the use case. We use UML sequence diagrams to describe the use cases.

Table 3: BUC and LUC description structure

[11] Cockburn, A, 2000, Writing Effective Use Case, Addison-Wesley Professional; Edition 1

3 Generic Use Cases

In this section, we present the identified generic actors, generic business use cases, and generic logical use cases.

A *generic use case* describes one or more general functionalities of the CREDENTIAL Wallet. It abstracts from any domain and focuses on the CREDENTIAL Wallet itself. A *generic actor* is a component, person, or system that is included in such a generic use case.

Generic use cases are derived through a bottom up approach from the pilot-specific use cases. The process has been carried out defining firstly the pilot storyboards and scenarios and then deepening into business and logical use cases and Actors definition before entering the generalization process to generic business and logical use cases and generic actors. For a matter of clarity this deliverable first presents the derived generic use cases and then the pilot specific use cases.

A total of 33 business use cases were identified and more refined in a total of 108 logical use cases.

3.1 Actors

3.1.1 Business Actors

The business actors are the entities which are defined on the Business Level. They are firstly introduced by identify the business use case and tend to be as abstract as possible.

3.1.1.1 Human Actors

CREDENTIAL Participant – A person who uses the CREDENTIAL Wallet. He can store data in the CREDENTIAL Wallet and uses its features in order to share his personal data. A user has a CREDENTIAL account and possesses credentials on his smartphone or computer which allows him to authenticate against the CREDENTIAL Wallet or other Identity Providers that support CREDENTIAL technology.

CREDENTIAL Admin – A user who has administrative privileges in the CREDENTIAL Wallet. An administrator is able to create new accounts, ban users, and similar tasks. He possesses credentials on his computer in order to authenticate against the CREDENTIAL Wallet.

3.1.1.2 System Actors

CREDENTIAL Wallet – The CREDENTIAL Wallet is the central platform where data storage, data exchange and authentication occurs. The CREDENTIAL Wallet can be either a portal offering services to users and other service provider or be a collection of libraries which supports the integration of CREDENTIAL technology in existing systems.

Service Provider – A Service Provider is an external Service which can be used by CREDENTIAL Participants.

Identity Provider – An entity or system responsible to authenticate users online. It guarantees that users are uniquely identified and properly authenticated. It usually issues an Identity Assertion which contains a proof of the user's identity a signature which states that the Identity Provider authenticates the user and

additional attributes that can be used by other Service Provider to identify and authorize the user. Attributes may be encrypted.

CREDENTIAL Participant's IT-System – The IT-System used by a CREDENTIAL Participant in order to use the CREDENTIAL Wallet. This could be a smartphone, a webserver, a computer, etc. Additional CREDENTIAL software may be installed on this IT-System which allows the integration in the CREDENTIAL Wallet workflow.

eID – eID is an acronym for electronic identification. This could be a smartcard, available for citizens and organizations, provided by government authorities, banks, or other companies. Usually they contain an X.509 digital certificate with the purpose of authenticate the user during online transactions.

CREDENTIAL Participant's Cold Storage – Place where participant's recovery keys are safely stored. For example, USB Stick, QR Code, etc.

Signing Service – An external signing service which allows to sign a document if a valid PIN is provided.

3.1.1.3 Legal Actors

No generic legal actors were defined.

3.1.2 Logical Actors

3.1.2.1 Human Actors

No generic human actors were defined.

3.1.2.2 System Actors

CREDENTIAL Re-Encryption Key Generation Service – This component is an integral part of the innovative and secure data sharing mechanism presented by CREDENTIAL. It generates re-encryption keys that will be used by the CREDENTIAL Wallet or independent re-encryption components to transform encrypted data so it can be decrypted by the data receiver. By generating this re-encryption key from her private key and distributing it to an authorized proxy, the participant owning encrypted data enables sharing and thereby provides some form of consent. After this key was generated, the user does not have to be actively involved in the sharing process anymore.

CREDENTIAL Personal Trust Store – The component Personal Trust Store is responsible to provide a secure place for storing the high confidential CREDENTIAL participants private key next to the public key. Only authorized participants are permitted to gain access to this private key.

CREDENTIAL Encryption Service – In order to ensure the confidentiality of the user's possibly sensitive data in untrusted environments, these attributes are protected by cryptography. CREDENTIAL uses proxy re-encryption instead of traditional public key encryption to support flexible sharing of the participants' ciphertexts. This component performs the encryption process, which requires public key material of the receiver. User's may encrypt data for themselves and upload the resulting ciphertext. However, a third party, for example another user, may also provide data that was encrypted for the user. Eventually, the recipient controls the sharing of encrypted data by issuing re-encryption keys.

CREDENTIAL Sign Service – The CREDENTIAL Sign Service as part of the CREDENTIAL Participant's IT-System or the CREDENTIAL Wallet.

CREDENTIAL Decryption Service – In order to ensure the confidentiality of the user's data the CREDENTIAL Wallet encrypts all data. All encrypted data have to be decrypted as well at a specific point. That is why this component is one of the fundamental parts of the CREDENTIAL Wallet. This component performs a service which decrypts a given ciphertext utilizing the related private key. A possible scenario is that the user wants to see his data and therefore the decrypt service has to be performed.

CREDENTIAL Proxy Re-Encryption Service – The CREDENTIAL Wallet offers novel cryptographic mechanism to ensure the confidentiality of the user's data. One cryptographic primitive is the proxy re-encryption which is utilized when sharing data while preserving the confidentiality. Conceptually, the re-encryption mechanism performs both a decryption of a ciphertext as well as the encryption in one step using the re-encryption key. The advantage of this re-encryption mechanism is that the proxy is not able to see the plain text but only to re-encrypt the ciphertext. For example, a ciphertext which is encrypted for participant A is re-encrypted for participant B.

CREDENTIAL Participant Registration Service – This component is responsible for registering a new, or deleting an existing account of a CREDENTIAL Wallet. Upon de-registration, also all data related to the specific user should be deleted from the wallet.

CREDENTIAL Participant Data Repository – This is the service where the actual data blobs of a user get stored. Data can be written through an interface to the repository and can be retrieved for returning data to a user or for re-encryption.

CREDENTIAL Participant Data Search Service – The CREDENTIAL Data Search Service as part of the CREDENTIAL Wallet. Data Search Service and Data Repository are closely coupled maybe even integrated as search operation will always use some meta-information of the stored data to discover it. If meta information might be stored in an independent registry the coupling might become more loose but additional operations to register the meta-information will have to be integrated.

CREDENTIAL Participant Index - This index contains identifiable information about users. It is written by the CREDENTIAL Participant Registration Service, and is queried by the CREDENTIAL Participant Search Service.

CREDENTIAL Participant Search Service – This service allows one to search for the public key of a participant, which is needed for re-encryption. The key might, e.g., be found given the user's email-address as input.

CREDENTIAL Authorization Service – The authorization service is responsible for giving or denying permission requests to services, data or resources in general. There is a close relationship between the Identity Provider and the authorization service, as the authorization policies may be directly linked to specific users (i.e. "user a" wishes to give "user b" full access to all his data).

CREDENTIAL Audit Trail Service – In general an audit trail is a full historic list of all actions that are relevant for a certain service or resource. This service/component will be responsible to keep reference

and allow querying all the relevant actions within CREDENTIAL i.e. whenever participants different from the owner access and/or modifies some data.

CREDENTIAL Data Repository Provider – Manages access to documents that are not stored in CREDENTIAL. The Data Repository Provider has to implement the same logical functionality as the Participant Directory and the Data Search Service.

CREDENTIAL Identity Provider – In the context of CREDENTIAL, an Identity Provider (IdP) is a component which is responsible for creating, maintaining and managing identity information of data subjects (citizens or organizations). It provides data subjects authentication to other stakeholders (i.e. online services). How the IdP interacts with the data subject in order to create, manages or maintain its data is out of CREDENTIAL's scope. The main purpose of the IdPs in CREDENTIAL's ecosystem is to provide identity information to other actors.

CREDENTIAL Attribute Service – The Attribute Service is used to manage access to information (identity attributes) stored about a CREDENTIAL user.

CREDENTIAL Redactor Service – This service is able to redact fields in a document but maintains the validity of the signature using malleable signature techniques. For example, all data on an electronic driver's license is blacked out, except for the name and date of birth. With this minimized but still signed document, a person would be able to prove her age.

CREDENTIAL Key Generation Service – This component generates public/private key-pairs, compatible with the re-encryption schemes chosen for CREDENTIAL. The public key will act the public Wallet account identifier, while the generated private key must be safely stored in the participant's IT systems and will be required to perform many actions within the wallet.

CREDENTIAL Authentication Service – The CREDENTIAL Authentication Service authenticates participants against the CREDENTIAL Wallet. It consumes credentials provided by the participant's, verifies them and in a successful case issues an Identity Assertion with which a participant is able to use CREDENTIAL services.

IdP Selector – A service which allows users to select from a list of available Identity Providers.

3.1.2.3 Legal Actors

No legal actors were defined.

3.2 Generic Use Case Description

In the following we give an overview of the generic business use cases and the related generic logical use cases. For the sake of readability, we only give a high-level description here. All technical details can be found in the appendix.

3.2.1 Generic Business Use Cases

The generic business use cases (generic BUCs) are grouped into the following categories:

- Data Management
- Authentication

- Authorization
- Account Management
- Cryptography

In the following, we give a brief introduction to each of those categories. Detailed specifications of all mentioned use cases can be found in Appendix 1A.1.

3.2.1.1 Data Management

This category covers all aspects of sharing data in the CREDENTIAL Wallet. Besides the obvious use cases like sending/storing, downloading/reading, or securely deleting data, it also covers the possibility of forwarding data to other users, or to export data from the CREDENTIAL Wallet for various purposes. Also, users can see all previous access to their data or get notified upon changes of their data. Finally, a user's personal data can be used to access a service provider.

In more detail, the following use cases are specified in this cluster:

Use Case Name	Unique ID	Main Actor
Export CREDENTIAL Wallet data into form	G-BUC-EXPFORM	CREDENTIAL Wallet
Send Data	G-BUC-SENDDATA	CREDENTIAL Participant's IT-System
Read Data	G-BUC-READDATA	CREDENTIAL Wallet
Forward Data	G-BUC-FORWARDDATA	CREDENTIAL Wallet
Send Notification	G-BUC-SENDNOTIFICATION	CREDENTIAL Wallet
Delete Data Set	G-BUC-DELETEDATASET	CREDENTIAL Wallet
Export Data from Wallet	G-BUC-EXPORTDATA	CREDENTIAL Wallet
View all accesses to my Data	G-BUC-VIEWACCESSES	CREDENTIAL Participant's IT-System
Recover CREDENTIAL Wallet data	G-BUC-RECOVERDATA	CREDENTIAL Wallet

Table 4: Generic Data Management BUCs

3.2.1.2 Authentication

This category is concerned with various aspects of authentication.

It contains the following use cases:

Use Case Name	Unique ID	Main Actor
Authentication using SmartCard	G-LUC-AUTHSMARTCARD	eID
Logout from CREDENTIAL Wallet	G-BUC-LOGOUTWALLET	CREDENTIAL Wallet
Authenticate towards CREDENTIAL Wallet	G-BUC-AUTHWALLET	CREDENTIAL Participant's IT-System
SP build up Trust relation to IdP	G-BUC-SPBUILDTRUSTIDP	Service Provider
Access Service Provider	G-LUC-ACCESSSP	CREDENTIAL Participant

Table 5: Generic Authentication BUCs

3.2.1.3 Authorization

Authorization is concerned with requesting and granting access rights to specific files to different users. Also, it covers the re-generation of access rights if a user has to change his cryptographic key material, e.g., because of a compromised device.

Use Case Name	Unique ID	Main Actor
Request Access Rights	G-BUC-REQACCESSRIGHTS	CREDENTIAL Wallet
Grant Access Rights	G-BUC-GRANTACCESSRIGHTS	CREDENTIAL Wallet
Re-Generate Access Rights	G-BUC-REGENACCESSRIGHTS	CREDENTIAL Participant's IT-System

Table 6: Generic Authorization BUCs

3.2.1.4 Account Management

Account management is concerned with all issues concerning registration or de-registration (through the user or through the CREDENTIAL admin). It allows users to list previous logins to their account, and allows them to link their CREDENTIAL Wallet with compatible service providers in order to authenticate to those services using CREDENTIAL in the following. Also, users can register new devices in order to access their wallet from this device in the following.

In more detail, the use cases associated to this category are:

Use Case Name	Unique ID	Main Actor
Link Service Provider account with CREDENTIAL account	G-BUC-LINKSPWITHCRED	CREDENTIAL Participant's IT-System
Register new CREDENTIAL Account	G-BUC-REGCREDACCOUNT	CREDENTIAL Participant's IT-System
De-Register From CREDENTIAL	G-BUC-DEREGISTERCREDENTIAL	CREDENTIAL Wallet
View Previous Logins to My Account	G-BUC-VIEWLOGINS	CREDENTIAL Wallet
Ban a User	G-BUC-BANUSER	CREDENTIAL Wallet
Register new device for accessing CREDENTIAL Wallet	G-BUC-REGNEWDEVICE	CREDENTIAL Participant's IT-System
Unlink device from CREDENTIAL Wallet	G-BUC-UNLNKDEVICE	CREDENTIAL Participant's IT-System

Table 7: Generic Account Management BUCs

3.2.1.5 Cryptography

This category contains all interactions inherently using cryptographic technologies such as proxy re-encryption or redactable signatures.

In particular, this category contains the following use cases:

Use Case Name	Unique ID	Main Actor
Generate new access-key for CREDENTIAL Wallet	G-BUC-GENACCESSKEY	CREDENTIAL Participant's IT-System
Generate new Recovery Key	G-BUC-GENRECKEY	CREDENTIAL Participant's IT-System
Proxy Re-Encryption	G-BUC-PROXYREENCRYPTION	CREDENTIAL Wallet
Remote Signature	G-BUC-REMOTESIGNATURE	CREDENTIAL Participant's IT-System
Selective Disclosure	G-BUC-SELECTIVEDISCLOSURE	CREDENTIAL Participant's IT-System

Table 8: Generic Cryptography BUCs

3.2.2 Generic Logical Use Cases

After the definition of the generic business use cases we are focusing now on the more detailed generic logical use cases (generic LUCs). While the business use cases describe the CREDENTIAL Wallet at a very high level the logical use cases break down each step in a business use case and describe in more detail the functional flow between components in the CREDENTIAL Wallet. Business use cases only use high level actors like the CREDENTIAL Wallet itself or a Service Provider. By breaking down the

functionality in logical use cases more fine granular actors are introduced with specific roles in- and outside of the CREDENTIAL Wallet.

The generic logical use cases are grouped into the following four categories:

- Data Management
- Authentication
- Authorization
- Account Management

Note that in contrast to the business use cases, we do not have a dedicated category "Cryptography" here. This is because the logical use cases are more detailed than the BUCs, and the different categories are more intertwined. Having a dedicated category for cryptographic steps here would split related LUCs into different categories. For instance, sending encrypted data would be part of "Data Management" (sending the data), and "Cryptography" (encrypting the data before), which would make it hard to navigate through the document.

Details on all generic logical use cases are given in Appendix 1A.2.

3.2.2.1 Data Management

The generic BUCs related to data management are made precise through the following 34 generic LUCs.

Use Case Name	Unique ID	Main Actor
Re-Encrypt Data	G-LUC-REENCDATA	CREDENTIAL Wallet
Verify Recovery Request	G-LUC-VERIFYRECOVERYREQUEST	CREDENTIAL Wallet
Read Recovery Private Key	G-LUC-READRECOVERYPRIVKEY	CREDENTIAL Participant's IT-System
Fill Registration Form	G-LUC-FILLREGFORM	Service Provider
Render Registration Form	G-LUC-RENDERREGFORM	Service Provider
Add additional attributes in Registration Form	G-LUC-ADDATTRIBUTSREGFORM	CREDENTIAL Participant
Submit Registration Form	G-LUC-SUBMITREGFORM	CREDENTIAL Participant's IT-System
Auditing	G-LUC-AUDITING	CREDENTIAL Wallet
Receive Data	G-LUC-RECDATA	CREDENTIAL Wallet
Decrypt Data	G-LUC-DECDATA	Service Provider
Encrypt Data using CREDENTIAL	G-LUC-ENCDATACREDENTIAL	CREDENTIAL Participant's IT-System
Send Encrypted Data	G-LUC-SENDENCDATA	CREDENTIAL Participant's IT-System
Register Data	G-LUC-REGDATA	CREDENTIAL Wallet
Define Request Parameters	G-LUC-DEFREQPARAMS	CREDENTIAL Participant's IT-System
Request Data	G-LUC-REQDATA	CREDENTIAL Participant's IT-System
Search Data	G-LUC-SEARCHDATA	CREDENTIAL Wallet
Request Signature	G-LUC-REQSIGN	CREDENTIAL Participant's IT-System
Create Signature Request	G-LUC-CREATESIGNREQ	External Signature Service
Provide Signature Request	G-LUC-PROVSIGNREQ	CREDENTIAL Participant's IT-System
Provide Data in Signature Request	G-LUC-PROVDATASIGNREQ	CREDENTIAL Wallet
Receive Signature Request	G-LUC-RECSIGNREQ	CREDENTIAL Wallet
Sign Document	G-LUC-SIGNDOC	External Signature Service
Receive Signed Document	G-LUC-RECSIGNDOC	External Signature Service
Recognize Externally triggered	G-LUC-RECEXTTRIGEVENT	CREDENTIAL Wallet

Use Case Name	Unique ID	Main Actor
Event		
Evaluate Notification Configuration	G-LUC-EVALNOTIFYCONF	CREDENTIAL Wallet
Create Notification List	G-LUC-CREATENOTIFYLIST	CREDENTIAL Wallet
Send Notification	G-LUC-SENDNOTIFY	CREDENTIAL Wallet
Process Notification	G-LUC-PROCNOTIFY	CREDENTIAL Wallet
Create Delete Data Request	G-LUC-CREATEDELDATAREQ	CREDENTIAL Participant's IT-System
Submit Delete Data Request	G-LUC-SUBMITDELDATAREQ	CREDENTIAL Participant's IT-System
Delete Data	G-LUC-DELDATA	CREDENTIAL Wallet
Encrypt Data	G-LUC-ENCDATA	CREDENTIAL Wallet
Request Re-Encryption Key	G-LUC-REQREK	CREDENTIAL Wallet
Process Exception	G-LUC-PROCEXC	CREDENTIAL Wallet

Table 9: Generic Data Management LUCs

3.2.2.2 Authentication

The generic BUCs related to authentication are covered by the following 25 generic LUCs.

Use Case Name	Unique ID	Main Actor
Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL- enabled IdP	G-LUC-AUTHSPUSINGWALLETENABLEDIDP	CREDENTIAL Participant
Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP	G-LUC-AUTHSPUSINGWALLETIDP	CREDENTIAL Participant
Authenticate towards CREDENTIAL Wallet using CREDENTIAL-enabled IdP	G-LUC-AUTHWALLETUSINGENABLEDIDP	CREDENTIAL Participant
Authenticate towards CREDENTIAL Wallet using an external IdP	G-LUC-AUTHWALLETUSINGEXTERNALIDP	CREDENTIAL Participant
Select CREDENTIAL Identity Provider	G-LUC-SELECTCREDIDP	CREDENTIAL Participant
Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation	G-LUC-AUTHSPUSINGWALLETANDIDENTITYFEDERATION	CREDENTIAL Participant
Attributes Collection	G-LUC-ATTCOLLECTION	Identity Provider
Request Identity Assertion	G-LUC-REQIDENTIYASSERTION	Service Provider
Re-Encrypt Attributes	G-LUC-ENCATTRIBUTES	Identity Provider
Issue Identity Assertion	G-LUC-ISSIDENTITYASSERTION	Identity Provider
Receive Identity Assertion	G-LUC-RECIDENTITYASSERTION	Service Provider
Decrypt Identity Assertion	G-LUC-DECIDENTITYASSERTION	Service Provider
Create Logout Request	G-LUC-CREATELOGOUTREQ	CREDENTIAL Participant's IT-System
Submit Logout Request	G-LUC-LOGOUTCREDWALLET	CREDENTIAL Participant's IT-System
Invalidate Session	G-LUC-INVSESSION	CREDENTIAL Wallet
Respond Successfully Logout	G-LUC-RESPSUCCLOGOUT	CREDENTIAL Wallet
User Authentication using IdP	G-LUC-XYZ	CREDENTIAL Participant
Ask for a List of IdPs	G-LUC-ASKIDPS	IdP Selector

Use Case Name	Unique ID	Main Actor
Ask to select an IdP from the provided List	G-LUC-ASKIDPFROMLIST	CREDENTIAL Participant
Select an IdP	G-LUC-SELECTIDP	CREDENTIAL Participant
IdP Selector Redirects User to the Selected IdP	G-LUC-REDIRECTUSER	IdP Selector
Select Attributes to Disclose	G-LUC-SELECTATTRDISCLOSE	CREDENTIAL Participant
Redact Identity Assertion	G-LUC-REDACTIDASSERTION	CREDENTIAL Redactor Service
Provide Identity Assertion	G-LUC-PROVIDASSERTION	CREDENTIAL Participant's IT-System
Verify Identity Assertion	G-LUC-VERIDASSERTION	Service Provider

Table 10: Generic Authentication LUCs

3.2.2.3 Authorization

The generic BUCs related to authorization are covered by the following 11 generic LUCs.

Use Case Name	Unique ID	Main Actor
Request Access Rights	G-LUC-REQACCESSRIGHTS	Service Provider
Register Access Rights Request	G-LUC-REGACCESSRIGHTSREQ	CREDENTIAL Authorization Service
Provide Access Rights Request	G-LUC-PROVACCESSRIGHTSREQ	CREDENTIAL Authorization Service
Define Access Rights	G-LUC-DEFINEACCESSRIGHTS	CREDENTIAL Participant's IT-System
Grant Access Rights	G-LUC-GRANTACCESSRIGHTS	CREDENTIAL Participant's IT-System
Provide Access Rights	G-LUC-PROVIDEACCESSRIGHTS	CREDENTIAL Participant's IT-System
Register Access Rights	G-LUC-REGACCESSRIGHTS	CREDENTIAL Authorization Service
Verify Re-Encryption Request	G-LUC-VERREENCREQ	CREDENTIAL Wallet
Request Access Rights List	G-LUC-REQACCRIGHTSLIST	CREDENTIAL Participant's IT-System
Receive Access Rights List	G-LUC-RECACCESSRIGHTSLIST	CREDENTIAL Participant's IT-System
Access Denied	G-LUC-ACCESSDENIED	CREDENTIAL Authorization Service

Table 11: Generic Authorization LUCs

3.2.2.4 Account Management

The generic BUCs related to authentication are covered by the following 35 generic LUCs.

Use Case Name	Unique ID	Main Actor
Register Link Account Request	G-LUC-REGLINKACCREQ	CREDENTIAL Wallet
Generate new Keypair	G-LUC-GENKEYPAIR	CREDENTIAL Participant's IT-System
Create Link Account Request using CREDENTIAL	G-LUC-LINKACCREQ	Service Provider
Redirect User to CREDENTIAL Authentication	G-LUC-REDIRECTUSERCREDAUTH	Service Provider
Provide Link Account Request	G-LUC-PROVLINKACCREQ	CREDENTIAL Participant's IT-System
Authorization	G-LUC-AUTHORIZATION	CREDENTIAL Wallet
Search User	G-LUC-SEARCHUSER	CREDENTIAL Wallet
Create De-Register CREDENTIAL account request	G-LUC-CREATEDEREGACCREQ	CREDENTIAL Participant's IT-System
Submit De-Register CREDENTIAL account request	G-LUC-SUBMITDEREGACCREQ	CREDENTIAL Participant's IT-System
De-Register Account	G-LUC-DEREGACC	CREDENTIAL Wallet

Use Case Name	Unique ID	Main Actor
Create new CREDENTIAL Account Request	G-LUC-CREATECREDACCREQ	CREDENTIAL Participant's IT-System
Submit new CREDENTIAL Account Request	G-LUC-SUBMITCREDACCREQ	CREDENTIAL Wallet
Create new CREDENTIAL Account	G-LUC-CREATECREDACC	CREDENTIAL Wallet
Create List Previous Logins Request	G-LUC-CREATELISTPREVLOGREQ	CREDENTIAL Participant's IT-System
Submit List Previous Logins Request	G-LUC-SUBMITLISTPREVLOGREQUEST	CREDENTIAL Wallet
Query List of Previous Logins for User	G-LUC-QRYLISTPREVLOGINS	CREDENTIAL Wallet
Return List of Previous Logins	G-LUC-RETLISTPREVLOGINS	CREDENTIAL Wallet
Create Ban a User Request	G-LUC-CREATEBANUSERREQ	CREDENTIAL Participant's IT-System
Submit Ban a User Request	G-LUC-SUBMITBANUSERREQ	CREDENTIAL Participant's IT-System
Ban User	G-LUC-BANUSER	CREDENTIAL Wallet
Submit Unban a User Request	G-LUC-SUBMITUNBANUSERREQ	CREDENTIAL Participant's IT-System
Unban User	G-LUC-UNBANUSER	CREDENTIAL Wallet
Create Export Data Request	G-LUC-CREATEEXPORTDATAREQ	CREDENTIAL Participant's IT-System
Submit Export Data Request	G-LUC-SUBEXPDATAREQ	CREDENTIAL Participant's IT-System
Return Exported Data	G-LUC-RETEXPDATA	CREDENTIAL Wallet
Create View All Accesses Request	G-LUC-CREATEVIEWACCESSESREQ	CREDENTIAL Participant's IT-System
Submit View All Accesses Request	G-LUC-SUBMITVIEWACCESSESREQ	CREDENTIAL Participant's IT-System
Search All Accesses	G-LUC-SEARCHACCESSES	CREDENTIAL Wallet
Return List of All Accesses	G-LUC-RETLISTALLACCESSES	CREDENTIAL Wallet
Associate new Keypair	G-LUC-ASSOCKEYPAIR	CREDENTIAL Wallet
Generate Update Re-Encryption Key	G-LUC-GENUPDREENCKEY	CREDENTIAL Participant's IT-System
Generate Re-Encryption Request	G-LUC-GENREENCREQ	CREDENTIAL Participant's IT-System
Data Registration Confirmed	G-LUC-DATAREGCONF	CREDENTIAL Wallet
Create Recovery Request	G-LUC-CREATERECREQ	CREDENTIAL Participant's IT-System
Submit Recovery Request	G-LUC-SUBMITRECOVREQ	CREDENTIAL Participant's IT-System
Export Private Key	G-LUC-EXPPRIVKEY	CREDENTIAL Participant's IT-System
Import Private Key	G-LUC-IMPPRIVKEY	CREDENTIAL Participant's IT-System

Table 12: Generic Account Management LUCs

4 Pilot domains: eGovernment, eHealth, eBusiness

This section explains how the three different pilots adopt the generic use cases. We start with a generic introduction and background information for each domain where state of the art technology and stakeholders are introduced. Every pilot explains how it can benefit by using CREDENTIAL technology and highlight how the CREDENTIAL Wallet could impact the current solutions. Afterwards each pilot defines storyboards and derives business use cases from them. Logical use cases associated to single business use cases will be described in D6.1.

4.1 eGovernment

eGovernment consists of the introduction of ICT technologies into Public administrations for providing services in a more innovative and usable way. The level of interaction depends on different involved actors. This could be between citizens and government, or between different public authorities, or between government and business/industrial world.

One of the main goal of eGovernment is to provide to the citizen a portfolio of improved public services from the point of view of accessibility, cost-effectiveness, efficiency, transparency and security. Many of these public services require the digital identity of the citizen to perform personal identification (authentication) and access rights assessment (authorisation). The citizen digital identity is the electronic representation of citizen's personal information.

In the context of CREDENTIAL Project the eGovernment use case takes place in Lombardy Region. Lombardy Region is a large Italian Region with over 10 million of citizens. Since 2007, all the Lombardy citizens are able to access to the eGoverment services using a digital identity, consisting of a Regional Authentication Card (CRS) and nowadays a National Authentication Card (CNS). The access is regulated by an identity provider named IdPC (Identity Provider of the Citizen).

Every year the Regional IdP (IdPC) provides about 8 millions of authentication for over 200 different Regional services.

The authentication is provided using the smartcard (the so called "CNS", National Card of Services) owned by each citizen living in Lombardy Region. Every CNS is associated to a PIN/PUK code. Since 2012 for some specific services (mainly eHealth environment) it is also available a One Time Password system, based on a multi-factor authentication scheme (username+password → something user knows; and SMS/OTP → something user has) to enhance the authentication service usability for end users and the security of the overall IAM service.

The IdPC "Identity Provider Cittadino" is a SAML 1.1/2.0 Identity Provider widely integrated in Lombardy Region and Italy. It is developed and hosted by LISPA. IdPC offers various types of authentication methods according to the level of security needed by the service requiring the authentication: CNS smartcard and PIN; username and password; username, password and OTP/SMS; OAUTH2 paradigm (Q3 2016).

Currently, at national level, there is a large project, called SPID (Public system of digital identity), aiming at federating identity and service providers. SPID is actually a national network, gathering identity and service providers, assuring they conform to a set of given rules and standards. The ultimate goal of the project is to give a "digital identity" to all Italian citizens. Every service provider has to decide the level of the authentication required to gain an access; SPID defines three different level of authentication: L1 (username and password), L2 (username, password and a third factor,

i.e. SMS/OTP), L3 (CNS smart card). Every domain will have its correct level, i.e. eHealth services will be typically accessible via L2 or L3 authentication factor. The SPID project confirms the great interest and competence of Italy in the digital identity.

4.1.1 Stakeholders

It is useful considering UCs stakeholders and their needs, with the goal of better fitting Identity Cloud Wallet, providing answers to their identified needs. Hence we identify the stakeholders of our pilot highlighting the interest they may have in the application of IAM innovative solutions.

To better understand where the different stakeholders of CREDENTIAL solutions are placed we stratify the environment in three levels as three concentric circles (see figure below): 1) the internal environment; 2) the near environment; 3) the far environment.

1. **Internal environment.** It is inside the organization's boundaries and it is made up of the resources available for doing business. It is common saying that the organization controls this environment and it should (even if it is not always that straightforward). In the case of CREDENTIAL, the organization is actually the consortium of several organizations providing solutions of security and privacy for services offered on the cloud.
2. **Near environment**. It is outside the organization's boundaries and includes customers, suppliers, business partners as well as competitors. This environment cannot be controlled by the organization; it should be influenced. A deeper analysis should allow the project team to have a good understanding of the actors playing on the near environment's stage.
3. **Far environment**. Far environment usually includes factors that cannot be neither controlled nor influenced, such as the ones usually referred to as STEEP factors (Social, Technological, Economic, Environmental, Political).

In the following table we list the stakeholders and their interests in the project results. Then we will fit those stakeholders into the appropriate "environment" categories.

The table shows the list of stakeholders and the interest they have on CREDENTIAL project. These stakeholders are labelled as actors if they have been identified as business actors – human and/or legal – (see later on in the business use cases description).

Stakeholder	Interest in project's results	Actor
Local Public Bodies	More secure Identity management for Local Public Bodies service. Local Public Bodies could enrich the citizen Credential Wallet with certified data. So the citizen could share certified data (attribute) in different services.	Y
Regional Governments	More secure Identity management for regional service.	Y
SW Developers	They may take advantage of increased workload deriving from the development of new cloud-based solutions fostered by improved security environments.	N
Law Enforcement Authorities	They may access evidences gathered and stored in secured cloud environments.	N

Stakeholder	Interest in project's results	Actor
Citizens	Improved privacy control. More services available thanks to improved security (easier to cope with Privacy regulations).	Y
Cloud Provider		N
Service Provider	Business opportunities coming from the diffusion of cloud solutions. For many SP could be an opportunity obtain directly sure and certified data.	Y
External Auditors	When certifying IT infrastructure, they need solutions that make their work easier.	N
Researchers	Easier access to anonymized data.	N
Internet Service Providers	Business opportunities coming from the diffusion of cloud solutions.	N
Private Companies	Competitors	N
Certification Authorities	Business opportunities coming from the diffusion of cloud solutions.	N

Table 13: eGovernment pilot stakeholders

In the following picture, the stakeholders identified in previous table, are classified into the respective environments.

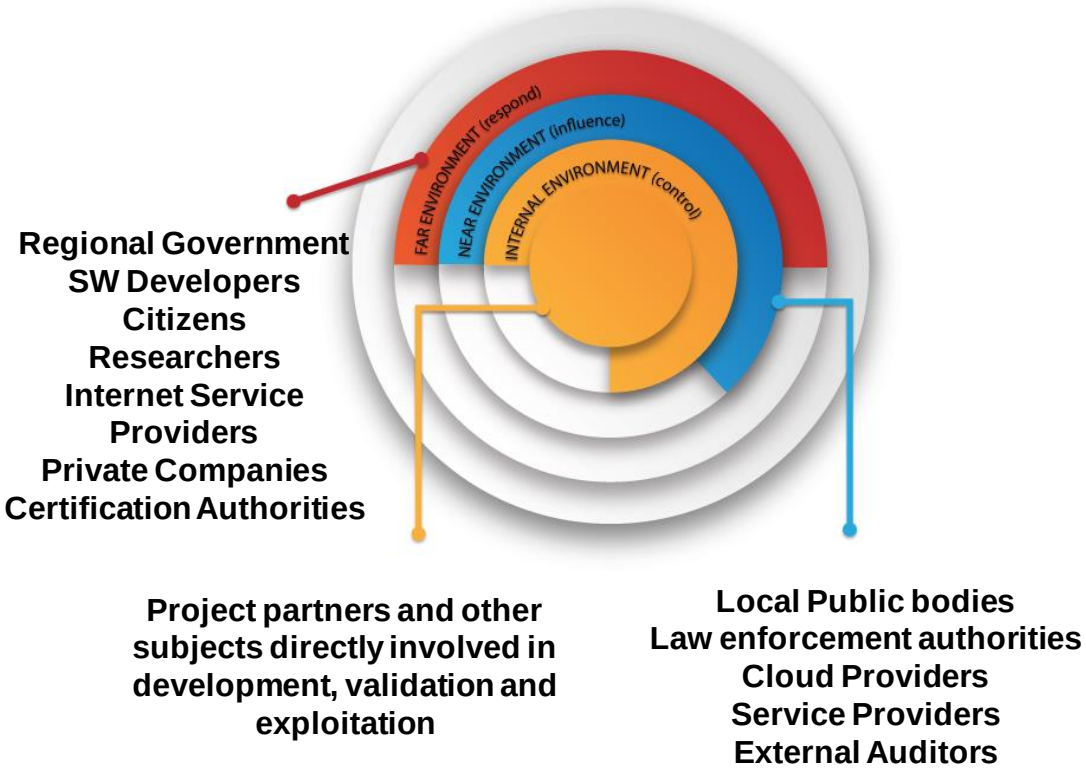


Figure 4: Environment Framework

4.1.2 State of Art

Authentication and authorisation are two different steps into the identification process: the first refers to the process of ascertaining that somebody is who he claims to be; the second refers to rules defining who is allowed to do what. The digital identity, within the eGovernment context, is provided and managed by a digital identity and access management framework (IAM).

In Lombardy Region the eGovernment digital identity and access management framework - as far as the CREDENTIAL use cases are concerned - is composed by:

- IdPC
- SIAGE (for a Lombardy Citizen or a Spanish Citizen living in Lombardy)
- Spanish eGovernment web site (for a Lombardy Citizen living in Spain)

Within the CREDENTIAL project a pilot will be carried out in a specific Lombardy Region environment based on the IdPC.

Two use cases are interacting with the SIAGE service and one with the Spanish eGovernment web site.

SIAGE service is based on the Lombardy Region IAM and it is accessible only through the component Lombardy IdPC to citizens who own the CNS smartcard.

In particular, the SIAGE service is based on the following requirements:

- Citizens should own Italian eID card
- Citizens access directly to services and authenticate when they enter the access phase
- Authentication is based on “chip&pin” paradigm
- The services delegate to the centralized regional service (Identity Provider Cittadini) the identification of the citizen
- Identity Provider uses standard SAML 1.1 & SAML 2.0

SIAGE service, as it is nowadays, is not accessible through other Identity providers and does not provide the opportunity to retrieve requested information which are not included into the Lombardy region IdPC assertions. In the near future an integration with SPID national system is foreseen.

The current version of SIAGE platform can be accessed in two ways. A first option requires the user’s CRS/CNS, hence involving strong authentication. Anyway, after the first authentication, the user receives ID and password allowing him to enter the service again without strong authentication; the final submission of tender documents requires the attachment of digitally signed documents. The reason for that is to enhance the system’s usability for users who need to enter the system several times as they are dealing with a tender. In the second option the authentication is carried out without strong authentication and in order to receive ID and password, a user has to send paper documents by mail.

For these reasons some scenario has been identified and pilot Uses Cases have been designed for the integration of CREDENTIAL Wallet into SIAGE service and IdPC. The integration of CREDENTIAL Wallet into IdPC is also foreseen for the application to the use case related to Spanish eGovernment web site.

The state of the art of Lombardy Region scenario is represented in the following picture where the access to SIAGE service provider is nowadays possible through the Lombardy Region Identity Provider (IdPC) or through the National IdP (SPID).

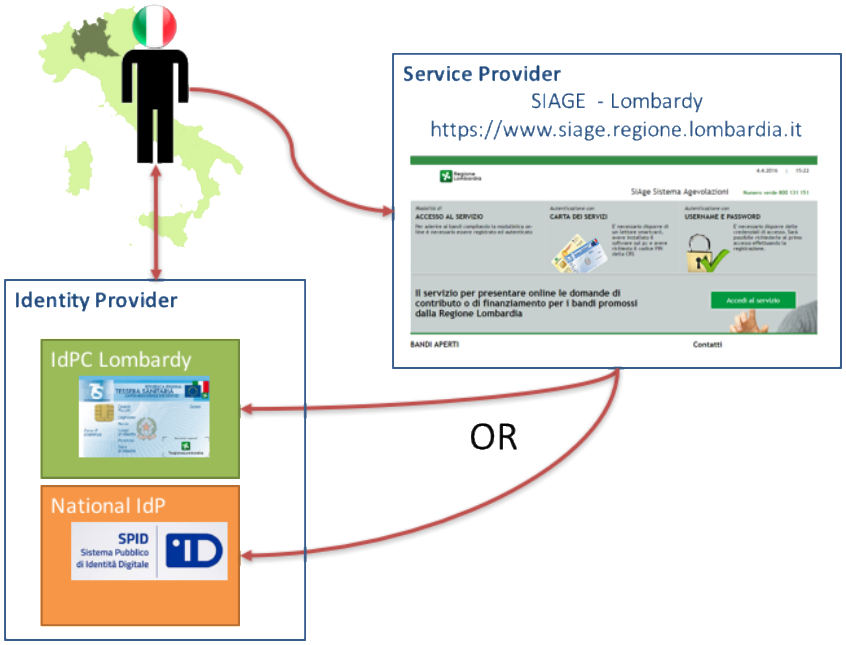


Figure 5: State of the art scenario in Lombardy Region

The above represented scenario can evolve into a more advanced system with added features of the CREDENTIAL Wallet. The access to different service providers (e.g. SIAGE in Lombardy region or a foreign service provider in other countries) is possible through the integration of existing Identity providers and the CREDENTIAL Wallet to Lombardy citizen and to foreigners.

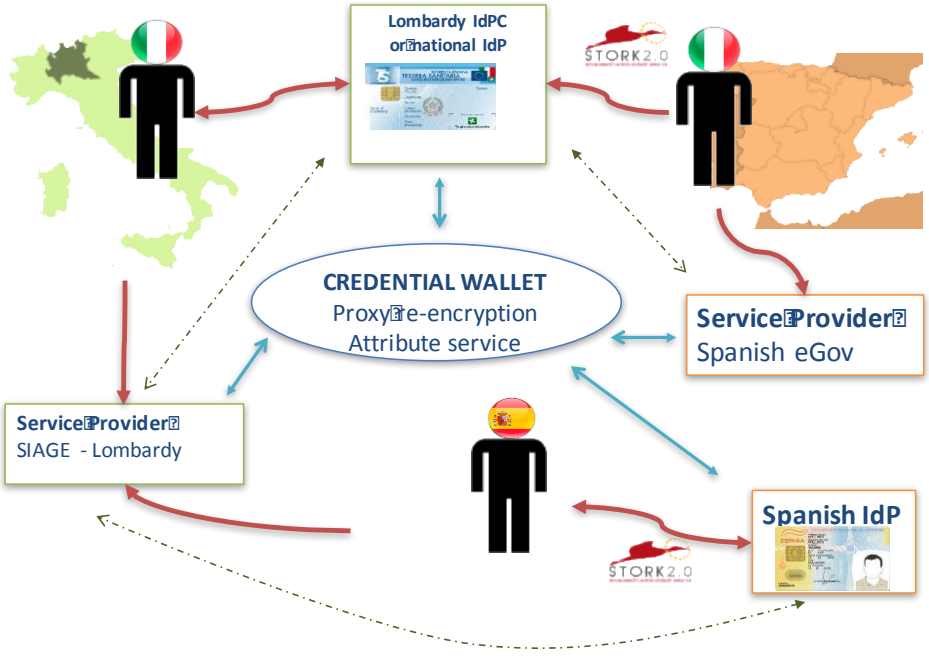


Figure 6: Lombardy Region scenario with CREDENTIAL added values

4.1.3 Value Proposition

The added value of introducing CREDENTIAL solution into the state of the art authentication process for accessing the SIAGE service provider in Lombardy Region is analyzed for each actor/stakeholder.

Actor / Stakeholder	Before	Benefit using CREDENTIAL
Citizen (Lombardy or foreigner)	The citizen's authentication can only happen through Lombardy IDPC The citizen has no control on his digital identity data (can't apply any disclosure) SP usage is possible with local IdP usage (i.e. Italian SP requires Italian IdP)	• The citizen can access using several IDPs • The citizen takes control of his digital identity (can also certify data) • The wallet provides that the data provided actually belongs to the citizen and are certified (either by the citizen himself or by the public provider) • Public administrations could provide the Wallet with further certified data • SP accessible with every IdP: the user data not released by IdP can be found in Wallet and used to enrich SAML assertion • Encryption level is improved thanks to proxy re-encryption and wallet
IdPC (Identity Provider)	Access through the Regional Identity Provider or the National Identity Provider using smartcard for authentication without the opportunity to retrieve or save other identity data	• Encryption level is improved thanks to the wallet
SIAGE (Service Provider)	SIAGE service, as it is nowadays, is not accessible through other Identity providers then the Lombardy IDPC. SIAGE does not provide the opportunity to retrieve requested information which are not included into the Lombardy region IdPC assertions.	• SIAGE platform allows authentication using several IDPs

Table 14: Value Proposition of eGovernment Pilot

4.1.4 Business Actors

eGovernment business actors are summarized in the following tree structure and detailed hereafter.

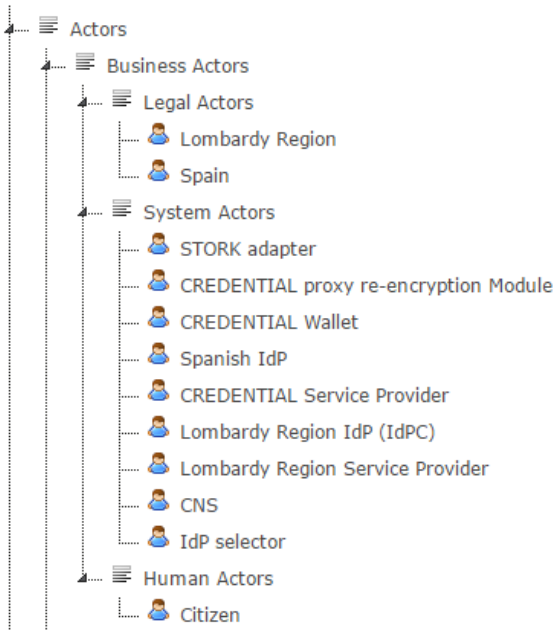


Figure 7: eGovernment business actors

4.1.4.1 Human Actors

Citizen - A natural person. An Italian citizen is anyone with a fiscal code[12]. The fiscal code is an alphanumeric unique id that identifies every citizen in Italy. Fiscal code is the key to access to almost every Italian service provider designed for a citizen access over the Internet. From the identity point of view, citizen could be a citizen or a public employee. If she/he is a public employee, the attribute is into the service and not directly linked (stored) into the digital identity. The citizen uses a set of "credentials" released by an Identity Provider in order to access a service provider. A Lombardy Region citizen is a citizen who lives in Lombardy Region for 6 months at least. A Lombardy Region citizen can have multiple identities in the CREDENTIAL network:

- a digital identity released by IdPC,
- a digital identity released by another Identity Provider (or Issuer of credentials) into the CREDENTIAL network.

The identities above can be used to access a Lombardy Region service provider or another service provider into the CREDENTIAL network.

4.1.4.2 System Actors

12

http://www.agenziaentrate.gov.it/wps/content/Nsilib/Nsi/Home/CosaDeviFare/Richiedere/Codice+fiscale+e+tessera+sanitaria/Richiesta+TS_CF/SchedaI/Informazioni+codificazione+pf/

STORK Adapter - The STORK adapter is the component responsible to manage browser redirection and protocol adjustments during the user authentication into a SP using a *foreign* IdP (i.e. login into a Spanish SP using an Italian IdP).

CREDENTIAL Proxy Re-Encryption - A collection of libraries, web services, browser plug-ins etc. which makes available a proxy re-encryption. Decrypt functions are also available.

CREDENTIAL Wallet - CREDENTIAL Wallet contains user specific data. All data is stored in an encrypted mode. Only a user's private key is able to decrypt this data. User data could be sensitive, personal, or generic. The Wallet offers web services to applications in order to store and retrieve user data. The Wallet also offers user interfaces to view and maintain data.

Spanish IdP - A Spanish CREDENTIAL Identity Provider is a SAML 2.0 Identity Provider developed and hosted by a CREDENTIAL partner different from LISPA. It releases authentication to a citizen (even a Lombardy Region citizen). Assertion can be enriched with data stored in CREDENTIAL Wallet. The CREDENTIAL Identity Provider could be an "issuer of credential" itself.

CREDENTIAL Service Provider - A CREDENTIAL Service Provider offers services to Citizens on the Internet. It is not a Lombardy Region Service Provider. A Lombardy Region Citizen should access to a CREDENTIAL Service Provider, gaining an authentication token from IdPC or another Identity Provider joining CREDENTIAL network. The SAML 2.0 assertion released by Identity Providers implies that the CREDENTIAL Service Provider is equipped with a component (i.e. Shibboleth) responsible for the assertion verification.

Lombardy Region IdP (IdPC) - IdPC is a SAML 1.1/2.0 Identity Provider developed and hosted in Lombardy Region. This Identity Provider is running since 2007 and has released about 8 million authentications in 2015. It is integrated by hundreds of service providers in Lombardy Region and Italy. IdPC can negotiate user authentication in several manners, mainly: smartcard+PIN, ans username/password/OTP-SMS. In the CREDENTIAL project, the proposed authentication paradigm involves smartcard+PIN.

Lombardy Region Service Provider - The Lombardy Region service providers typically make available services specifically targeted for Lombardy Region citizens. The Lombardy Region service provider chosen for CREDENTIAL project is named "SIAGE" ("SIstema AGEvolazioni"). SIAGE makes available contributions, tax breaks and subsidies to Lombardy Region citizens - and companies - facing economic difficulties.

CNS - CNS is an acronym which stands for Carta Nazionale dei Servizi. It is a dual-interface smartcard, available for almost all Italian citizens. It contains an X.509 digital certificate with the purpose to authenticate the user during online transactions.

IdP Selector - This component allows the citizen to choose her/his preferred IdP for that authentication session. A citizen could have several digital identities released by several IdP (or issuer of credential).

4.1.4.3 Legal Actors

Lombardy Region - Lombardy Region is one of the twenty Italian regions. Lombardy Region offers to its citizen several eGovernment and eHealth services over the internet.

Spain - Spain is one of the fifty European states. Like other countries, Spain offers to its citizen several kinds of services in the internet.

4.1.5 Storyboards

As represented hereafter, the eGovernment scenario in Lombardy region would involve different types of actors interacting with some of the CREDENTIAL Wallet components. Figure 8 helps to depict all the involved actors in the eGovernment scenario and all the interactions between actors and credential components. In the orange box there is the Spanish context, in the green box there is the Lombardy Region context, the blue boxes include all the CREDENTIAL related components. Actors are highlighted according to their category: system, human, legal. Human actors have the head with the associated color (orange for Spain and green for Lombardy region).

Our eGovernment pilot include three different storyboards which are detailed in the following paragraphs:

- A Lombardy citizen living in Lombardy asks for a contribution from Lombardy Region through the SIAGE service provider;
- A Lombardy citizen living in Spain pays some taxes on a Spanish eGovernment website;
- A Spanish citizen living in Lombardy asks for a contribution from Lombardy Region through the SIAGE service provider.

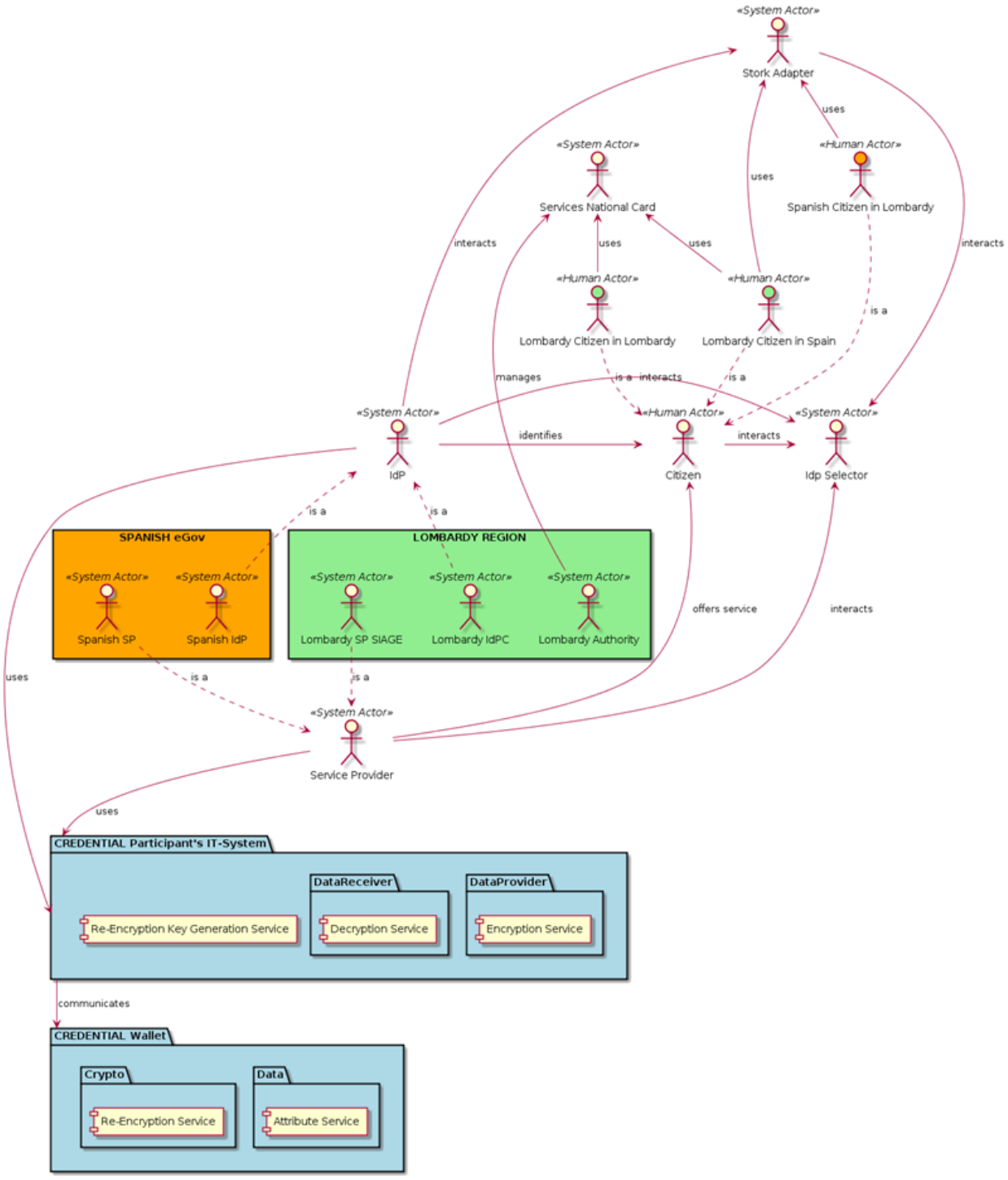
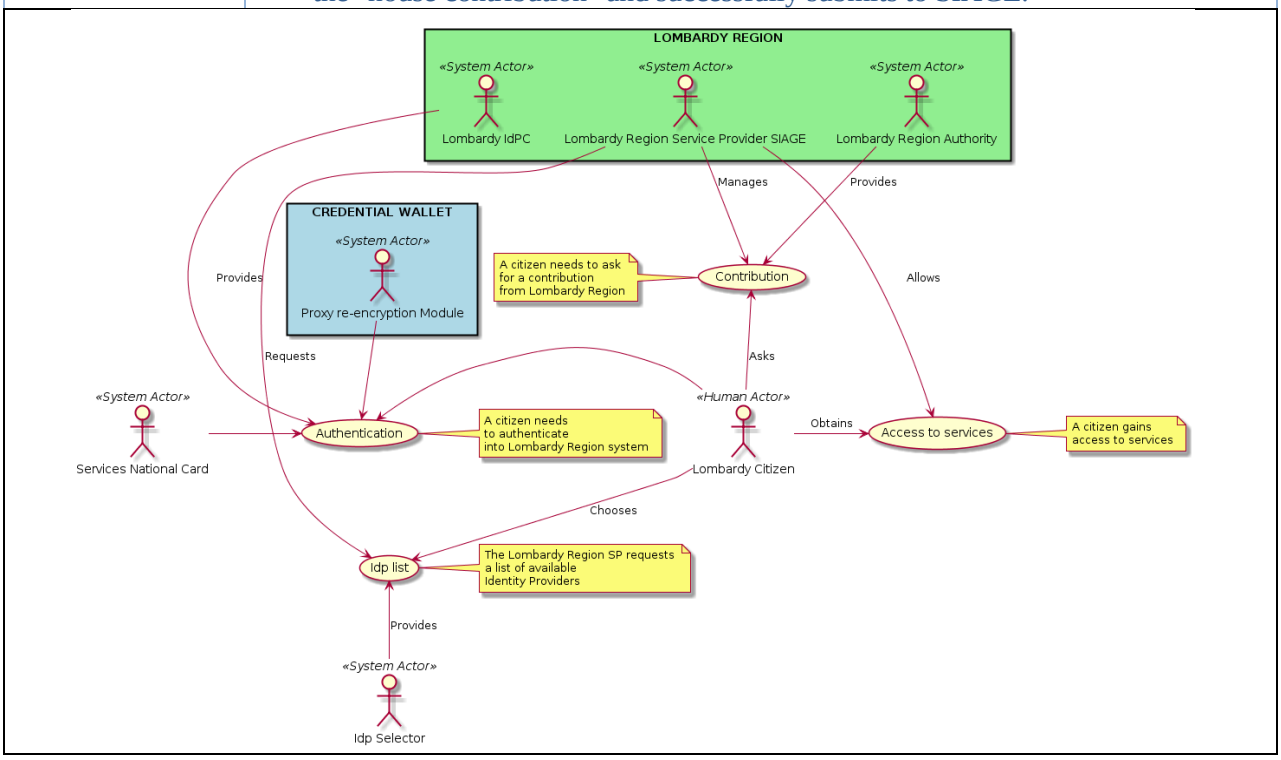


Figure 8: eGovernment actors and interactions

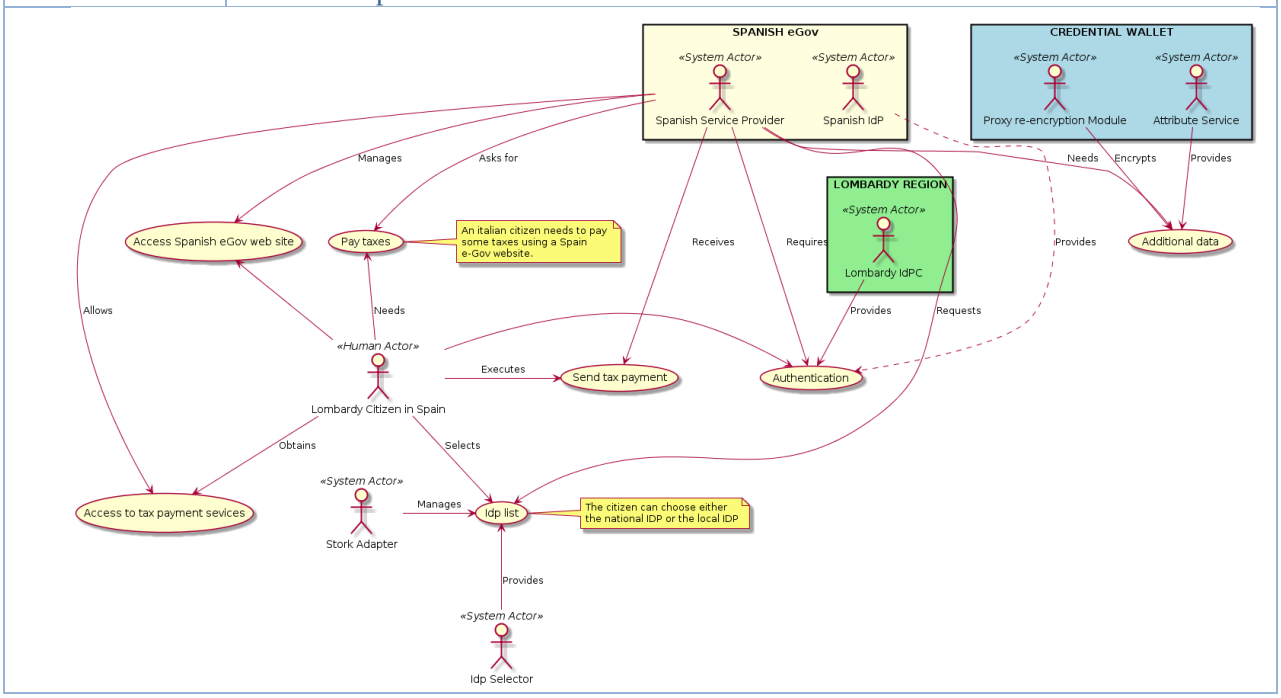
4.1.5.1 A Lombardy citizen asks for a contribution from Lombardy Region

Story Name	A Lombardy citizen asks for a contribution from Lombardy Region
ID	E-GOV-S-LOMBARDYCTZNASKCONTRIBUTION
Purpose	Authenticate a Lombardy citizen to a Lombardy Regional Service (SIAGE) using IdPC, the Lombardy Region Identity Provider.
Human Actor	Citizen
System Actors	1 Lombardy Region IdP (IdPC) 2 Lombardy Region Service Provider 3 IdP selector 4 Proxy re-encryption module of Credential wallet 5 CNS services national card
Legal Actors	Lombardy Region
Pre-conditions	Citizen has the capability to gain authentication from IdPC; in other words, citizen has a CNS smartcard, its PIN, and a smartcard reader.
Post-conditions	The citizen is authenticated to IdPC and can access to Lombardy Regional Service (SIAGE)
Scenario	Antonio, a Lombardy citizen who lives in Bergamo, has problem to pay the house rent. Antonio wants to ask a contribution from Lombardy Region. Lombardy Region makes available a web site for this kind of requests, named SIAGE. He wants to use his Lombardy Id - in other words, his CNS. Antonio tries to access to an SIAGE protected by authentication request; the system asks the user to choose from a list of IdP; Antonio selects IDPC. Antonio proceeds with the authentication and confirms the mandatory data for access to SIAGE (Name, Family Name and Italian Fiscal Code). Note that he could have selected optional data collected into the CREDENTIAL Wallet in order to transmit them too. Antonio obtains the authentication and now could fulfill the form for requesting the "house contribution" and successfully submits to SIAGE.



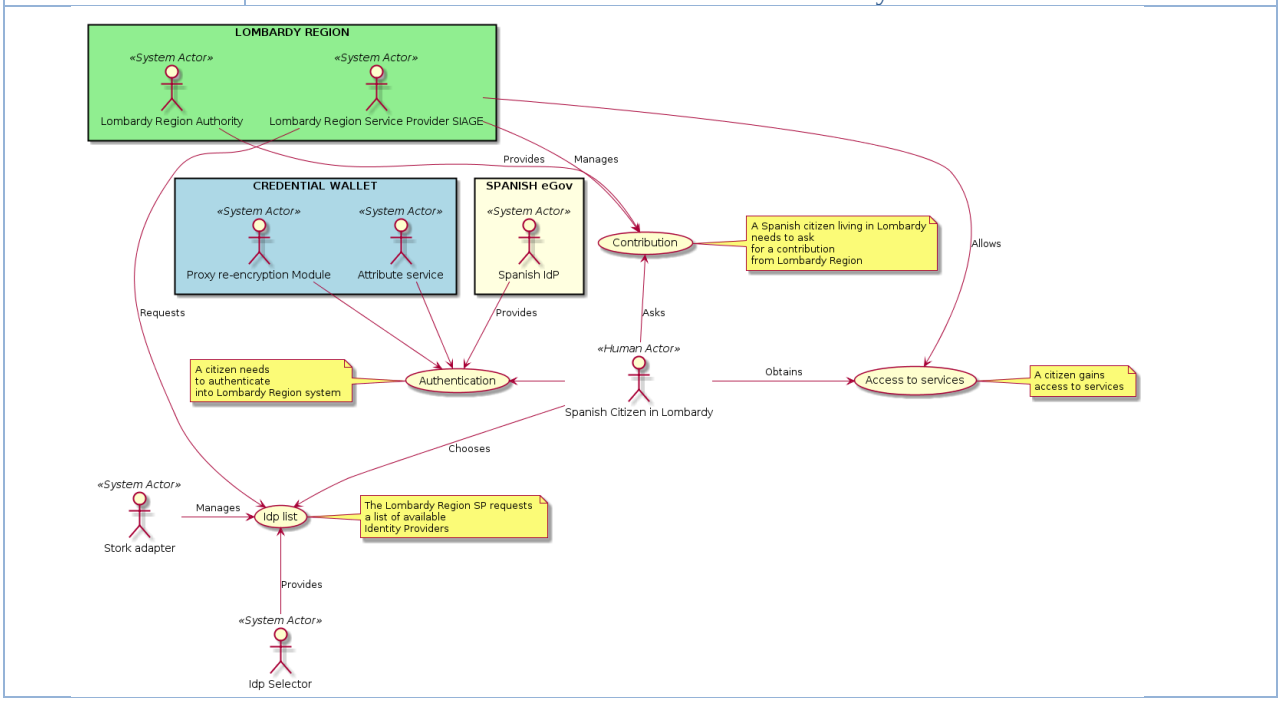
4.1.5.2 A Lombardy citizen pays some taxes on a Spanish eGovernment website

Story Name	A Lombardy citizen pays some taxes on a Spanish eGovernment website
ID	E-GOV-S- LOMBARDYCTZNPAYSTAXES
Purpose	Authenticate a Lombardy citizen to a CREDENTIAL Service Provider using IdPC.
Human Actor	Citizen
System Actors	1 CREDENTIAL Service Provider 2 Lombardy Region IdP (IdPC) 3 Spanish IdP 4 CREDENTIAL Wallet 5 STORK Adapter
Legal Actors	Spain
Pre-conditions	Citizen has the capability to gain an authentication from the IdPC (or from an external CREDENTIAL Identity Provider). Being a Lombardy citizen, it is highly likely that citizen would use Lombardy Id (his CNS).
Post-conditions	The citizen is authenticated to the CREDENTIAL Service Provider (Spanish eGovernment website).
Scenario	Danilo, a Lombardy citizen who works and lives in Madrid, needs to pay some local taxes on a Spanish website. In order to perform this operation, a strong authentication is required. Danilo chooses the taxes he has to pay and just before payment the website requires authentication. The user browser shows several authentication systems. Danilo chooses IdPC. The user insert his CNS into the smartcard reader and digits its PIN. IdPC performs authentication; according to CREDENTIAL paradigm, the user data into the assertion are crypted. The user also adds some optional data, stored in CREDENTIAL Wallet, to speed up the buying procedure (i.e. his complete address in Spain, and NIF - Numero de Identificacion Fiscal). All data is transferred to the website, then Danilo uses his credit card and the taxes are correctly paid. Danilo could have used a Spanish identity released by a Spain IdP to perform the same operation.



4.1.5.3 A Spanish citizen asks for a contribution from Lombardy Region

Story Name	A Spanish citizen asks for a contribution from Lombardy Region
ID	E-GOV-S- SPANCTZNASKCONTRIBUTION
Purpose	Authenticate a Spanish citizen to a Lombardy Regional Service using a Spanish ID and a Spanish IdP.
Human Actor	Citizen
System Actors	1 Lombardy Region Service Provider 2 Spanish IdP 3 CREDENTIAL Wallet 4 STORK Adapter
Legal Actors	Lombardy Region
Pre-conditions	1 The Wallet has to be enriched with the Italian Fiscal Code 2 Citizen has a Wallet account 3 Citizen has a Spanish IdP account
Post-conditions	Spanish citizen is correctly logged in Lombardy Region SP (SIAGE) using his Spanish Id
Scenario	Cristiano, a Spanish worker, is transferred in Italy a year ago. He becomes dad and he would like obtain a contribution by Lombardy Region for the child's school. He has a fiscal code in Italy because he is living in Rho. He wants to use his Spanish digital identity to access to SIAGE to submit the contribution request. He wants to use his Spanish Id because he is confident in his national identity system and he is used to access other Spanish SP with the Spanish IdP. Cristiano access to SIAGE; the system asks for an authentication; user selects "CREDENTIAL IdP" and then "Spanish IdP". Cristiano proceeds with the authentication and choose between the attribute available into his CREDENTIAL Wallet the mandatory data for access to SIAGE (Italian Fiscal Code). Cristiano obtains the authentication and now can fulfill the form for requesting the "child's school contribution" and successfully submits to SIAGE.



4.1.6 Business Use Cases

The three eGovernment storyboards are described specifically in 9 BUCs, which are formally defined in Appendix 1A.3.1. The following table provides an overview.

Use Case Name	Unique ID	Main Actor
Citizen asks for a contribution from Lombardy Region	E-GOV-BUC-ASKLOMBCONTRIB	Citizen
Citizen authenticates and access to SP	E-GOV-BUC-AUTHSP	Citizen
Citizen pays some taxes using a Spain eGovernment website	E-GOV-BUC-PAYTAX	Citizen
Citizen chooses taxes to pay and try to access to SP	E-GOV-BUC-ACCSP	Citizen
Citizen performs authentication	E-GOV-BUC-AUTHENT	Citizen
Citizen pays taxes on Spanish eGovernment website	E-GOV-BUC-COMPLETEPAYM	Citizen
Foreign citizen looks for a contribution from Lombardy Region	E-GOV-BUC-FOREIGNASKCONTRIB	Citizen
Citizen gains on-line authentication	E-GOV-BUC-FOREIGNAUTH	Citizen
Citizen completes online request to SIAGE	E-GOV-BUC-FOREIGNCOMPLCONTRIB	Citizen

Table 15: eGovernment specific BUCs

The following table now show which of the above BUCs are associated with which of the eGovernment story boards defined before.

	A Lombardy citizen asks for a contribution from Lombardy Region	A Lombardy citizen pays some taxes on a Spanish eGoverment website	A Spanish citizen asks for a contribution from Lombardy Region
Citizen asks for a contribution from Lombardy Region	✓		
Citizen authenticates and access to SP	✓		
Citizen pays some taxes using a Spain eGovernment website		✓	
Citizen chooses taxes to pay and try to access to SP		✓	
Citizen performs authentication		✓	
Citizen pays taxes on Spanish eGovernment website		✓	
Foreign citizen looks for a contribution from Lombardy Region			✓
Citizen gains on-line authentication			✓
Citizen completes online request to SIAGE			✓

Table 16: Relation of BUCs and story boards in the eGovernment pilot

4.2 eHealth

The increase of healthcare costs in nearly every country worldwide is closely linked to the increase in chronical diseases which e.g. in Germany make up 75% of the overall expenses in the statuary health insurance system[13]. Given the high potential for valuable effects and sustainability of solutions improving treatment and care in this domain, it was decided to focus the CREDENTIAL eHealth use case on treatment and monitoring of diabetes mellitus patients. As these patients receive treatment from many different specialist doctors a seamless exchange of medical data among these doctors is crucial for an efficient treatment and to prevent patients from complications and comorbidities.

4.2.1 Medical Background

The human body transforms ingested carbohydrate into glucose which is absorbed by body cells and then utilized by various parts of the body (esp. muscles). The hormone Insulin plays an important role in this glucose metabolism as it regulates blood sugar level and "unlocks" the cell walls for absorbing glucose.

Diabetes mellitus is a distortion of the glucose metabolism where glucose is not sufficiently absorbed due to missing insulin production (type-1) or due to modifications of the cell walls (type-2). Especially type-2 diabetes is a highly prevalent chronical disease (approx. 90% of the 7 million diabetes patients in Germany suffer from type-2).

Type-2 diabetes results when the body is unable to produce the amount of insulin it needs to convert food into energy or when it is unable to use insulin appropriately. Sometimes the body is actually producing more insulin than is needed by a person to keep blood glucose in a normal range. Yet blood glucose remains high, because the body's cells are resistant to the effects of insulin. Physicians and scientists believe that type-2 diabetes is caused by many factors, including insufficient insulin and insulin resistance. They increasingly believe that the relative contribution each factor makes toward causing diabetes varies from person to person.

While some people with type-2 diabetes can manage their diabetes with healthy eating and exercise, the doctor may need to also prescribe oral medications (pills) and/or insulin to help patients meeting their target blood glucose levels. Other drugs are on the horizon as well, as scientists work to improve the variety of medications to treat type-2 diabetes. Frequently physicians will prescribe one type of oral medication and discover it isn't really helping to control blood glucose that much. In the past, this would have meant that the patient would likely be put on insulin. Now, physicians can try another type of medication to see if it helps correct problems. Physicians often notice that a particular medication works well for a period of time and then begins to work less well for a patient. Now they can mix and match medications that work on different aspects of the diabetes problem to see if that will improve blood glucose control[14].

[13] Deutsche Bank Research (2010): Telemedizin verbessert Patientenversorgung. Online: https://www.dbresearch.de/MAIL/DBR_INTERNET_DE-PROD/PROD0000000000253251.pdf

[14] Joslin Diabetes Center (2016): Oral Diabetes Medications Summary Chart. Online: http://www.joslin.org/info/oral_diabetes_medications_summary_chart.html

Type-1 diabetes is an autoimmune disease, where the body - usually at a juvenile age - stops producing insulin. Therefore, type-1 patients are always treated with Insulin which they inject themselves.

4.2.2 Stakeholders

As a chronic disease, diabetes mellitus is subject to statutory managed care programs (e. g. Disease Management Programs, Integrated Care Contracts). These programs are agreed between governmental bodies, payer organizations and/or provider associations. They are implemented by the single health insurers which make respective contracts with single healthcare provider organizations and/or patients. Such programs usually follow evidence-based clinical guidelines which are provided through medical associations. Such guidelines not only provide guidance to doctors but even define specific pathways a treatment shall follow. On top of this, a managed care program regulates the flow of information between doctors, health insurance and patients, defines specific diagnostics a patient shall regularly receive, and determines quality indicators which doctors shall implement. Managed care programs usually consider the patient as an active partner who not only receives additional benefits (e. g. certain diagnosis and training courses being paid by the health insurance) but also has duties in cooperating with doctors and being compliant to his individual treatment plan.

For the CREDENTIAL eHealth use case, the considered stakeholders can directly be derived from the typical operational setting of a managed care program:

Stakeholder	**Interest in project's results**	**Actor**
Medical Associations	Define clinical guidelines based on evidence and good practice in diabetes treatment.	N
Governmental Bodies	Agree on managed care programs that define the operational and monetary framing for diabetes treatment.	N
Payer Organizations	Agree on managed care programs that define the operational and monetary framing for diabetes treatment.	N
Provider Associations	Agree on managed care programs that define the operational and monetary framing for diabetes treatment.	N
Statutory Health Insurance	Participate in the specific implementation of a managed care program. In the case of CREDENTIAL a fictive structured Diabetes Prevention Program based on the German S3 guidelines on Diabetes type-1[15] and type-2[16] therapy is considered.	Y

[15] http://www.awmf.org/leitlinien/detail/ll/057-013.html
[16] http://www.awmf.org/leitlinien/detail/ll/nvl-001g.html

Stakeholder	Interest in project's results	Actor
Healthcare Providers	Participate in the specific implementation of a managed care program. In the case of CREDENTIAL a fictive structured Diabetes Prevention Program based on the German S3 guidelines on Diabetes type-1 and type-2 therapy is considered.	Y
Patients	High risk for diabetes or already in an early stage of diabetes may subscribe to such a program.	Y

Table 17: eHealth pilot stakeholders list

4.2.3 State of Art

Diabetes Treatment

The CREDENTIAL eHealth use case will be designed to cover treatment for both type-1 and type-2 diabetes. Nevertheless, as the inclusion of children (which are a major group of type-1 diabetes patients) into the use case would impose the need to consider very specific and heterogeneous national legislation, a strong focus will be on type-2 patients.

A major cause for diabetes type-2 is hypertension even though the concrete developing of the disease is influenced by further factors (e.g. nutrition, genetic disposition). Diabetes type-2 therapy starts with means for changing the patient's lifestyle and escalates into medication regimes only if this does not lead to a normalization of the blood sugar level. This results in a multi-staged therapy which is standardized in respective guidelines published by responsible diabetes medical associations:

- Therapy stage 1 (base therapy): education, physical activity, non-smoking
- Therapy stage 2 (Pharmaka-Monotherapy): adding a single medication
- Therapy stage 3 (Insulin or combined medication): adding further medication
- Therapy stage 4 (intensive Insulin and medication): intensifying medication

The CREDENTIAL eHealth use cases will follow these recommendations and therapy stages while utilizing CREDENTIAL services for managing and sharing the various medical data that is collected from patients and created by physicians.

Diabetes Diary

Especially for patients who depend on insulin injections, the most important tool today is a diabetes diary where the patient records

- results of regular blood sugar measurements,
- carbohydrates consumed through meals,
- units of insulin injected.

While most patients still use a paper diabetes diary, mobile solutions are more and more being used due to their ability to automatically read data from glucometers which reduces the burden for the patient. Forthcoming solutions will even be able to read data from insulin pens[17]. For the CREDENTIAL eHealth use case we will not compete with such professional solutions, e. g. by implementing a diabetes diary in a secure cloud. Instead we will only record data which can be automatically provided by personal health devices (e. g. a glucometer or a scale). For the full diabetes diary we assume that the patient either records the required data on paper or uses a commercial mHealth App. Patients and doctors may transfer selected, aggregated data and diagrams from these Apps into the secure cloud that is used for the CREDENTIAL eHealth use case.

Legal Foundation

CREDENTIAL is well suited for the diabetes use case because it provides means for secure and privacy aware sharing of monitoring data through a cloud platform. By this it fulfils the regulatory constraints usually linked with the use of such platforms for health information exchanges; e.g.

- § 6(3) of the Austrian ELGA legislation[18] requests for state-of-the art data encryption whenever medical data is stored or processed in a cloud platform
- German legislation on professional disclosure requests for end-to-end encryption if data is transmitted through a cloud platform[19]

Actors and Flow of Information

The figure below sketches the actors and information flows as implemented with recent state-of-the-art diabetes treatment.

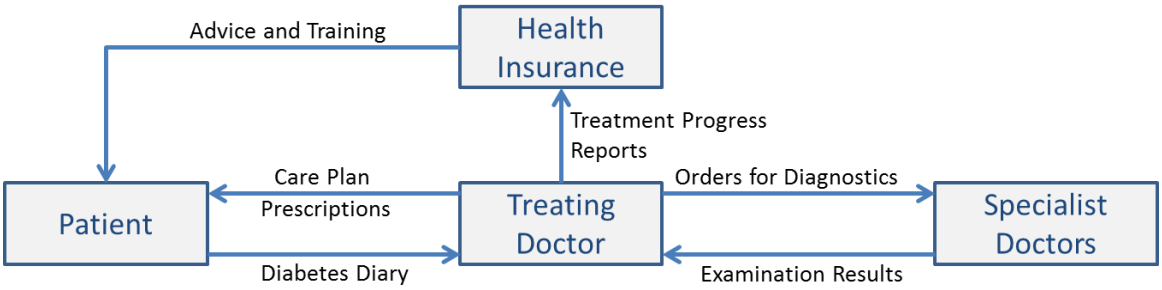


Figure 9: Actors and Flow of Information

[17] https://www.emperra.com/bluetooth-insulin-pen--der-prototyp.html

[18] http://www.elga.gv.at/fileadmin/user_upload/Dokumente_PDF_MP4/Recht/BGBLA_2012_I_111.pdf

[19] Kompetenzzentrum Trusted Cloud: Leitfaden - Vertragsgestaltung beim Cloud Computing. März 2014. Online: http://www.trusted-cloud.de/media/content/140317_Vertragsleitfaden_gesamt_RZ_Ansicht.pdf

As can be seen from the kind of information flowing between the actors, the whole care process is rather based on work sharing than on knowledge sharing; there is no piece of information which is share among all actors, every actor just gets to know the minimum of information he needs to perform a specialized task:

- Patients provide information to their treating doctor through their diabetes diary.
- Based on defined schedules, the treating doctor requests specific diagnostics from specialists who respond with their examination results.
- From all this information the treating doctor assembles a care plan for the patient and progress reports for the patient's health insurance.

In order to give an impression on the degree of IT-penetration in sharing this information, the following table summarizes which of the named documents are shared through which means in Germany. The recently most relevant means of data sharing is marked through a green shaded background.

Information Item	Transmission via Paper	Electronic Transmission
Diabetes Diary	Diary books are provided by all pharma companies as give-aways to doctors.	The market leading company MySugr has 500.000 downloads in the EU and the USA. This is ca. 1% of the diabetics in these regions.
Care Plan	Patients receive their care plans on paper. Due to missing dedicated forms in major hospital information systems, doctors usually even fill out paper forms.	-
Prescription	Doctors fill in prescription electronically and print them out in order to hand them over to the patient.	-
Orders	Doctors fill in orders electronically and print them out in order to hand them over to the patient.	Electronic orders only if the requested examination is performed within the same healthcare organization.
Examination Results	Forms and letters given to the patient on paper.	Electronic result transmission only if the requested examination is performed within the same healthcare organization.
Progress Reports	Paper forms available but rarely used.	All major IT-systems for doctors and hospitals provide electronic forms for assembling reports and sending them to the health insurance.
Training/Advice	Directed communication between health insurances and patients is solely on paper.	Generic web portals for specific disease groups.

Table 18: Overview of the German state of the art for sharing eHealth data

4.2.4 Value Proposition

The CREDENTIAL eHealth use case will implement a Personal Health Record (PHR) for sharing information among all actors who are involved in the patient's treatment. CREDENTIAL technologies

will be used to safeguard PHR data from unauthorized disclosure and to provide means to the patient to have full control over who may see which information.

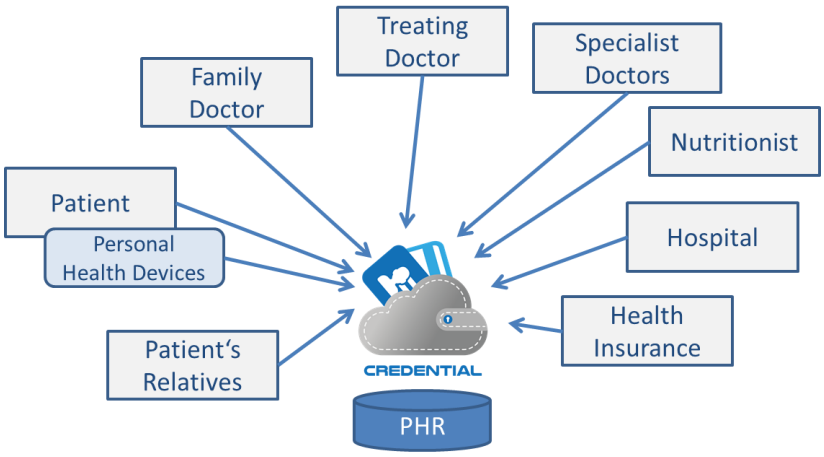


Figure 10: Information Sharing

By this we will push forward an information sharing paradigm instead of the very much reimbursement driven work sharing approach. This reflects joint responsibility for the patient's health and is a prerequisite for any form of managed care where payers do not contract single care providers but regional care networks. The implicit benefits that come with this information sharing paradigm are:

- All data is shared electronically by the means of a PHR. By this there are no media breaks along the information chain.
- Access to information is not determined by workflow constraints but by information needs.
- Further actors (e. g. patients' relatives, nutritionists and hospital emergency departments) can easily be integrated into the system and by this gain access to information as soon as they become part of the care team.

The table below breaks these general improvements down into concrete value propositions for the actors.

Actor / Stakeholder	Before	Benefit using CREDENTIAL
Patient	Has to go to the doctor in order to share his diabetes data	Sharing of diabetes data from anywhere at any time
	Relevant information often not available when needed most (e.g. emergency admission)	Information can easily be made accessible to any actor
Treating Doctor	Needs to actively request and collect relevant information	Available information can be seen at a glance. All actors can proactively provide new information.
	Same information needs to be re-assembled into different forms and documents for different actors	All actors may get access to the same set of documents.
Specialist Doctors	Forced to perform orders without having a full picture of the patient	Do not depend on other doctors with respect to the information they get
Health Insurance	Offers bonus programs for patient for patients.	Can receive progress information directly from patients in order to issue bonus program achievements.

Table 19:eHealth value proposition

4.2.5 Business Actors

4.2.5.1 Human Actors

Patient - The patient is the subject to services provided by one or more healthcare professionals. In the CREDENTIAL eHealth use case the patient is considered to suffer from diabetes and seeking help from health professionals to better cope with his disease and to prevent complications and comorbidities.

Health Professional – The term health professional (HP) denotes a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the country of treatment. Health professionals are allowed to process medical patient data according to the legislation of the country of the health professional's residence. For the CREDENTIAL eHealth use case different professions of health professionals are considered:

- **Family Doctor** - The family doctor is the patient's primary care provider who takes responsibility for overseeing the whole medical history of the patient. In addition, the family doctor assembles and maintains common care documents such as medication plans and emergency data.
- **Diabetologist** - The diabetologist is a specialist doctor for treating diabetes patients. In the CREDENTIAL eHealth use case the diabetologist oversees all diabetes-related treatment and care activities. He creates and controls the patient's care plan and acts as the main contact for both the patient and the health insurance within the legal framing of the structured diabetes program.
- **Nutritionist** - In the CREDENTIAL eHealth business scenario the nutritionist gives advice to the patient with respect to a healthy and balanced diet. He assembles and maintains the patient's diet plan and tracks the adherence of the patient with that plan.
- **Other Specialist Doctors** - Other specialist doctors get involved in the patient's diabetes treatment for performing regular prevention examinations and in cases of complications or comorbidities. Typical examples of specialists involved in diabetes treatment are ophthalmologists, cardiologists and nephrologists.

4.2.5.2 System Actors

Personal Heath Record (PHR) – The CREDENTIAL eHealth scenario utilizes a Personal Health Record (PHR) under the full control of the patient. The PHR is operated and hosted by a provider of the patient's choice. All respective contractual relationships are solely between the patient and his PHR provider. Health professionals may be authorized by the patient to read data from the PHR or to contribute data to the PHR. It is the responsibility of the patient as the owner of his PHR to assure that data is only disclosed from the PHR for the purposes it was originally collected and stored in the PHR.

Clinical IT Systems - Health Professionals interact with the patient's PHR through their clinical IT systems. In particular clinical IT systems (1) provide means for creating, editing and displaying medical documents, (2) provide all interfaces and workflows for sharing medical data though a PHR, (3) receive notifications about new data available from PHRs and (4) register alerts, validate alerts against new data and trigger defined activities. For CREDENTIAL two kinds of clinical IT systems are considered:

- **Practice Management Systems –** IT systems used by resident physicians for managing patient data and practice operations.
- **Hospital Information Systems** – IT systems used by hospitals which provide an electronic medical record (EMR), order-entry services and clinical workflow support services.

Personal Health Device - Personal Health Devices are devices which are used and operated by the patient. Using various kinds of sensors, personal health devices capture, process, visualize and/or transmit data about the patient's health, activity and/or lifestyle. Fort CREDENTIAL eHealth use case the following personal health devices will be considered:

- **Glucometer** – Personal health device for measuring a blood glucose level
- **Scale** - Personal health device for measuring a body weight
- **Blood Pressure Monitor** - Personal health device for measuring a blood pressure
- **Activity Tracker** - Personal health device for continuously measuring pulse, steps, skin resistance and other vital/activity data

Application Hosting Device - An application hosting device is a central point of control with the patient. It contains a number of client components that use the PAN, LAN, TAN and WAN interfaces to access one or more services on other devices to coordinate data collection, data analysis, data sharing and alerting. For CREDENTIAL the patient's **SmartPhone** will take the role of an Application Hosting Device.

4.2.5.3 Legal Actors

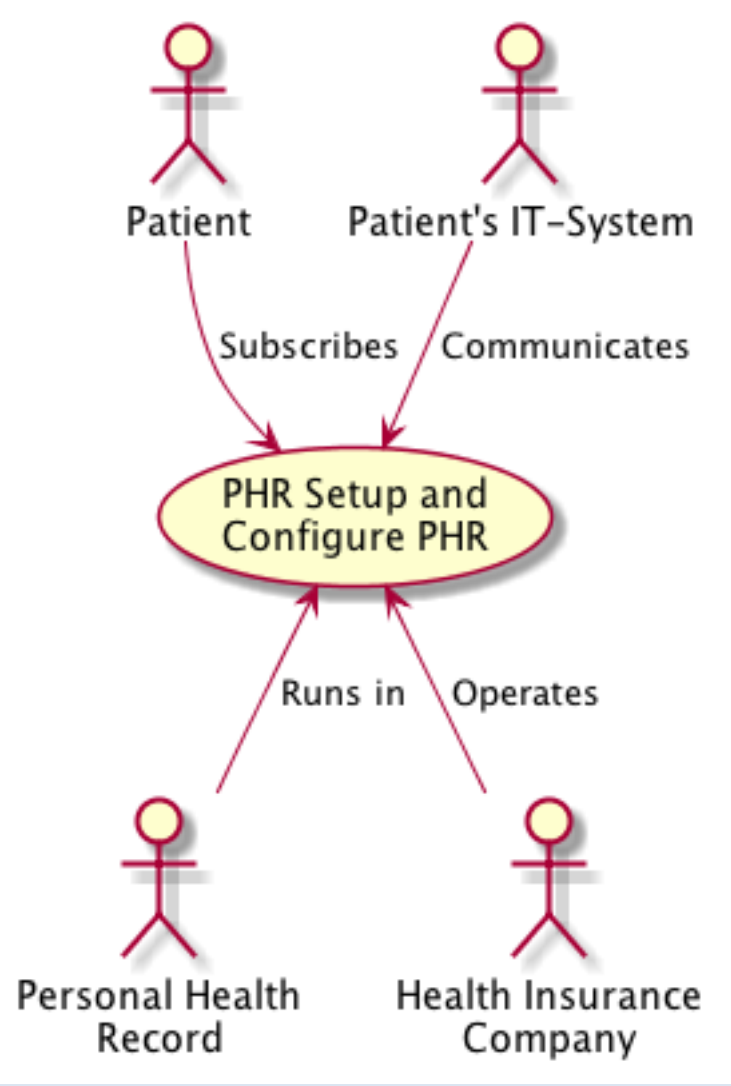
Healthcare Professional Organization of the Diabetologist – In the CREDENTIAL eHealth use case the HPO of the diabetologist contracts with the patient's health insurance company on the implementation of a disease management program about diabetes prevention and treatment. By this the HPO of the diabetologist takes responsibility for an efficient flow of information among all actors.

Health Insurance Company – The patient's health insurance company defines the framing conditions for the patient's treatment by setting up quality indicators and regulating the cooperation among the involved actors. In the CREDENTIAL eHealth use case the patient's health insurance company contracts with the HPO of the diabetologist on the implementation of a disease management program about diabetes prevention and treatment.

4.2.6 Storyboards

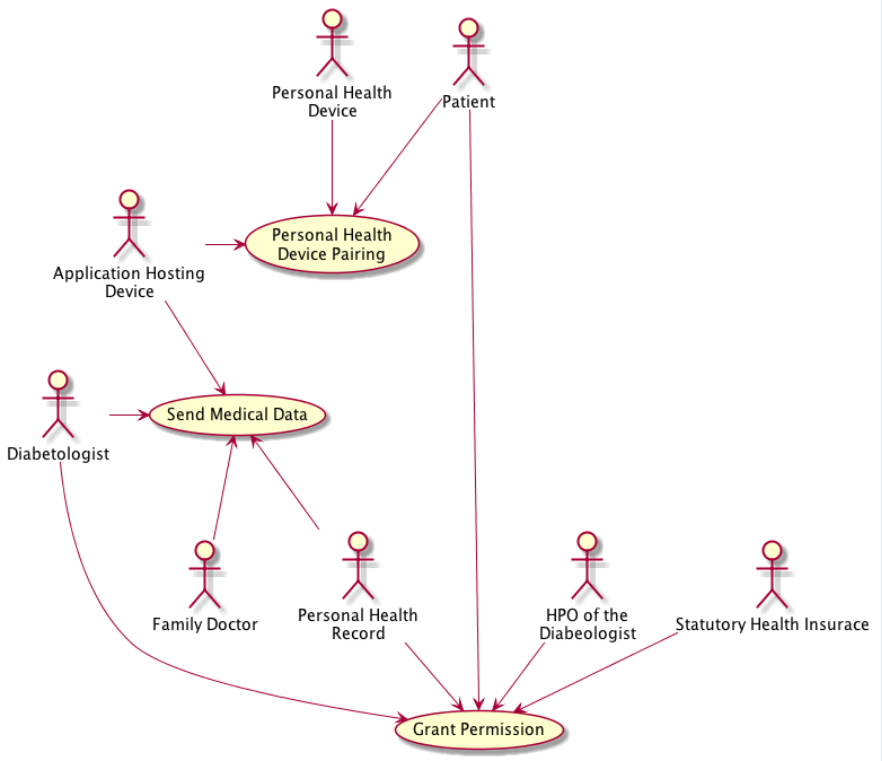
4.2.6.1 PHR Setup

Story Name	PHR Setup
ID	E-HEA-PHRSTUP
Purpose	The CREDENTIAL eHealth storyboard builds upon a Personal Health Record (PHR) as the primary means for sharing health data among the various actors. This story describes the setup of a PHR for a patient.
Human Actor	- Patient
System Actors	- Personal Health Record (for sharing data between patient and health professionals) - Application Hosting Devices (Smartphone for connecting to the PHR)
Legal Actors	-
Pre-conditions	The patient's statutory health insurance is operating a PHR platform. The insurer's customers may subscribe into using a private PHR instance for collecting and sharing their personal health data.
Post-conditions	A shared Personal Health record (PHR) has been set up for collecting and sharing medical data. The patient has signed the PHR provider's terms and conditions and is aware about how to use the various services the PHR platform offers. The patient's Smartphone is registered as a trusted device with the PHR.
Scenario	While prescribing an antibiotic, a doctor asks Alice if she has known resistance against certain types of antibiotics. Alice remembers that there was something written about this in a doctors letter she received after a stay in hospital 2 years ago but can neither remember what this was about nor where she may have deposited a copy of that letter. The doctor tells Alice that Alice's health insurance is offering a Personal Health Record to its customers where doctors' letters and other medical documents can be stored electronically in order to be available when needed. Back at home Alice visits her health insurer's home page in the WWW and fills in an online form for requesting her Personal Health Record (PHR). Two hours later she receives an e-Mail from the health insurance saying that her PHR has been instantiated any may be activated through her electronic health insurance card. Additionally, she may download a free PHR App from an App Store which allows for managing the PHR and its contained document through a mobile device. Allice installs the PHR App on her Smartphone and steps through the PHR activation procedure. After a few clicks she has activated and personalized her PHR and registered her Smartphone as a trusted device for granting permissions to doctors and exchanging documents between the PHR and the Smartphone.

Image	 Patient Patient's IT-System Subscribes Communicates PHR Setup and Configure PHR Runs in Operates Personal Health Record Health Insurance Company	

4.2.6.2 Care Planning and Progress Tracking

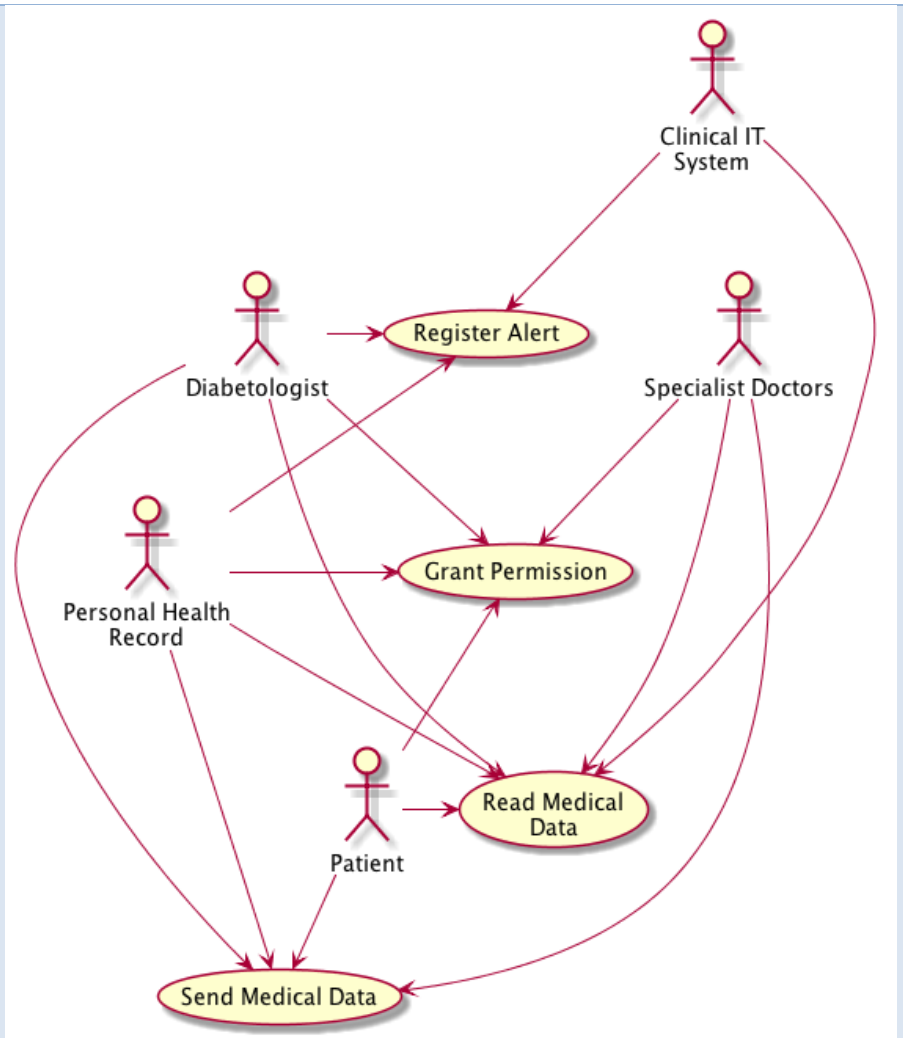
Story Name	Care Planning and Progress Tracking
ID	E-HEA-CAREPLANPROGTRAC
Purpose	This story covers the definition of therapy goals and continuous tracking of progress towards these goals. It is the baseline story for the CREDENTIAL eHealth proof-of-concept which covers the initialization of the covered care episode and continuously repeated activities.
Human Actor	- Patient - Diabetologist - Family Doctor (optional)
System Actors	- Personal Health Record (for sharing data between patient and health professionals) - Personal Health Devices (for monitoring blood sugar, body weight and blood pressure) - Application Hosting Devices (Smartphone for connecting to the PHR)
Legal Actors	- HPO of the Diabetologist (as DPP contractual partner) - Statutory Health Insurance (as DPP contractual partner)
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data in accordance with the patient's consent - The patient is equipped with a personal hub device (e.g. a SmartPhone) that forwards all data collected by the patient to the PHR and receives data from the PHR - All human actors are technically enabled to interact with the PHR through their existing IT systems (patient: SmartPhone; Diabetologist: clinical IT system) - All human actors have been advised and trained in interacting with the PHR
Post-conditions	The formal framing has been set up and all actors are enabled to share treatment relevant data securely via a PHR. Care goals have been defined and the diabetologist has all data available to continuously track the patient's progress in reaching the care goals.
Scenario	Alice is suffering from hypertension for several years and is showing symptoms of Diabetes type-2. For patients like Alice her health insurance company offers a dedicated Diabetes Prevention Program (DPP) where a diabetologist supports patients to change their lifestyle and to prevent follow-up diseases. This program is highly standardized and builds upon a PHR as a core tool for collecting and assessing treatment related data. While she is actively participating in the program, Alice receives all required devices for home monitoring from the diabetologist. At the first visit with the diabetologist, the diabetologist collects core vital data (height, weight, blood pressure, HbA1c, blood sugar) from Alice and informs her about her recent situation and further diseases which may show up in case that one will not be able to control her diabetes at a reasonable level. For this the Diabetologist defines as a care goal that Alice shall reduce her Body Mass Index from 34 kg/m2 to 25 kg/m2, shall stay with a HbA1c of 7.4 mmol/mol max, and request help from her family doctor to reduce her recent systolic blood pressure of 170 mmHg to 130 mmHg max. Alice signs a consent which grants permissions to the diabetologist and Alice's family doctor that allow them full access to her PHR. Through her smartphone she registers respective access rights to these doctors with her PHR. The diabetologist assembles several documents from the data gathered so far and uploads them to the PHR. Among these are: * (initial) health status summary

	* definition of care goals * documentation of the given consent The diabetologist hands over to Alice a glucometer and advices her how and when to measure her blood sugar level at home. In addition he gives her a digital scale and a blood pressure monitor which she shall use for measuring her weight and blood pressure every morning and evening. All devices have integrated Bluetooth connectivity for sending measured data to a SmartPhone. Together Alice and the Diabetologist install and configure the required _Apps_ on Alice's SmartPhone which not only allows Alice to see the measured data for her own in a patient friendly manner but even utilizes connectivity services of the SmartPhone for uploading the measured data to the PHR so that the Diabetologist has these immediately available when needed. The Diabetes Prevention Program foresees that Alice will visit her diabetologist every 3 months. At these visits he will measure the HBA1c blood sugar amount (long time blood sugar), as well as the LDL (Low Density Lipoprotein) and the creatinine which is an important indicator of renal health. The diabetologist will add these lab reports to Alice's PHR. Alice will be notified about this by receiving a message on her mobile phone.
Image	

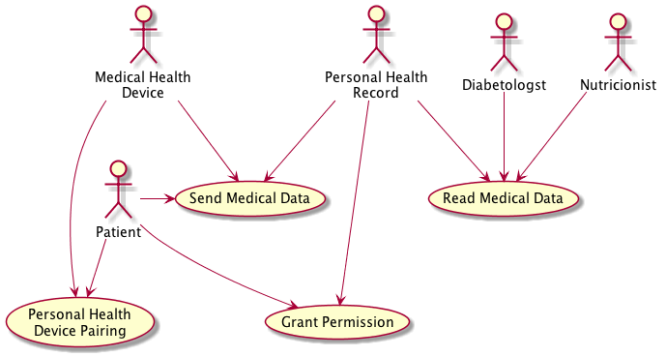
4.2.6.3 Therapy Monitoring and Screening for Complications

Story Name	Therapy Monitoring and Screening for Complications
ID	E-HEA-S-THERMONSCREENCOMPL
Purpose	This storyboard collects all processes the Diabetologist may perform on the patient's PHR for best monitoring the therapy and involving other actors into the treatment process.
Human Actor	- Patient - Diabetologist - Specialist Doctors (resident or at a hospital)
System Actors	- Personal Health Record (for sharing data among health professionals and with the patient) - Clinical IT System (for analyzing data and assembling reports)
Legal Actors	- HPO of the diabetologist (as DPP contractual partner) - Statuary health insurance company (as DPP contractual partner)
Pre-conditions	- The patient has given consent to sharing her medical data using an PHR and granted to her diabetologist and family doctor all required permissions - Care goals have been defined and the patient provides all data that is needed for tracking the progress towards these goals to her PHR
Post-conditions	- Thresholds have been defined and registered for supporting a fine grained monitoring of the patient's performance and compliance. - Relevant specialists use the PHR for sharing treatment related (diagnostic) data with the patient and her diabetologist. Required permissions are granted.
Scenario	The Diabetes Prevention Program requests the Diabetologist to assess Alice's daily measured data at least once per month and to provide feedback to Alice about any change in treatment or life style. To support the Diabetologist in this, daily and quarterly measured data and various statistics can be visualized and correlated in various ways through the Diabetologist's IT system. Selected annotated reports and diagrams may be stored in the PHR for better informing and involving Alice and her family doctor. In order to better catch critical situations the diabetologist may register thresholds on defined aggregated data within his clinical IT system. In case a threshold is met, an alarm notice is sent to the diabetologist. The diabetologist assesses the situation and decides on whether a modification of the care plan is required or if a phone call with the patient may be sufficient. In Alice's case the diabetologist registers thresholds for getting notified, if there is no decrease in body weight within the last 10 days and if Alice has not provided certain monitoring data for more than 3 days. The diabetologist takes responsibility for scheduling regular visists to other specialists. The Diabetes Prevention Program requests for such referrals for annual screening of eyes, feet and kidney by respective specialists. In advance to these visits the diabetologist assembles relevant data into a short report that is stored in the patient's PHR. The patient may grant a specialist access to this data by giving respective permissions. Again specialists may use the means of the PHR to transmit diagnostic reports back to the patient, her family doctor and her diabetologist. The same procedures apply in cases where the patient needs to be referred to hospital.

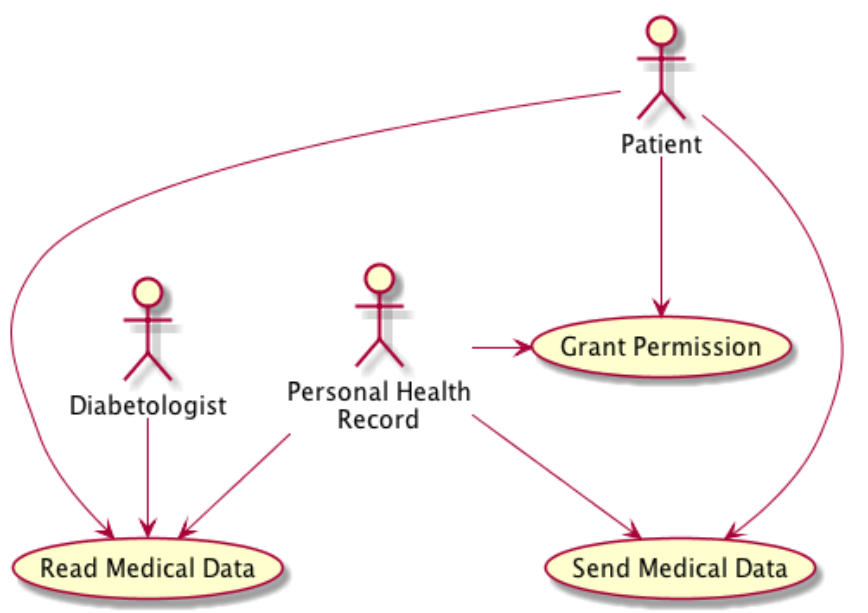
Image	


Clinical IT System
Register Alert
Diabetologist
Specialist Doctors
Grant Permission
Personal Health Record
Read Medical Data
Patient
Send Medical Data

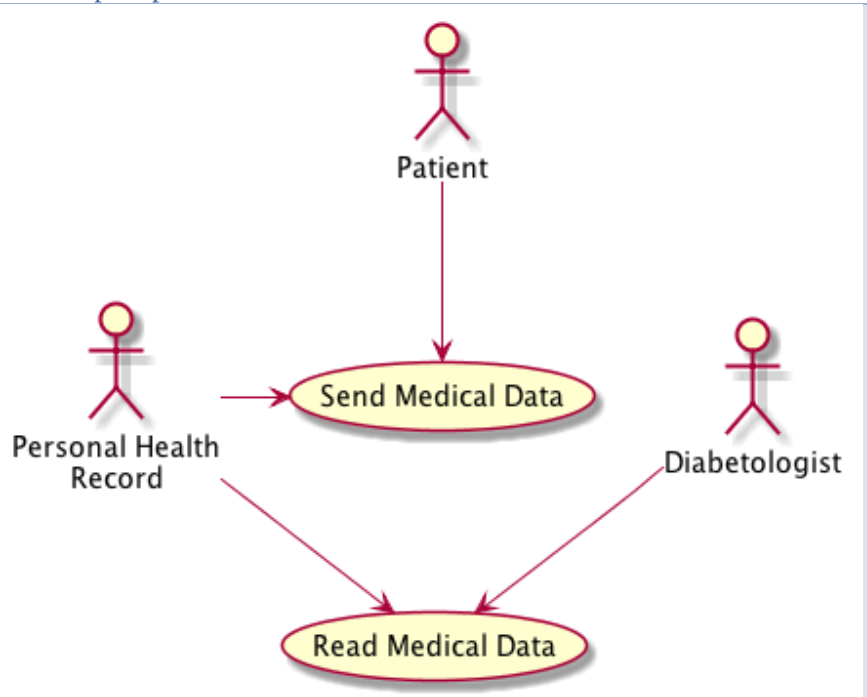
4.2.6.4 Nutrition and Activity

Story Name	Nutrition and Activity
ID	E-HEA-S-NUTRACTI
Purpose	This storyboard reflects the core processes of diabetes therapy stage 1 (Nutrition and Activity).
Human Actor	- Patient - Diabetologist - Nutritionist
System Actors	- Medical Health Devices - Personal Health Record
Legal Actors	- HPO of the diabetologist (as DPP contractual partner) - Statuary health insurance company (as DPP contractual partner)
Pre-conditions	- The patient has given consent to sharing her medical data using an PHR and granted to her diabetologist and other involved doctors all required permissions - Care goals have been defined and the patient provides all data that is needed for tracking the progress towards these goals to her PHR
Post-conditions	- Further vital data is monitored, stored and assessed. - A nutritionist is involved in the treatment and is granted all permissions for accessing nutrition and activity related data within the PHR.
Scenario	Even though Alice performed some slight changes in her lifestyle, her BMI is still at 34 kg/m2 after 4 weeks within the Diabetes Prevention Program. She requests for a visit with the diabetologist. The diabetologist is familiar with such cases and therefore brings his assistant who is a diet specialist to the meeting. During the meeting it becomes obvious the Alice has no idea about how much she moves a day and how much calories and fat certain of her common meals have. For increasing her awareness and allowing her for a better self-monitoring the diet specialist gives an activity belt to Alice which allows her to record the number of steps she takes a day. Like the other devices, the belt is linked with the SmartPhone and configured that initially only aggregated weekly data is disclosed to the diabetologist through the PHR. As an additional care goal Alice and the diabetologist agree that she will take 50.000 steps per week initially. For optimizing her diet, Alice agrees that she will record all food intake of the next week and provide the list to the diet specialist via the PHR. The diet specialist will assess her eating habits and give recommendation on how this can be optimized towards a more balanced diet. For better tracking this, the diet specialist recommends Alice to run a Nutrition App on her SmartPhone that supports her in counting calories. Alice agrees to disclose this information to the diabetologist. For better informing Alice on her performance and progress the newly gathered data on activity and nutrition will be correlated to the other monitoring data and an automatically rendered report will be placed in the PHR every week.
Image	

4.2.6.5 Oral Medication

Story Name	Oral Medication
ID	E-HEA-S-ORALMED
Purpose	This storyboard reflects the core processes of diabetes therapy stage 2 (Oral Medication).
Human Actor	- Patient - Diabetologist
System Actors	- Medical Health Devices - Personal Health Record
Legal Actors	- HPO of the diabetologist (as DPP contractual partner) - Statuary health insurance company (as DPP contractual partner)
Pre-conditions	- The patient has given consent to sharing her medical data using an PHR and granted to her diabetologist and other involved doctors all required permissions - Care goals have been defined and the patient provides all data that is needed for tracking the progress towards these goals to her PHR
Post-conditions	- A medication plan is assembled and shared through the PHR.
Scenario	Even though Alice's BMI is getting lower, her HbA1C is still above 8 and consequently her daily blood sugar is rarely below 130. In order to complement the ongoing changes in lifestyle and nutrition, the diabetologist prescribes Metformin to Alice. Because Alice is also taking other pills prescribed by her family doctor and other specialists, the diabetologist recommends her to ask her family doctor for a medication plan that not only lists all required medication but even gives advice on how and when to take the different pills. The medication plan will be stored electronically in the PHR and as such is accessible to all doctors who are involved in Alice's diabetes treatment.
Image	

4.2.6.6 Insulin Therapy

Story Name	Insulin Therapy
ID	E-HEA-S-INSTHERPY
Purpose	This storyboard reflects the core processes of diabetes therapy stage 3 (Insulin Therapy).
Human Actor	- Patient - Diabetologist
System Actors	- Personal Health Record
Legal Actors	- HPO of the diabetologist (as DPP contractual partner) - Statuary health insurance company (as DPP contractual partner)
Pre-conditions	- The patient has given consent to sharing her medical data using an PHR and granted to her diabetologist and other involved doctors all required permissions - Care goals have been defined and the patient provides all data that is needed for tracking the progress towards these goals to her PHR
Post-conditions	- All plans are updated to reflect the changes that come with intensivation of the therapy.
Scenario	During the last months Alice suffered from two hyperglycemia which leads her diabetologist to the decision that she needs to inject insulin for stabilizing her blood sugar level. His assistant gives Alice advice and training in how to inject insulin at home. The diabetologist assembles a care plan that shows when she needs to inject how many units of insulin. Additionally - the medication plan is updated to include the insulin that is prescribed to Alice, - the frequency of blood sugar measurements is adapted so that Alice now needs to measure her blood sugar 30 minutes before every meal, 2 hours after every meal and 1 hour before going to bed. The adapted plans are stored in the PHR.
Image	

4.2.7 Business Use Cases

The six eHealth storyboards are described specifically in 8 BUCs, which are formally defined in the Appendix. The following table provides an overview:

Use Case Name	Unique ID	Main Actor
Setup and Configure PHR	E-HEA-BUC-SETUPCONFPHR	Personal Health Record (PHR)
Grant Permission	E-HEA-BUC-GRANDPERM	Personal Health Record (PHR)
Revoke Permission	E-HEA-BUC-REVOKEPERM	Personal Health Record (PHR)
Send (Medical) Data	E-HEA-BUC-SENDMEDDATA	Personal Health Record (PHR)
Read (Medical) Data	E-HEA-BUC-READMEDDATA	Personal Health Record (PHR)
Personal Health Device Pairing	E-HEA-BUC-PERSHEALTHDEVPAIR	Patient's IT-System
Register Alert	E-HEA-BUC-REGALERT	Clinical IT System
View Permissions	E-HEA-BUC-VIEWPERM	Personal Health Record (PHR)

Table 20: eHealth specific BUCs

Note here that, in order to reduce the number of domain specific BUCs, "Register Alert" also covers the deletion or modification of existing alerts. This is made explicit in the formal specification of the BUC in Appendix 1A.3.2.

The following table now show which of the above BUCs are associated with which of the eHealth story boards defined before:

	PHR Setup	Care Planning and Progress Tracking	Therapy Monitoring and Screening for Complications	Nutrition and Activity	Oral Medication	Insulin Therapy
Setup and Configure PHR	✓					
Grant Permission		✓	✓	✓	✓	
Revoke Permission		■	■	■	■	
Send (Medical) Data		✓	✓	✓	✓	✓
Read (Medical) Data			✓	✓	✓	✓
Personal Health Device Pairing		✓		✓		
Register Alert			✓			
View Permissions		■	■	■	■	

Table 21: Relation of BUCs and story boards in the eHealth pilot

We note that two of the BUCs, namely "Revoke Permission" and "View Permissions" are not covered by any of the story boards. This is because of our top-down approach, where we first started defining the story boards, reflecting typical goals a user wants to achieve when using our system. The uncovered BUCs were then inferred by considering less frequent yet inherently needed interactions. For instance, changing one's diabetologist and thus revoking the access rights of the previous doctor is not a very frequent action, and therefore it is not covered in the story boards. However, it is obvious that such a step needs to be supported by the system. BUCs that are not directly covered by a story board but might still be relevant in their context are indicated with grey boxes.

4.3 eBusiness

In eBusiness environment, there are different opportunities given by CREDENTIAL technologies to make user authentication safer and easier, service subscription faster and data sharing really secure. In fact, the aim of eBusiness pilot is to demonstrate how users can leverage on CREDENTIAL Wallet and which is the value added. To achieve this goal, we focused on setting and evaluating different use cases in which CREDENTIAL is used "as a service" or integrating specific components (e.g. re-encryption libraries).

Use CREDENTIAL for Identity federation

Users access a lot of websites and online services every day: for each one of these they have to login into the website, often with username and password, sometimes, for some service such as bank account, with username, password and an OTP (one-time-password). This means that users must remember dozens of passwords. For this reason, many websites and applications allow the registration with existing users' social media account (e.g. Facebook). But this could not be the solution for such online services that deal with "certified" account, based on a contract and user recognition. In this Scenario CREDENTIAL would be the perfect tool to realize a "trusted Identity Federation".

Use CREDENTIAL for empower trust in legal communication

Thanks to the technology of proxy re-encryption, within CREDENTIAL project will be possible to test the sharing of information and data with other users in a trusted way. In eBusiness Pilot, InfoCert Registered e-mail service, Legalmail, could be the application in which integrate the re-encryption technology to demonstrate how more security in sharing legal communications do not affect usability and allow confidentiality within users.

Use CREDENTIAL as a Digital Wallet to import data

Part of CREDENTIAL project consist in develop a digital secure wallet in which users can store their personal information and sensitive data with the assurance of a high level of privacy guaranteed but with also the flexibility to securely share those data. Saving his data within the wallet, User has the opportunity to use CREDENTIAL service to fulfill forms online and subscribe contracts wherever he is, with all information needed available at any time.

Use CREDENTIAL to store Digital Signature PIN to protect and simplify signature experience

Digital Signature is becoming one of the most important key-points in the digitalization era for the impact it might have in allowing the transactions' dematerialization. Thanks to digital signature, users and organizations can digitally sign documents with the legal evidence of integrity and authenticity of transaction. To use a digital signature certificate based on PKI (*Public Key Infrastructure*) system, user must authenticate himself entering his PIN and confirm the transaction. Thanks to CREDENTIAL he could store this sensitive information within the wallet and authenticate himself with credential to disclose the PIN at the moment of transaction.

Use CREDENTIAL to store and share private data

CREDENTIAL project provides a high level of privacy guaranteed on the user's sensitive data and a secure way to share with other CREDENTIAL users. Several business use cases exploit the

CREDENTIAL technology of proxy re-encryption to share user private information in a trusted way. In eBusiness Pilot, CREDENTIAL users could be able to afford access to private data integrate the re-encryption technology in secure communications.

4.3.1 Stakeholders

Although in the eBusiness IAM domain there could be involved potentially everyone, in a service provider – service user (customer) relationship, the eBusiness domain focuses in the B2B and B2C relationships and service offerings. With that in mind there are some distinct roles identified according to their perspective and impact on the management, operation and use of an IAM system.

- Process owners (or Business owners) are responsible for interacting with corporate systems or applications in order to manage identities from a functional and procedural perspective. These individuals often do not interact with the systems or applications from a technical operations perspective, but are rather end users from a business process perspective.
- System/Application owners are responsible for maintaining various systems or applications from a technical perspective. These individuals may leverage an application-specific administrative interface in order to maintain user accounts.
- Data owners are responsible for managing identity data within a given environment - major identity data repositories. They are usually database administrators and directory administrators with an in-depth understanding of the size and flow of data in the infrastructure. Data owners should be knowledgeable of any online or offline synchronization activities that occur between repositories, as well as data transfer methods that are employed.
- An executive sponsor is an individual (or set of individuals) who has the authority to make relevant decisions and changes regarding existing processes that manage identity data in the organization.
- End users, who are the ones who are using the system, to get the service they need or want.

The above categorization does not exclude stakeholders to have more than one role, often depending on the size of an organization. Where, the larger the organization the higher the possibility that a stakeholder may have a distinct role, while in smaller organizations a stakeholder is likely to have more than one role. Finally, in the case of end users, when being the customers, they may probably be the data owners as well.

4.3.2 State of Art

In the current state, with respect to all the services mentioned above, the user communicates directly with the systems within the InfoCert domain, which in this case does not offer the opportunity to simplify their experience leveraging on other authentication system or cloud wallet to share information already stored in digital form, ext.

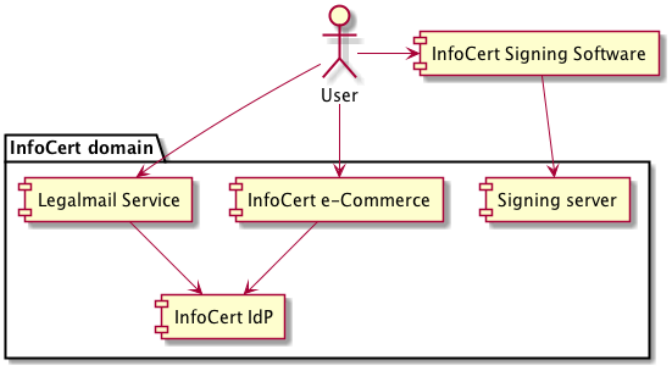


Figure 11: InfoCert State of the Art

Looking in detail the single use cases, the following functional diagrams are showing the actual user experience.

Legalmail login

In the first scenario, User is a legalmail active customer, so he possesses a personal account with which simply log in every time he needs to access in his personal mailbox.

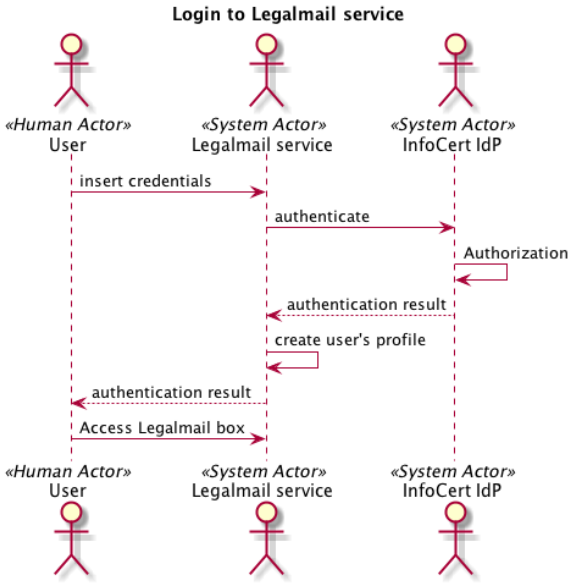


Figure 12: Login to Legalmail

E-Commerce subscription

Today, an e-commerce client has to fulfill a web-form to complete his subscription, sign the contract and send it back to InfoCert. All these operations are now completed manually for each service he wants to activate.

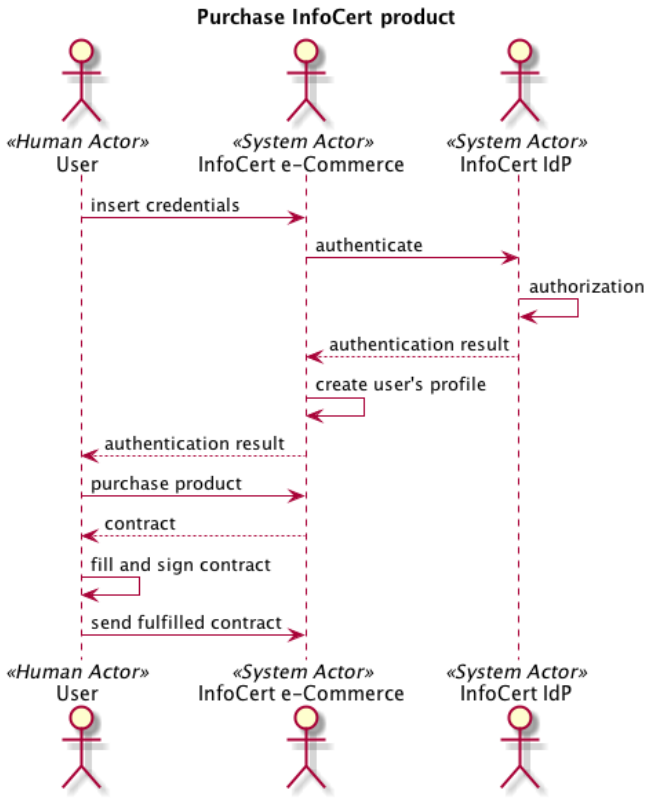


Figure 13: Purchase a InfoCert product

Digital Signature experience.

A user who possesses an InfoCert Digital Signature Certificate, today must remember different credentials:

- User id of remote signature account
- Password of remote signature account
- PIN of signature, that is used every time he wants to digitally subscribe a document
- OTP via SMS or App, to confirm his identity in signing

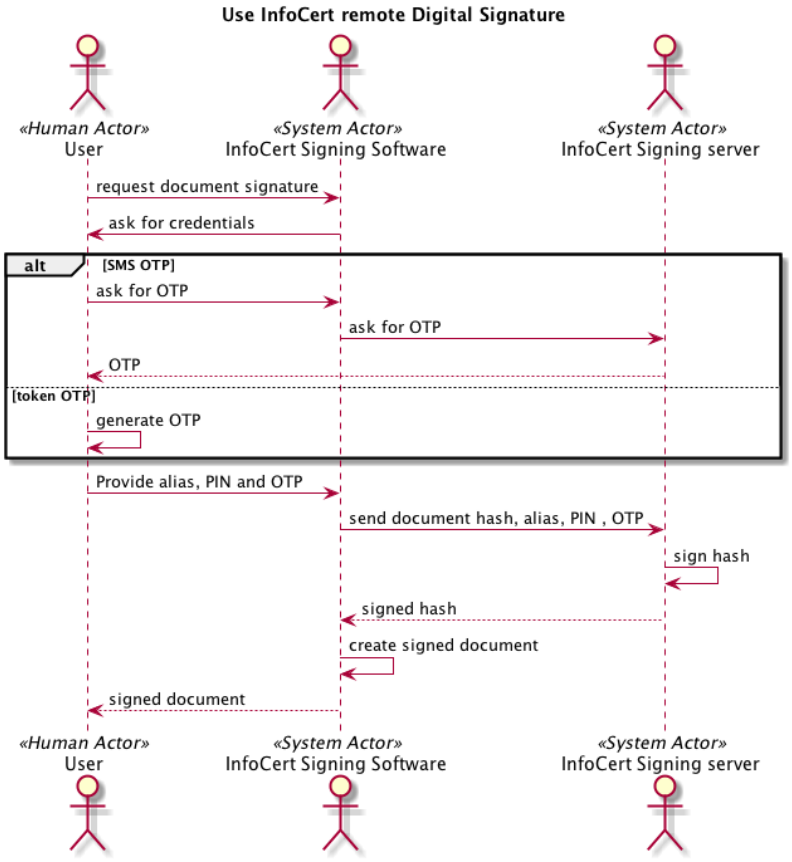


Figure 14: Remote Signature using InfoCert services

4.3.3 Value Proposition

As described above, in eBusiness what we want to show is how CREDENTIAL can make digital life of users safer, by protecting their sensitive information, whether these data are represented by login credentials or personal information. Not only, the aim is also to provide tools that, through a simple user experience, could give the opportunity to share personal information without compromising security of data.

For this reason, all use cases under evaluation have been proposed in order to achieve this dual objective of security and simplicity:

a) In the case of the Identity Federation, user who has a credential account can easily access to a service like Legalmail without having to remember many, too many credentials, but with a big level of security offered by the system.

b) In the case of proxy re-encryption, Legalmail user can forward an important mail to a trusted user, protecting the message itself.

c) In the case of subscription within the e-commerce, there are several advantages: in fact, customers can tap into the information stored in the wallet by having them all at hand and share them securely with the application.

d) In the latter case, the user stores in CREDENTIAL a very important piece of information: the PIN for the digital signature with which he gives legal value to digital transaction.

Actor / Stakeholder	Before	Benefit using CREDENTIAL
Legalmail User	Has to manage many credentials and many passwords	Thanks to CREDENTIAL he can login with different services using same credentials.
Legalmail User	Cannot encrypt important message before sending.	Messages containing sensitive data are being shared with a trusted user.
InfoCert Customer	Has to have all the information needed to subscribe contract available and has to fulfill manually each label	Importing data from wallet, he has all data always available and the fulfilling is automatic
Digital Signature User	For each signature has to remember and clearly disclose his signature PIN	Using CREDENTIAL, user experience is easier and transactions more secure, thanks to the re-encryption service.

Table 22: eBusiness Stakeholders

4.3.4 Business Actors

4.3.4.1 Human Actors

InfoCert Customer: someone who activate one of the InfoCert subscription services. In the different use cases considered, an InfoCert Customer is a user that requires a Legalmail account or a Digital Signature user.

Legalmail User: Someone who possesses a Legalmail account.

4.3.4.2 System Actors

CREDENTIAL Wallet – The Wallet

InfoCert E-commerce - the web portal on which users subscribe InfoCert services online

Legalmail Service - is the InfoCert registered e-mail service, a communication system similar to standard e-mail with some extra security features and certification of delivery that make messages enforceable against third parties. The PEC Legalmail makes it possible to send / receive text messages and attachments with the same legal validity as a registered letter with acknowledgment of receipt.

InfoCert Dike - is the software for digital signature, thanks to which it is possible to digitally sign documents and files using digital qualified certificates and verify validity of signatures and certificates.

InfoCert Remote-sign service - is the cloud service through which Digital Certificate of users are stored on tamperproof devices kept in secure vaults in the InfoCert premises (Hardware Security Module, or HSM).

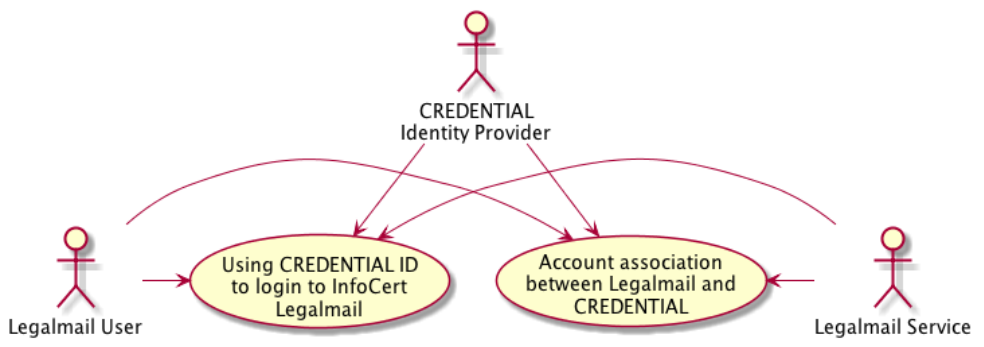
CREDENTIAL re-encryption libraries – The CREDENTIAL libraries which enabled proxy-re-encryption functionality.

4.3.4.3 Legal Actors

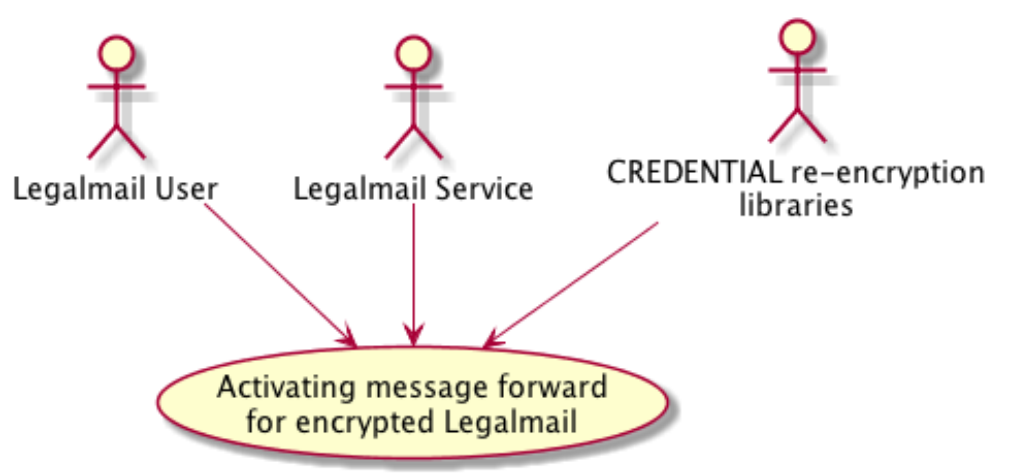
- InfoCert Operating Manual of registered e-mail service
- InfoCert Operating Manual of Remote Digital Signature

4.3.5 Storyboards

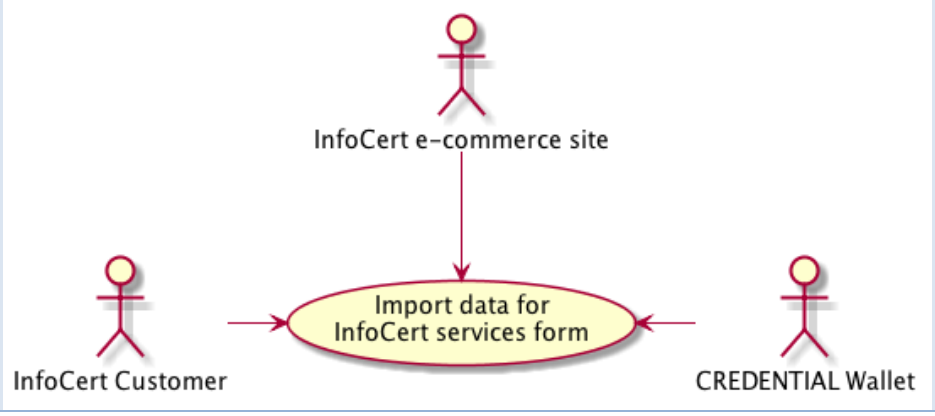
4.3.5.1 Set up login to Legalmail by using CREDENTIAL

Story Name	**Set up login to Legalmail by using CREDENTIAL**
ID	E-BUS-S-SETUPLMAIL
Purpose	Login to Legalmail account using a CREDENTIAL account (it demonstrates the identity and access management functionalities)
Human Actor	Legalmail User
System Actors	• Legalmail service (that manages users electronic mail boxes) • CREDENTIAL Identity Provider
Legal Actors	InfoCert operating manual of the registered e-mail service, clause 4.11
Pre-conditions	• CREDENTIAL Identity Provider satisfies what stated in clause 4.11 of InfoCert operating manual of the registered e-mail service • User has a Legalmail account • User has a CREDENTIAL account
Post-conditions	
Scenario	Andrea is an architect and works for a multinational company. He leads different projects and often sends and exchanges information with various entities via internet. For this reason, he has chosen CREDENTIAL Wallet to protect his sensitive data and to authenticate in internet. In Italy he uses Legalmail as a communication system to send and receive official mail to/from customers, suppliers, etc. One day, logging in Legalmail, he discovers that InfoCert, as a service provider, accepts the ID Federation with CREDENTIAL: so he decides to federate his two accounts to be safer by storing his Legalmail account information within CREDENTIAL Wallet. So he authenticates to CREDENTIAL (i.e. entering username and password), that return to Legalmail service a signed assertion confirming the successful authentication as shown in the illustrations below. Legalmail associates the CREDENTIAL ID to the Legalmail account. Since that moment, Andrea will be able to use CREDENTIAL to authenticate to Legalmail as shown in the illustrations below. InfoCert, on its side, will accept every authentication method used by CREDENTIAL.
Image	

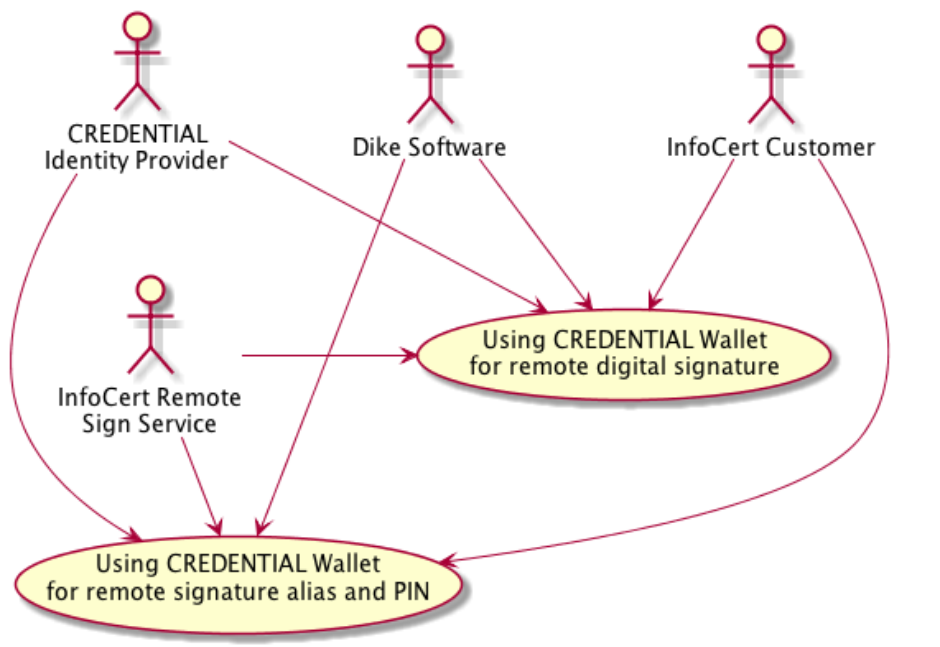
4.3.5.2 Activate encrypted Legalmail forward

Story Name	Activate encrypted Legalmail forward
ID	E-BUS-2-LMAIL
Purpose	Messages containing sensitive data are being shared with a trusted users
Human Actor	Legalmail_User
System Actors	• Legalmail service (that manages users electronic mail boxes) • CREDENTIAL re-encryption libraries
Legal Actors	InfoCert operating manual of the registered e-mail service, clause 4.11
Pre-conditions	• Users have an encryption service configured in their Legalmail account • Users are sending registered mails with legalmail client software
Post-conditions	• A trusted user was able to read encrypted message received in my mailbox and forwarded to him
Scenario	Bob is sharing sensitive contents regarding business strategies with a partner, Alice. To share their data, Bob and Alice are using encrypted Legalmail service, sending registered emails with the legalmail clients. Just before an important deadline, Bob have some problems that prevents him from frequently checking his legalmail inbox and be up to date with the strategy evolutions. He therefore wants Charlie, a trusted colleague, to check for him the messages sent by Alice, but he doesn't want to give away the password of his legalmail. Bob activates a forward rule, forwarding to Charlie all the messages received by Alice and asking Charlie to warn him for any urgency.
Image	

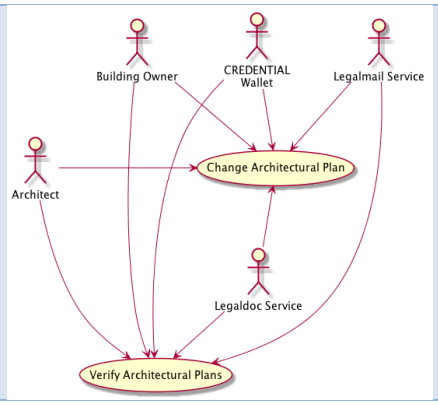
4.3.5.3 Import data into Legalmail subscription form. Choose CREDENTIAL for authentication

Story Name	Import data into Legalmail subscription form. Choose CREDENTIAL for authentication
ID	E-BUS-3-SHOP
Purpose	Purchase Legalmail service. Fulfill the subscription form by importing data from the CREDENTIAL Wallet. Associate the newly created Legalmail account to CREDENTIAL ID.
Human Actor	InfoCert Customer
System Actors	• CREDENTIAL Wallet • InfoCert e-commerce site
Legal Actors	• InfoCert Subscription form • Legalmail contract
Pre-conditions	• Customer has a CREDENTIAL account and has the needed data stored in the CREDENTIAL Wallet
Post-conditions	The subscription form is filled with the data from the CREDENTIAL Wallet. The customer will use only CREDENTIAL account to access InfoCert LegalMail service.
Scenario	Laura is the administrative responsible in a small company which is supplier of local public administrations. She is looking for an electronic Registered e-mail service to manage the billing cycle between her company and its customers. She discovers the e-commerce solution from InfoCert and decides to purchase the Legalmail service. Once she has chosen to purchase the service, she needs to fill a web form with her data and her company's data to be able to register to InfoCert e-commerce site and to sign the service's contract. She has a CREDENTIAL account and InfoCert is a Service Provider in the CREDENTIAL network. So she can fill the forms by sharing safely the needed data directly from CREDENTIAL Wallet without any risk. After completing the purchasing, she will be able to login to InfoCert Legalmail by using her CREDENTIAL account.
Image	

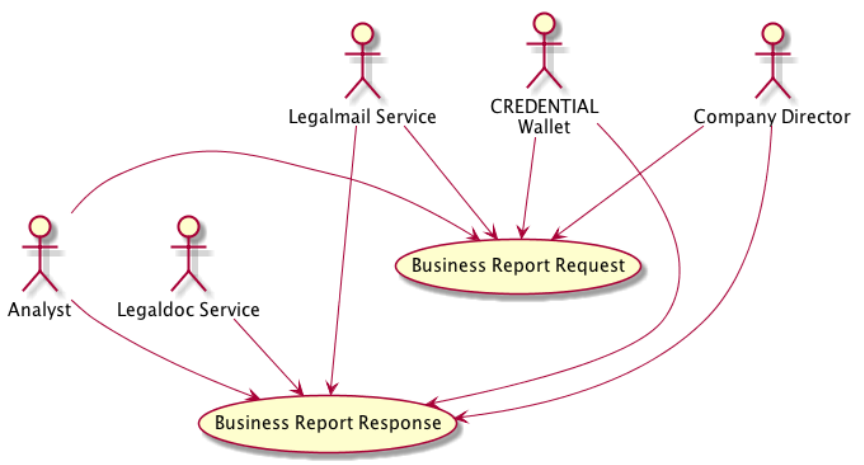
4.3.5.4 Signing a document by using a remote digital signature credential stored in a HSM

Story Name	Signing a document by using a remote digital signature credential stored in a HSM
ID	E-BUS-4-SIGN
Purpose	Signing a document by using the signature alias and PIN stored at the CREDENTIAL Provider.
Human Actor	InfoCert Customer
System Actors	• CREDENTIAL Identity Provider • InfoCert Remote Sign Service • Dike Software
Legal Actors	• InfoCert Subscription form • Legalmail contract
Pre-conditions	• User has stored his signature alias and PIN in CREDENTIAL
Post-conditions	The document is signed.
Scenario	Bob has a Remote Digital Signature credential. His key pair and the associated Qualified Certificate are stored within a HSM managed by InfoCert. In order to digitally sign his document/s he needs to download the software Dike and to know 3 important data. - The alias that's the reference to his Remote Digital Signature credential (the key pair and certificate). - The signature PIN. - An OTP, usually sent via SMS or generated by means of a token. Within Dike, he can use CREDENTIAL to store in the wallet his alias and signature pin: in this way he can easily authenticates to CREDENTIAL when signing avoiding to clearly type these information on the device he is using (PC, SmartPhone, Tablet, etc.).
Image	

4.3.5.5 Editing Architectural Plans

Story Name	Editing Architectural Plans
ID	E-BUS-5-AP
Purpose	Building owner (Bob) wants to change the architectural plans of a building.
Human Actor	• Building Owner • Architect
System Actors	• CREDENTIAL Wallet • Legaldoc Service • Legalmail Service
Legal Actors	• State Engineer
Pre-conditions	• All users have CREDENTIAL account. • All users have Legaldoc account. • All users have Legalmail account. • Building owner has stored architectural plan in CREDENTIAL.
Post-conditions	Building owner saves the final version of architectural plans in CREDENTIAL Wallet.
Scenario	Bob needs to rearrange the rooms of a floor to his building plans to make some offices. So Bob needs to change the architectural plan with an updated version. Bob retrieves the architectural plans from Legaldoc using the CREDENTIAL Wallet as Identity provider. After getting the plans from Legaldoc, he encrypts and uploads into the CREDENTIAL Wallet. Subsequently Bob creates two proxy-re-encryption keys for Archi and Sam (State engineer) for editing and verifying the architectural plans. Then Bob sends an email to Archi (Architect), using Legalmail as mail service. So from now on, Bob will be offline until he receives the confirmation email of the procedure termination. Archi receives email from the Bob to apply the changes on architectural plans. Archi downloads the plans using the proxy-re-encryption key. Archi decrypts the architectural plans using CREDENTIAL and makes the changes on plans. In the end, he saves the re-encrypted plans and uploads them in Credential Wallet. After that, CREDENTIAL Wallet sends a notification to Sam (State engineer) to inform him about the architecture plans. Sam receives the plans from Credential Wallet using the proxy-re-encryption key and acts as follow. Decrypts the plans with CREDENTIAL technology and verifies the changes on the architectural plans. Encrypts and finally uploads the architectural plans into CREDENTIAL Wallet. Finally, CREDENTIAL Wallet receives the architectural plans and notifies the offline Bob to check the architectural plans. After that Bob uploads the final version of the plans into Legaldoc.
Image	

4.3.5.6 Business report ordering by Company

Story Name	Business report ordering by Company
ID	E-BUS-6-BR
Purpose	Business report is being received and verified by Consultant.
Human Actor	• Company director (Ordering Business report) • Analyst (Verifying Business report)
System Actors	• Legaldoc Service (managing users data) • CREDENTIAL Wallet (CREDENTIAL Identity Provider) • Legalmail Service (managing users electronic mails)
Legal Actors	-
Pre-conditions	• Legaldoc Service. • Users have CREDENTIAL account. • Users have stored signature alias, public key. • Users have Legalmail account. • Users can use CREDENTIAL technics (Encryption and Decryption).
Post-conditions	Business report is verified and stored in Legaldoc.
Scenario	Codie (Company director) decides to make an order for his Company. Codie makes the order for his company and he uses C. Wallet (with his public key) to encrypt the order. He stores the order in C. Wallet and sends a notification request to Anna(Analyst) via Legalmail. Anna decrypts the business order and checks/verifies it. After the verification step she creates the business report. Encrypts and stores business report into C. Wallet. Then she sends a notification back to Codie. Codie decrypts with C. Wallet and reads it. The process stops when he stores the business report in Legaldoc.
Image	

4.3.6 Business Use Cases

The six eBusiness storyboards are described specifically in 10 BUCs. The following table provides an overview:

Use Case Name	Unique ID	Main Actor
Account association between Legalmail and CREDENTIAL	E-BUS-1-LMAIL-A	Legalmail User
Using CREDENTIAL ID to login to InfoCert Legalmail	E-BUS-1-LMAIL-B	Legalmail User
Activating message forward for encrypted Legalmail	E-BUS-2-LMAIL	Legalmail User
Import data from CREDENTIAL Wallet to create the contract to be signed to activate Legalmail	E-BUS-3-SHOP	InfoCert Customer
Using CREDENTIAL Wallet to store remote signature alias and PIN	E-BUS-4-SIGN-A	InfoCert Customer
Using CREDENTIAL Wallet for remote digital signature	E-BUS-4-SIGN-B	InfoCert Customer
Change Architectural Plan	E-BUS-5-AP-A	Building Owner
Verify Architectural Plans	E-BUS-5-AP-B	State Engineer
Business Report Request	E-BUS-6-BR-A	Company Director
Business Report Response	E-BUS-6-BR-B	Analyst

Table 23: eBusiness specific BUCs

All use cases are formally specified in Appendix 1A.3.3.

The following table now show which of the above BUCs are associated with which of the eBusiness story boards defined before:

	Set up login to Legalmail by using CREDENTIAL	Activate encrypted Legalmail forward	Import data into Legalmail subscription form. Choose CREDENTIAL for authentication	Signing a document by using a remote digital signature credential stored in a HSM	Editing Archi-tectural Plans	Business report ordering by Company
Account association between Legalmail and CREDENTIAL	✓					
Using CREDENTIAL ID to login to InfoCert Legalmail	✓					
Activating message forward for encrypted Legalmail		✓				
Import data from CREDENTIAL Wallet to create the contract to be signed to activate Legalmail			✓			

	Set up login to Legalmail by using CREDENTIAL	Activate encrypted Legalmail forward	Import data into Legalmail subscription form. Choose CREDENTIAL for authentication	Signing a document by using a remote digital signature credential stored in a HSM	Editing Archi-tectural Plans	Business report ordering by Company
Using CREDENTIAL Wallet to store remote signature alias and PIN				✓		
Using CREDENTIAL Wallet for remote digital signature				✓		
Change Architectural Plan					✓	
Verify Architectural Plans					✓	
Business Report Request						✓
Business Report Response						✓

Table 24: Relation of BUCs and story boards in the eBusiness pilot

5 Conclusion

This document introduced the use cases for a CREDENTIAL Wallet. We distinguish between generic use cases and Pilot Specific use cases. We started by identifying generic business and logical use cases which describe what the CREDENTIAL Wallet can offer as functionality. Each pilot derived from these ideas multiple storyboards in their domain.

We identified a total of 33 generic business use cases and 108 generic logical use cases. All of them together describing the whole functionality of the CREDENTIAL Wallet as an IAM in the cloud and a data sharing platform for user and services.

The future work based on these results are identification and selection of applicable technologies for the CREDENTIAL Wallet, the architecture design of the CREDENTIAL Wallet, the requirements, and the preparation of the pilots. There exists already multiple variants of Proxy-Re-Encryption and Malleable Signature algorithms as well as IAM protocols like OpenID, SAML and XACML. The use cases will guide these decision thus that the best fitting technology for the CREDENTIAL Wallet is selected and further extended according to the feature described by the use cases.

The architecture design is the next big step towards the implementation. Some architectural design decisions might have already been made by the use cases and will be further discussed in the corresponding work packages.

The use cases will help by deriving the requirements for the CREDENTIAL Wallet. Different aspects like functionality, security, privacy, usability, etc. have to be considered and should be fully covered by the use cases developed in this document. By using Redmine we are able to keep track of the use cases and their corresponding requirements. If changes need to be done, for example because some privacy and security requirements can contradict each other, we are able to do so.

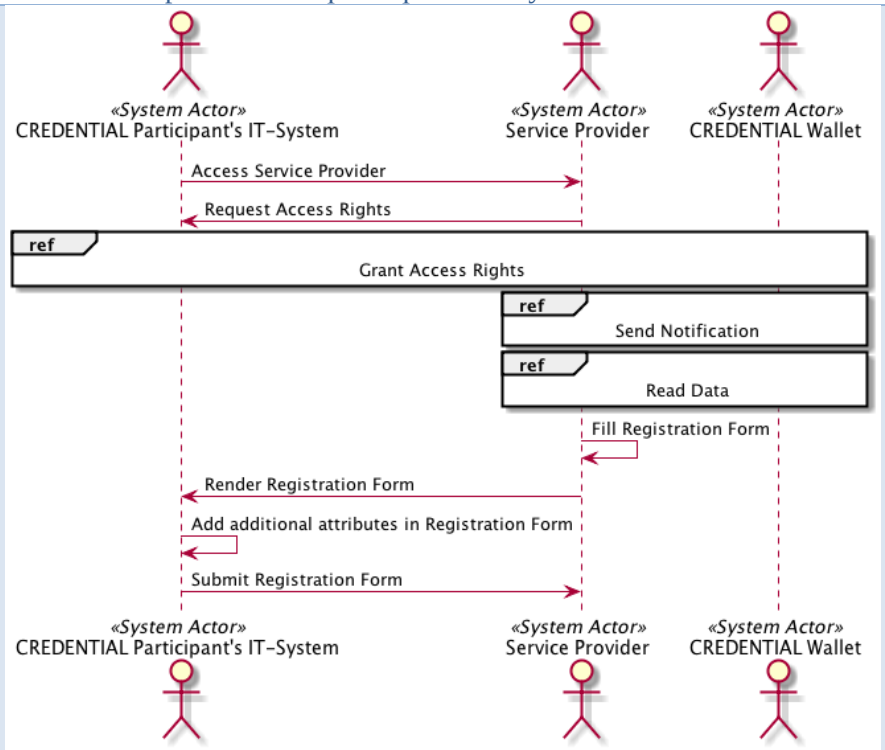
Finally, the pilots can use their proposed business use cases and refine them in logical use cases and Technical use cases where special characteristics of each pilot can be taken into account.

A Formal Specifications of Use Cases

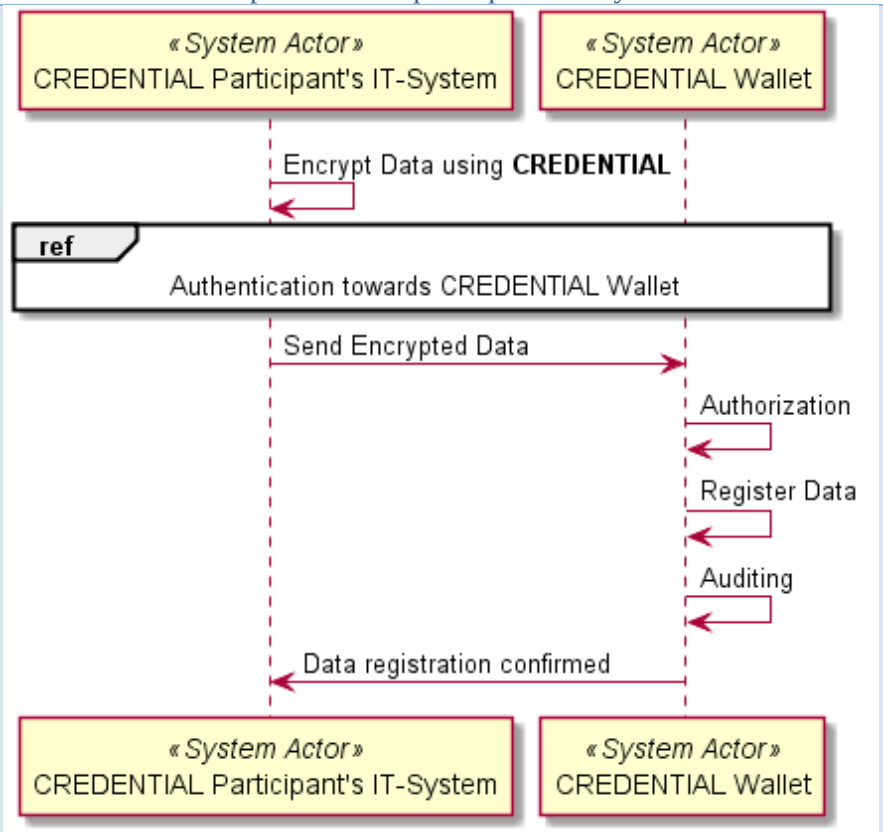
A.1 Generic Business Use Cases

A.1.1 Data Management

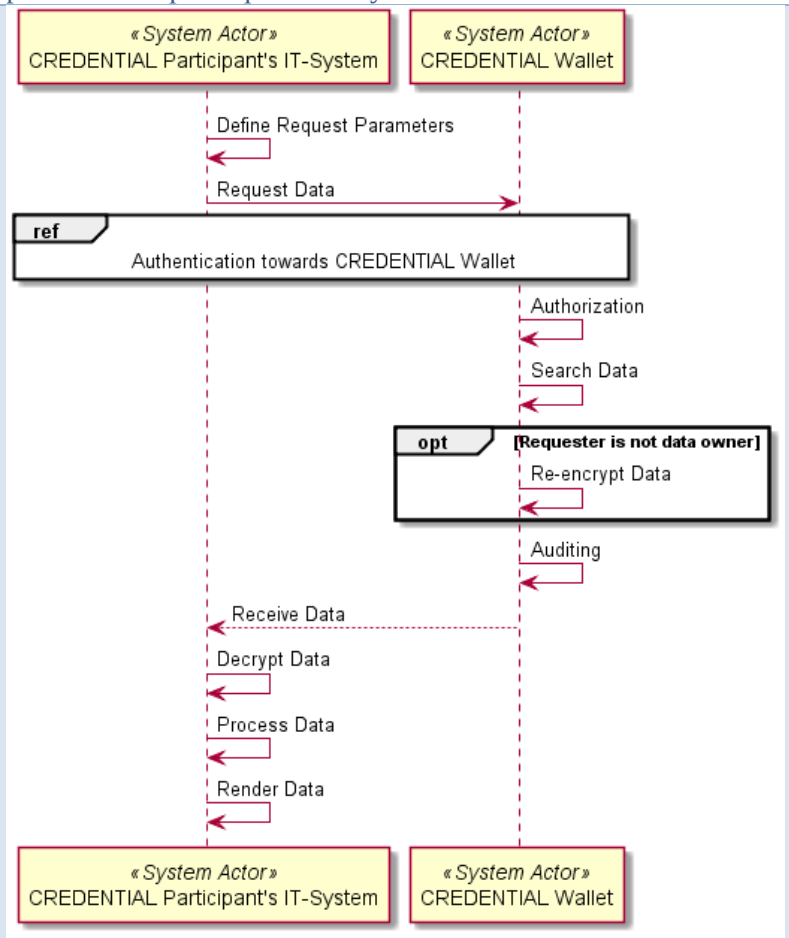
A.1.1.1 Export CREDENTIAL Wallet data into form

Use Case Name	Export CREDENTIAL Wallet data into form
ID	G-BUC-EXPFORM
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System - Service Provider
Pre-conditions	- Service Provider needs to have CREDENTIAL Key Material
Post-conditions	- CREDENTIAL Data is unencrypted available at the Service Provider
Description	A user provides a form to the CREDENTIAL Wallet. The CREDENTIAL Wallet re-encrypts the user's data and fills them into the form. A human interaction is possible with participant's IT system.
Image	

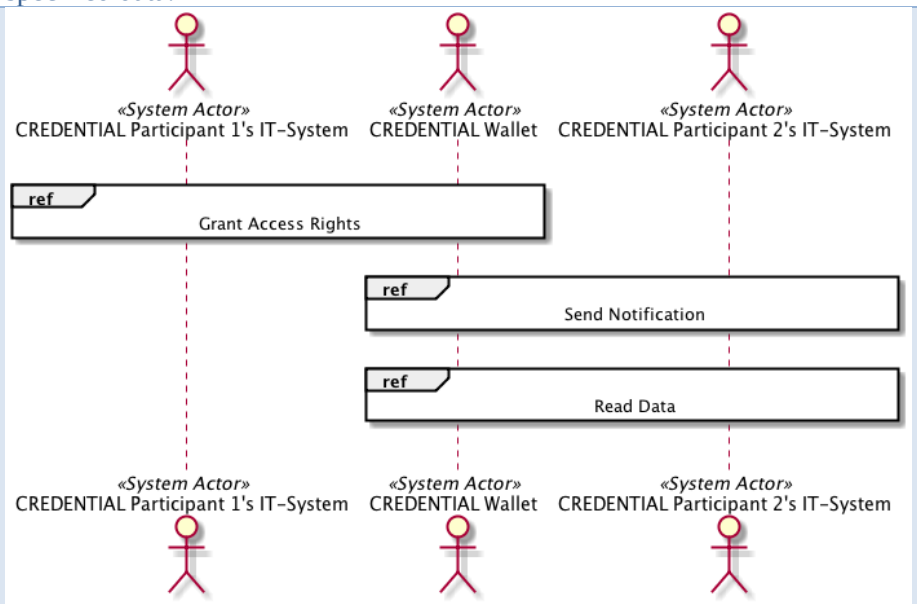
A.1.1.2 Send Data

Use Case Name	Send Data
ID	G-BUC-SENDDATA
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- User has a CREDENTIAL account - User has write access rights
Post-conditions	- Data is registered in the wallet
Description	A user sends data from his IT-System to CREDENTIAL Wallet or to a Service Provider protected by CREDENTIAL technology. The user encrypts his data using CREDENTIAL technology. He authenticates himself against the wallet and submits the data to the wallet. The wallet performs an authorization on the performed action. After a successfully authorization the data is registered in the wallet. When the process is finished the wallet performs an auditing of every previous action performed in this step. A human interaction is possible with participant's IT system.
Image	

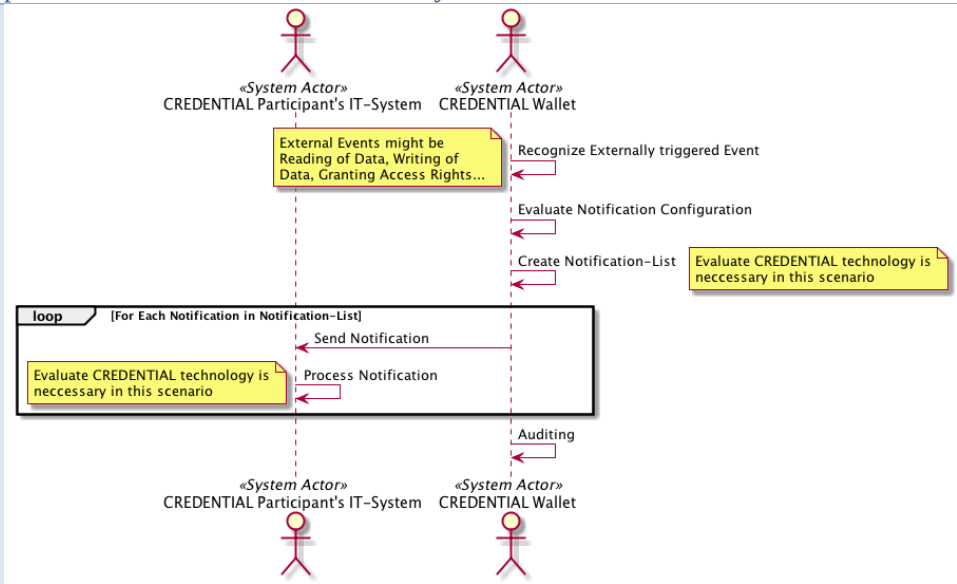
A.1.1.3 Read Data

Use Case Name	Read Data
ID	G-BUC-READDATA
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant has a CREDENTIAL account - Participant has read access rights
Post-conditions	- Data is decrypted on participant's IT-System
Description	A CREDENTIAL participant reads data from the CREDENTIAL Wallet. The participant defines request parameters which specify the requested data. The participant authenticates himself against the wallet. The wallet performs an authorization. After a successful authorization the data is searched. In case the requester is not the data owner, the data is re-encrypted. The wallet performs auditing of every previous steps and sends the data back to be participant. The participant decrypts, processes and renders the data. A human interaction is possible with participant's IT system.
Image	

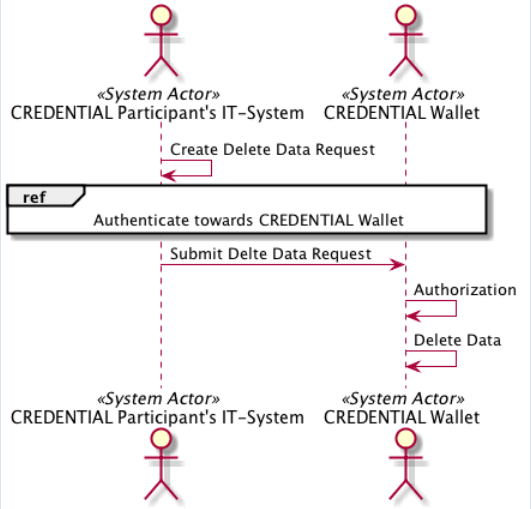
A.1.1.4 Forward Data

Use Case Name	Forward Data
ID	G-BUC-FORWARDDATA
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- The participant who grants access rights needs the right to grant read access - Both participants have a CREDENTIAL account
Post-conditions	- The receiving participant has read access rights
Description	A CREDENTIAL participant forwards data from the CREDENTIAL Wallet to another CREDENTIAL participant. In order to forward data, the participant has to grant read access rights to the receiving participant. After successfully granted access rights the wallet sends a notification to the receiving participant's IT-System. The receiving participant performs a read data on the specified data.
Image	

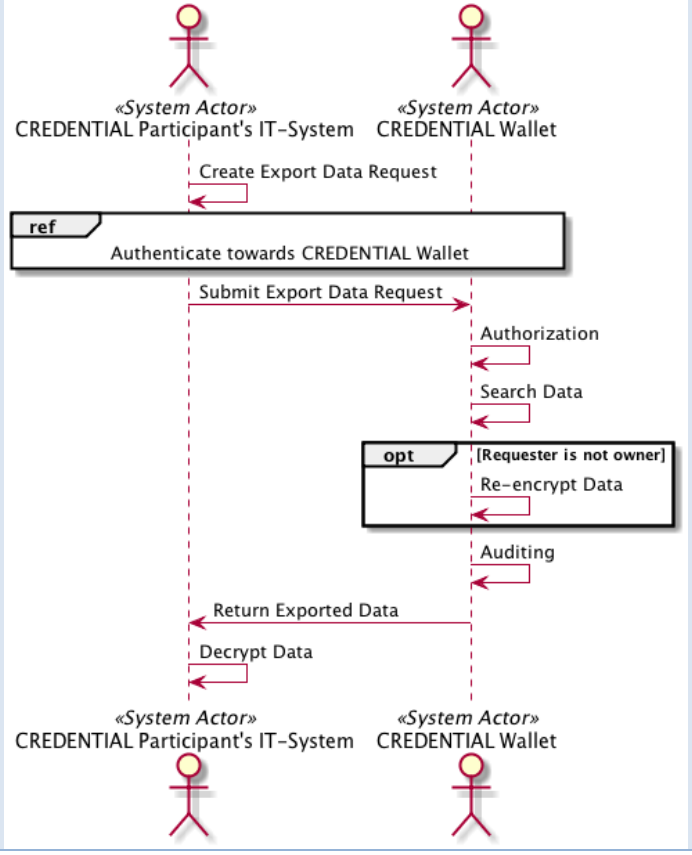
A.1.1.5 Send Notification

Use Case Name	Send Notification
ID	G-BUC-SENDNOTIFICATION
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- A notification on a specific event is registered in the wallet - Participant has a CREDENTIAL account
Post-conditions	- The participant has received a notification about a specific event
Description	The wallet recognizes an externally triggered event. An event can be for example a reading of data, writing of data or granting of access rights. The wallet evaluates a notification configuration. For each participant who wants to be notified a Notification is created and sent to the participant. The participant processes the notification if necessary.
Image	

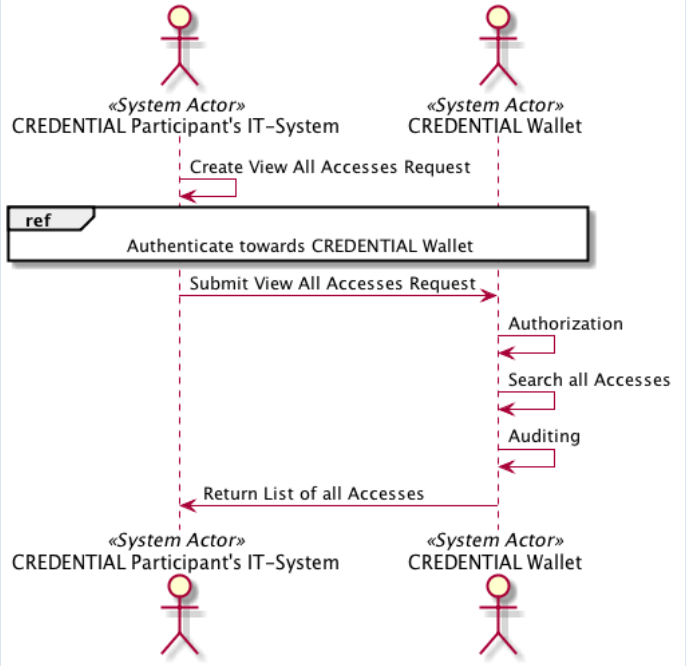
A.1.1.6 Delete Data Set

Use Case Name	Delete Data Set
ID	G-BUC-DELETEDATASET
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- The participant has delete rights on the data set - The participant logged-in on the CREDENTIAL Wallet
Post-conditions	- The specified data set is deleted
Description	A participant creates a delete data request. He specifies which data set should be deleted. He authenticates himself against the wallet and sends the delete request to the wallet. The wallet performs the authorization on the given operation. After a successful authorization the wallet deletes the data record.
Image	

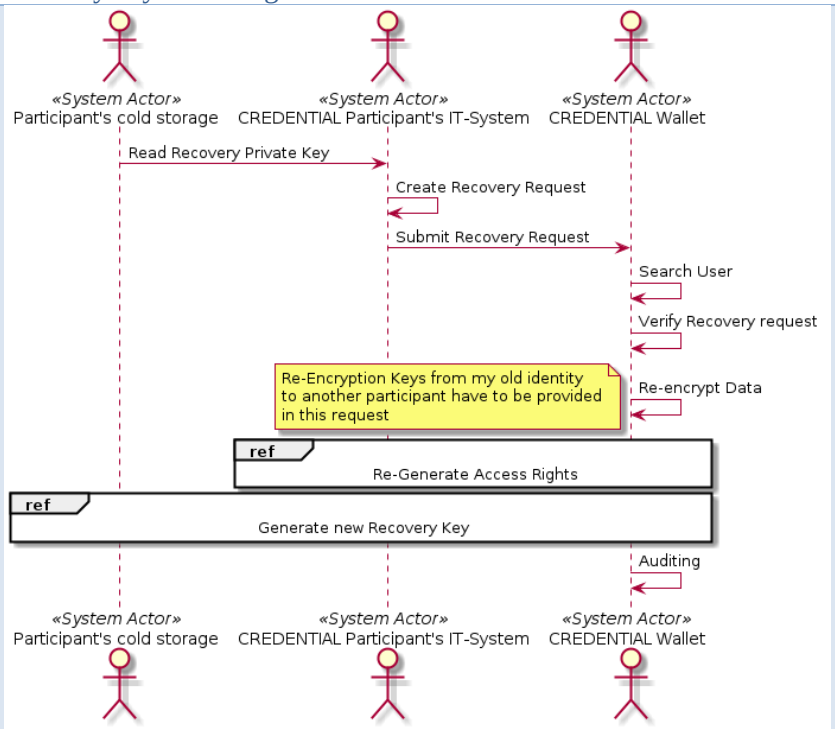
A.1.1.7 Export Data from Wallet

Use Case Name	Export Data from Wallet
ID	G-BUC-EXPORTDATA
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- The participant is logged-in on the CREDENTIAL Wallet - The participant has read access rights on the data
Post-conditions	- The data is exported and decrypted on the participant's IT-System
Description	A participant creates an export data request. He authenticates himself against the wallet and sends the export request to the wallet. The wallet performs an authorization. After a successful authorization the wallet searches the data. If the requester is not the data owner by himself, then the wallet performs a re-encryption of the data. The wallet audits every previously performed action. The exported data is send to the participant. The participant decrypts the data.
Image	

A.1.1.8 View all accesses to my Data

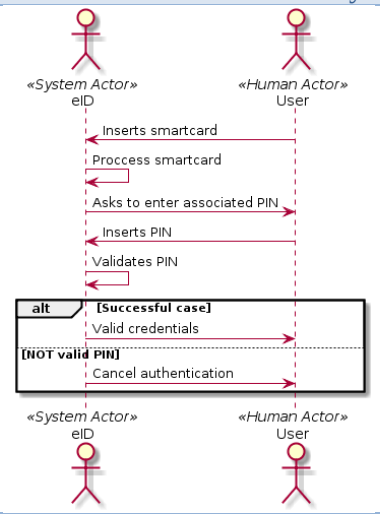
Use Case Name	View all accesses to my Data
ID	G-BUC-VIEWACCESSES
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- The participant is the data owner
Post-conditions	- A List of all accesses to the participant's data are displayed to the participant. - An audit log of this action is available at the CREDENTIAL Wallet
Description	The participant creates a view all access to his data request. He authenticates himself against the CREDENTIAL Wallet and submits the view all access request to the wallet. The wallet performs an authorization. After a successful authorization the wallet searches for all access to the the participant's data. The wallet performs an auditing of every previous performed action. The wallet returns the list of all accesses to the participant.
Image	

A.1.1.9 Recover CREDENTIAL Wallet Data

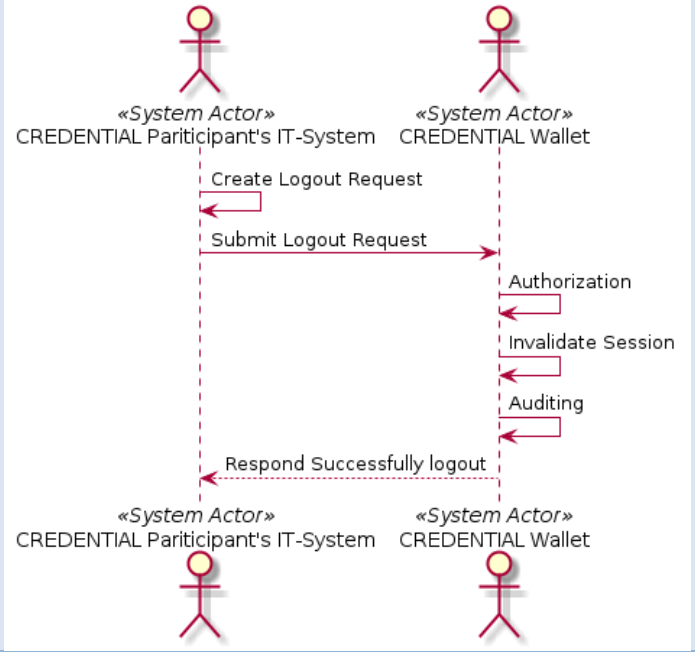
Use Case Name	Recover CREDENTIAL Wallet data
ID	G-BUC-RECOVERDATA
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System - CREDENTIAL Participant's Cold Storage
Pre-conditions	- User has a CREDENTIAL account - User has a recovery key registered in CREDENTIAL and stored offline
Post-conditions	- User has a new main key pair - Data is re-encrypted so it can be controlled with the new key pair - Re-Encryption Keys have been re-computed
Description	Participants will mostly have their private keys to access the CREDENTIAL data stored in some secure HW in their own devices. While this is the most convenient option, it has to be considered what happens when the device (and the private key) is lost but there is need to access the old CREDENTIAL Wallet, and the data is stored in it. In traditional systems, this would mean authenticating the participant by an alternative mean (email, SMS) and generating a new key pair. However, for the CREDENTIAL Wallet, as the data is encrypted, this is not feasible. The existing data should also be re-encrypted so it can be used with the new key pair. Hence, the best approach is to have a separate recovery key pair and its corresponding re-encryption key. The same recovery key will serve as a mean to authenticate the user and trigger the re-encryption and it will be established as the new man key. A new recovery key must be generated and sent to the wallet.
Image	

A.1.2 Authentication

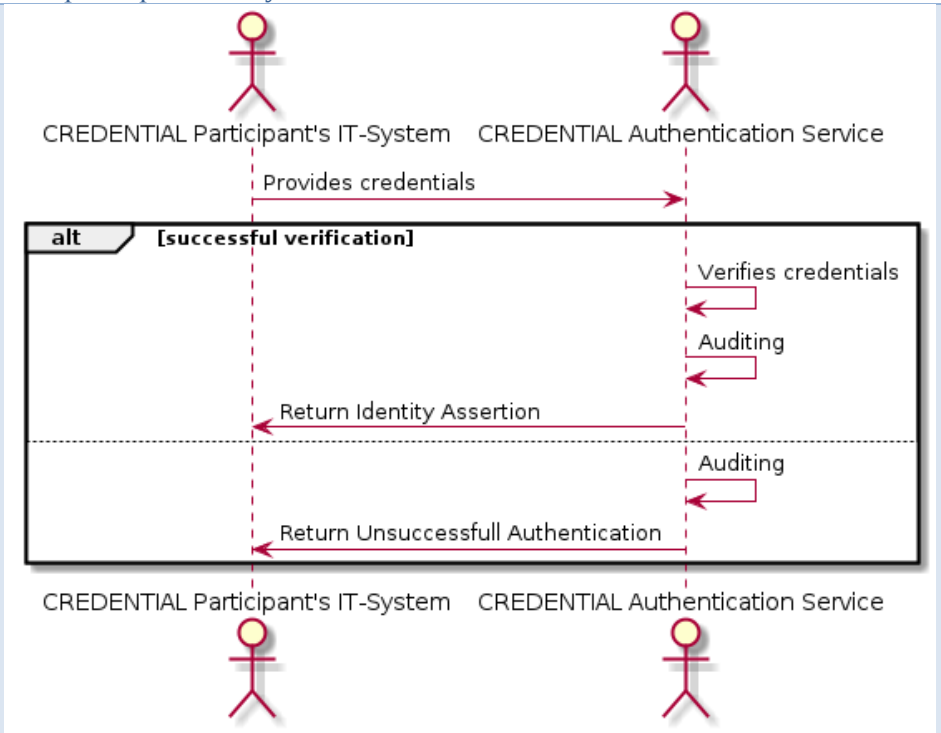
A.1.2.1 Authentication using SmartCard

Use Case Name	Authentication using SmartCard
ID	G-LUC-AUTHSMARTCARD
LUC_in	Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- eID
Secondary Actors	- CREDENTIAL Participant
Pre-conditions	- User is registered in the eID system - User has a valid smartcard
Post-conditions	- The user is authenticated to e-ID system
Description	The user has to validate the identity against an electronic ID system, using a two-factor authentication based on smartcard technology. The smartcard must be inserted in the e-ID system. The user must type a valid PIN.
Image	

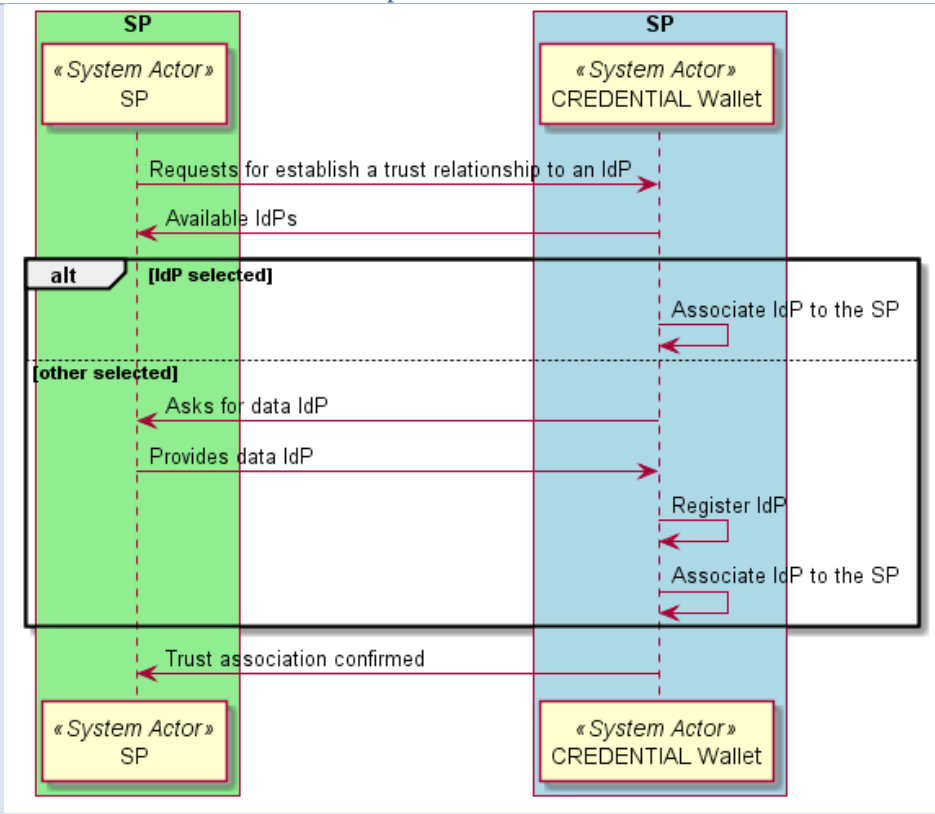
A.1.2.2 Logout from CREDENTIAL Wallet

Use Case Name	Logout from CREDENTIAL Wallet
ID	G-BUC-LOGOUTWALLET
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- The user has a valid session on the CREDENTIAL Wallet
Post-conditions	- The user's session is expired
Description	The participant selects the logout functionality. The CREDENTIAL Wallet processes the participant's logout request. If the participant has a valid session the CREDENTIAL Wallet invalidates this session. The CREDENTIAL Wallet write a log entry for the logout process. A human interaction is possible with participant's IT system.
Image	

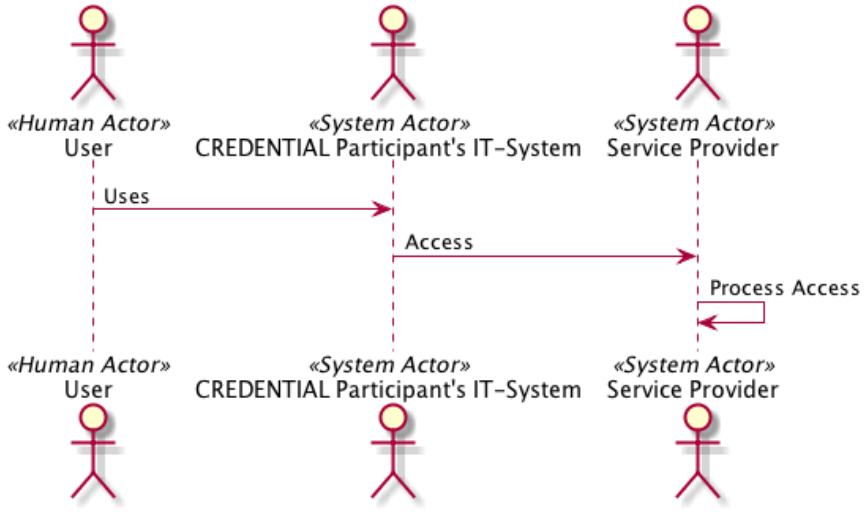
A.1.2.3 Authenticate towards CREDENTIAL Wallet

Use Case Name	Authenticate towards CREDENTIAL Wallet
ID	G-BUC-AUTHWALLET
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Authentication Service
Pre-conditions	- User has an account - User has access to his credentials
Post-conditions	- User has an Identity Assertion - User is able to access CREDENTIAL services
Description	The user wants to authenticate against the CREDENTIAL Wallet. He uses the CREDENTIAL Authentication Service and provide his credentials. The CREDENTIAL Authentication Service verifies the credentials and issues an Identity Assertion for the user. The user is able to access any CREDENTIAL Wallet service with this Identity Assertion. A human interaction is possible with participant's IT system.
Image	

A.1.2.4 SP build up Trust relation to IdP

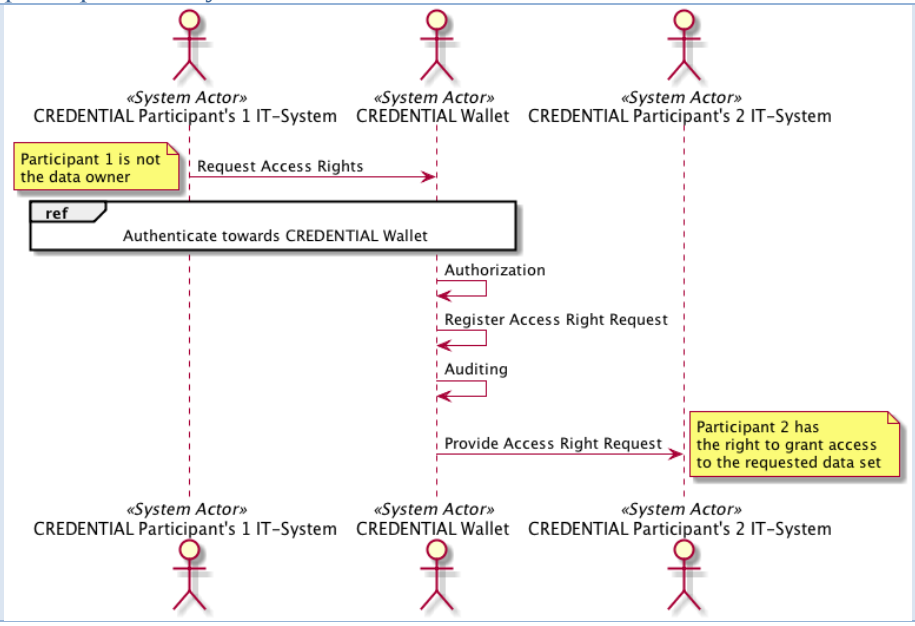
Use Case Name	SP build up Trust relation to IdP
ID	G-BUC-SPBUILDTRUSTIDP
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- A CREDENTIAL enabled SP must exist
Post-conditions	- The SP establish a trust relationship to an IdP in CREDENTIAL Wallet
Description	A SP establish a trust relationship to an IdP in CREDENTIAL Wallet
Image	

A.1.2.5 Access Service Provider

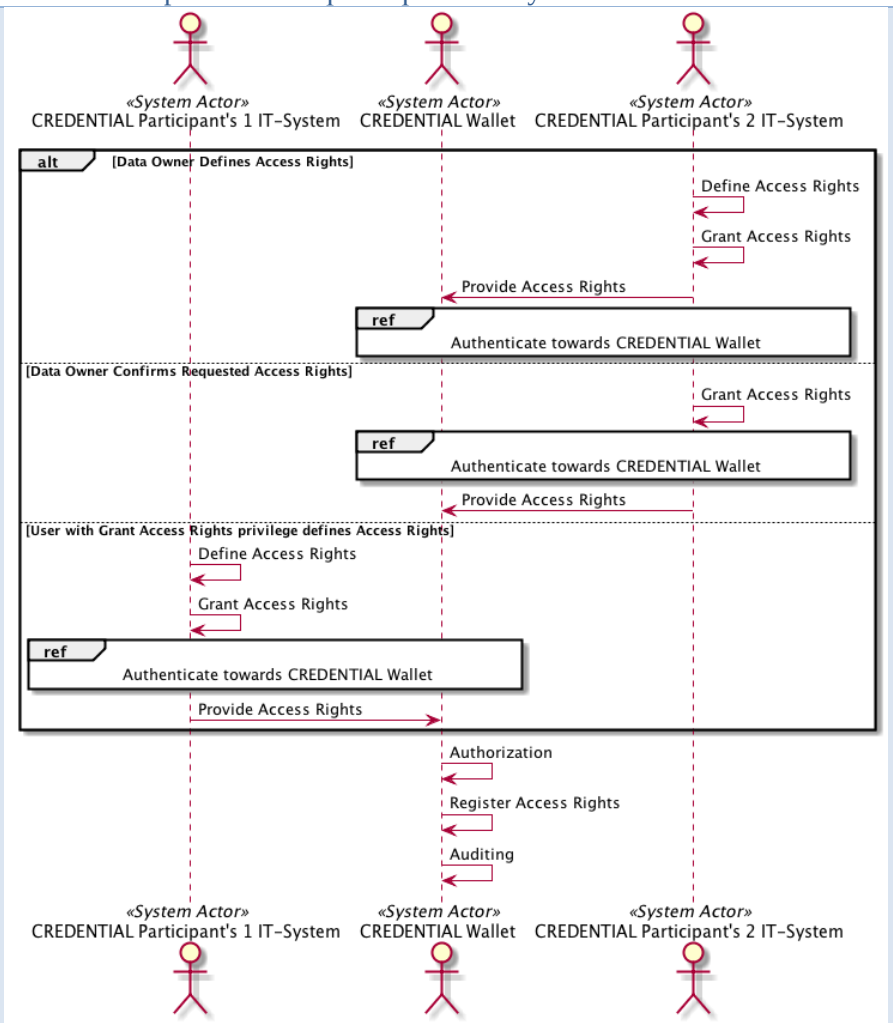
Use Case Name	Access Service Provider
ID	G-LUC-ACCESSSP
LUC_in	Export CREDENTIAL Wallet data into form
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Participant's IT-System - Service Provider
Pre-conditions	
Post-conditions	
Description	A user uses his IT-System to access some functionality on a service provider.
Image	

A.1.3 Authorization

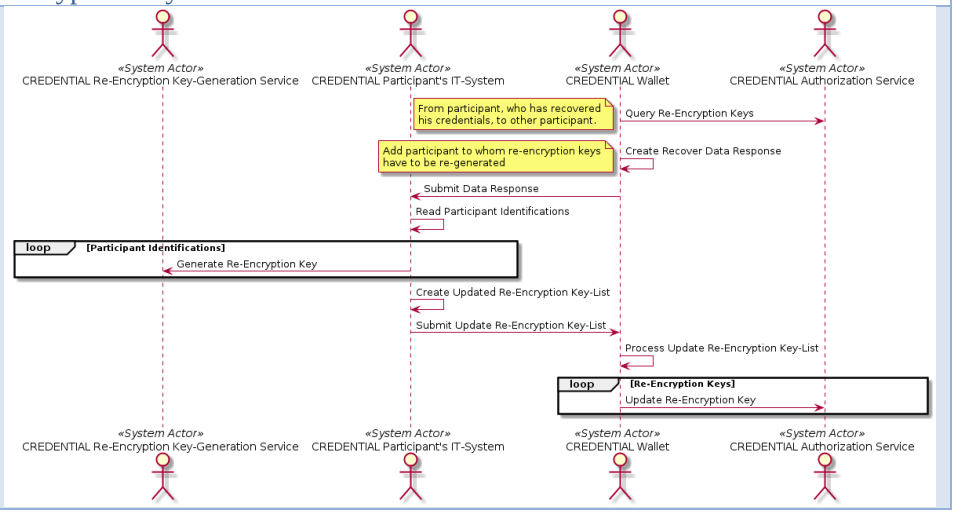
A.1.3.1 Request Access Rights

Use Case Name	Request Access Rights
ID	G-BUC-REQACCESSRIGHTS
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant 1 is not the data owner - Participant 2 is the data owner - Both participants have a CREDENTIAL account
Post-conditions	- Participant 2 has received the request for access rights
Description	A participant who is not a data owner requests access rights to data stored in the CREDENTIAL Wallet. The wallet authenticates the requester and registers the access rights request. The wallet identifies the data owner and submits the access rights request to the data owner. A human interaction is possible with participant's IT system.
Image	

A.1.3.2 Grant Access Rights

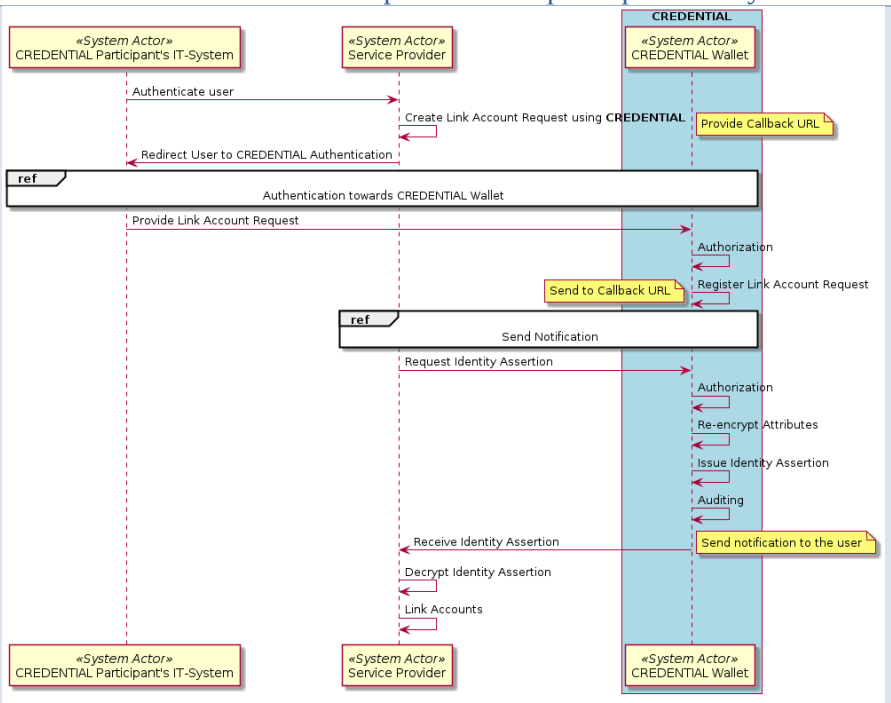
Use Case Name	Grant Access Rights
ID	G-BUC-GRANTACCESSRIGHTS
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Both participants have CREDENTIAL accounts.
Post-conditions	- The access rights are registered in the wallet.
Description	A CREDENTIAL participant grants access rights to his data in the CREDENTIAL Wallet to another participant. There are three different scenarios. The participant who is the data owner defines the access rights on its own, a participant who receives a request access rights confirms the request and a participant who has grant access rights privileges defines access rights for another participant. In all scenarios the access rights will be provided to the wallet. The wallet performs an authorization on the request. On successful authorization the access rights will be registered. A human interaction is possible with participant's IT system.
Image	

A.1.3.3 Re-Generate Access Rights

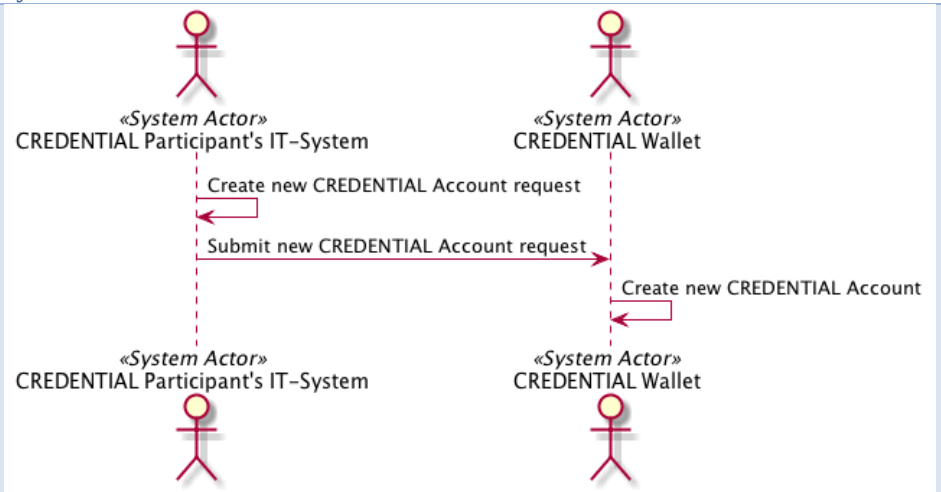
Use Case Name	Re-Generate Access Rights
ID	G-BUC-REGENACCESSRIGHTS
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet - CREDENTIAL Participant's IT-System - CREDENTIAL Re-Encryption Key Generation Service
Pre-conditions	- User is authenticated to the CREDENTIAL Wallet - User has a CREDENTIAL Account - User has provided access rights to participants - Participant receives a successfully response about his recover request
Post-conditions	- Re-encryption keys have been generated for the new private key - Re-encryption keys are updated in the CREDENTIAL Wallet
Description	Whenever a participant modifies its master key-pair, all their re-encryption keys based on them are no longer valid. Hence, it is required to re-generate the re-encryption keys associated to access rights already provided to the wallet. The participant requests a list of all access rights associated to his account and then re-generate the access rights based with new key-material. The Access Rights are re-generated and provided to the wallet. A participant receives a successfully response that his credentials for CREDENTIAL Wallet have been updated. In order to fully complete this request he has to update the re-encryption keys that are stored within the Wallet.
Image	

A.1.4 Account Management

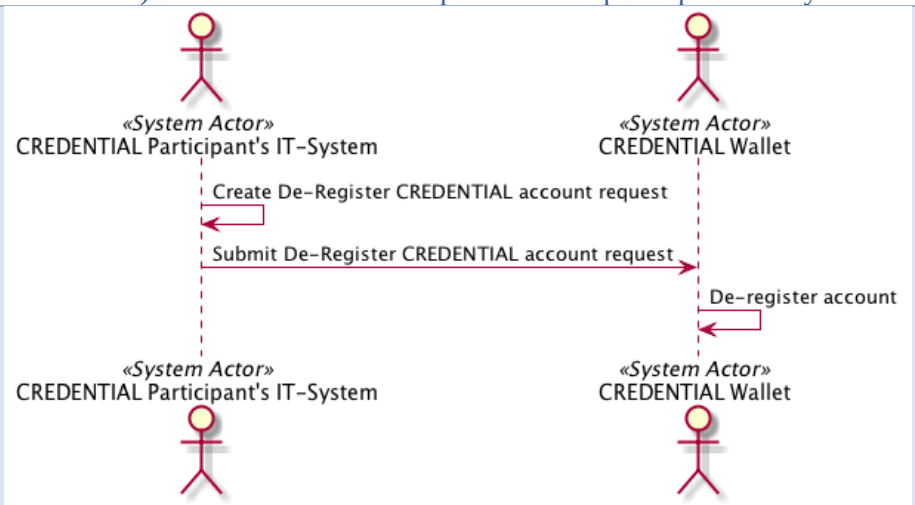
A.1.4.1 Link Service Provider account with CREDENTIAL account

Use Case Name	Link Service Provider account with CREDENTIAL account
ID	G-BUC-LINKSPWITHCRED
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- Service Provider - CREDENTIAL Wallet
Pre-conditions	- User has both accounts, the CREDENTIAL account and the SP account
Post-conditions	- CREDENTIAL account and the SP account are linked
Description	A user links his CREDENTIAL Account to his Service Provider account. He is able to login to his Service Provider account using his CREDENTIAL account. A human interaction is possible with participant's IT system.
Image	

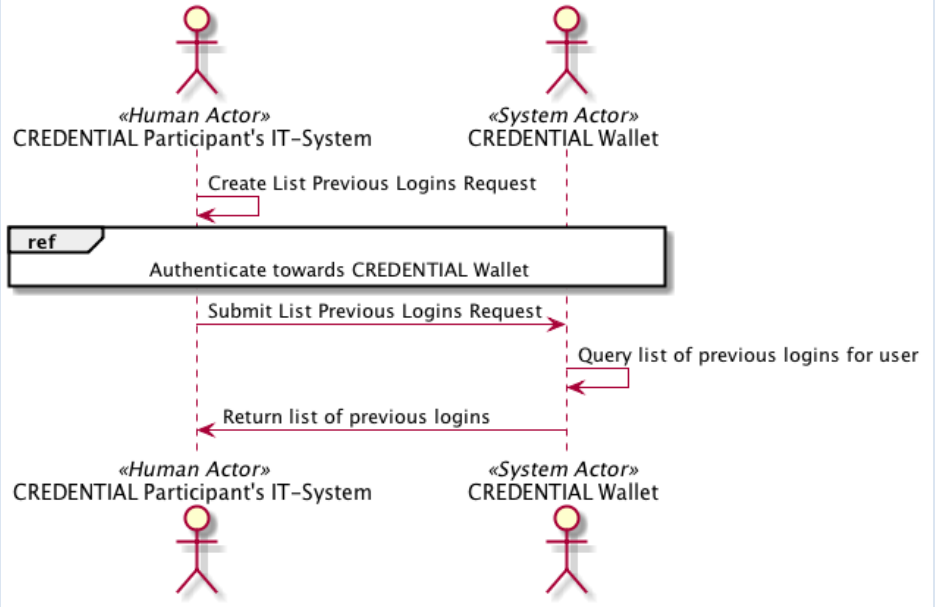
A.1.4.2 Register new CREDENTIAL Account

Use Case Name	Register new CREDENTIAL Account
ID	G-BUC-REGCREDACCOUNT
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- The participant has no account on the CREDENTIAL Wallet - The participant has locally access to a "Proxy-Re-Encryption-Ready" Key Generation Service
Post-conditions	- Public and Private "Proxy-Re-Encryption-Ready"-Keys are generated - CREDENTIAL knows the generated "Proxy-Re-Encryption-Ready"-Public Key - Participant knows the generated "Proxy-Re-Encryption-Ready"-Private Key - Account is linked to the "Proxy-Re-Encryption-Ready"-Public Key
Description	A participant creates a new account on the CREDENTIAL Wallet. He creates a new "Proxy-Re-Encryption-Ready"-Key on his IT-System. He adds additional registration information and creates a CREDENTIAL Account request. This request is send to the wallet. The wallet verifies the request and creates a new participant account on the wallet. The wallet and the provided key by the user are linked together. A human interaction is possible with participant's IT system.
Image	

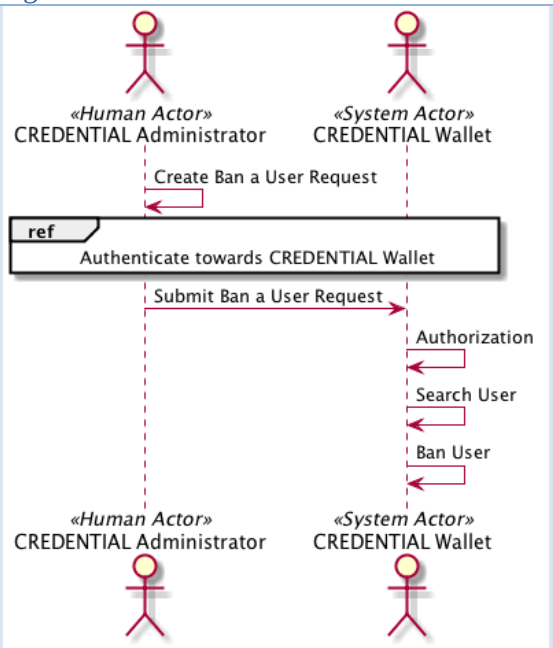
A.1.4.3 De-Register From CREDENTIAL

Use Case Name	De-Register From CREDENTIAL
ID	G-BUC-DEREGISTERCREDENTIAL
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- User has account on CREDENTIAL Wallet - User is logged-in on the CREDENTIAL Wallet
Post-conditions	- User's account is closed - Login attempts to this account are no longer possible
Description	A user de-registers from CREDENTIAL Wallet. This implies user's data deletion, i.e. user specific data stored in Wallet, user grants rights given to another user, user notification lists (in terms of devices and types of notification). A human interaction is possible with participant's IT system.
Image	

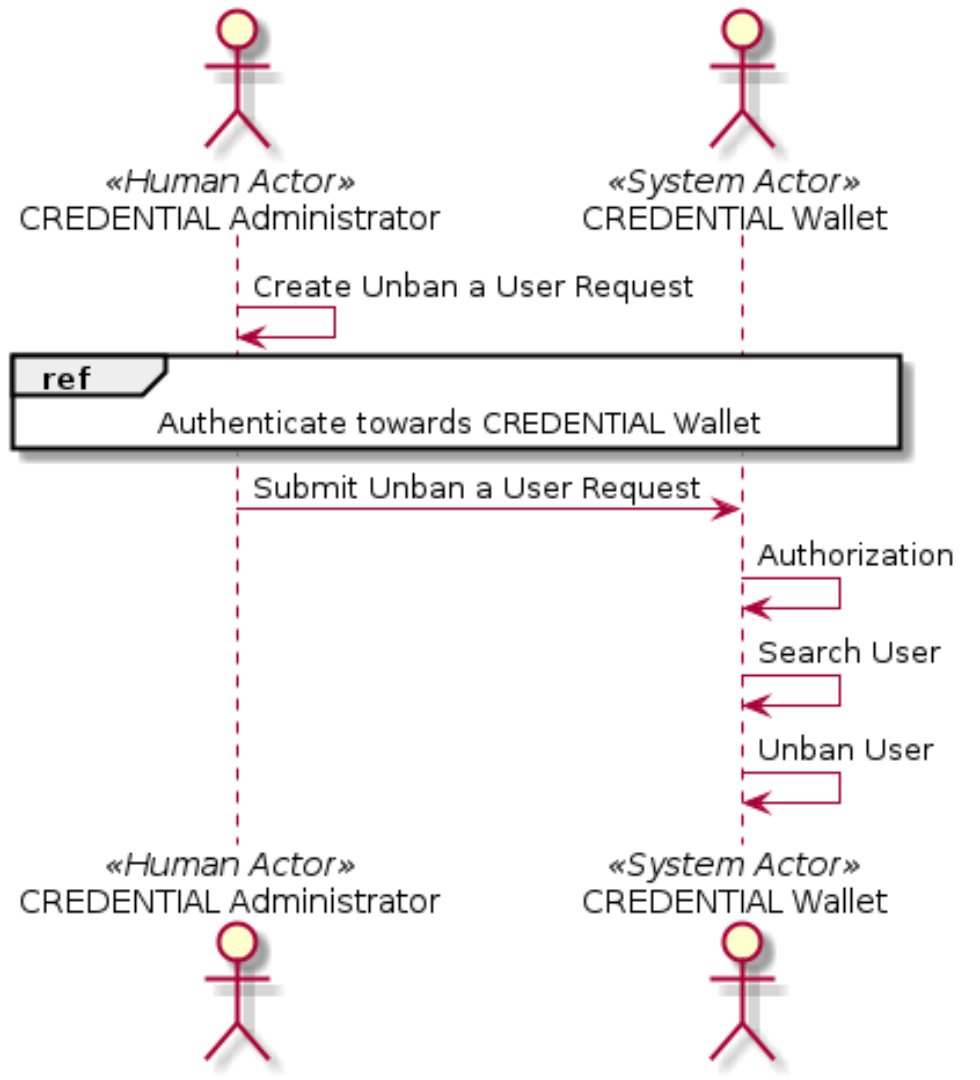
A.1.4.4 View Previous Logins to My Account

Use Case Name	View Previous Logins to My Account
ID	G-BUC-VIEWLOGINS
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- A user is logged-in on the CREDENTIAL Wallet
Post-conditions	- A list of previous logins to his accounts is rendered to the user.
Description	A user requests the list of the previous logins to his account. He authenticates himself against the wallet. The wallet queries the list of all previous logins to the account. The wallet returns the list of all previous logins to the user.
Image	

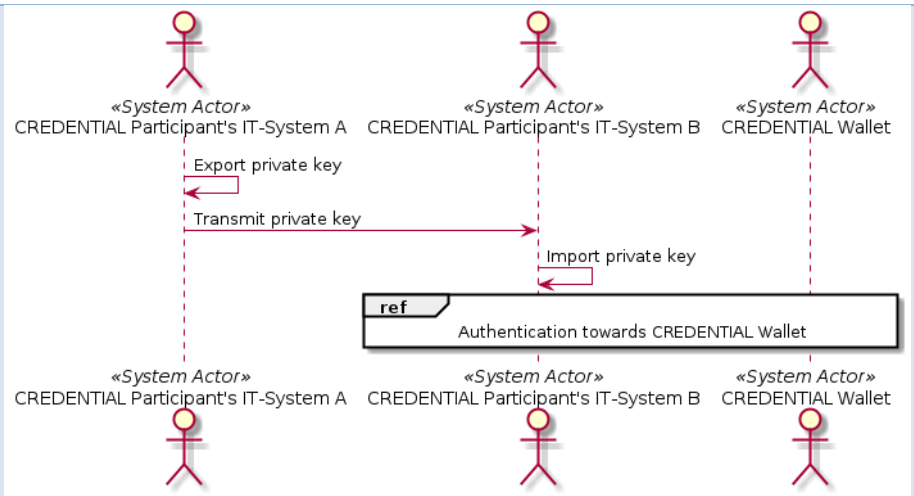
A.1.4.5 Ban a User

Use Case Name	Ban a User
ID	G-BUC-BANUSER
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Administrator
Pre-conditions	- A User has a CREDENTIAL account - The CREDENTIAL Administrator has admin rights
Post-conditions	- User is no longer able to login. Account is still present at CREDENTIAL Wallet.
Description	The CREDENTIAL Administrator bans a user. The user is no longer able to login to his account.
Image	

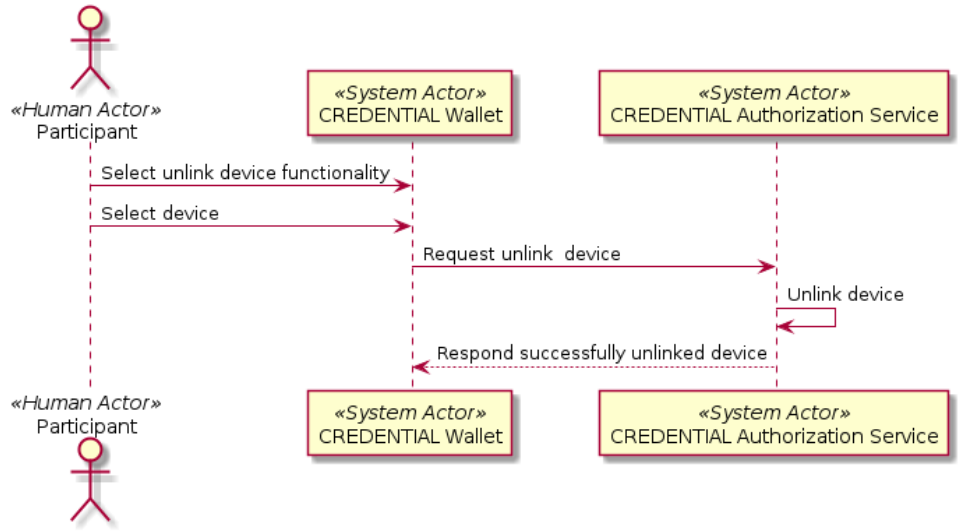
A.1.4.6 Unban a User

Use Case Name	Unban a banned User
ID	G-BUC-UNBANUSER
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Administrator
Pre-conditions	- A User has been banned
Post-conditions	- User is no longer banned and can again access his data.
Description	The CREDENTIAL Administrator re-activates the account of a banned user. This may be necessary, e.g., if the user has been banned because of leaked authentication credentials, and if the user now has renewed his credentials.
Image	

A.1.4.7 Register new device for accessing CREDENTIAL Wallet

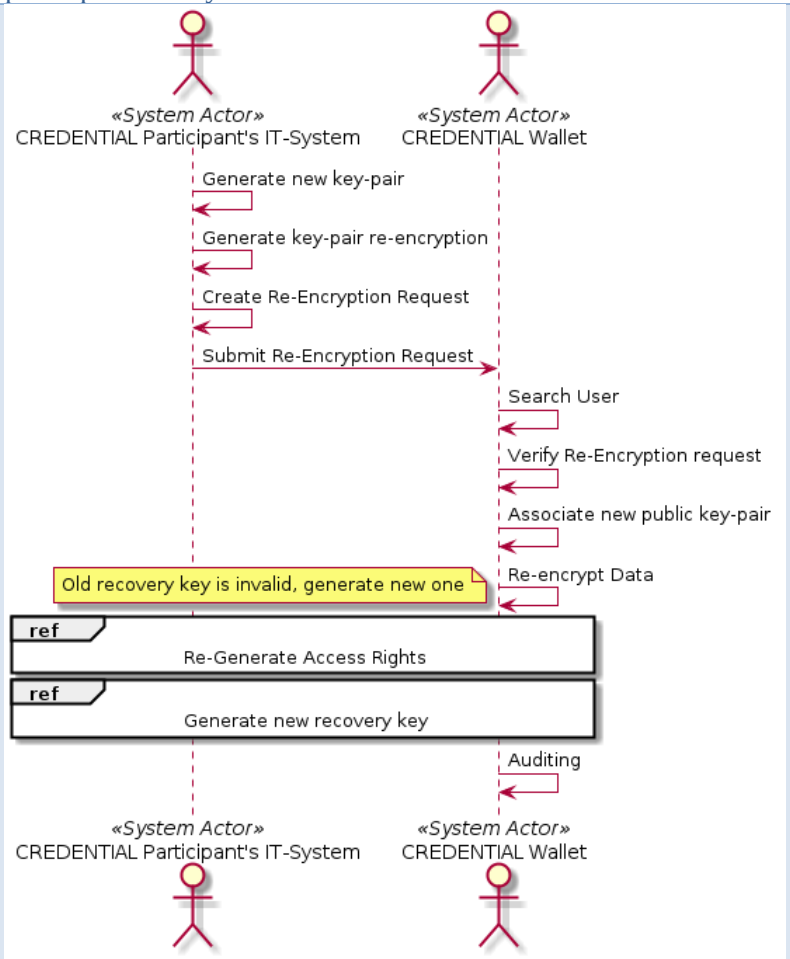
Use Case Name	Register new device for accessing CREDENTIAL Wallet
ID	G-BUC-REGNEWDEVICE
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- User has a CREDENTIAL account in one device - User has a device not associated to a CREDENTIAL account
Post-conditions	- User can access its wallet from both devices
Description	One of the main benefits of having a cloud wallet is that it can be accessed by many devices. While in general several authentication keys can be associated to one identity or to one wallet, the re-encryption mechanisms require one unique private key to control all the data stored in the participants' wallet. A mechanism has to devised for securely sharing this private key among devices.
Image	

A.1.4.8 Unlink device from CREDENTIAL Wallet

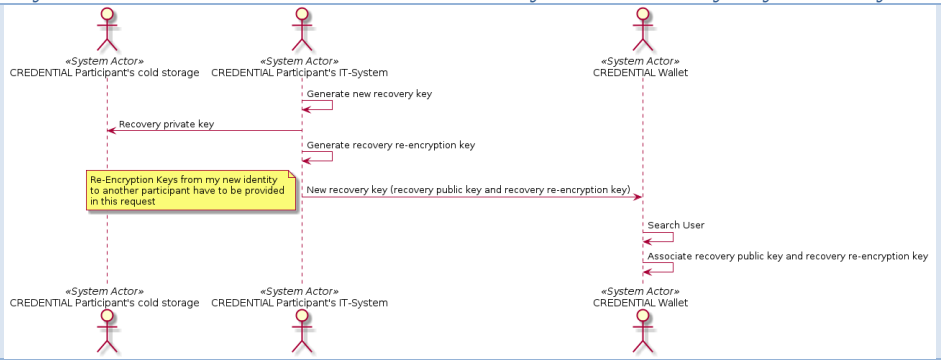
Use Case Name	Unlink device from CREDENTIAL Wallet
ID	G-BUC-UNLNKDEVICE
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Wallet - CREDENTIAL Authorization Service
Pre-conditions	- Device is linked to CREDENTIAL Wallet - Pushing data from the device to the CREDENTIAL Wallet is possible
Post-conditions	- Device is unlinked to the CREDENTIAL Wallet - Pushing data from device to CREDENTIAL Wallet is no longer possible
Description	A participant selects the unlink device functionality in the CREDENTIAL Wallet. The Wallet presents him a list of all associated devices with his account. He selects one device and confirms his decision.
Image	

A.1.5 Cryptography

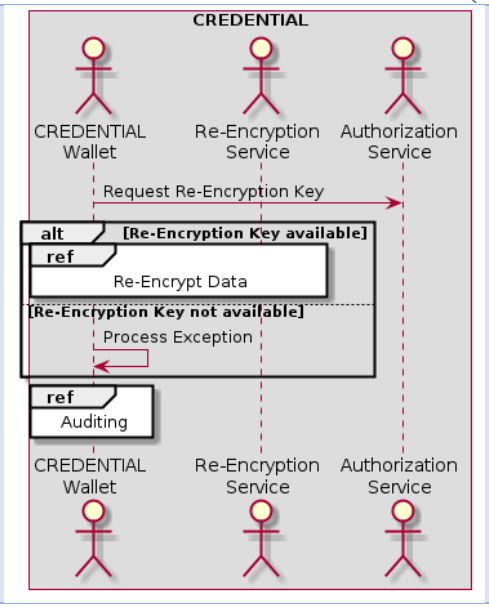
A.1.5.1 Generate new access-key for CREDENTIAL Wallet

Use Case Name	Generate new access-key for CREDENTIAL Wallet
ID	G-BUC-GENACCESSKEY
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- User has a CREDENTIAL Account
Post-conditions	- User has a new main key-pair for accessing the Wallet - Data is re-encrypted according to the new key-pair - A new recovery key is generated - Re-Encryption Keys with old identity are update to new identity
Description	Whenever a participant registers a CRDENTIAL account a public and private key are generated and stored in the participant's IT system. After some time there are several reasons that could trigger the need to generate a new public and private key pair: i.e. a security policy. For these cases, the participant may trigger the generation of a new key pair. A human interaction is possible with participant's IT system.
Image	

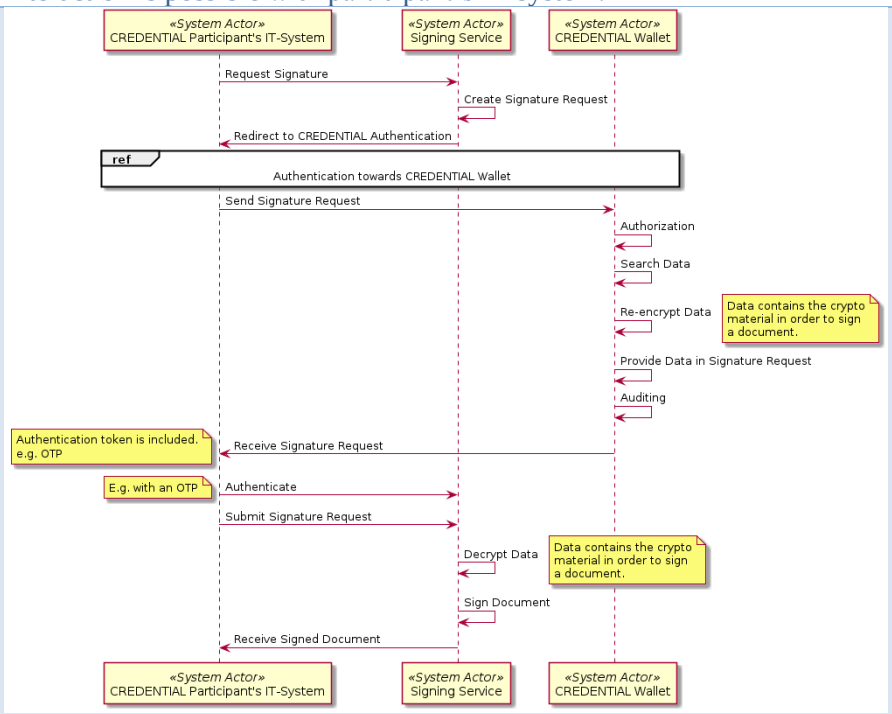
A.1.5.2 Generate new Recovery Key

Use Case Name	Generate new Recovery Key
ID	G-BUC-GENRECKEY
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet - CREDENTIAL Participant's Cold Storage
Pre-conditions	- Participant has changed his master key in the CREDENTIAL Wallet
Post-conditions	- New Recovery Private Key is stored in cold storage - New Recovery Public Key is stored in CREDENTIAL Wallet - New Recovery Public Key is associated with the participant's identification within the CREDENTIAL Wallet
Description	In order to recover the CREDENTIAL Wallet in case of a lost master key a user has to store a recovery key on a cold storage. If he recovers his old identity, he has to create a new recovery key. In addition a new re-encryption key has to be created from his current identity to the recovery key's identity.
Image	

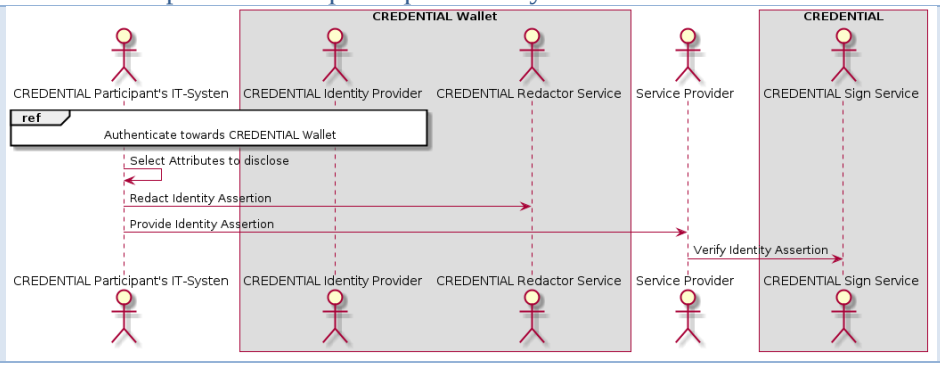
A.1.5.3 Proxy Re-Encryption

Use Case Name	Proxy Re-Encryption
ID	G-BUC-PROXYREENCRYPTION
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Re-Encryption Service - CREDENTIAL Authorization Service
Pre-conditions	- Data set to re-encrypt is available at the CREDENTIAL Wallet - Identifier of data set owner is known to the CREDENTIAL Wallet - Identifier to whom to re-encrypt the data is known - Permission to re-encrypt the data set is available at CREDENTIAL Wallet
Post-conditions	- Data set is re-encrypted in case of Re-Encryption Key is available - Exception is processed in case of Re-Encryption Key is not available
Description	Proxy re-encryption usage is made during the assertion data transmission from several CREDENTIAL network actors (i.e. from IdP to SP).
Image	

A.1.5.4 Remote Signature

Use Case Name	Remote Signature
ID	G-BUC-REMOTESIGNATURE
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- User has stored his PIN in the wallet
Post-conditions	- PIN is re-encrypted for the Signing Service - Document is signed by the Signing Service
Description	A user requests a signature from a signing service. The signing service creates a signature request and sends it back to the user. The user authenticates himself against the wallet. The user generates a proxy-re-encryption key, provides it in the signature request and sends it to the wallet. The wallet performs an authorization. After a successful authorization the wallet searches the encrypted PIN, re-encrypts it for the signing service and sends it back to the user. The user sends an authentication to the signing service and submits the re-encrypted PIN to the signing service. The signing service can decrypt the PIN using CREDENTIAL technology and signs the document. A human interaction is possible with participant's IT system.
Image	

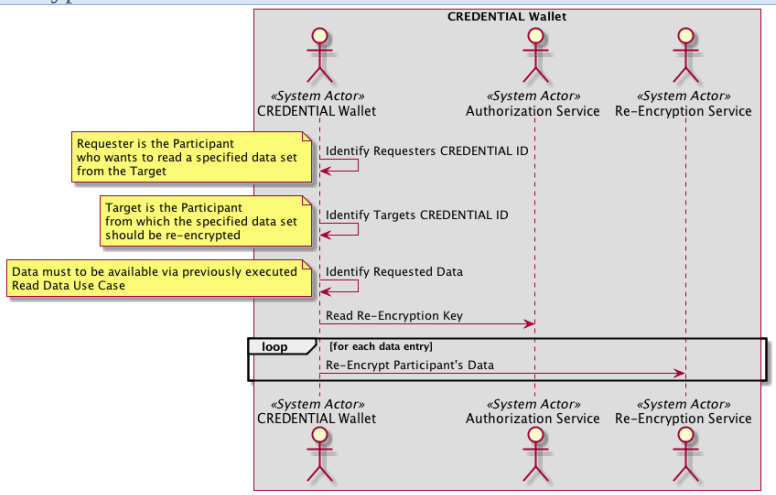
A.1.5.5 Selective Disclosure

Use Case Name	Selective Disclosure
ID	G-BUC-SELECTIVEDISCLOSURE
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Identity Provider - Service Provider - CREDENTIAL Sign Service - CREDENTIAL Redactor Service
Pre-conditions	- User has a CREDENTIAL account - Identity Provider is able to issue an Identity Assertion which is redactable
Post-conditions	- User possesses an Identity Assertion with hidden attributes - Identity Assertion signature is valid - Redacted Identity Assertion signature is valid
Description	During an authentication process, user add or delete some data from an assertion released from an IdP, using malleable signatures techniques. The user sends a redact request to the Redactor Service. The Redactor Service responds with the Identity Assertion including the hidden attributes. The user provides this Identity Assertion in his request to the Service Provider. A human interaction is possible with participant's IT system.
Image	

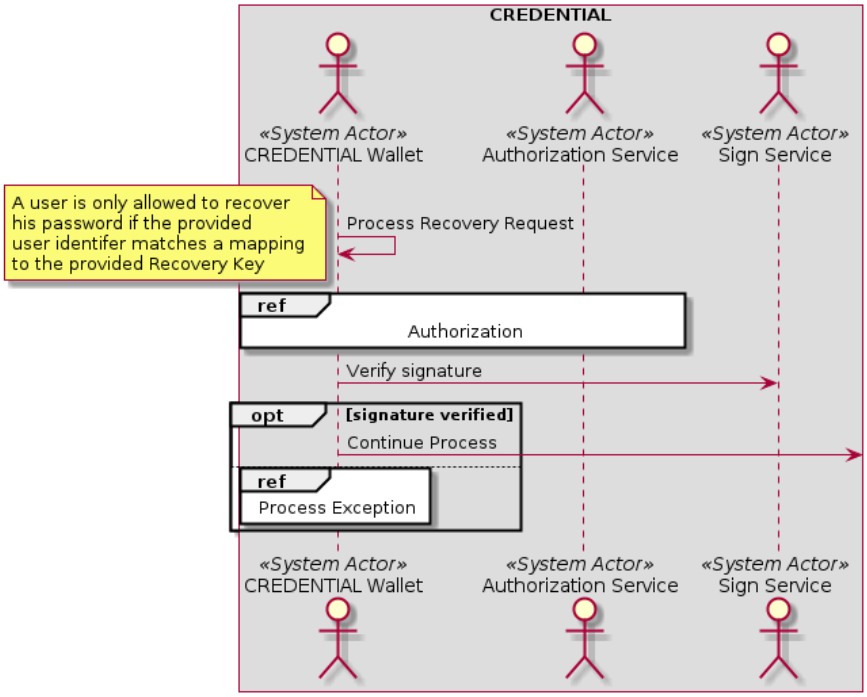
A.2 Generic Logical Use Cases

A.2.1 Data Management

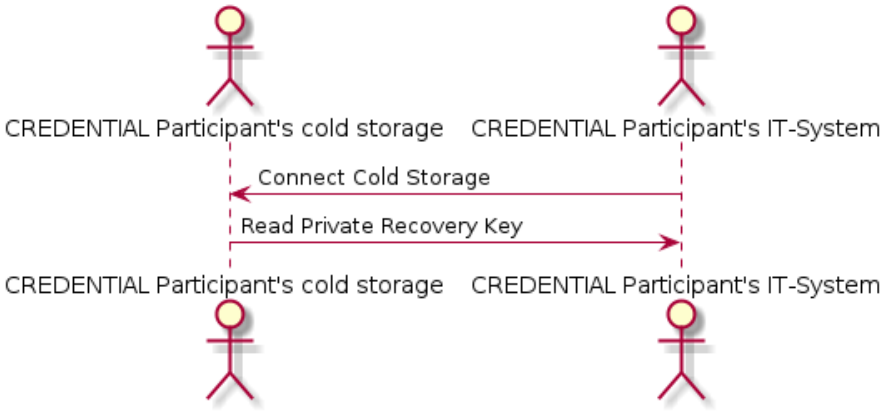
A.2.1.1 Re-Encrypt Data

Use Case Name	Re-Encrypt Data
ID	G-LUC-REENCDATA
LUC_in	- Read Data - Proxy re-encryption - Recover CREDENTIAL Wallet data - Remote Signature - Export data from wallet - Generate new access-key for CREDENTIAL Wallet - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Authorization Service - CREDENTIAL Re-Encryption Service
Pre-conditions	- Target Identifier is available to the wallet - Requester Identifier is available to the wallet - The requested data set is available to the wallet - A Read Access Rule on the specified data set for the requester exists. - A Re-Encryption Key from the Target to the Requester exists.
Post-conditions	- The Data is re-encrypted for the Requester
Description	The specified data set of the CREDENTIAL Wallet is re-encrypted from the target to the requester. The requester is the participant who wants to receive the data. The target is the participant from which the data set should be re-encrypted.
Image	

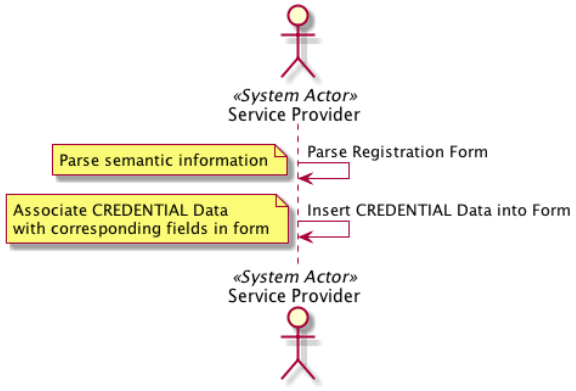
A.2.1.2 Verify Recovery Request

Use Case Name	Verify Recovery Request
ID	G-LUC-VERIFYRECOVERYREQUEST
LUC_in	Recover CREDENTIAL Wallet data
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Authorization Service - Sign Service
Pre-conditions	- Recovery Request is available at the Wallet
Post-conditions	- Recovery Request has been verified
Description	A recovery request has to be verified in order to proceed with the recovery process. A user is only allowed to change the key if the associated recovery key in the request matches a mapping between this id and the user's identification. This is checked by querying the Authorization Service. If this checks succeeds the signature of the request is verified. If the signature is valid and verified the recovery process can continue.
Image	

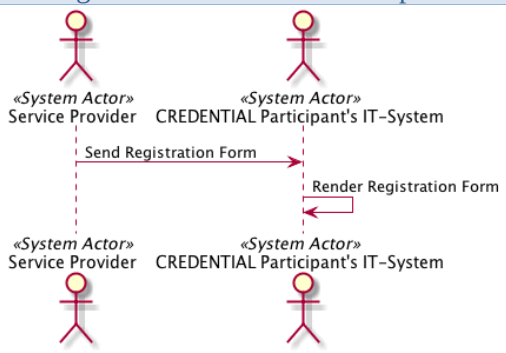
A.2.1.3 Read Recovery Private Key

Use Case Name	Read Recovery Private Key
ID	G-LUC-READRECOVERYPRIVKEY
LUC_in	Recover CREDENTIAL Wallet data
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Participant's Cold Storage
Pre-conditions	- Cold Storage available with recovery key on it
Post-conditions	- Recovery Key is available at the CREDENTIAL Participant's IT-System
Description	A participant reads his recovery private key from a cold storage. For example by using a USB stick or scanning a barcode.
Image	

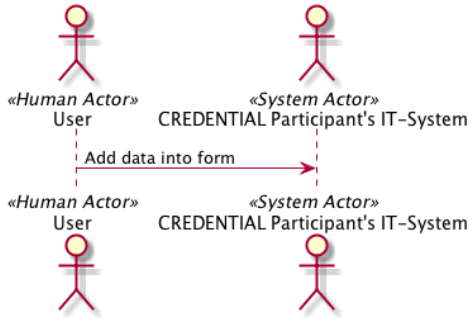
A.2.1.4 Fill Registration Form

Use Case Name	Fill Registration Form
ID	G-LUC-FILLREGFORM
LUC_in	Export CREDENTIAL Wallet data into form
Main Actor	- Service Provider
Secondary Actors	
Pre-conditions	- The Service Providers received data from the CREDENTIAL Wallet - Data is decrypted
Post-conditions	- The registration form is filled with the CREDENTIAL Wallet data - Registration form is unencrypted
Description	The Service Provider processes the CREDENTIAL Wallet data he receives and fills the data in a registration form.
Image	

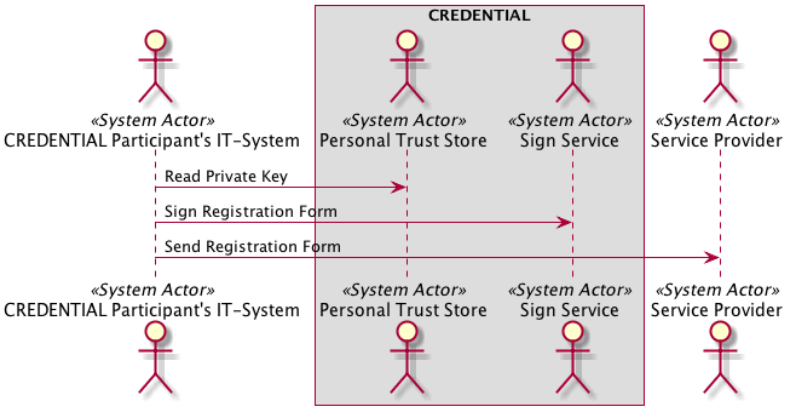
A.2.1.5 Render Registration Form

Use Case Name	Render Registration Form
ID	G-LUC-RENDERREGFORM
LUC_in	Export CREDENTIAL Wallet data into form
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Registration Form is enriched with CREDENTIAL data
Post-conditions	- Registration Form is rendered to the User
Description	The registration form to a service provider is rendered to the user.
Image	

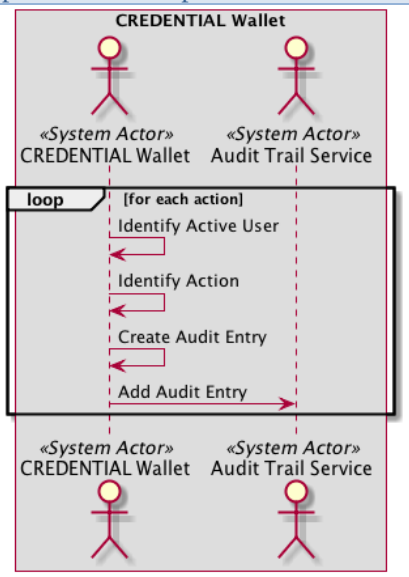
A.2.1.6 Add additional attributes in Registration Form

Use Case Name	Add additional attributes in Registration Form
ID	G-LUC-ADDATTRIBUTSREGFORM
LUC_in	Export CREDENTIAL Wallet data into form
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Registration Form is rendered to the User
Post-conditions	- Registration Form is enriched with user provided attributes
Description	The user adds additional attributes in a registration form.
Image	

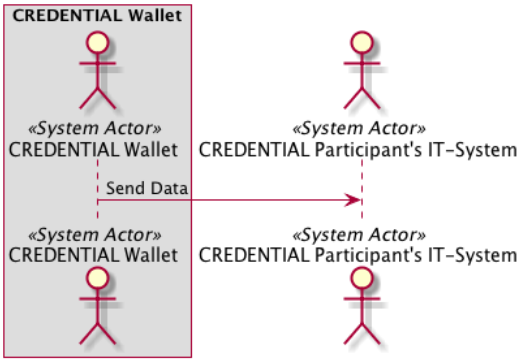
A.2.1.7 Submit Registration Form

Use Case Name	Submit Registration Form
ID	G-LUC-SUBMITREGFORM
LUC_in	Export CREDENTIAL Wallet data into form
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Sign Service - CREDENTIAL Personal Trust Store - Service Provider
Pre-conditions	- User has a CREDENTIAL account
Post-conditions	- Registration Form is sent to the Service Provider - Registration Form is signed by the User
Description	The user submits a registration form filled with CREDENTIAL Wallet data and self-added information to the Service Provider.
Image	

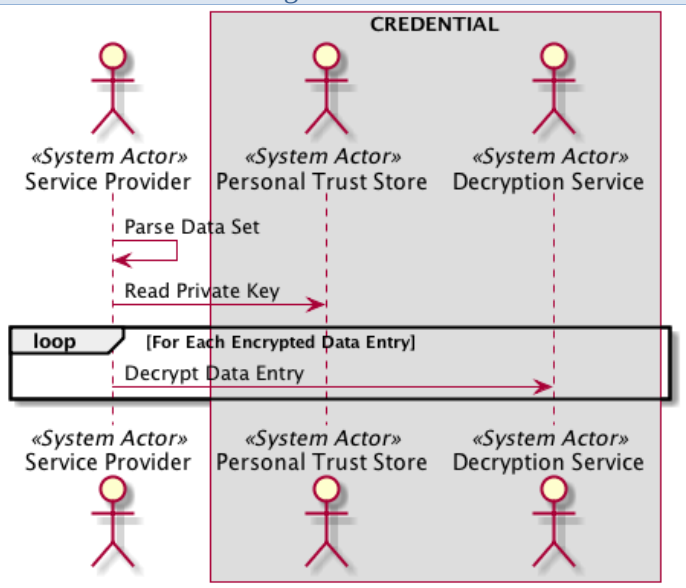
A.2.1.8 Auditing

Use Case Name	Auditing
ID	G-LUC-AUDITING
LUC_in	Request Access Rights
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Audit Trail Service
Pre-conditions	- Active User is known to the wallet
Post-conditions	- For each action an audit entry was created
Description	The CREDENTIAL Wallet performs auditing of every previous action in a specific session performed on the CREDENTIAL Wallet.
Image	

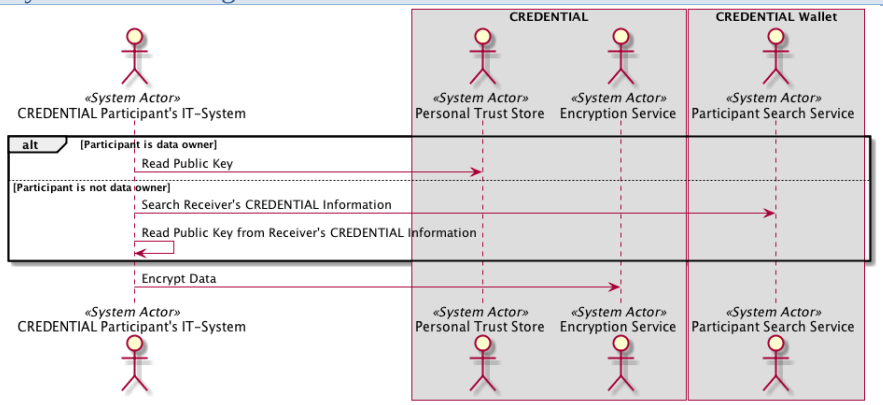
A.2.1.9 Receive Data

Use Case Name	Receive Data
ID	G-LUC-RECDATA
LUC_in	Read Data
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	
Post-conditions	
Description	The CREDENTIAL Participant's IT-System receives the re-encrypted data from the CREDENTIAL Wallet.
Image	

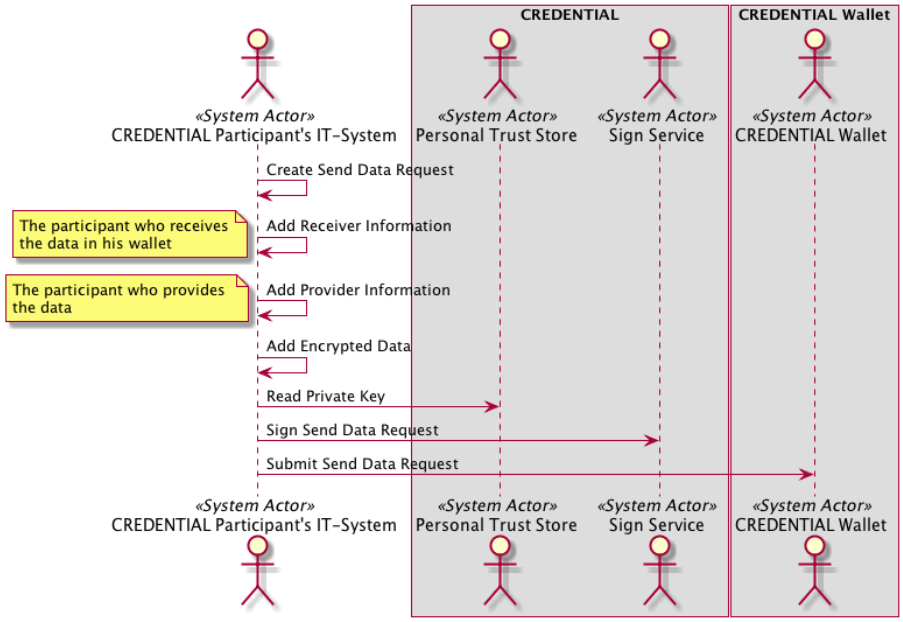
A.2.1.10 Decrypt Data

Use Case Name	Decrypt Data
ID	G-LUC-DECDATA
LUC_in	- Read Data - Export data from wallet
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Decryption Service
Pre-conditions	- The Service Provider has a CREDENTIAL Account - The data is decrypted for the Participant - The data is encrypted with a proxy-re-encryption schema
Post-conditions	- The Service Provider can read the data
Description	The CREDENTIAL Participant's IT-System decrypts the data using CREDENTIAL technologies.
Image	

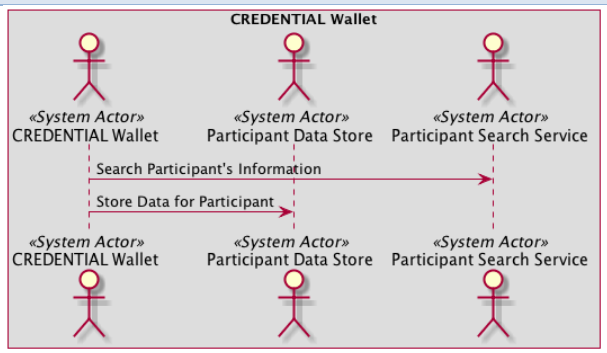
A.2.1.11 Encrypt Data using CREDENTIAL

Use Case Name	Encrypt Data using CREDENTIAL
ID	G-LUC-ENCDATACREDENTIAL
LUC_in	- Send Data - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Encryption Service - CREDENTIAL Personal Trust Store - CREDENTIAL Participant Search Service
Pre-conditions	- Participant has a CREDENTIAL Account - Participant can identify the data owner
Post-conditions	- Data is encrypted for the data owner
Description	A CREDENTAL Participant encrypts data on his IT-System using CREDENTIAL technology. E.g. encrypting medical data using proxy-re-encryption-enabled cryptographic key material and algorithms.
Image	

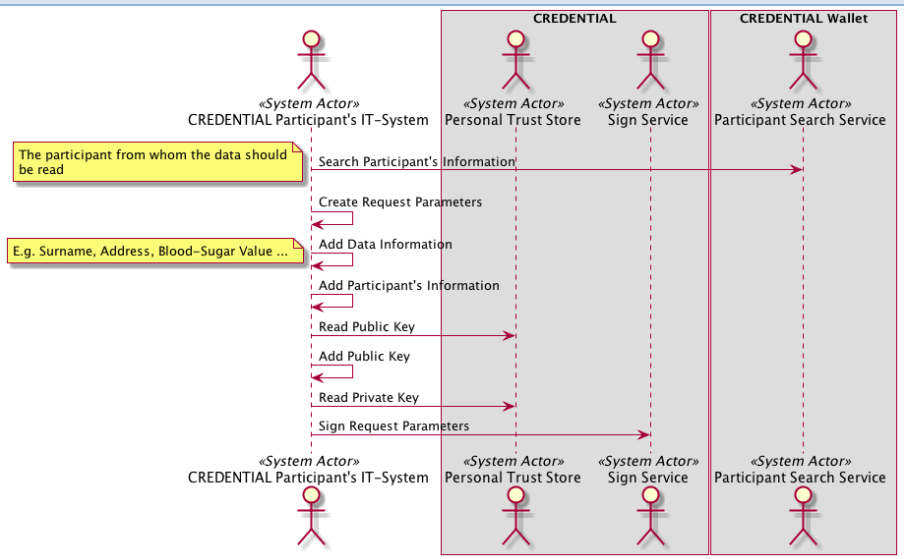
A.2.1.12 Send Encrypted Data

Use Case Name	Send Encrypted Data
ID	G-LUC-SENDENCDATA
LUC_in	- Send Data - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet - CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service
Pre-conditions	- Data is encrypted - Receiver's Information is available - Provider's Information is available - Provider has a CREDENTIAL account
Post-conditions	- Send Data Request is available at the wallet
Description	A CREDENTIAL Participant sends encrypted data to the CREDENTIAL Wallet.
Image	

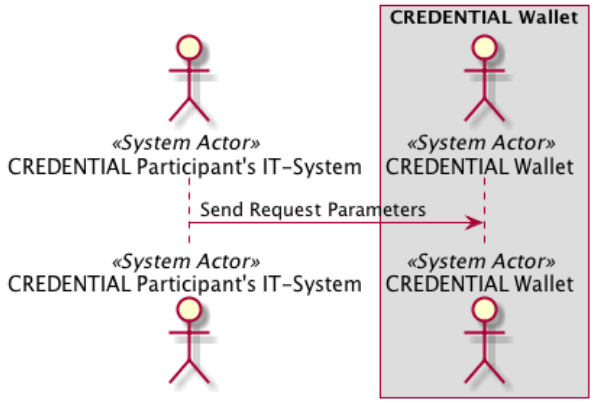
A.2.1.13 Register Data

Use Case Name	Register Data
ID	G-LUC-REGDATA
LUC_in	Send Data
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Data Repository - CREDENTIAL Participant Search Service
Pre-conditions	- Data is encrypted for the user
Post-conditions	- Data is stored for the user in the CREDENTIAL Wallet.
Description	The CREDENTIAL Wallet registers data for a CREDENTIAL user in his data store.
Image	

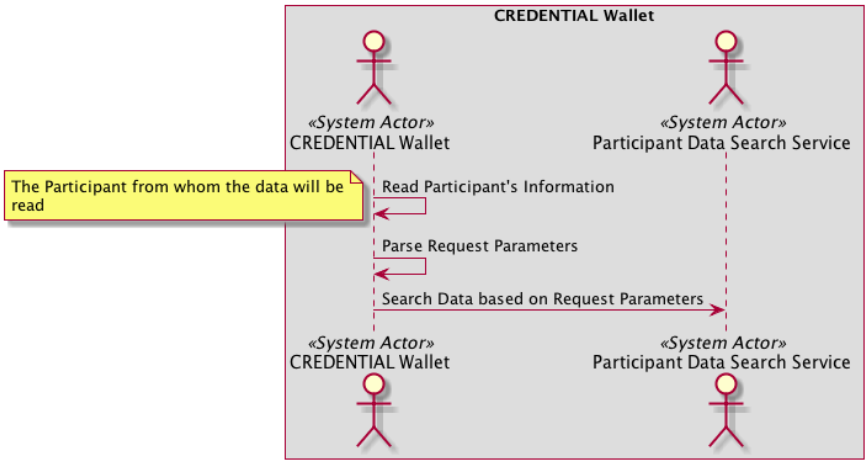
A.2.1.14 Define Request Parameters

Use Case Name	Define Request Parameters
ID	G-LUC-DEFREQPARAMS
LUC_in	Read Data
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service - CREDENTIAL Participant Search Service
Pre-conditions	- Participant from whom the data should be read is known - Requester has a CREDENTIAL Account - Requester has Read Access Rights on the specified data set
Post-conditions	- Request Parameters are created
Description	A CREDENTIAL Participant defines with his IT-System Request Parameters in order to retrieve Data from the Wallet.
Image	

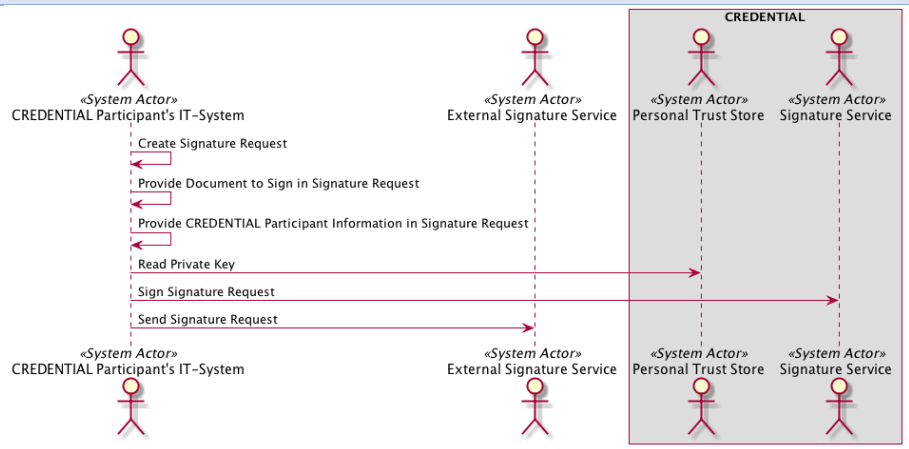
A.2.1.15 Request Data

Use Case Name	Request Data
ID	G-LUC-REQDATA
LUC_in	Read Data
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Request Parameters have been defined
Post-conditions	- Request Parameters are sent to the wallet
Description	A CREDENTIAL Participant's IT-System requests data from the Wallet.
Image	

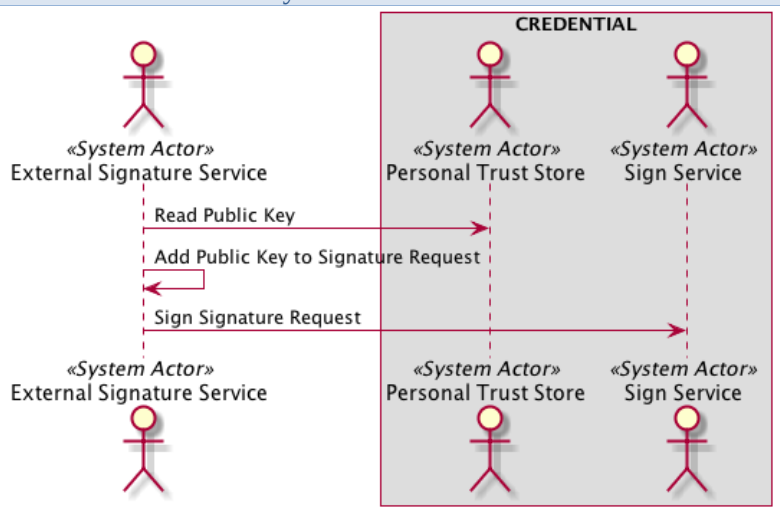
A.2.1.16 Search Data

Use Case Name	Search Data
ID	G-LUC-SEARCHDATA
LUC_in	- Read Data - Remote Signature - Export data from wallet
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Data Search Service
Pre-conditions	- Request Parameters are available to the CREDENTIAL Wallet
Post-conditions	- Data specified in the Request Parameters have been read from the Data Search Service
Description	The CREDENTIAL Wallet searches for the requested data specified by the given request parameters.
Image	

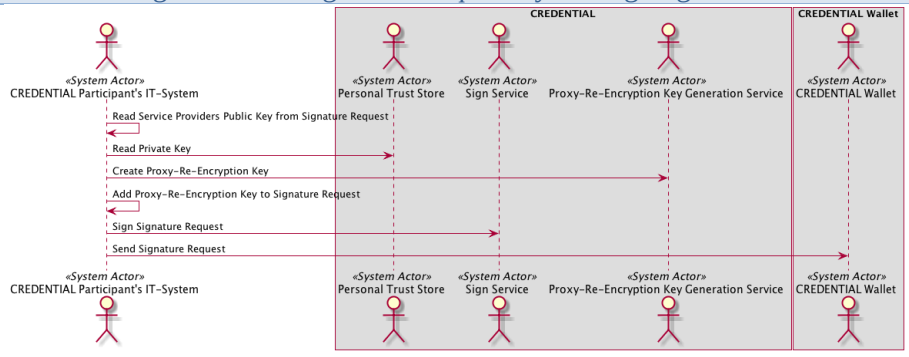
A.2.1.17 Request Signature

Use Case Name	Request Signature
ID	G-LUC-REQSIGN
LUC_in	Remote Signature
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service - External Signature Service
Pre-conditions	- The Participant has a CREDENTIAL account - The External Signature Service has a CREDENTIAL account
Post-conditions	- The Signature Request is available at the External Signature Service
Description	A CREDENTIAL Participant requests a signature from an external signing service.
Image	

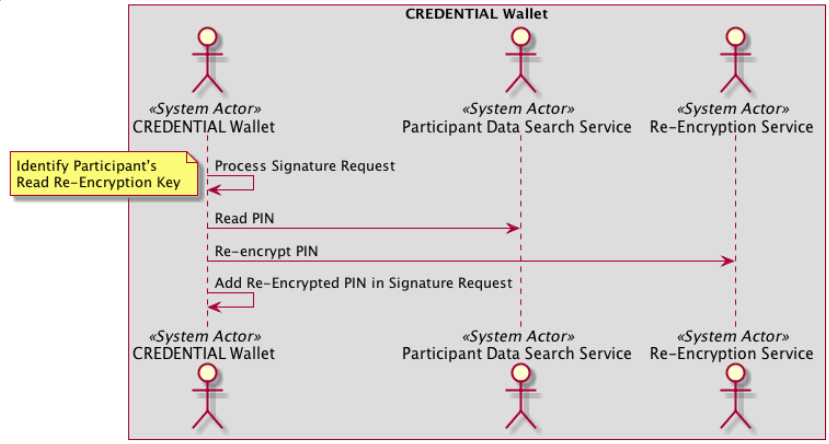
A.2.1.18 Create Signature Request

Use Case Name	Create Signature Request
ID	G-LUC-CREATESIGNREQ
LUC_in	Remote Signature
Main Actor	- External Signature Service
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service
Pre-conditions	- The External Signing Service has a CREDENTIAL Account - The external Signing Service has received a Signature Request
Post-conditions	- The Signature Request is enriched with the External Signing Service Public Key - The Signature Request is signed by the External Signing Service
Description	A Signing Service creates a Signature Request including his CREDENTIAL Identifier and Public Key.
Image	

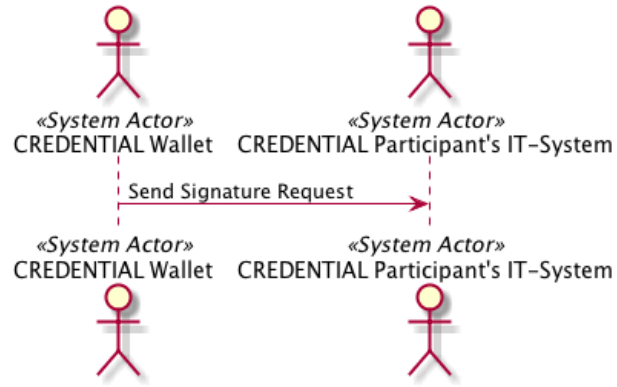
A.2.1.19 Provide Signature Request

Use Case Name	Provide Signature Request
ID	G-LUC-PROVSIGNREQ
LUC_in	Remote Signature
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service - CREDENTIAL Re-Encryption Key Generation Service
Pre-conditions	- Signature Request from the external Signing Service is available at the Participant's IT-System
Post-conditions	- Signature Request is signed by the CREDENTIAL Participant
Description	A CREDENTIAL Participant provides via his IT-System a signature request to the CREDENTIAL Wallet. He creates a Re-Encryption Key based on the Information given in the Signature Request by the Signing Service.
Image	

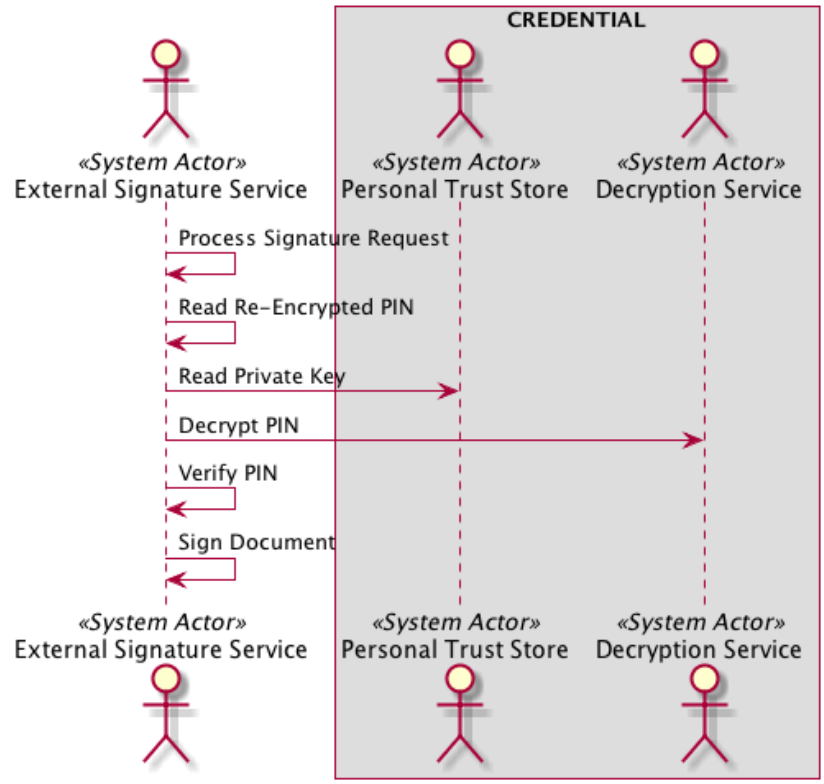
A.2.1.20 Provide Data in Signature Request

Use Case Name	Provide Data in Signature Request
ID	G-LUC-PROVDATASIGNREQ
LUC_in	Remote Signature
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Data Search Service - CREDENTIAL Re-Encryption Service
Pre-conditions	- Signature Request is available at the wallet
Post-conditions	- Signature Request is enriched with re-encrypted PIN
Description	The CREDENTIAL Wallet provides the re-encrypted data, e.g. the PIN, in the signature request.
Image	

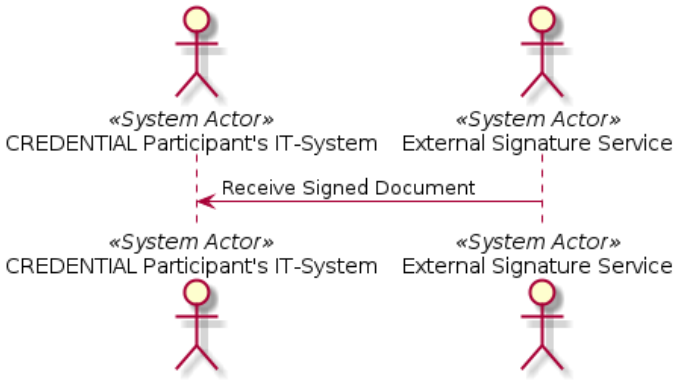
A.2.1.21 Receive Signature Request

Use Case Name	Receive Signature Request
ID	G-LUC-RECSIGNREQ
LUC_in	Remote Signature
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	
Post-conditions	
Description	The CREDENTIAL Participant receives the signature request with the enriched re-encrypted data, e.g. the PIN.
Image	

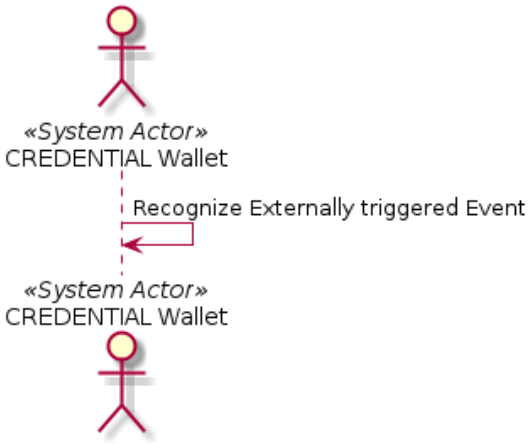
A.2.1.22 Sign Document

Use Case Name	Sign Document
ID	G-LUC-SIGNDOC
LUC_in	Remote Signature
Main Actor	- External Signature Service
Secondary Actors	- CREDENTIAL Decryption Service - CREDENTIAL Personal Trust Store
Pre-conditions	- Signature Request with Re-Encrypted PIN is available
Post-conditions	- Document is signed - PIN was verified by the external Signature Service
Description	The Signing Services signs the specified document.
Image	

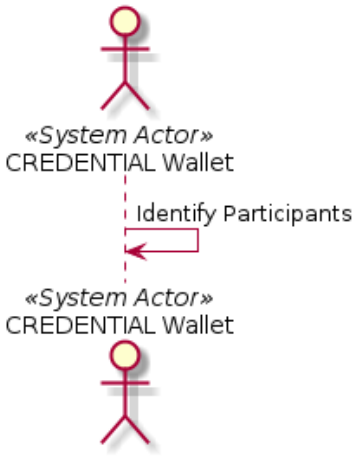
A.2.1.23 Receive Signed Document

Use Case Name	Receive Signed Document
ID	G-LUC-RECSIGNDOC
LUC_in	Remote Signature
Main Actor	- External Signature Service
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant initiated signature of a document - External Signature Service computed signature over document
Post-conditions	- Signed document is available at the Participant's IT-System
Description	The CREDENTIAL Participant's IT-System receives the signed document from the signature service.
Image	

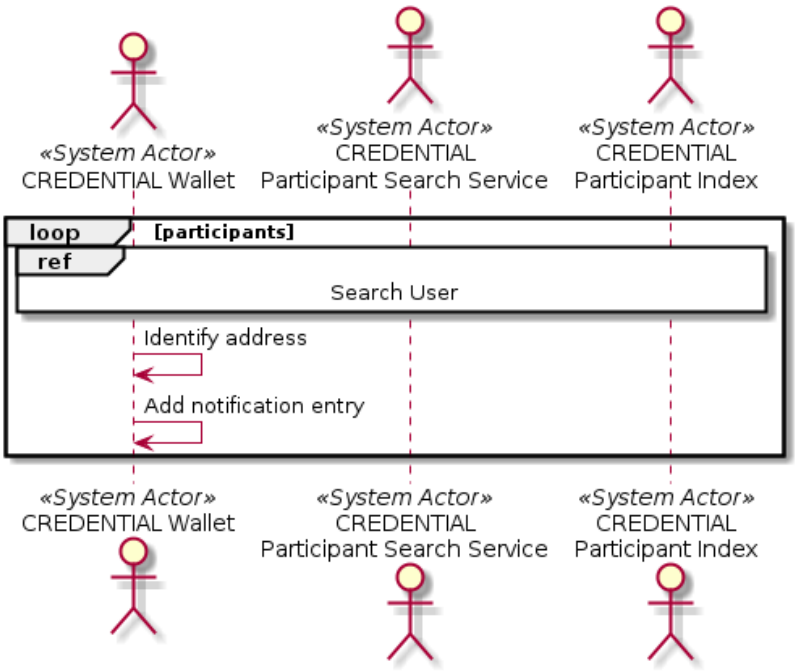
A.2.1.24 Recognize Externally triggered Event

Use Case Name	Recognize Externally triggered Event
ID	G-LUC-RECEXTTRIGEVENT
LUC_in	Send Notification
Main Actor	- CREDENTIAL Wallet
Secondary Actors	
Pre-conditions	- Event occurred in the CREDENTIAL Wallet
Post-conditions	- Event is recognized for the Notification process flow
Description	The CREDENTIAL Wallet recognizes an externally triggered event. E.g. reading of data, writing of data, granting access rights ...
Image	

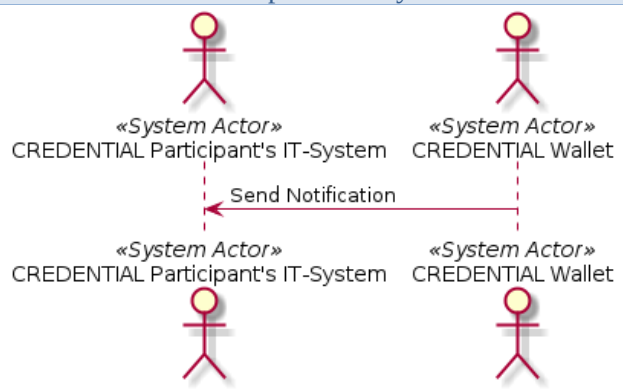
A.2.1.25 Evaluate Notification Configuration

Use Case Name	Evaluate Notification Configuration
ID	G-LUC-EVALNOTIFYCONF
LUC_in	Send Notification
Main Actor	- CREDENTIAL Wallet
Secondary Actors	
Pre-conditions	- An event occurred in the CREDENTIAL Wallet
Post-conditions	- The List of participants who needs to receive a notification are known
Description	The CREDENTIAL Wallet evaluates the notification configuration if the triggered event might trigger one or multiple notifications.
Image	

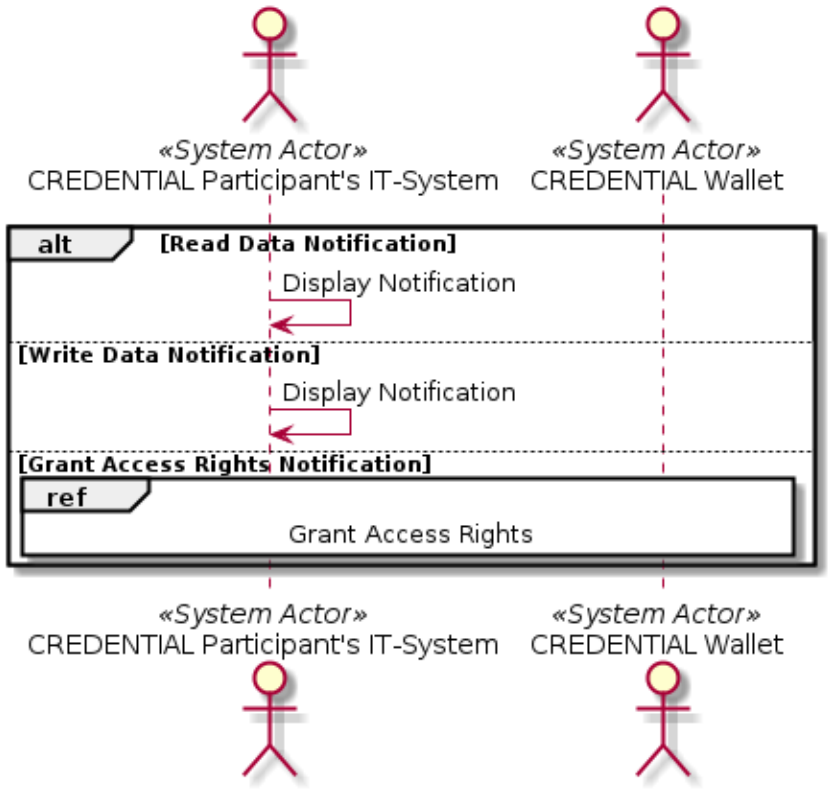
A.2.1.26 Create Notification List

Use Case Name	Create Notification List
ID	G-LUC-CREATENOTIFYLIST
LUC_in	Send Notification
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Search Service
Pre-conditions	- Participant who receives a notification are known
Post-conditions	- List of notifications is created - Addresses of recipient is contained in notification list
Description	The CREDENTIAL Wallet creates a notification list containing the recipients who will receive a notification triggered by an event.
Image	

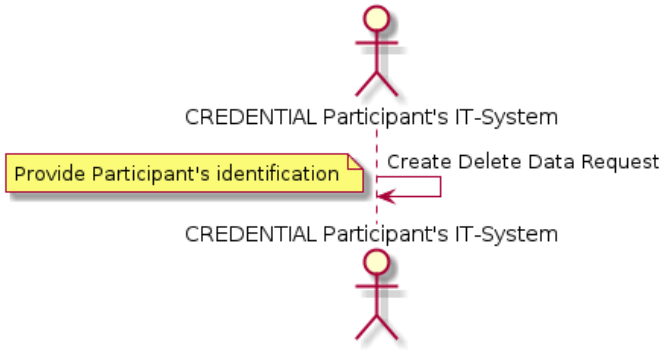
A.2.1.27 Send Notification

Use Case Name	Send Notification
ID	G-LUC-SENDNOTIFY
LUC_in	- Send Notification - Link Service Provider account with CREDENTIAL account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Notification occurred in the CREDENTIAL Wallet about particular event - Participant needs to be informed about event - Participant's IT-System address is known
Post-conditions	- Notification is available at the Participant's IT-System
Description	The CREDENTIAL Wallet sends a notification about an event to a CREDENTIAL Participant's IT-System.
Image	

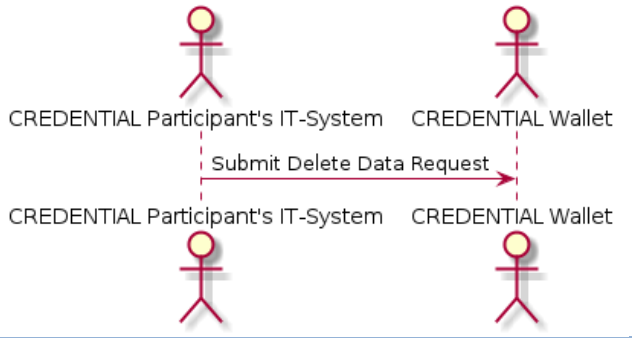
A.2.1.28 Process Notification

Use Case Name	Process Notification
ID	G-LUC-PROCNOTIFY
LUC_in	Send Notification
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Notification available at the IT-System
Post-conditions	- Further process flows have been triggered
Description	The CREDENTIAL Participant's IT-System processes a notification. A notification is generic and can be information about reading of data, writing of data or requesting of access rights. The participant's IT-System has to detect the kind of notification and trigger the further process flows. This logical use case triggers other business use cases. Human interaction may be possible.
Image	

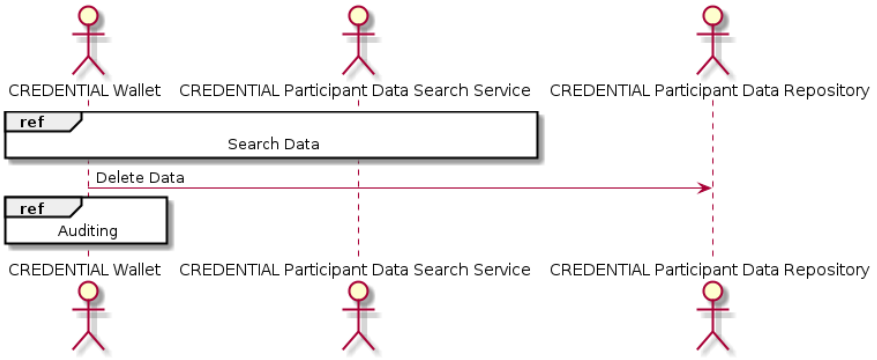
A.2.1.29 Create Delete Data Request

Use Case Name	Create Delete Data Request
ID	G-LUC-CREATEDELDATAREQ
LUC_in	Delete data set
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	
Pre-conditions	- Participant's Identifier is known
Post-conditions	- Delete Data Request is created
Description	The CREDENTIAL Participant's IT-System creates a delete data request.
Image	

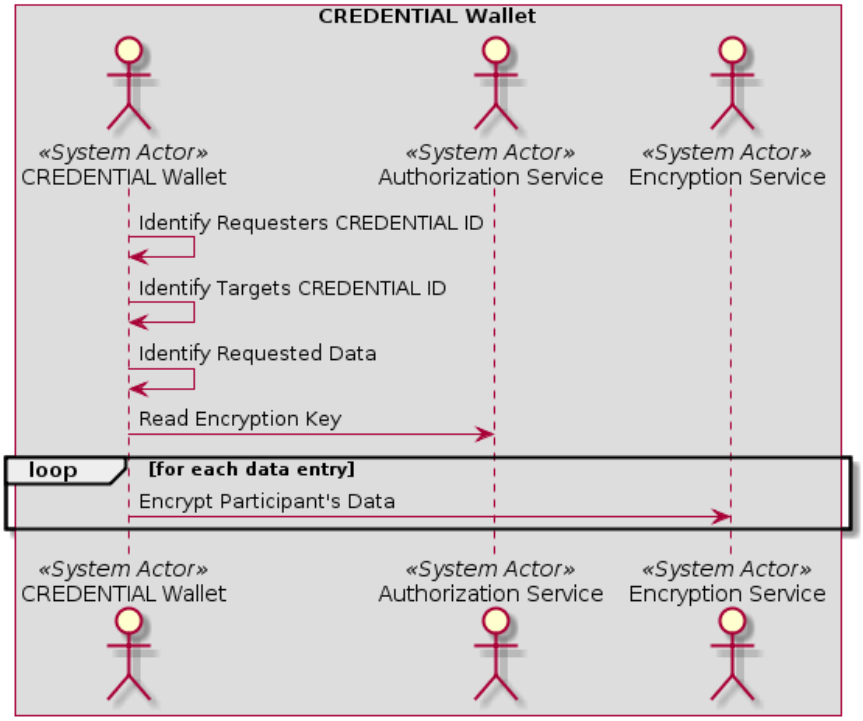
A.2.1.30 Submit Delete Data Request

Use Case Name	Submit Delete Data Request
ID	G-LUC-SUBMITDELDATAREQ
LUC_in	Delete data set
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Participant has created a Delete Data Request
Post-conditions	- Delete Data Request is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Participant's IT-System sends the delete data request to the CREDENTIAL Wallet.
Image	

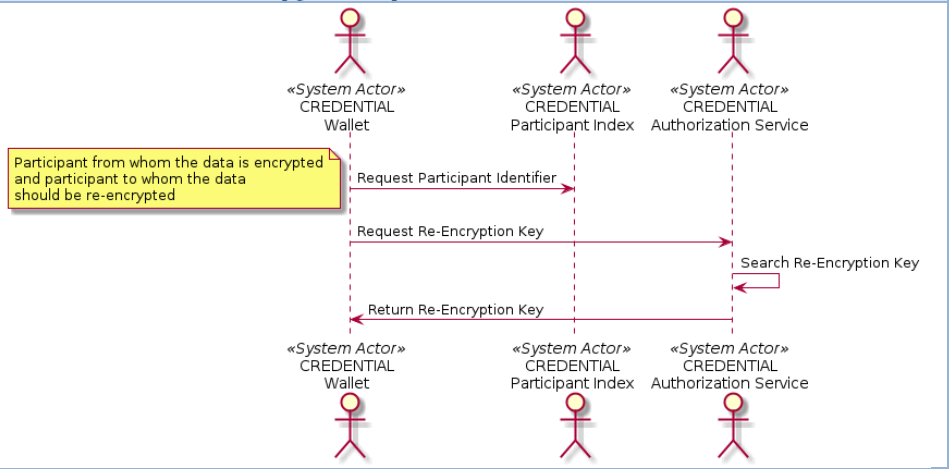
A.2.1.31 Delete Data

Use Case Name	Delete Data
ID	G-LUC-DELDATA
LUC_in	Delete data set
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Data Search Service - CREDENTIAL Data Repository Provider
Pre-conditions	- Participant's Identifier is known - Data set to delete is known - Participant is allowed to delete data set
Post-conditions	- Data set is deleted.
Description	The CREDENTIAL Wallet deletes the specified data. The identifier of the data is searched through the Data Search Service. With the identifier the delete operation at the Data Repository is triggered.
Image	

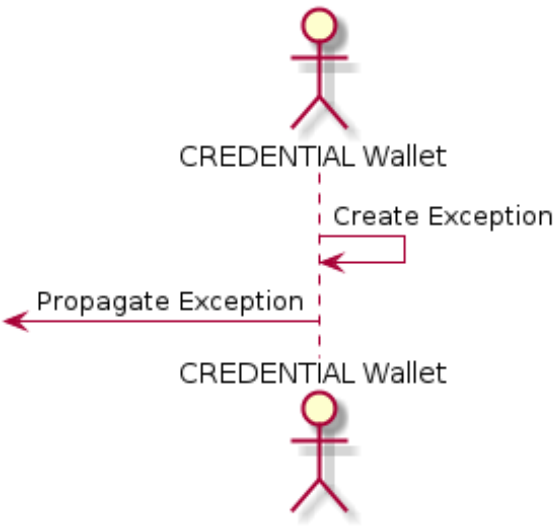
A.2.1.32 Encrypt Data

Use Case Name	Encrypt Data
ID	G-LUC-ENCDATA
LUC_in	
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Authorization Service - CREDENTIAL Encryption Service
Pre-conditions	- Target Identifier is available to the CREDENTIAL - Requester Identifier is available to the CREDENTIAL - The requested data set is available to the CREDENTIAL - A Read Access Rule on the specified data set for the requester exists. - A Re-Encryption Key from the Target to the Requester exists.
Post-conditions	- The Data is encrypted for the Requester
Description	The specified data set of the CREDENTIAL Wallet is encrypted from the target to the requester. The requester is the participant who wants to receive the data. The target is the participant from which the data set should be encrypted.
Image	

A.2.1.33 Request Re-Encryption Key

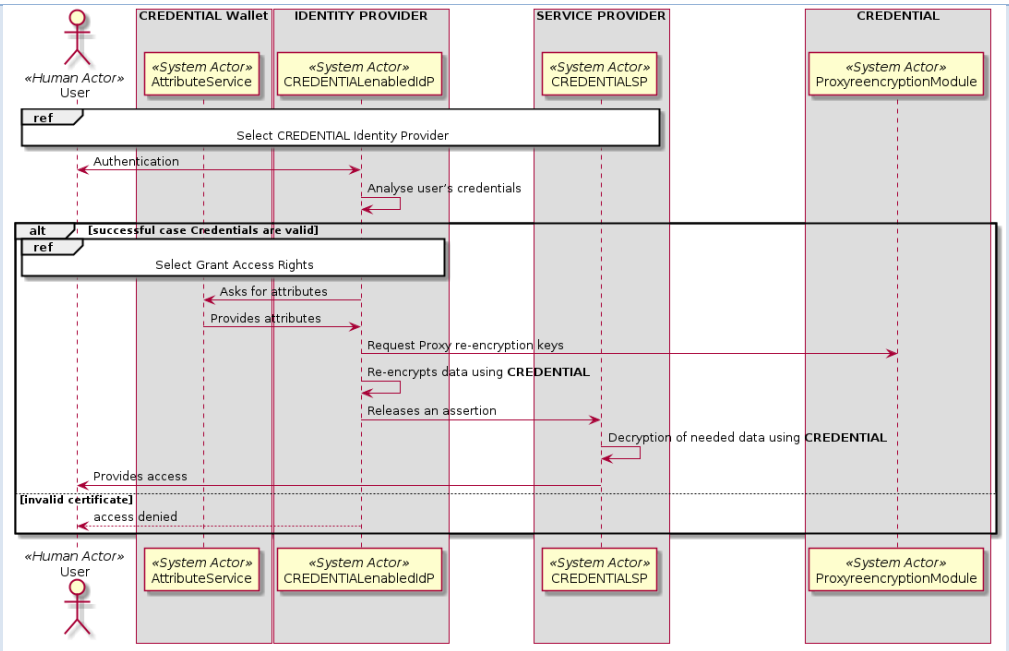
Use Case Name	Request Re-Encryption Key
ID	G-LUC-REQREK
LUC_in	Proxy Re-Encryption
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Index - CREDENTIAL Authorization Service
Pre-conditions	- Information about participant's to find there identifier is available at the CREDENTIAL Wallet
Post-conditions	- Re-Encryption Key is available at the CREDENTIAL Wallet
Description	In order to process a proxy-re-encryption the CREDENTIAL Wallet needs a Proxy-Re-Encryption Key. Usually a Proxy-Re-Encryption Key is associated with a participant from whom data is encrypted and a participant to whom the data will be re-encrypted. With this information a CREDENTIAL Wallet is able to receive a re-encryption key from the Authorization Service.
Image	

A.2.1.34 Process Exception

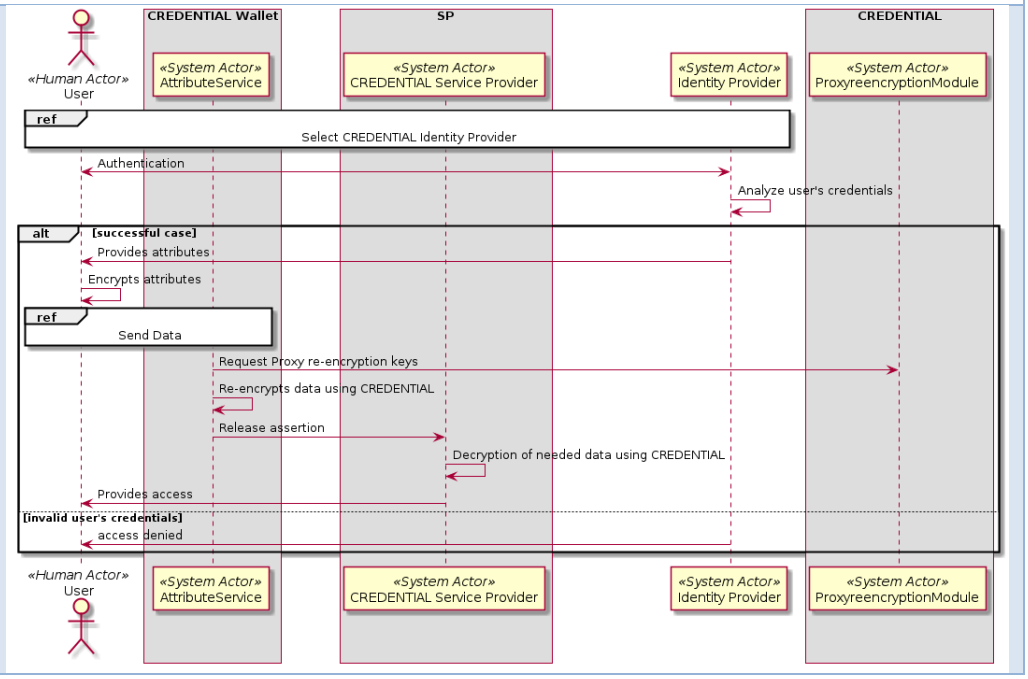
Use Case Name	Process Exception
ID	G-LUC-PROCEXC
LUC_in	Proxy Re-Encryption
Main Actor	- CREDENTIAL Wallet
Secondary Actors	
Pre-conditions	- An exception occurs - Originator of the most recent request is known
Post-conditions	- Exception has been propagated to the most recent request originator
Description	If an exception occurs in a use case the CREDENTIAL Wallet has to provide an exception with enough information to the most recent originator of a request to the CREDENTIAL Wallet. For example, a user wants to request data but is not allowed to read the data. Then an exception has to be propagated to the user.
Image	

A.2.2 Authentication

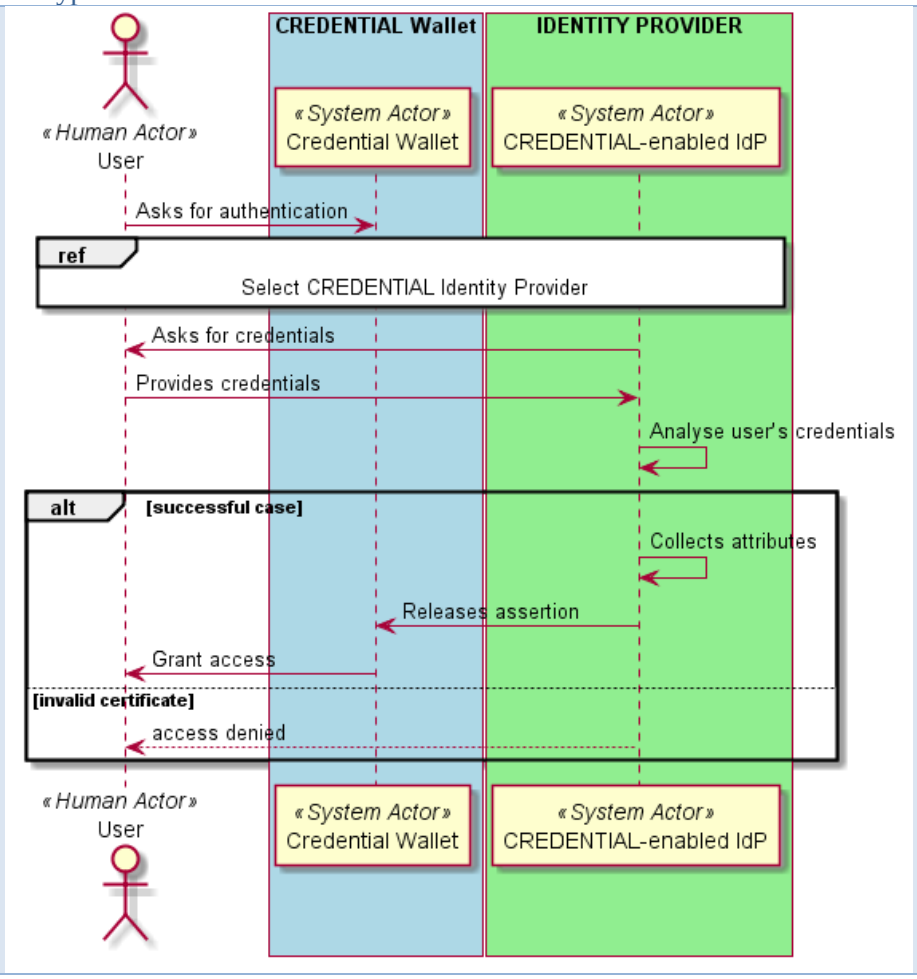
A.2.2.1 Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP

Use Case Name	**Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL- enabled IdP**
ID	G-LUC-AUTHSPUSINGWALLETENABLEDIDP
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Attribute Service - CREDENTIAL Identity Provider - Service Provider - CREDENTIAL Proxy Re-Encryption Service
Pre-conditions	- A Re-Encryption Key from the User to the Service Provider is available in the CREDENTIAL Wallet or will be generated during the process flow - The SP established a trust relation with the IdP - A list of trusted IdPs is defined
Post-conditions	- Attributes are disclosed to the Service Provider - User is authenticated to the Service Provider
Description	A user authenticates himself against a Service Provider which supports CREDENTIAL technology. He uses a CREDENTIAL-enabled IdP. The attributes inside his Identity Assertion are re-encrypted by the IdP for the CREDENTIAL SP. The attributes are read from the CREDENTIAL Wallet.
Image	

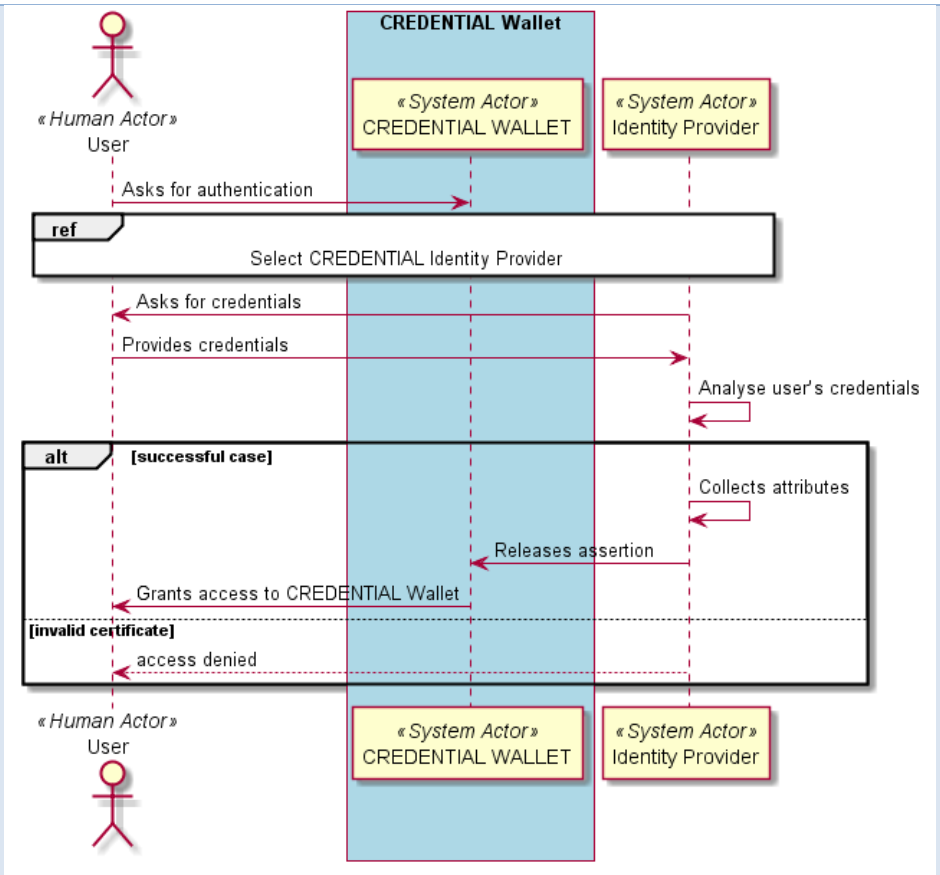
A.2.2.2 Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP

Use Case Name	Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP
ID	G-LUC-AUTHSPUSINGWALLETIDP
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Attribute Service - Service Provider - CREDENTIAL Proxy Re-Encryption Service - IdP Selector - Identity Provider
Pre-conditions	- A Re-Encryption Key from the User to the Service Provider is available in the CREDENTIAL Wallet or will be generated during the process flow. - SP establish a trust relation to the IdP. - A list of trusted IdPs is needed.
Post-conditions	- Attributes are disclosed for the Service Provider - User is authenticated to the Service Provider
Description	A user authenticates himself against a Service Provider which supports CREDENTIAL technology. He uses a normal IdP. The attributes are read from the CREDENTIAL Wallet.
Image	

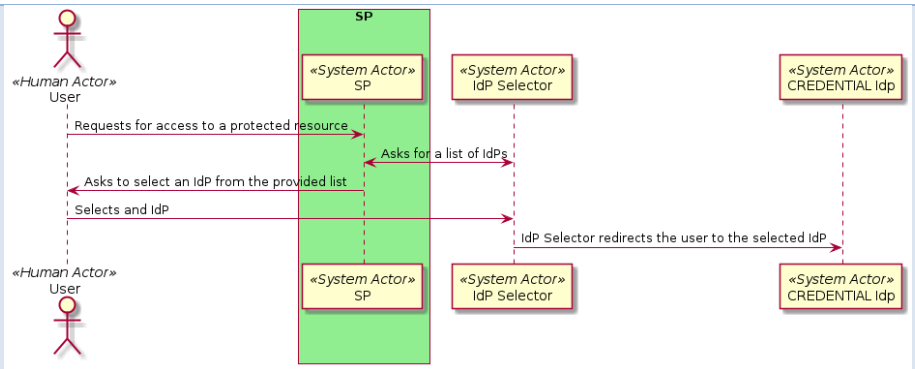
A.2.2.3 Authenticate towards CREDENTIAL Wallet using CREDENTIAL-enabled IdP

Use Case Name	Authenticate towards CREDENTIAL Wallet using CREDENTIAL-enabled IdP
ID	G-LUC-AUTHWALLETUSINGENABLEDIDP
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Proxy Re-Encryption Service - CREDENTIAL Identity Provider
Pre-conditions	- CREDENTIAL Wallet establish a trust relation to the IdP - A list of Trusted IdPs is available
Post-conditions	- User is authenticated to CREDENTIAL Wallet
Description	A user authenticates towards the CREDENTIAL Wallet. He uses a CREDENTIAL-enabled IdP. The attributes inside the assertion are re-encrypted from the IdP to the CREDENTIAL Wallet.
Image	

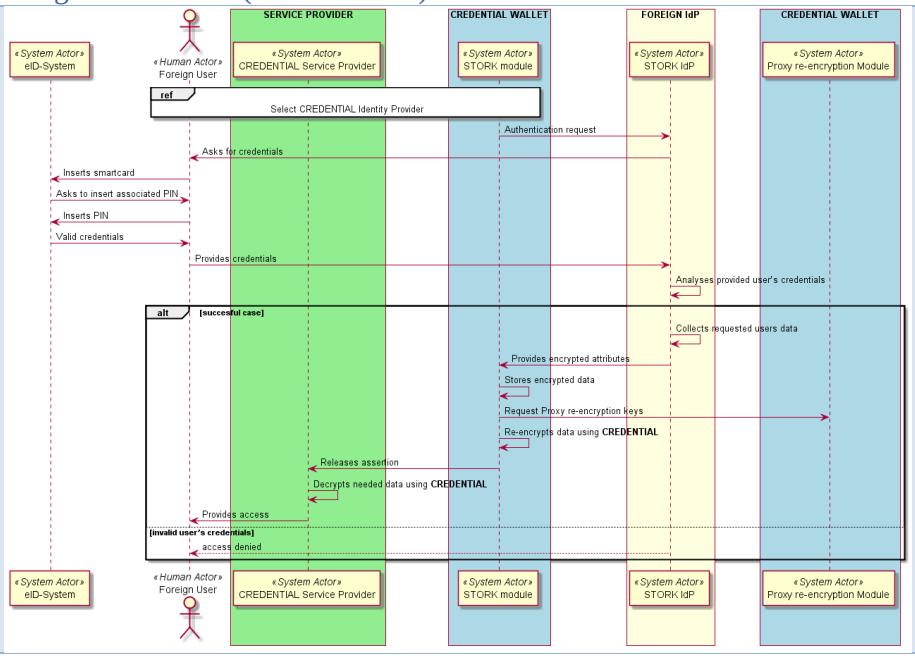
A.2.2.4 Authenticate towards CREDENTIAL Wallet using an external IdP

Use Case Name	Authenticate towards CREDENTIAL Wallet using an external IdP
ID	G-LUC-AUTHWALLETUSINGEXTERNALIDP
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Attribute Service - CREDENTIAL Wallet
Pre-conditions	- CREDENTIAL Wallet establish a trust relation to the IdP - A list of Trusted IdPs is needed - The user has linked the external account with his CREDENTIAL account.
Post-conditions	- User is authenticated to CREDENTIAL Wallet
Description	A user authenticates towards the CREDENTIAL Wallet. He uses an external IdP. The CREDENTIAL Wallet authenticates the user if he has linked the external account with his CREDENTIAL account.
Image	

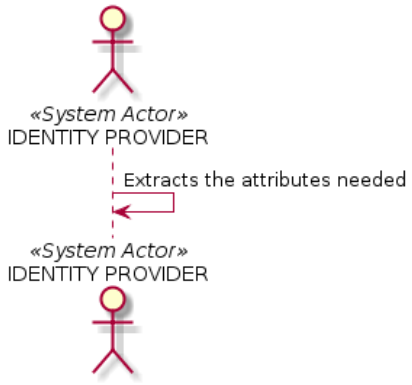
A.2.2.5 Select CREDENTIAL Identity Provider

Use Case Name	Select CREDENTIAL Identity Provider
ID	G-LUC-SELECTCREDIDP
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Identity Provider - IdP Selector - Service Provider
Pre-conditions	- SP establish a trust relation to the IdPs - The SP establish a trust relation to CREDENTIAL Wallet - The user has to be registered in an IdP
Post-conditions	- The user is redirected to the selected IdP
Description	A User tries to get access to a protected resource. The SP asks the IdP Selector for a list of available IdPs. The IdP Selector provides a list of IdPs to the user. The user selects an IdP from the list and the IdP Selector redirects the user to the selected IdP.
Image	

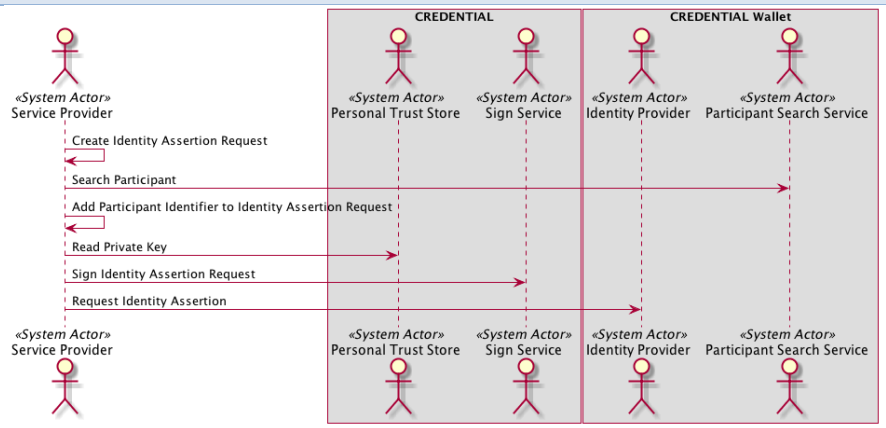
A.2.2.6 Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation

Use Case Name	Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
ID	G-LUC-AUTHSPUSINGWALLETANDIDENTITYFEDERATION
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Wallet - Service Provider - eID-System - STORK module - STORK IdP - CREDENTIAL Proxy Re-Encryption Service - CREDENTIAL Identity Provider
Pre-conditions	- SP establish a trust relation to Federated IdP - User is registered in a Federated IdP
Post-conditions	- The user is authenticated to a Federated IdP
Description	A User tries to authenticate to a CREDENTIAL SP using the CREDENTAIL Wallet and a Federated IdP (STORK). A strong authentication is performed using eID identities (eID smartcard)
Image	

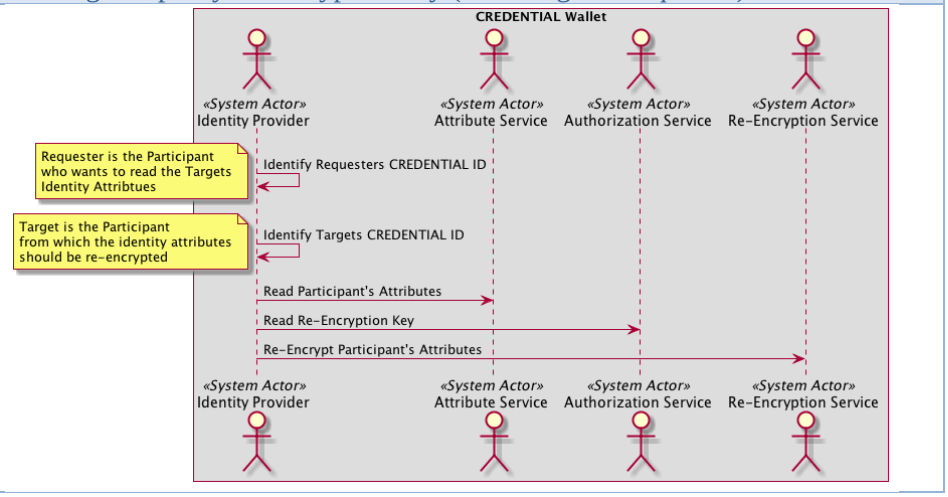
A.2.2.7 Attributes Collection

Use Case Name	Attributes Collection
ID	G-LUC-ATTCOLLECTION
LUC_in	- Authenticate towards CREDENTIAL Wallet using a CREDENTIAL-enabled IdP - Authenticates towards CREDENTIAL Wallet using an external IdP - Authenticates towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- Identity Provider
Secondary Actors	
Pre-conditions	- The User is authenticated in the Identity provider
Post-conditions	- The IdP collects the attributes needed from the user´s credential
Description	The Identity Provider extracts from its database the related information needed from the user´s credentials
Image	

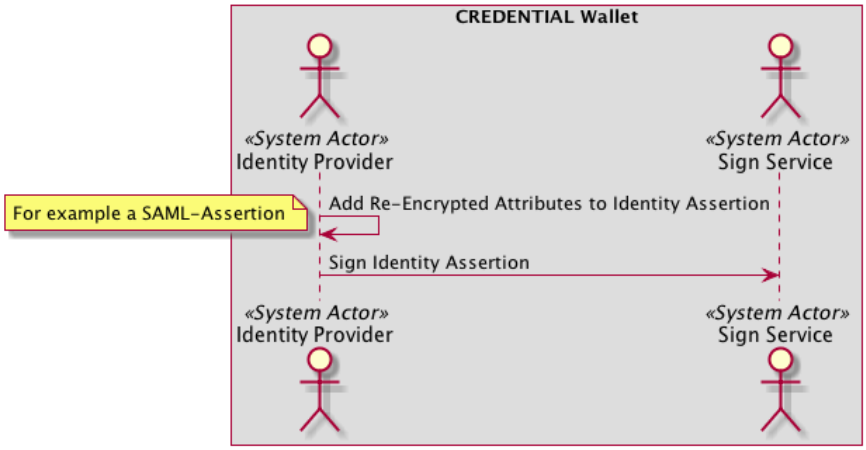
A.2.2.8 Request Identity Assertion

Use Case Name	Request Identity Assertion
ID	G-LUC-REQIDENTIYASSERTION
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service - CREDENTIAL Identity Provider - CREDENTIAL Participant Search Service
Pre-conditions	- Service Provider can identify the user's CREDENTIAL identifier
Post-conditions	- Identity Assertion Request is sent to the CREDENTIAL Identity Provider
Description	A Service Provider requests an Identity Assertion for a user who wants to access his service.
Image	

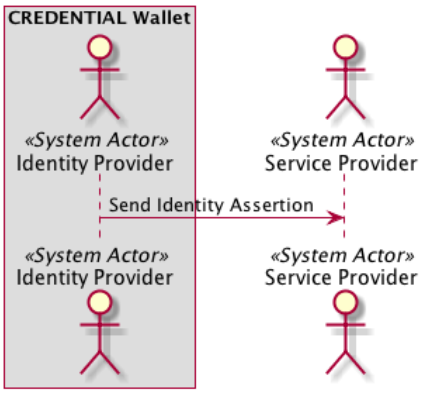
A.2.2.9 Re-Encrypt Attributes

Use Case Name	Re-Encrypt Attributes
ID	G-LUC-ENCATTRIBUTES
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- Identity Provider
Secondary Actors	- CREDENTIAL Attribute Service - CREDENTIAL Authorization Service - CREDENTIAL Proxy Re-Encryption Service
Pre-conditions	- Requesters Information are available to the Identity Provider - Targets Information are available to the Identity Provider - Read Access Rights for the Requester on the Targets Identity Attributes are available at the Authorization Service
Post-conditions	- Identity Attributes are re-encrypted for the Requester
Description	The CREDENTIAL Wallet re-encrypts identity attributes of a user (the target) with a given proxy-re-encryption key (from target to requester).
Image	

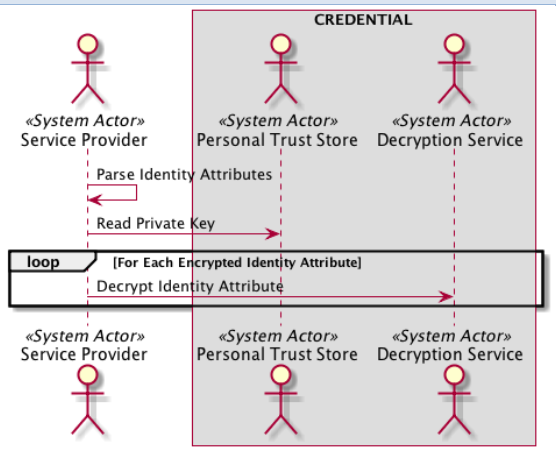
A.2.2.10 Issue Identity Assertion

Use Case Name	Issue Identity Assertion
ID	G-LUC-ISSIDENTITYASSERTION
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- Identity Provider
Secondary Actors	- CREDENTIAL Sign Service
Pre-conditions	- Re-Encrypted Attributes are available to the Identity Provider
Post-conditions	- Re-Encrypted Attributes are added to the Identity Assertion - Identity Assertion is signed
Description	The CREDENTIAL Identity Provider issues an Identity Assertion with re-encrypted Attributes.
Image	

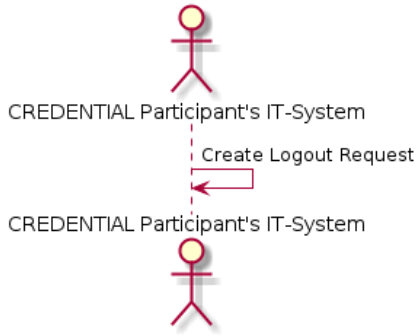
A.2.2.11 Receive Identity Assertion

Use Case Name	Receive Identity Assertion
ID	G-LUC-RECIDENTITYASSERTION
LUC_in	- Link Service Provider account with CREDENTIAL account - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP - Authenticate towards CREDENTIAL Wallet using CREDENTIAL-enabled IdP - Authenticate towards CREDENTIAL Wallet using an external IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- Service Provider
Secondary Actors	- Identity Provider
Pre-conditions	
Post-conditions	
Description	The Service Providers receives the re-encrypted Identity Assertion from the CREDENTIAL Wallet.
Image	

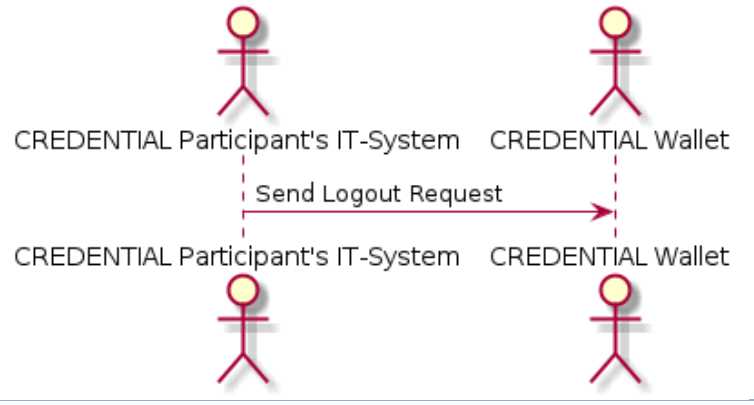
A.2.2.12 Decrypt Identity Assertion

Use Case Name	Decrypt Identity Assertion
ID	G-LUC-DECIDENTITYASSERTION
LUC_in	- Link Service Provider account with CREDENTIAL account - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Decryption Service
Pre-conditions	- Service Provider has CREDENTIAL account - Identity Assertion is issued for the Service Provider - Identity Attributes are encrypted with a proxy-re-encryption schema
Post-conditions	- Service Provider can read the Identity Attributes
Description	The Service Provider decrypts an Identity Assertion issued by a CREDENTIAL Wallet.
Image	

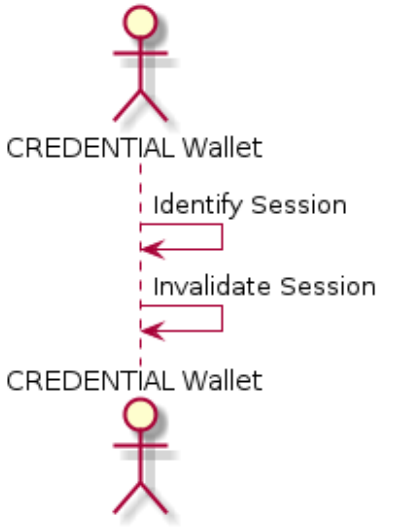
A.2.2.13 Create Logout Request

Use Case Name	Create Logout Request
ID	G-LUC-CREATELOGOUTREQ
LUC_in	Logout from CREDENTIAL Wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	
Pre-conditions	- Participant has a valid session
Post-conditions	- Logout Request is available at Participant's IT-System
Description	The CREDENTIAL Participant's IT-System creates a logout request.
Image	

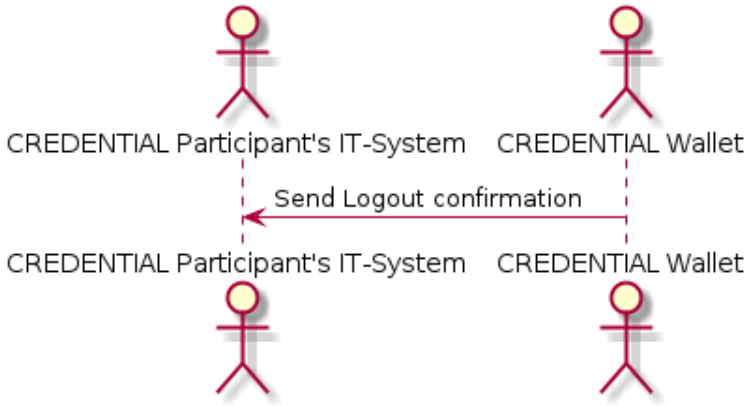
A.2.2.14 Submit Logout Request

Use Case Name	Submit Logout Request
ID	G-LUC-LOGOUTCREDWALLET
LUC_in	Logout from CREDENTIAL Wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Logout Request was created on the Participant's IT-System
Post-conditions	- Logout Request is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Participant's IT-System sends the logout request to the CREDENTIAL Wallet.
Image	

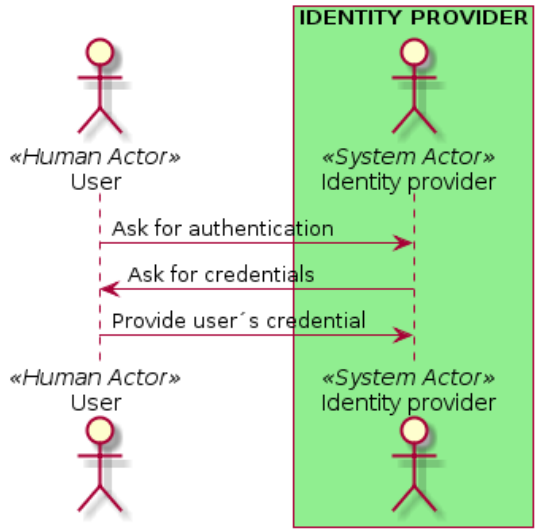
A.2.2.15 Invalidate Session

Use Case Name	Invalidate Session
ID	G-LUC-INVSESSION
LUC_in	Logout from CREDENTIAL Wallet
Main Actor	- CREDENTIAL Wallet
Secondary Actors	
Pre-conditions	- Participant requests a logout - Participant has a valid session
Post-conditions	- Session is invalidated - Participant is not able to use CREDENTIAL services
Description	The CREDENTIAL Wallet invalidates the specified session. The user can no longer use this session.
Image	

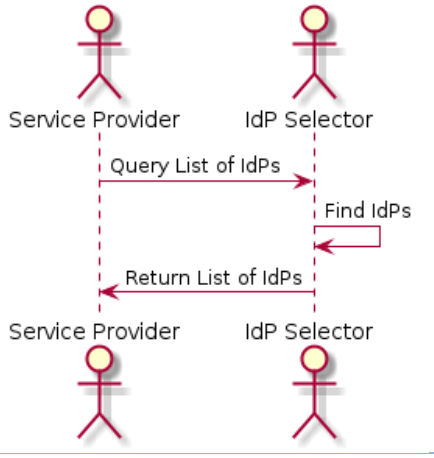
A.2.2.16 Respond Successfully Logout

Use Case Name	Respond Successfully Logout
ID	G-LUC-RESPSUCCLOGOUT
LUC_in	Logout from CREDENTIAL Wallet
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant requests a logout - Participant was logout from the CREDENTIAL Wallet
Post-conditions	- Participant received a logout confirmation
Description	The CREDENTIAL Wallet sends a successfully logout confirmation to the CREDENTIAL Participant's IT-System.
Image	

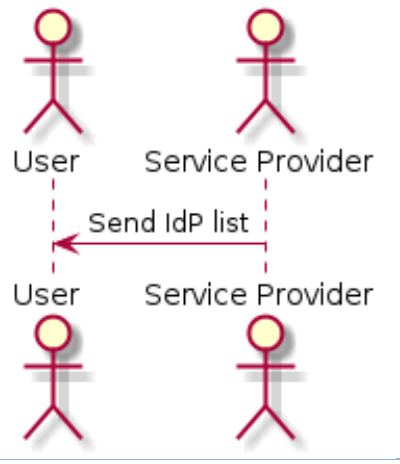
A.2.2.17 User Authentication using IdP

Use Case Name	User Authentication using IdP
ID	G-LUC-XYZ
LUC_in	- Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP - Authenticate towards CREDENTIAL Wallet using a CREDENTIAL-enabled IdP - Authenticate towards CREDENTIAL Wallet using an external IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- CREDENTIAL Participant
Secondary Actors	- Identity Provider
Pre-conditions	- User has a CREDENTIAL account - User has write access rights
Post-conditions	- The IdP receives the user´s credentials
Description	A user initiates an authentication against an Identity Provider, using the credentials.
Image	

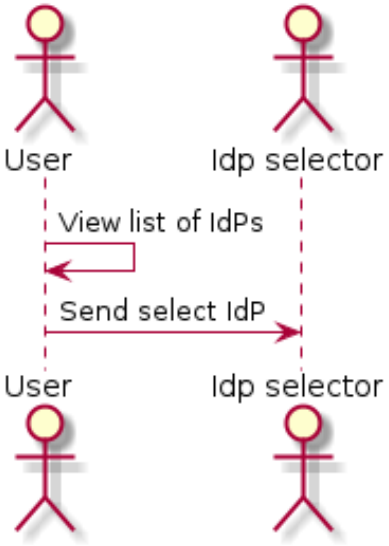
A.2.2.18 Ask for a List of IdPs

Use Case Name	Ask for a List of IdPs
ID	G-LUC-ASKIDPS
LUC_in	Select CREDENTIAL Identity Provider
Main Actor	- IdP Selector
Secondary Actors	- Service Provider
Pre-conditions	
Post-conditions	- List of IdPs is available at the Service Provider
Description	A Service Provider requests a list of IdPs which are available using CREDENTIAL technology.
Image	

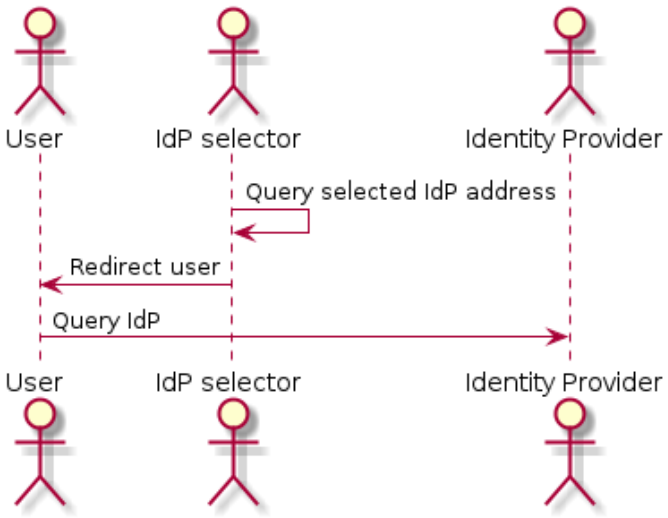
A.2.2.19 Ask to select an IdP from the provided List

Use Case Name	Ask to select an IdP from the provided List
ID	G-LUC-ASKIDPFROMLIST
LUC_in	Select CREDENTIAL Identity Provider
Main Actor	- CREDENTIAL Participant
Secondary Actors	- Service Provider
Pre-conditions	- User has requested access to protected resource
Post-conditions	- List of IdPs available at user.
Description	A Service Provider sends a list of available IdPs to the user. The user is know able to choose which IdP to use for the authentication process against the Service Provider.
Image	

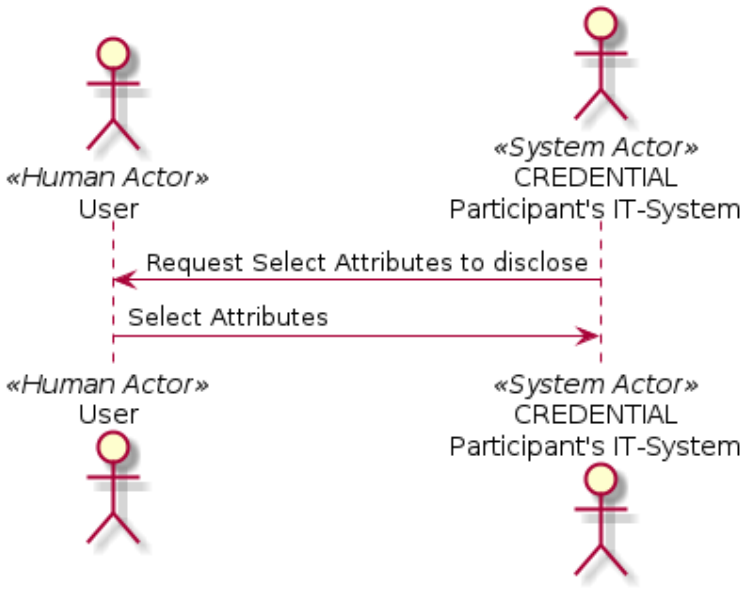
A.2.2.20 Select an IdP

Use Case Name	Select an IdP
ID	G-LUC-SELECTIDP
LUC_in	Select CREDENTIAL Identity Provider
Main Actor	- CREDENTIAL Participant
Secondary Actors	- IdP Selector
Pre-conditions	- User has a list of IdPs - User requested access to a protected resource
Post-conditions	- Selected IdP is known to the IdP selector
Description	A user received a list of IdPs. He is now challenged to choose one of the IdPs.
Image	

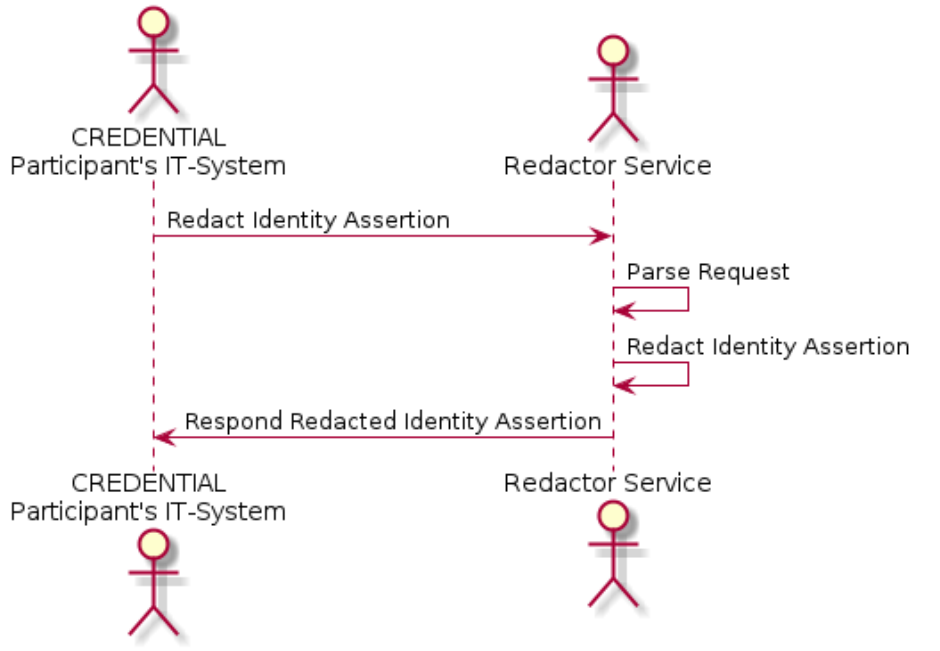
A.2.2.21 IdP Selector Redirects User to the Selected IdP

Use Case Name	IdP Selector Redirects User to the Selected IdP
ID	G-LUC-REDIRECTUSER
LUC_in	Select CREDENTIAL Identity Provider
Main Actor	- IdP Selector
Secondary Actors	- CREDENTIAL Participant - Identity Provider
Pre-conditions	- User has sent a selected IdP to the IdP selector
Post-conditions	- User is redirected to IdP
Description	An IdP selector queries the address of a selected IdP. The user is redirected to this IdP.
Image	

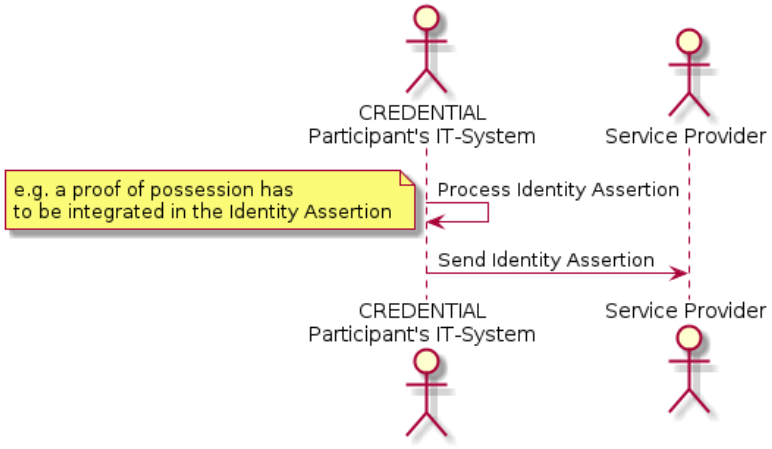
A.2.2.22 Select Attributes to Disclose

Use Case Name	Select Attributes to Disclose
ID	G-LUC-SELECTATTRDISCLOSE
LUC_in	Selective Disclosure
Main Actor	- CREDENTIAL Participant
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- User has an Identity Assertion
Post-conditions	- User has selected the Attributes to disclose
Description	A user wants to disclose attributes from an Identity Assertion. He sees the available attributes in his Identity Assertion and selects which one of them should be disclosed.
Image	

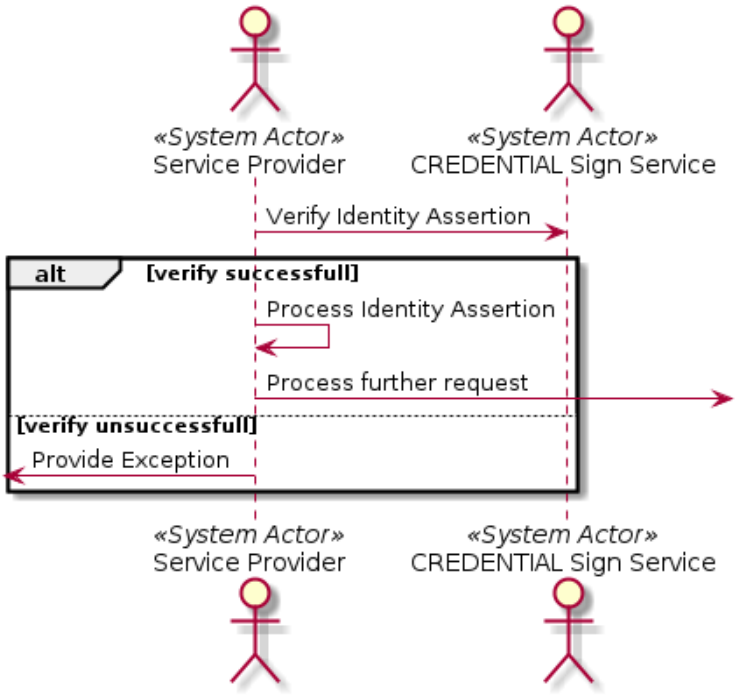
A.2.2.23 Redact Identity Assertion

Use Case Name	Redact Identity Assertion
ID	G-LUC-REDACTIDASSERTION
LUC_in	Selective Disclosure
Main Actor	- CREDENTIAL Redactor Service
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant possesses an Identity Assertion - Signature of Identity Assertion is capable to redact attributes
Post-conditions	- Attributes of Identity Assertion are redacted - Signature still valid - Redacted Identity Assertion available at Participant's IT-System
Description	A Participant want to redact attributes in his Identity Assertion. He requests this operation at the Redactor Service by providing the Identity Assertion and the attributes to redact.
Image	

A.2.2.24 Provide Identity Assertion

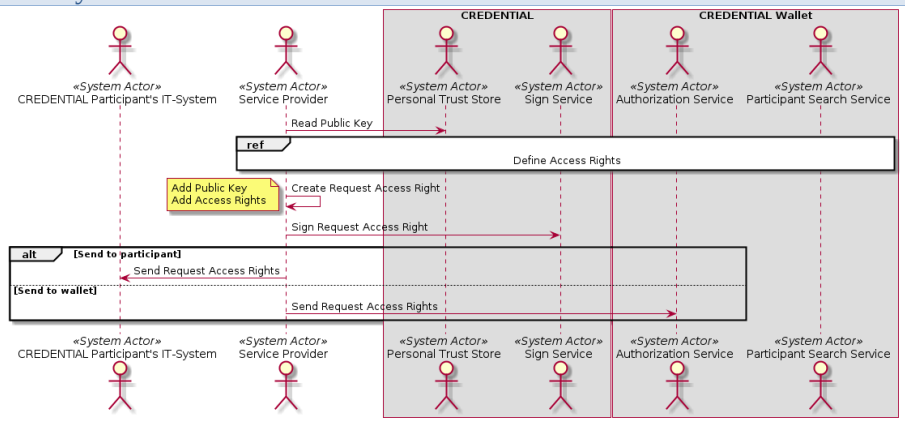
Use Case Name	Provide Identity Assertion
ID	G-LUC-PROVIDASSERTION
LUC_in	Selective Disclosure
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- Service Provider
Pre-conditions	- Participant owns an Identity Assertion - Identity Assertion may be redacted
Post-conditions	- Participant has performed necessary steps to process the Identity Assertion - Identity Assertion is available at Service Provider
Description	A participant possesses an Identity Assertion. The Identity Assertion has to be provided towards a Service Provider in order to access a protected resource.
Image	

A.2.2.25 Verify Identity Assertion

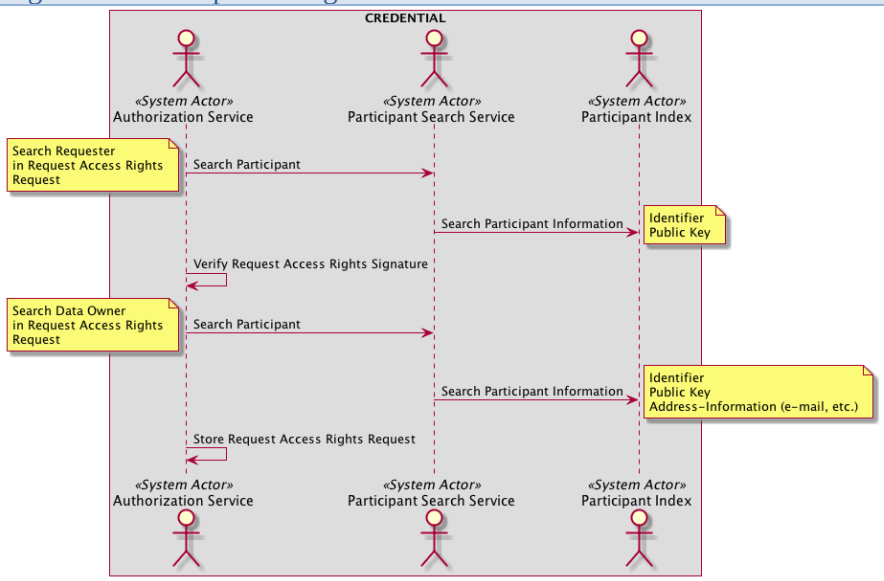
Use Case Name	Verify Identity Assertion
ID	G-LUC-VERIDASSERTION
LUC_in	Selective Disclosure
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Sign Service
Pre-conditions	- Identity Assertion is issued by a CREDENTIAL enabled Identity Provider - A Service Provider receives an Identity Assertion
Post-conditions	- Service Provider has verified the Identity Assertion
Description	In order to access protected resources on a Service Provider a user has to provide an Identity Assertion. In case CREDENTIAL technology is used in the issuing process the Service Provider has to use some CREDENTIAL services in order to process an Identity Assertion. For example, the Identity Assertion can be protected by a malleable signature which is created by CREDENTIAL technology. By using the CREDENTIAL Sign Service such a signature can still be verified.
Image	

A.2.3 Authorization

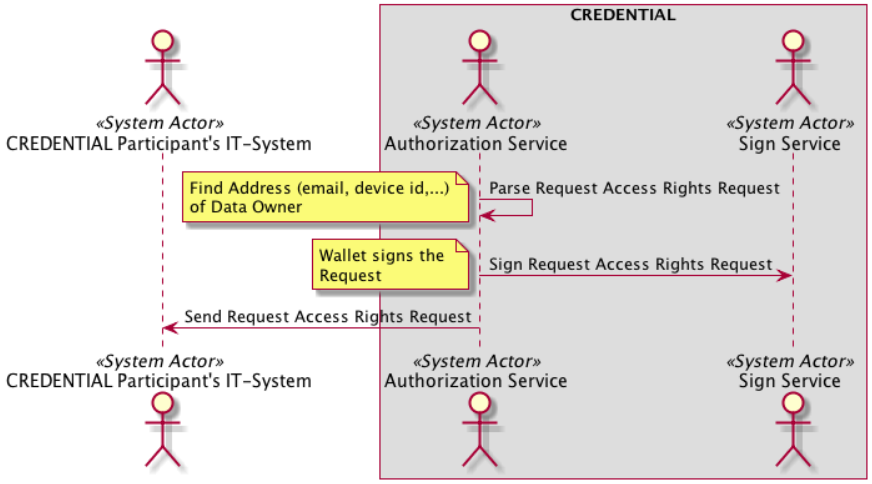
A.2.3.1 Request Access Rights

Use Case Name	Request Access Rights
ID	G-LUC-REQACCESSRIGHTS
LUC_in	EXPORT CREDENTIAL Wallet data into form
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Authorization Service - CREDENTIAL Personal Trust Store - CREDENTIAL Participant's IT-System - CREDENTIAL Sign Service - CREDENTIAL Participant Search Service
Pre-conditions	- Service Provider has a CREDENTIAL account
Post-conditions	- The information which data the Service Provider wants to access is propagated to the user or the CREDENTIAL Wallet - The Service Provider's CREDENTIAL account information is propagated to the user or the CREDENTIAL Wallet.
Description	The Service Providers needs access to data from the user from his CREDENTIAL Wallet. The Service Providers reads his public key from his Personal Trust Store. The Service Provider creates the Access Rights he wants to have. The Public Key and the Access Rights are compiled in a Request Access Rights object and signed with the Sign Service. In a Request Access Rights, the Service Provider requests access to the data in the CREDENTIAL Wallet. The Request Access Rights object is send to the user's IT-System or directly to the CREDENTIAL Wallet.
Image	

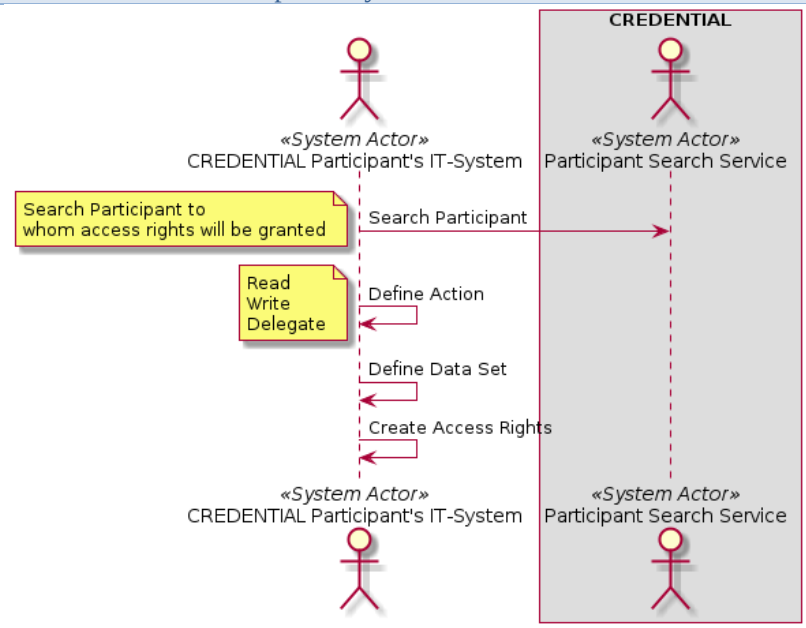
A.2.3.2 Register Access Rights Request

Use Case Name	Register Access Rights Request
ID	G-LUC-REGACCESSRIGHTSREQ
LUC_in	Request Access Rights
Main Actor	- CREDENTIAL Authorization Service
Secondary Actors	- CREDENTIAL Participant Search Service - CREDENTIAL Participant Index
Pre-conditions	- Authorization Service has received a Request Access Rights Request
Post-conditions	- Authorization Service has stored the Request Access Rights Request - Authorization Service has identified the Data Owner's Information - Authorization Service has identified the Requester's Information
Description	The CREDENTIAL Wallet registers and processes the access rights request. The Authorization Service searches for the participant who originates the Access Rights Request. The Participant Search Service uses the Participant Index to retrieve the participant's public key. The Authorization Service verifies the provided signature in the Request Access Rights. If verified, the Authorization service searches for the data owner mentioned in the Request Access Rights. If found, the Authorization Service stores the Request Access Rights for further processing.
Image	

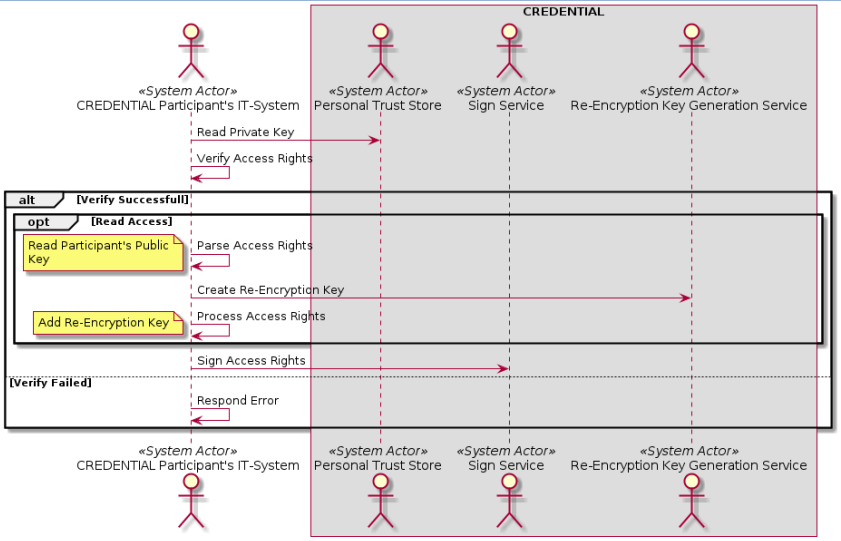
A.2.3.3 Provide Access Rights Request

Use Case Name	Provide Access Rights Request
ID	G-LUC-PROVACCESSRIGHTSREQ
LUC_in	Request Access Rights
Main Actor	- CREDENTIAL Authorization Service
Secondary Actors	- CREDENTIAL Sign Service - CREDENTIAL Participant's IT-System
Pre-conditions	- Request Access Rights Request is available at the Authorization Service
Post-conditions	- Request Access Rights Request is signed by the CREDENTIAL Wallet - Request Access Rights Request is provided to the data owner
Description	The CREDENTIAL Wallet provides the access right request to the specified CREDENTIAL Participant's IT-System. The Request Access Rights is parsed by the Authorization Service and the user's destination address or device id are identified. The Request Access Rights Request is signed by the CREDENTIAL Wallet. The signed Request Access Rights Request is send to the Participant's IT-System.
Image	

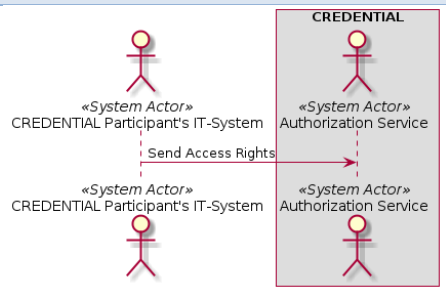
A.2.3.4 Define Access Rights

Use Case Name	Define Access Rights
ID	G-LUC-DEFINEACCESSRIGHTS
LUC_in	Grant Access Rights
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Participant Search Service
Pre-conditions	
Post-conditions	- Access Rights have been defined
Description	A CREDENTIAL Participant defines access rights for data in a CREDENTIAL Wallet using his IT-System. The Participant's IT-System uses the Participant Search Service in order to search for the Participant to whom access rights will be granted. The Participant defines the action he wants to perform on the data set and identifies the data set. Finally, the Access Rights are created by the Participant's IT-System with the information provided so far. User interaction is probably involved in this use case.
Image	

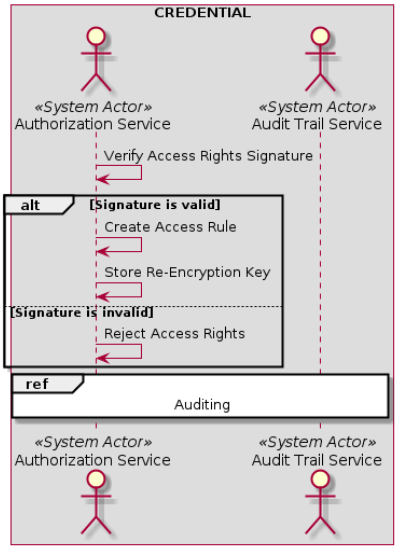
A.2.3.5 Grant Access Rights

Use Case Name	Grant Access Rights
ID	G-LUC-GRANTACCESSRIGHTS
LUC_in	Grant Access Rights
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service - CREDENTIAL Re-Encryption Key Generation Service
Pre-conditions	- Access Rights Request is present to the IT-System - Participant has a CREDENTIAL account
Post-conditions	- Re-Encryption Key is added to Access Rights - Access Rights are signed by the Participant
Description	A CREDENTIAL Participant uses his IT-System to grant access rights on data in the CREDENTIAL Wallet using CREDENTIAL technology. E.g. a proxy-re-encryption key has to be generated. The Participant's IT-Systems reads the private key from the Personal Trust Store. The Participant's IT-System verifies the Access Rights. It checks if the provided signature by the CREDENTIAL Wallet and the requester are created properly. On success, the requester's public key is parsed from the Access Rights. If the Access Rights describe a read access to a resource, together with the private key and the public key a proxy-re-encryption key is created. The Re-Encryption Key is added to the Access Rights and signed by the Sign Service. If the Access Rights are not successfully verified, an error is respond to the Participant's IT-System.
Image	

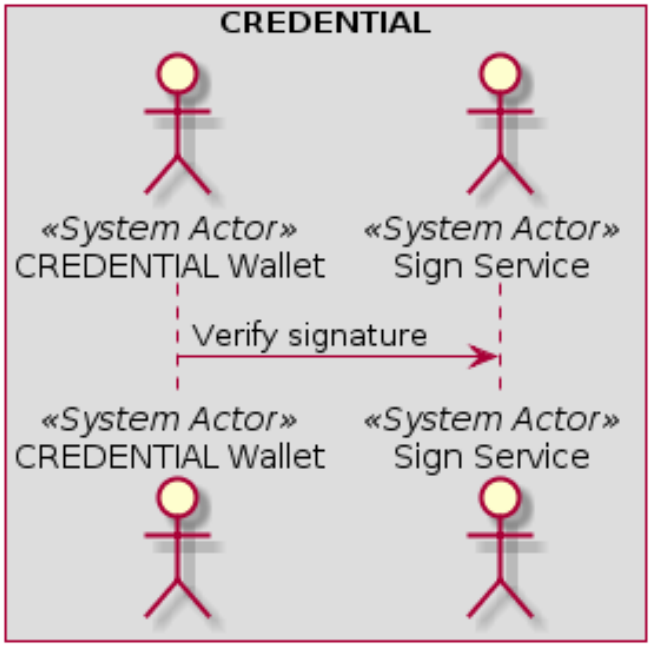
A.2.3.6 Provide Access Rights

Use Case Name	Provide Access Rights
ID	G-LUC-PROVIDEACCESSRIGHTS
LUC_in	- Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP - Authenticate towards CREDENTIAL Wallet using a CREDENTIAL-enabled IdP - Authenticate towards CREDENTIAL Wallet using an external IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation - Grant Access Rights
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Authorization Service
Pre-conditions	- Access Rights were created or modified by the Participant's IT-System
Post-conditions	- Access Rights are available in the CREDENTIAL Wallet at the Authorization Service.
Description	The CREDENTIAL Participant's IT-System provides the granted access rights to the CREDENTIAL Wallet.
Image	

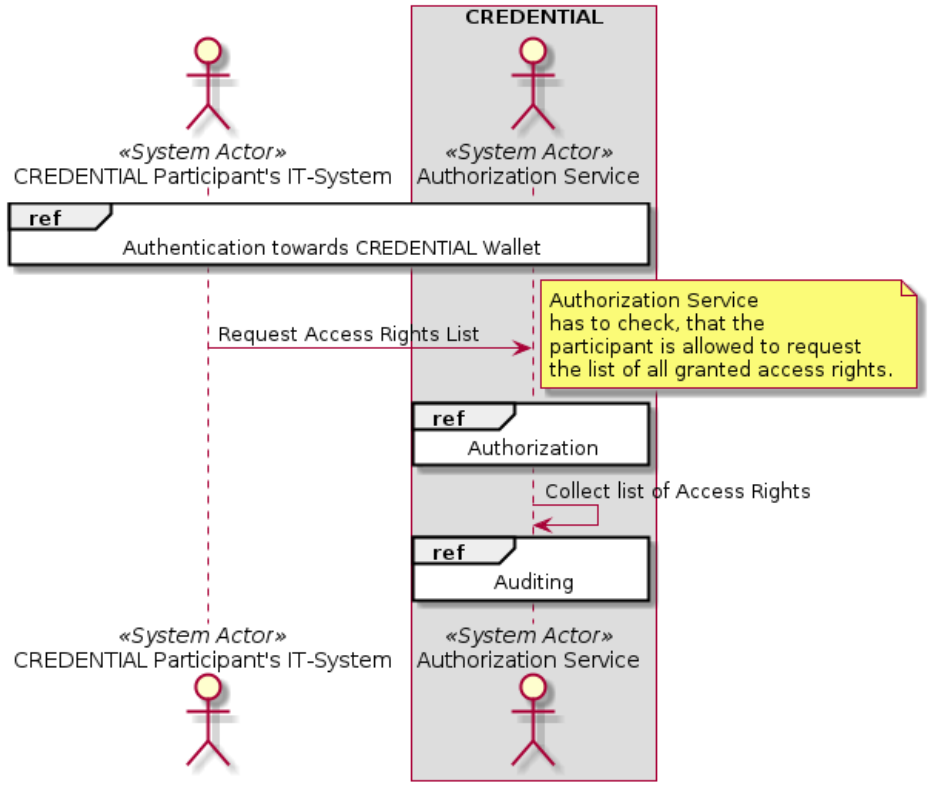
A.2.3.7 Register Access Rights

Use Case Name	Register Access Rights
ID	G-LUC-REGACCESSRIGHTS
LUC_in	Grant Access Rights
Main Actor	- CREDENTIAL Authorization Service
Secondary Actors	- CREDENTIAL Audit Trail Service
Pre-conditions	- Unregistered Access Rights are available to the Authorization Service
Post-conditions	- Access Rules have been created - Re-Encryption Key has been stored
Description	The CREDENTIAL Wallet registers the access rights. The Authorization Service verifies the signature of the participant who grants the access rights contained in the Access Rights. If the signature is valid a new Access Rule is created at the Authorization Service based on the information provided in the Access Rights. The Re-Encryption Key is extracted from the Access Rights and stored at the Authorization Service. If the signature is not valid, the Access Rights are rejected and no Access Rule or Re-Encryption Key has been created or stored.
Image	

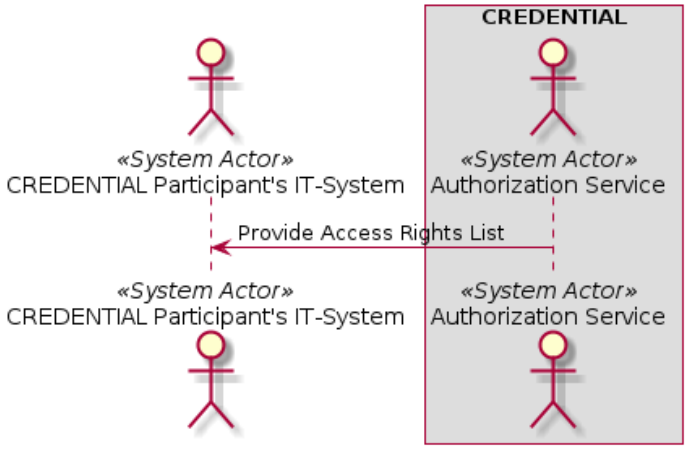
A.2.3.8 Verify Re-Encryption Request

Use Case Name	Verify Re-Encryption Request
ID	G-LUC-VERREENCREQ
LUC_in	Generate new access-key for CREDENTIAL Wallet
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Sign Service
Pre-conditions	
Post-conditions	
Description	The Wallet must ensure the re-encryption requests are valid (from the data owner)
Image	

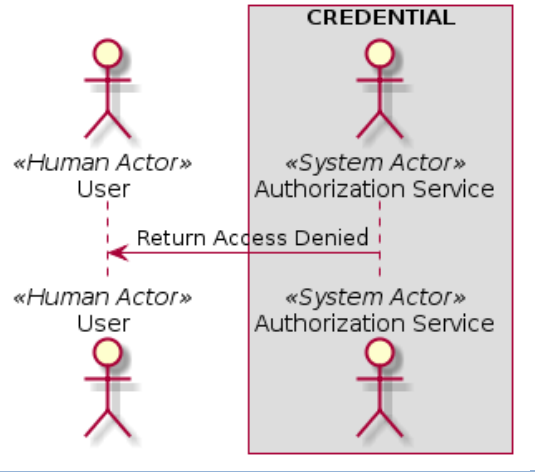
A.2.3.9 Request Access Rights List

Use Case Name	Request Access Rights List
ID	G-LUC-REQACCRIGHTSLIST
LUC_in	Re-Generate Access Rights
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Authorization Service
Pre-conditions	- Participant has a CREDENTIAL account
Post-conditions	- List of Access Rights is available at Authorization Service for participant
Description	The CREDENTIAL Participant's IT-System requests a list of the granted access rights related to the participant to the CREDENTIAL Wallet.
Image	

A.2.3.10 Receive Access Rights List

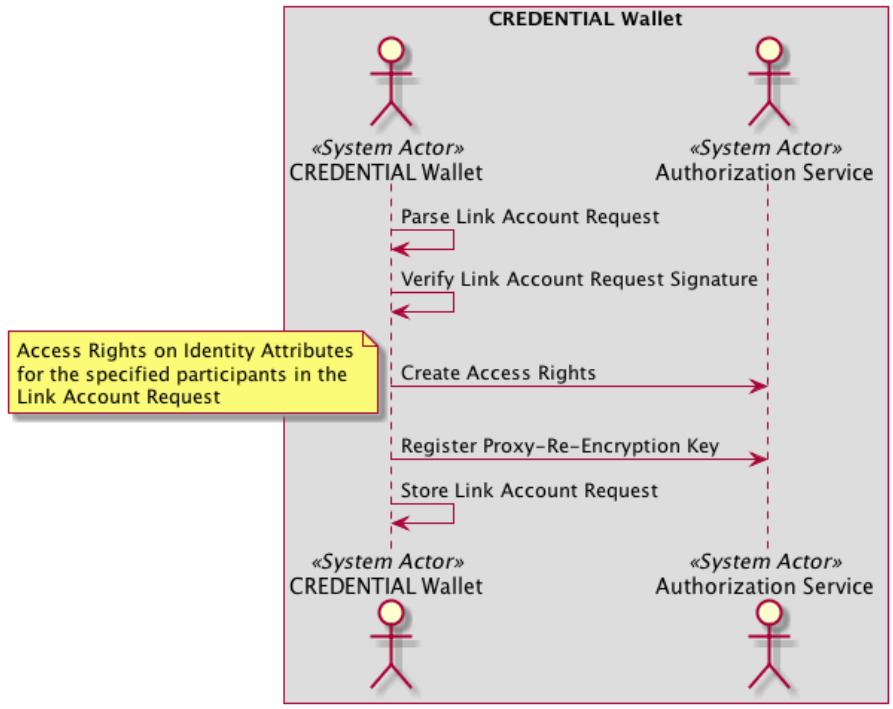
Use Case Name	Receive Access Rights List
ID	G-LUC-RECACCESSRIGHTSLIST
LUC_in	Re-Generate Access Rights
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Access Rights List was requested by the participant
Post-conditions	- Access Rights List is available at the participant's IT-System
Description	The CREDENTIAL Participant's IT-System receives the granted access rights related to the participant stored in the CREDENTIAL Wallet.
Image	

A.2.3.11 Access Denied

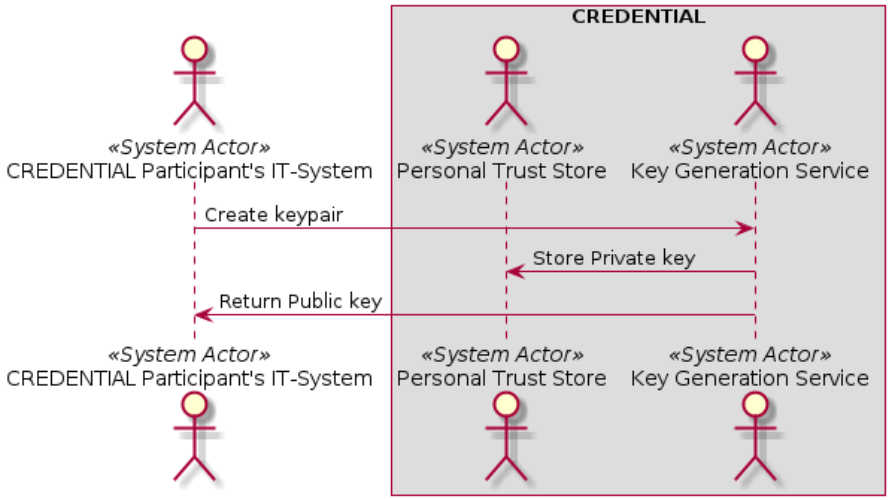
Use Case Name	Access Denied
ID	G-LUC-ACCESSDENIED
LUC_in	- Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP - Authenticate towards CREDENTIAL Wallet using a CREDENTIAL-enabled IdP - Authenticate towards CREDENTIAL Wallet using an external IdP - Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and Identity Federation
Main Actor	- CREDENTIAL Authorization Service
Secondary Actors	- CREDENTIAL Participant
Pre-conditions	- User has an account - User has access to his credentials
Post-conditions	- User is not able to access CREDENTIAL services
Description	The access for a user is denied by CREDENTIAL.
Image	

A.2.4 Account Management

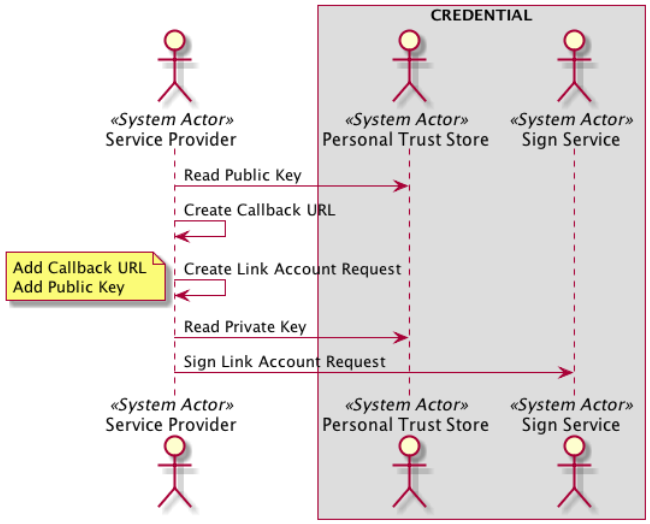
A.2.4.1 Register Link Account Request

Use Case Name	Register Link Account Request
ID	G-LUC-REGLINKACCREQ
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Authorization Service
Pre-conditions	- New Link Account Request is available to the wallet
Post-conditions	- Link Account Request is stored in the wallet - Read Access Rule on the Identity Attributes of the Participant for the Requester are created - Re-Encryption Key is stored
Description	The CREDENTIAL Wallet registers a link account request. E.g. Register the proxy-re-encryption key. Register the callback URL
Image	

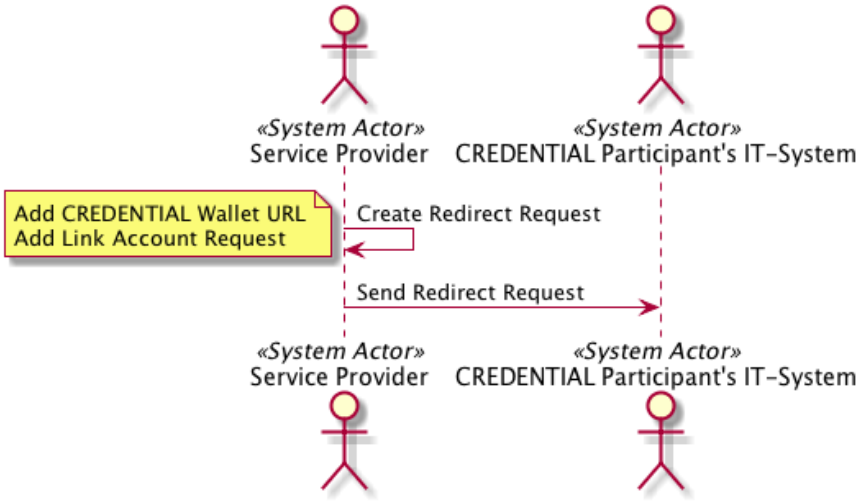
A.2.4.2 Generate new Keypair

Use Case Name	Generate new Keypair
ID	G-LUC-GENKEYPAIR
LUC_in	Generate new access-key for CREDENTIAL Wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Key Generation Service
Pre-conditions	- CREDENTIAL Services are installed on the Participant's IT-System
Post-conditions	- The participant has a new public key component and its private counterpart stored in its trust store
Description	The participant requires a new public key/pair, whether it is for registering for the first time in CREDENTIAL or to replace his old one. The private key component is stored in the participant's trust store while the public one is directly returned.
Image	

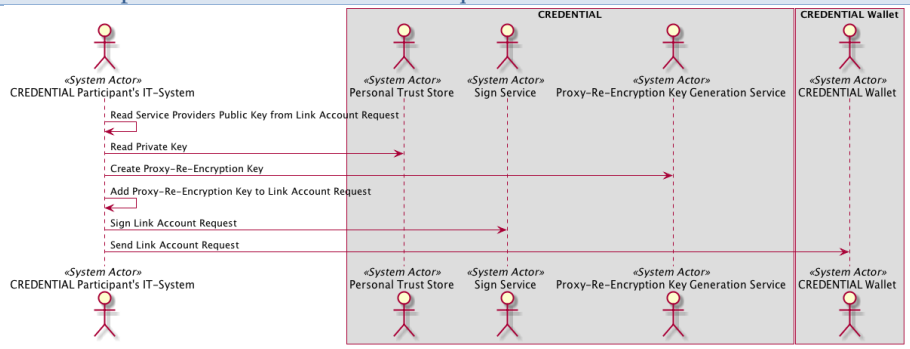
A.2.4.3 Create Link Account Request using CREDENTIAL

Use Case Name	Create Link Account Request using CREDENTIAL
ID	G-LUC-LINKACCREQ
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service
Pre-conditions	- Service Provider has a CREDENTIAL account
Post-conditions	- Link Account Request has been created - Callback URL is accessible
Description	The Service Provider creates a Link Account Request. The Link Account Request contains of - a callback URL - Service Provider's CREDENTIAL account information. The purpose of a link account is to combine the accounts of a participant registered at the service provider with his CREDENTIAL account. Thus he is able to login to the Service Provider with his CREDENTIAL account.
Image	

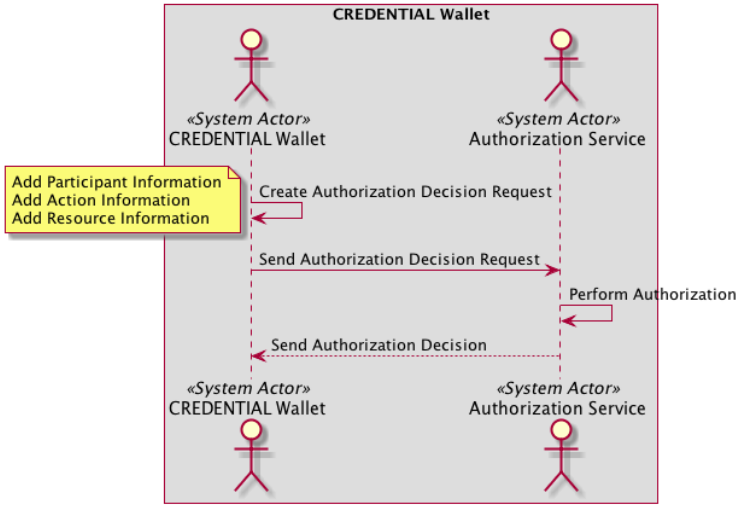
A.2.4.4 Redirect User to CREDENTIAL Authentication

Use Case Name	Redirect User to CREDENTIAL Authentication
ID	G-LUC-REDIRECTUSERCREDAUTH
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- Service Provider
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Link Account Request has been created
Post-conditions	- Participant's IT-System has received the Link Account Request - Participant's IT-System has received the Redirect Request
Description	The Service Provider redirects a user to the CREDENTIAL Authentication page. The Service Provider provides additional information to the User while redirecting. E.g. providing Link Account Request.
Image	

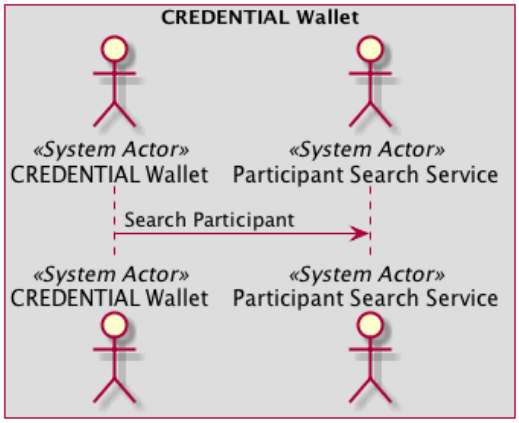
A.2.4.5 Provide Link Account Request

Use Case Name	Provide Link Account Request
ID	G-LUC-PROVLINKACCREQ
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Sign Service - CREDENTIAL Proxy Re-Encryption Key Generation Service - CREDENTIAL Wallet
Pre-conditions	- The user is authenticated - Link Account Request is provided to the Participant's IT-System
Post-conditions	- Re-Encryption Key has been created - Link Account Request has been signed by the Participant - Link Account Request is available at the wallet.
Description	The User provides a Link Account Request to the CREDENTIAL Wallet.
Image	

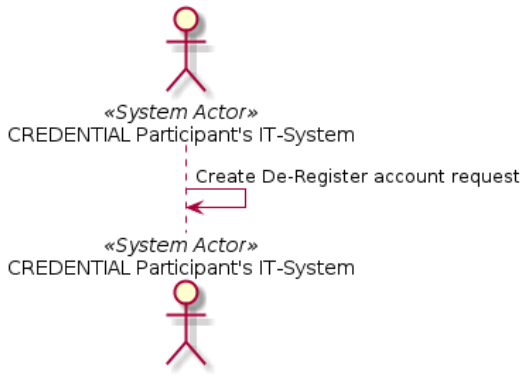
A.2.4.6 Authorization

Use Case Name	Authorization
ID	G-LUC-AUTHORIZATION
LUC_in	Link Service Provider account with CREDENTIAL account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Authorization Service
Pre-conditions	- Participant is authenticated - CREDENTIAL Wallet knows the action the user wants to perform - CREDENTIAL Wallet know the resource he wants to access
Post-conditions	- Authorization decision has been made
Description	The CREDENTIAL Wallet authorizes a participant for a specific action he wants to perform on a given resource. E.g. participant wants to read user data.
Image	

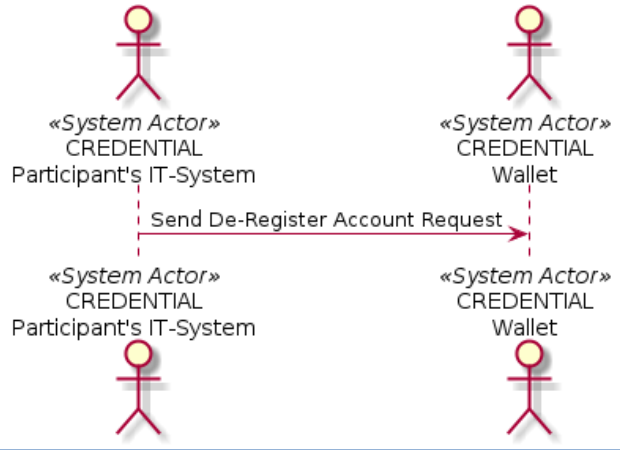
A.2.4.7 Search User

Use Case Name	Search User
ID	G-LUC-SEARCHUSER
LUC_in	- Ban a User - Generate new access-key for CREDENTIAL Wallet - Recover CREDENTIAL Wallet Data
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Search Service
Pre-conditions	- A user identifier is known
Post-conditions	- The User information are available at the wallet.
Description	The CREDENTIAL Wallet searches for a given user.
Image	

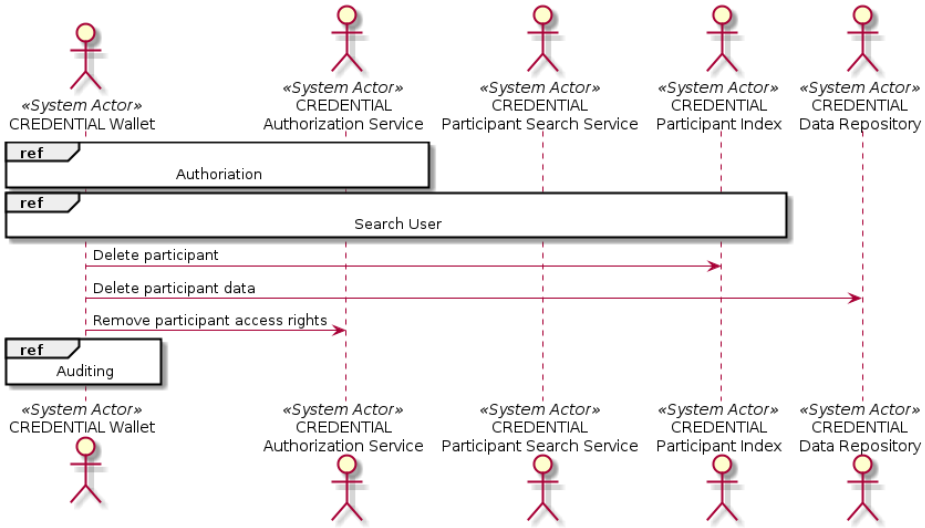
A.2.4.8 Create De-Register CREDENTIAL account request

Use Case Name	Create De-Register CREDENTIAL account request
ID	G-LUC-CREATEDEREGACCREQ
LUC_in	Re-Register from CREDENTIAL
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	
Pre-conditions	- Participant wants to de-register from CREDENTIAL
Post-conditions	- De-register account request has been created.
Description	The CREDENTIAL Participant creates a de-register account request.
Image	

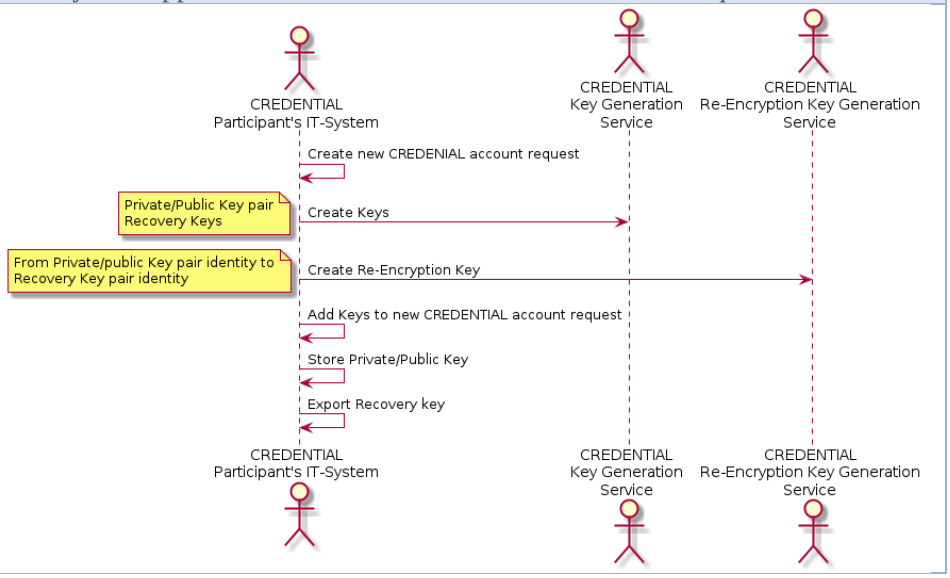
A.2.4.9 Submit De-Register CREDENTIAL account request

Use Case Name	Submit De-Register CREDENTIAL account request
ID	G-LUC-SUBMITDEREGACCREQ
LUC_in	De-register from CREDENTIAL
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	
Pre-conditions	- De-Register Account Request has been created by participant - Participant is logged in on the CREDENTIAL Wallet
Post-conditions	- De-Register Account Request is available at the CREDENTIAL Wallet
Description	- The CREDENTIAL Participant's IT-System submits the de-register request to the CREDENTIAL Wallet.
Image	

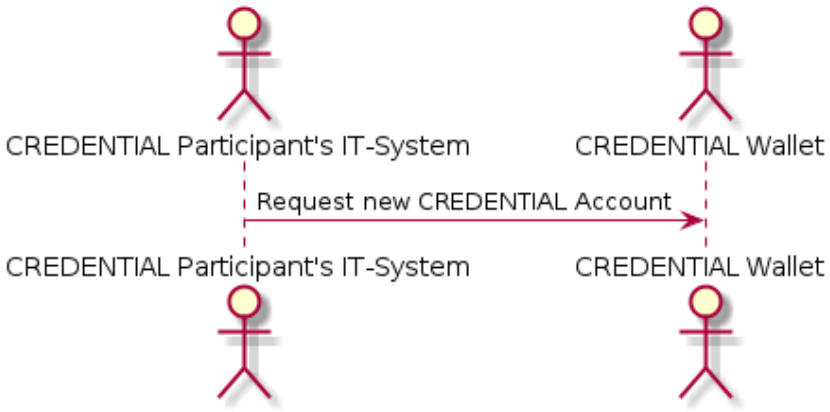
A.2.4.10 De-Register Account

Use Case Name	De-Register Account
ID	G-LUC-DEREGACC
LUC_in	De-Register from CREDENTIAL
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Authorization Service - CREDENTIAL Participant Search Service - CREDENTIAL Participant Index - CREDENTIAL Data Repository
Pre-conditions	- Participant requested a de-register account
Post-conditions	- Participant is fully de-registered from CREDENTIAL Wallet
Description	The CREDENTIAL Wallet processes the de-register account request.
Image	

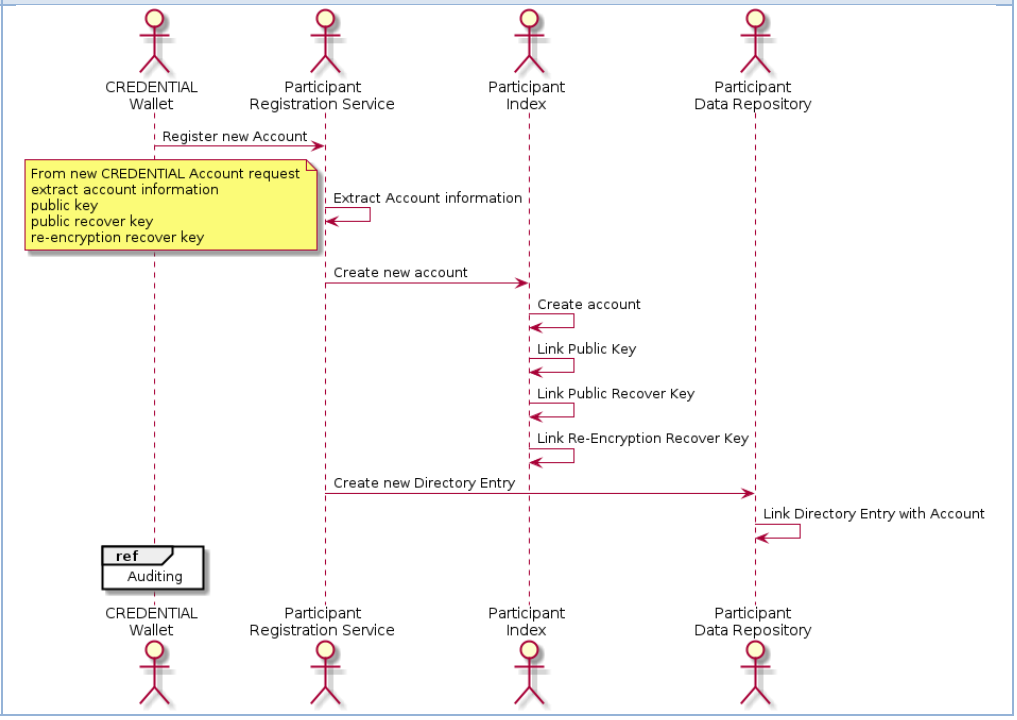
A.2.4.11 Create new CREDENTIAL Account Request

Use Case Name	Create new CREDENTIAL Account Request
ID	G-LUC-CREATECREDACCREQ
LUC_in	Register a new CREDENTIAL Account
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Key Generation Service - CREDENTIAL Re-Encryption Key Generation Service
Pre-conditions	
Post-conditions	- New CREDENTIAL account request has been created - Recovery Key is exported
Description	A User creates on his IT-System a create new CREDENTIAL account request. e.g. create private key. The IT-System uses the Key Generation Service in order to create a public/private key pair for the CREDENTIAL identity of the upcoming account. In addition, a Recovery key/pair is generated. A Re-Encryption Key from the public/private key pair to the recovery key is created. All keys are appended to the new CREDENTIAL account request.
Image	

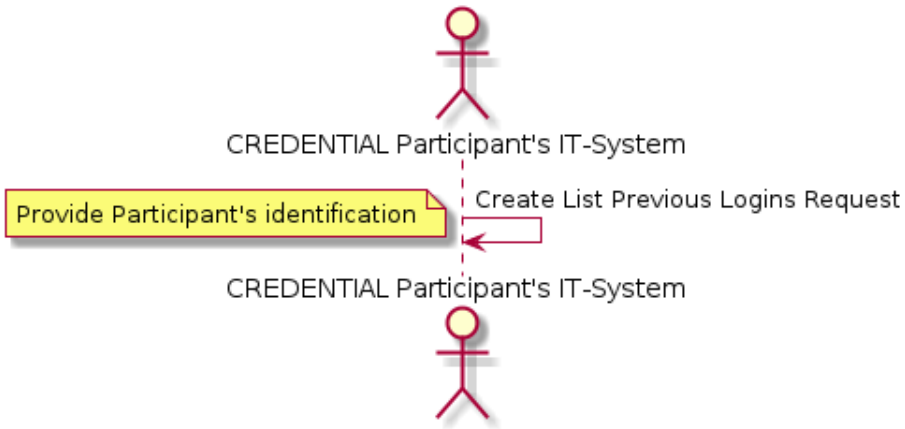
A.2.4.12 Submit new CREDENTIAL Account Request

Use Case Name	Submit new CREDENTIAL Account Request
ID	G-LUC-SUBMITCREDACCREQ
LUC_in	Register a new CREDENTIAL Account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant has created a new CREDENTIAL Account request with the needed information
Post-conditions	- Create new Account Request is available at the CREDENTIAL Wallet
Description	The Participant's IT-System submits the create new CREDENTIAL Account Request to the CREDENTIAL Wallet.
Image	

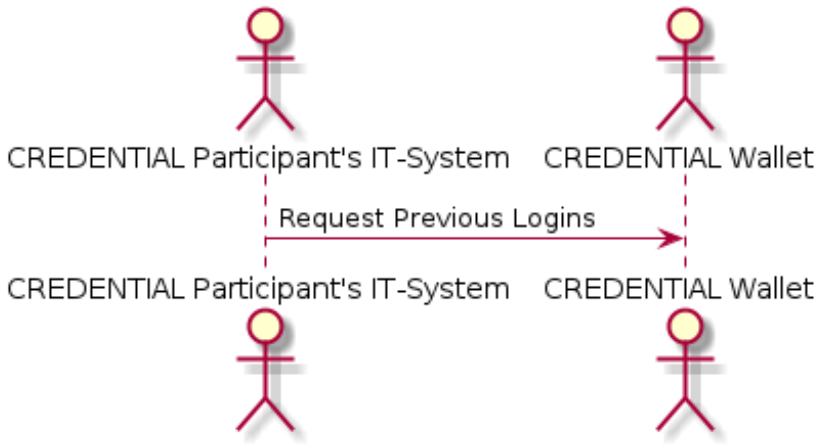
A.2.4.13 Create new CREDENTIAL Account

Use Case Name	Create new CREDENTIAL Account
ID	G-LUC-CREATECREDACC
LUC_in	Register a new CREDENTIAL Account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Index - CREDENTIAL Participant Data Repository
Pre-conditions	- Create a new Account Request is available at the CREDENTIAL Wallet
Post-conditions	- A new account is created in the CREDENTIAL Wallet
Description	The CREDENTIAL Wallet creates a new account. The newly created account contains of user information provided during the registration process, his public key, a public recovery key and the re-encryption recovery key. A new directory entry is created and associated with this account.
Image	

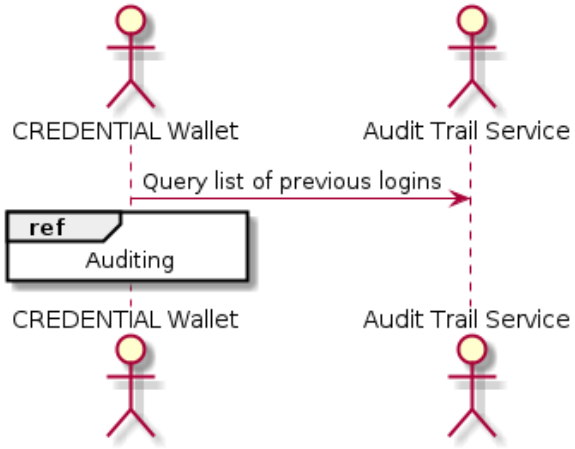
A.2.4.14 Create List Previous Logins Request

Use Case Name	Create List Previous Logins Request
ID	G-LUC-CREATELISTPREVLOGREQ
LUC_in	View previous logins to my account
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	
Pre-conditions	- Participant's identification is known
Post-conditions	- List Previous Logins Request is created
Description	The CREDENTIAL Participant's IT-System creates a list previous logins request.
Image	

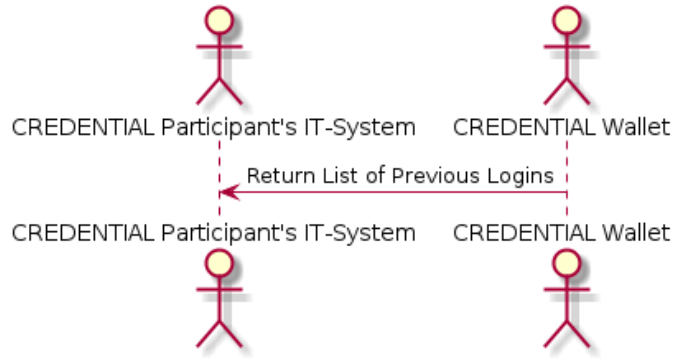
A.2.4.15 Submit List Previous Logins Request

Use Case Name	Submit List Previous Logins Request
ID	G-LUC-SUBMITLISTPREVLOGREQUEST
LUC_in	View previous logins to my account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant is allowed to view list previous logins - Participant is authenticated against the CREDENTIAL Wallet
Post-conditions	- List Previous Login Request is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Participant's IT-System submits the list previous logins request to the CREDENTIAL Wallet.
Image	

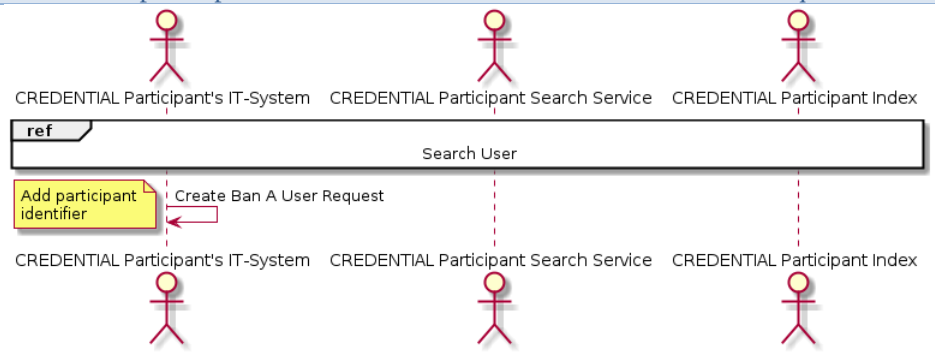
A.2.4.16 Query List of Previous Logins for User

Use Case Name	Query List of Previous Logins for User
ID	G-LUC-QRYLISTPREVLOGINS
LUC_in	View previous logins to my account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Audit Trail Service
Pre-conditions	- CREDENTIAL Wallet is permitted to access the list of previous logins for user - User identification is known to the CREDENTIAL Wallet
Post-conditions	- List of previous logins is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Wallet queries the list of previous logins for the user based on the list previous logins request. The information is available at the audit trail service. Thus the CREDENTIAL Wallet queries this service for the needed information.
Image	

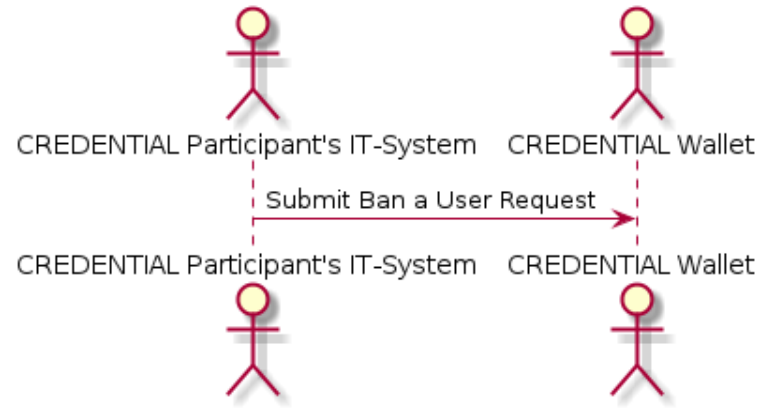
A.2.4.17 Return List of Previous Logins

Use Case Name	Return List of Previous Logins
ID	G-LUC-RETLISTPREVLOGINS
LUC_in	View previous logins to my account
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant requested a list of previous logins
Post-conditions	- List of previous logins is available at the Participant's IT-System
Description	The CREDENTIAL Wallet returns the list of previous logins to the CREDENTIAL Participant's IT-System.
Image	

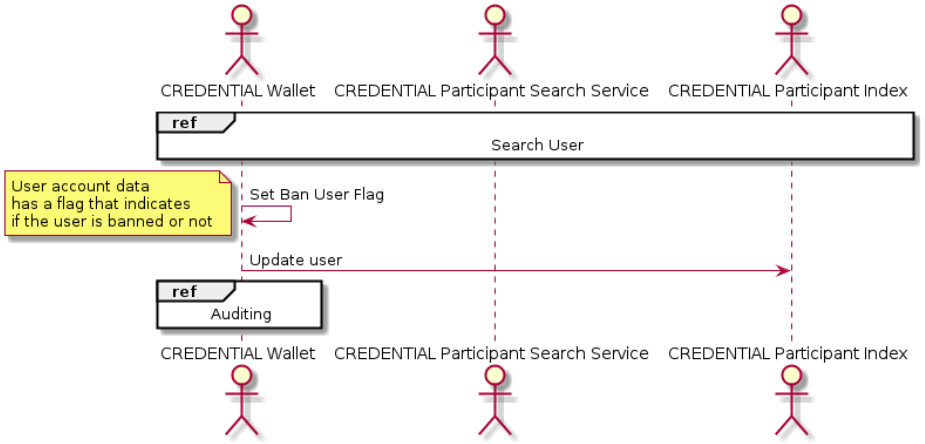
A.2.4.18 Create Ban a User Request

Use Case Name	Create Ban a User Request
ID	G-LUC-CREATEBANUSERREQ
LUC_in	Ban a user
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Participant Search Service - CREDENTIAL Participant Index
Pre-conditions	- The originator has administrator privileges - The originator is logged in as administrator - Sufficient information to uniquely identify the participant to ban is available
Post-conditions	- The ban a user request is created
Description	The CREDENTIAL Administrator creates a ban user request. The participant's identifier is searched through the Participant Search Service and Participant Index. The participant's identifier is used to create the ban a user request.
Image	

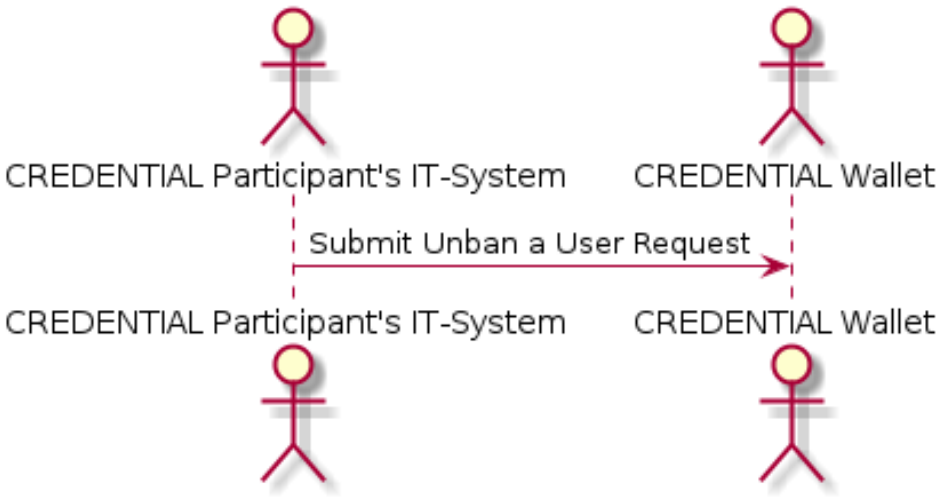
A.2.4.19 Submit Ban a User Request

Use Case Name	Submit Ban a User Request
ID	G-LUC-SUBMITBANUSERREQ
LUC_in	Ban a user
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Participant has created a ban a user request - Participant is logged in as Administrator
Post-conditions	- Ban a user request is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Administrator IT-System sends the ban user request to the CREDENTIAL Wallet.
Image	

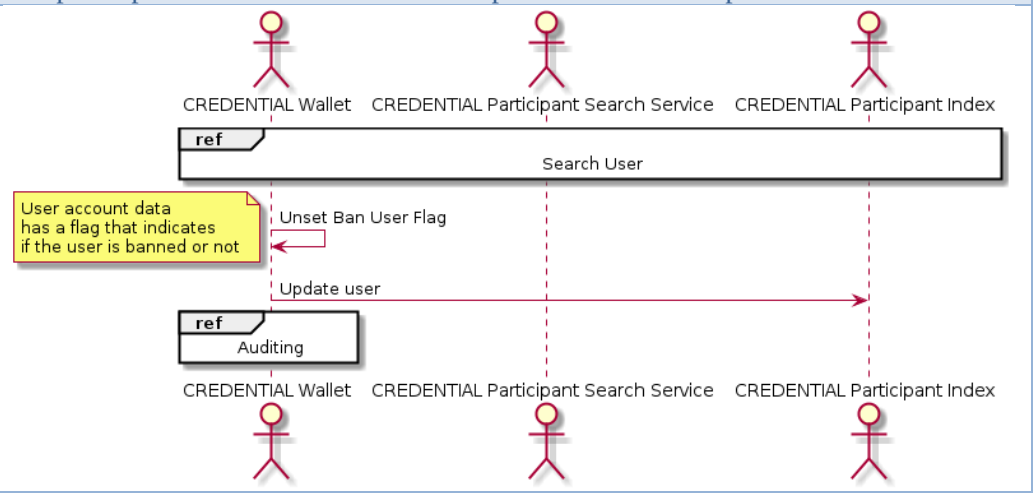
A.2.4.20 Ban User

Use Case Name	Ban User
ID	G-LUC-BANUSER
LUC_in	Ban a user
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Search Service - CREDENTIAL Participant Index
Pre-conditions	- Wallet knows enough information to uniquely search for participant
Post-conditions	- Ban User flag is active in the participant's account information
Description	The CREDENTIAL Wallet processes the ban user requests. The participant is no longer be able to login to his account. The Wallet searches for the participant's account information. The ban user flag is activated in the participant's account information. The participant's account information is updated at the Participant Index.
Image	

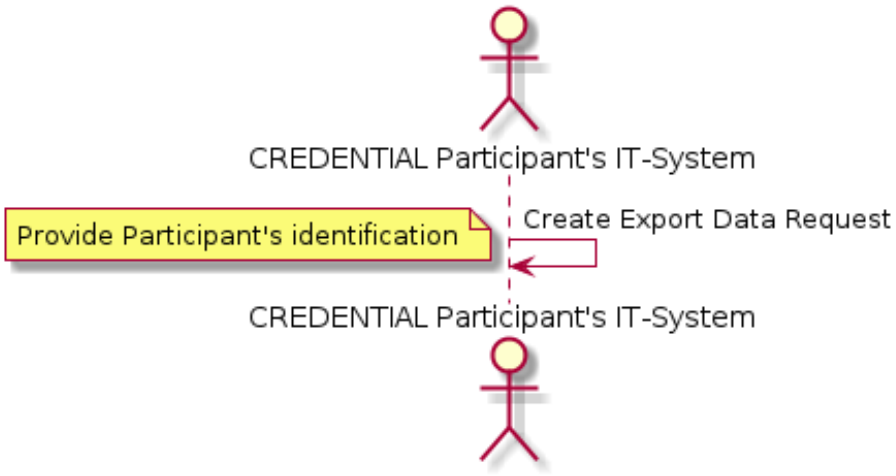
A.2.4.21 Submit Unban a User Request

Use Case Name	Submit Unban a User Request
ID	G-LUC-SUBMITUNBANUSERREQ
LUC_in	Unban a banned User
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Participant has created a unban a user request - Participant is logged in as Administrator
Post-conditions	- Unban a user request is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Administrator IT-System sends the Unban a user request to the CREDENTIAL Wallet.
Image	

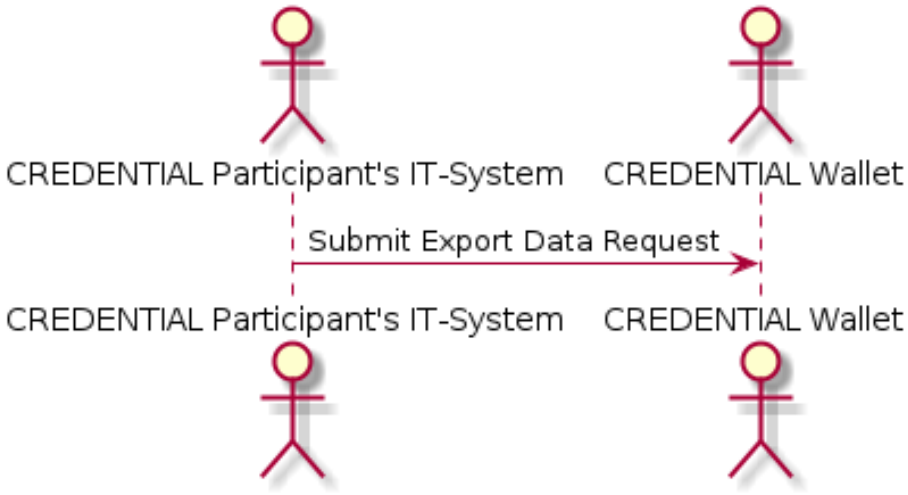
A.2.4.22 Unban User

Use Case Name	Unban User
ID	G-LUC-UNBANUSER
LUC_in	Unban a user
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Search Service - CREDENTIAL Participant Index
Pre-conditions	- Wallet knows enough information to uniquely search for participant
Post-conditions	- Ban User flag is deactive in the participant's account information
Description	The CREDENTIAL Wallet processes the unban user requests. The participant is now able to login to his account. The Wallet searches for the participant's account information. The ban user flag is deactivated in the participant's account information. The participant's account information is updated at the Participant Index.
Image	

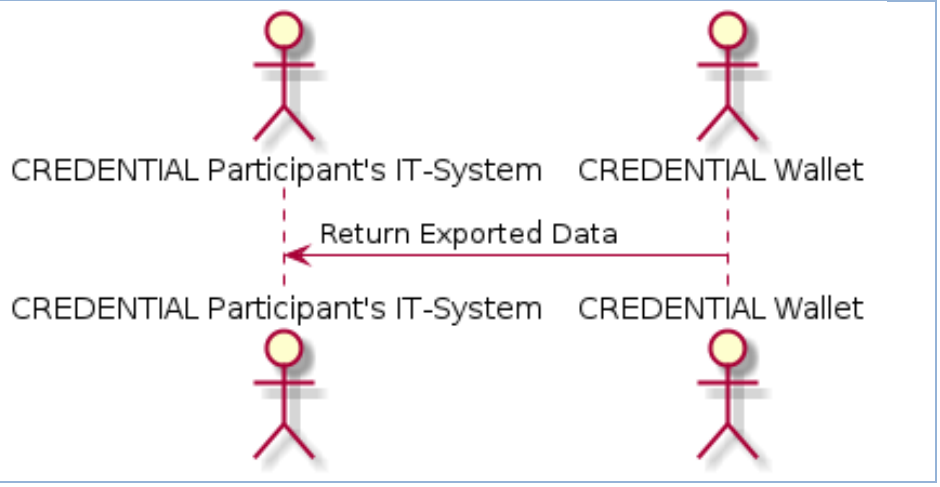
A.2.4.23 Create Export Data Request

Use Case Name	Create Export Data Request
ID	G-LUC-CREATEEXPORTDATAREQ
LUC_in	Export data from wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	
Pre-conditions	- Participant's identification is known
Post-conditions	- Export Data Request is created
Description	- The CREDENTIAL Participant creates an export data request.
Image	

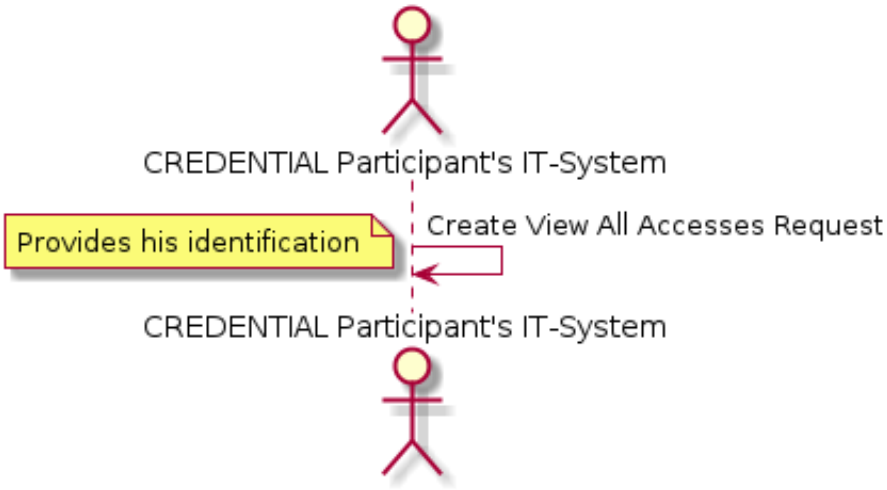
A.2.4.24 Submit Export Data Request

Use Case Name	Submit Export Data Request
ID	G-LUC-SUBEXPDATAREQ
LUC_in	Export data from wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Participant has created an Export Data Request
Post-conditions	- Export data request is available at the CREDENTIAL Wallet.
Description	The CREDENTIAL Participant's IT-System submits the export data request to the CREDENTIAL Wallet.
Image	

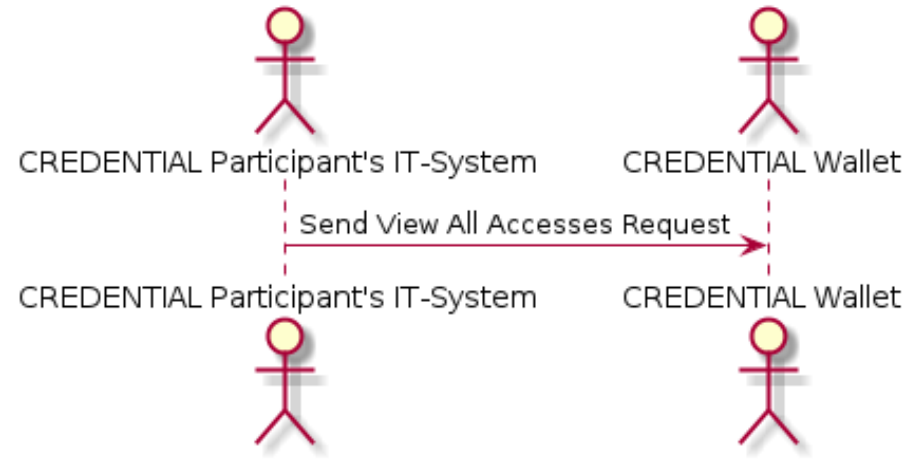
A.2.4.25 Return Exported Data

Use Case Name	Return Exported Data
ID	G-LUC-RETEXPDATA
LUC_in	Export data from wallet
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant requested an export data
Post-conditions	- Exported data is available at the Participant's IT-System
Description	The CREDENTIAL Wallet returns the exported data to the CREDENTIAL Participant's IT-System.
Image	

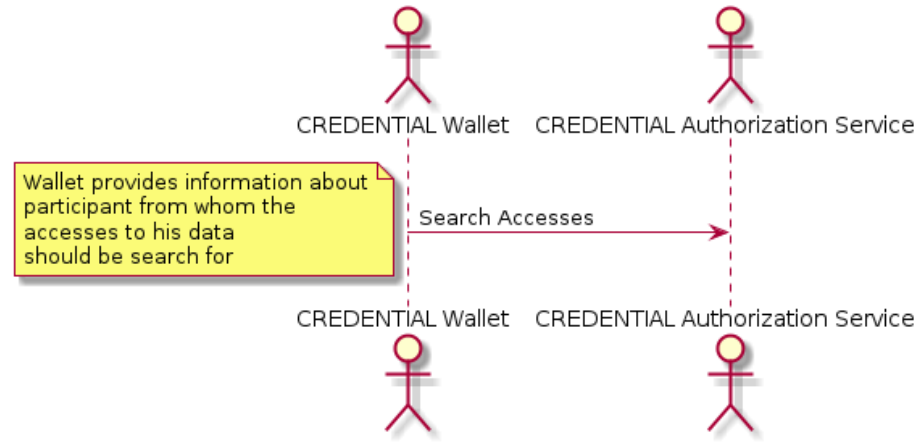
A.2.4.26 Create View All Accesses Request

Use Case Name	Create View All Accesses Request
ID	G-LUC-CREATEVIEWACCESSESREQ
LUC_in	View all accesses to my data
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	
Pre-conditions	- Participant identification is known to the Participant's IT-System
Post-conditions	- View All Accesses Request is created
Description	The CREDENTIAL Participant's IT-System creates a view all accesses request. He provides his participant identification (identifier or public key) in the request.
Image	

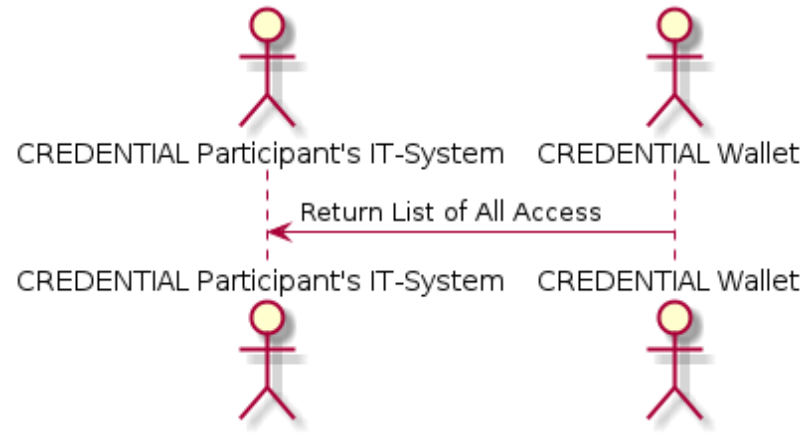
A.2.4.27 Submit View All Accesses Request

Use Case Name	Submit View All Accesses Request
ID	G-LUC-SUBMITVIEWACCESSESREQ
LUC_in	View all accesses to my data
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Participant is allowed to View all accesses to his data - Participant is authenticated against the CREDENTIAL Wallet
Post-conditions	- View All Accesses Request is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Participant's IT-System sends the view all accesses request to the CREDENTIAL Wallet.
Image	

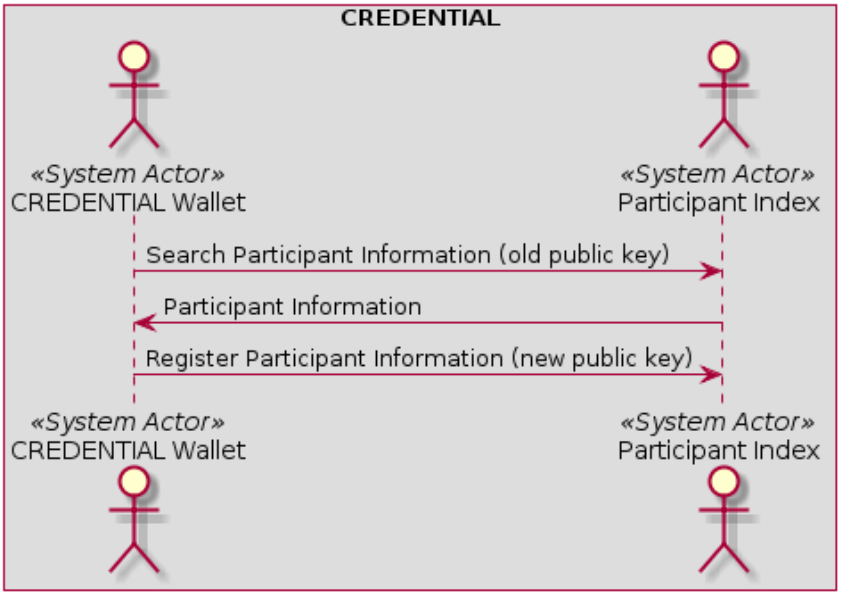
A.2.4.28 Search All Accesses

Use Case Name	Search All Accesses
ID	G-LUC-SEARCHACCESSES
LUC_in	View all accesses to my data
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Authorization Service
Pre-conditions	- Participant identification is available at the CREDENTIAL Wallet - View all accesses is provided to the CREDENTIAL Wallet
Post-conditions	- A list of all accesses is available at the CREDENTIAL Wallet
Description	The CREDENTIAL Wallet processes the view all accesses request.
Image	

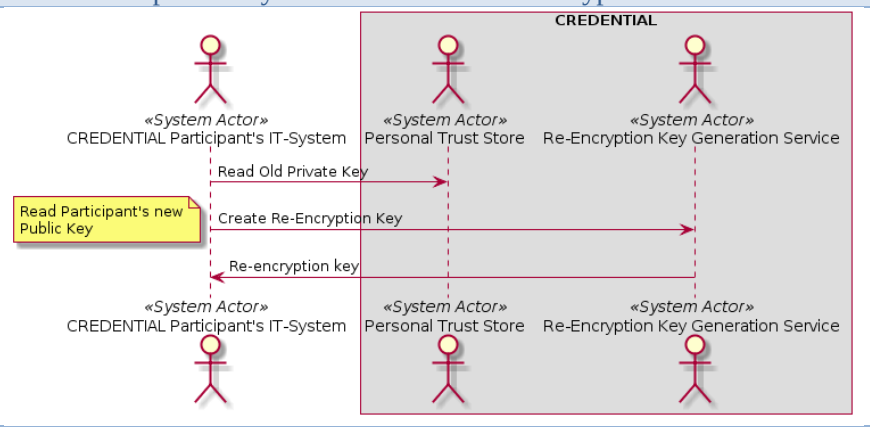
A.2.4.29 Return List of All Accesses

Use Case Name	Return List of All Accesses
ID	G-LUC-RETLISTALLACCESSES
LUC_in	View all accesses to my data
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant has requested the list of all access to his data
Post-conditions	- List of all access to participant's data is available at the Participant's IT-System
Description	The CREDENTIAL Wallet returns the list of all access to the CREDENTIAL Participant's IT-System
Image	

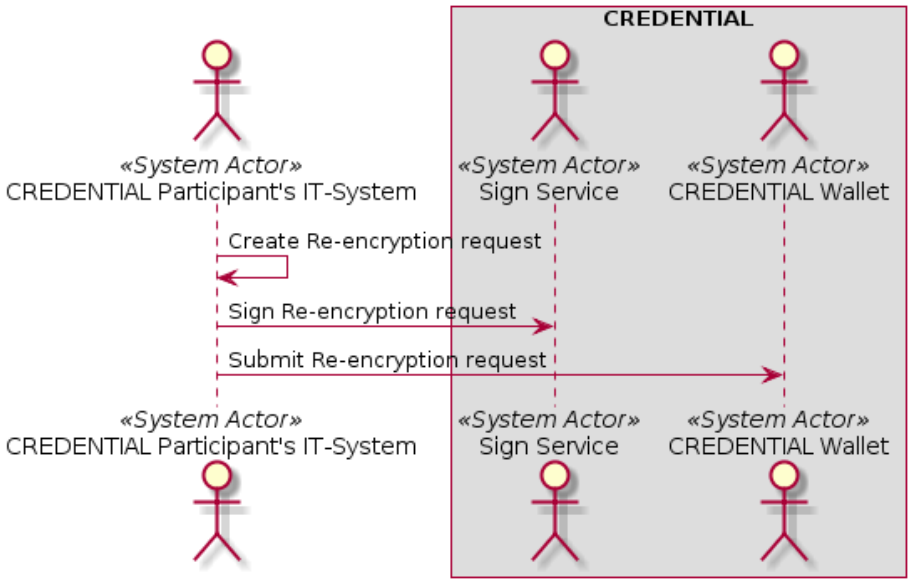
A.2.4.30 Associate new Keypair

Use Case Name	Associate new Keypair
ID	G-LUC-ASSOCKEYPAIR
LUC_in	Generate new access-key for CREDENTIAL Wallet
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant Index
Pre-conditions	
Post-conditions	
Description	Once the data is re-encrypted, the participant has to to be associates to his new public key, so other participant can create working re-encryption keys and it accepts operations related to the new public key pair
Image	

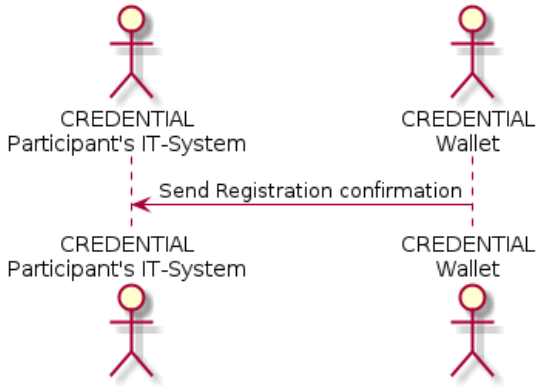
A.2.4.31 Generate Update Re-Encryption Key

Use Case Name	Generate Update Re-Encryption Key
ID	G-LUC-GENUPDREENCKEY
LUC_in	Generate new access-key for CREDENTIAL Wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store - CREDENTIAL Re-Encryption Key Generation Service
Pre-conditions	- There is data already encrypted with the old private key - The old private key is available - There is a new keypair
Post-conditions	- There is a re-encryption key that allows the Wallet to re-encrypt data encrypted with the old key
Description	A re-encryption key is created based on the old private key of the participant and his new public key so the data can be re-encrypted
Image	

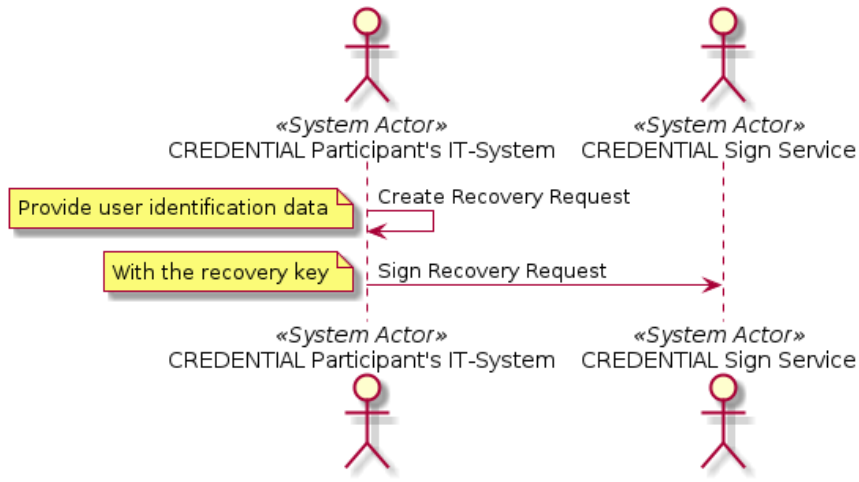
A.2.4.32 Create Re-Encryption Request

Use Case Name	Generate Re-Encryption Request
ID	G-LUC-GENREENCREQ
LUC_in	Generate new access-key for CREDENTIAL Wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Sign Service - CREDENTIAL Personal Trust Store
Pre-conditions	- The private key currently associated to the participant is available and there is a new re-encryption key available
Post-conditions	
Description	As the participant wishes to renew its keypair it is required to re-encrypt all encrypted data stored in the wallet. The request must be signed with the old private key to ensure the validity of the request
Image	

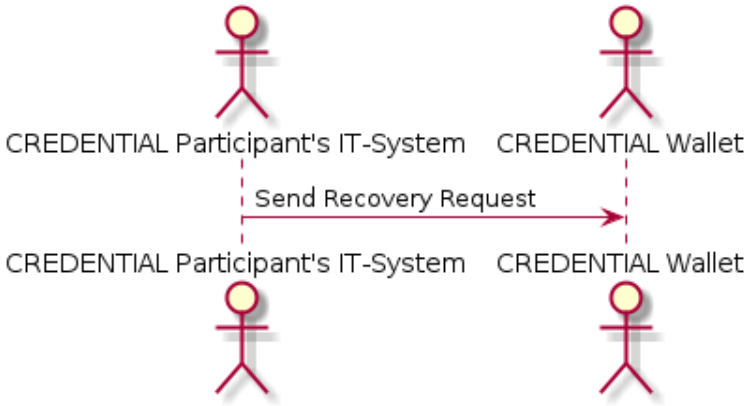
A.2.4.33 Data Registration Confirmed

Use Case Name	Data Registration Confirmed
ID	G-LUC-DATAREGCONF
LUC_in	Send Data
Main Actor	- CREDENTIAL Wallet
Secondary Actors	- CREDENTIAL Participant's IT-System
Pre-conditions	- Participant requests a registration to CREDENTIAL
Post-conditions	- Participant is informed about successfully registered
Description	The CREDENTIAL Wallet responds with a registration confirmation to the participant.
Image	

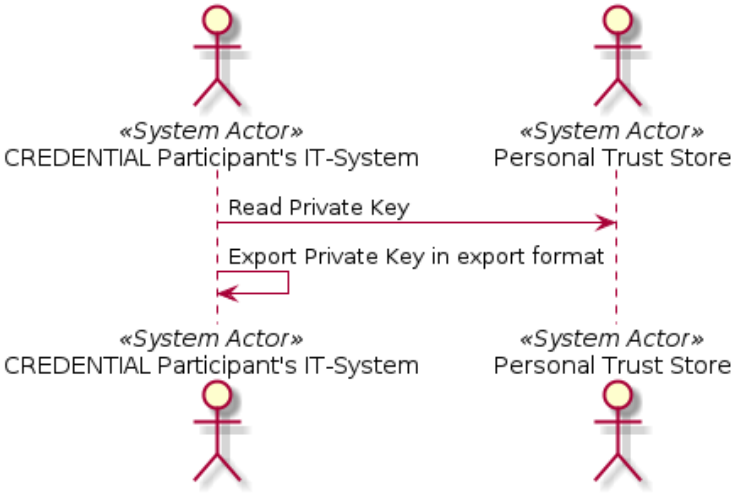
A.2.4.34 Create Recovery Request

Use Case Name	Create Recovery Request
ID	G-LUC-CREATERECREQ
LUC_in	Recover CREDENTIAL Wallet Data
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Sign Service
Pre-conditions	- Participant wants to recover his credentials
Post-conditions	- Recovery Request has been created
Description	A Participant want to recover his credentials for the CREDENTIAL Wallet. He creates a recovery request and signs it with his recovery key.
Image	

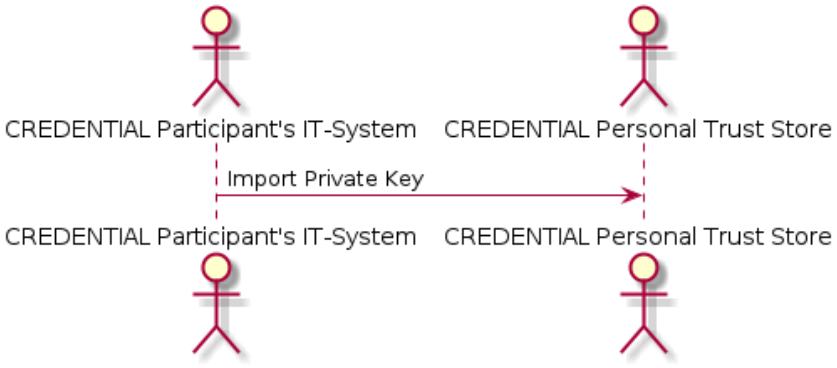
A.2.4.35 Submit Recovery Request

Use Case Name	Submit Recovery Request
ID	G-LUC-SUBMITRECOVREQ
LUC_in	Recover CREDENTIAL Wallet Data
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Wallet
Pre-conditions	- Recovery Request has been created
Post-conditions	- Recovery Request is available at the CREDENTIAL Wallet
Description	A participant transmits the recovery request to the CREDENTIAL Wallet.
Image	

A.2.4.36 Export Private Key

Use Case Name	Export Private Key
ID	G-LUC-EXPPRIVKEY
LUC_in	Register new device for accessing CREDENTIAL Wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store
Pre-conditions	- User has a private key for CREDENTIAL Wallet stored in his Personal Trust Store
Post-conditions	- Private Key is exported in an export format
Description	A user needs to export his private key. The key is exported in an export format.
Image	

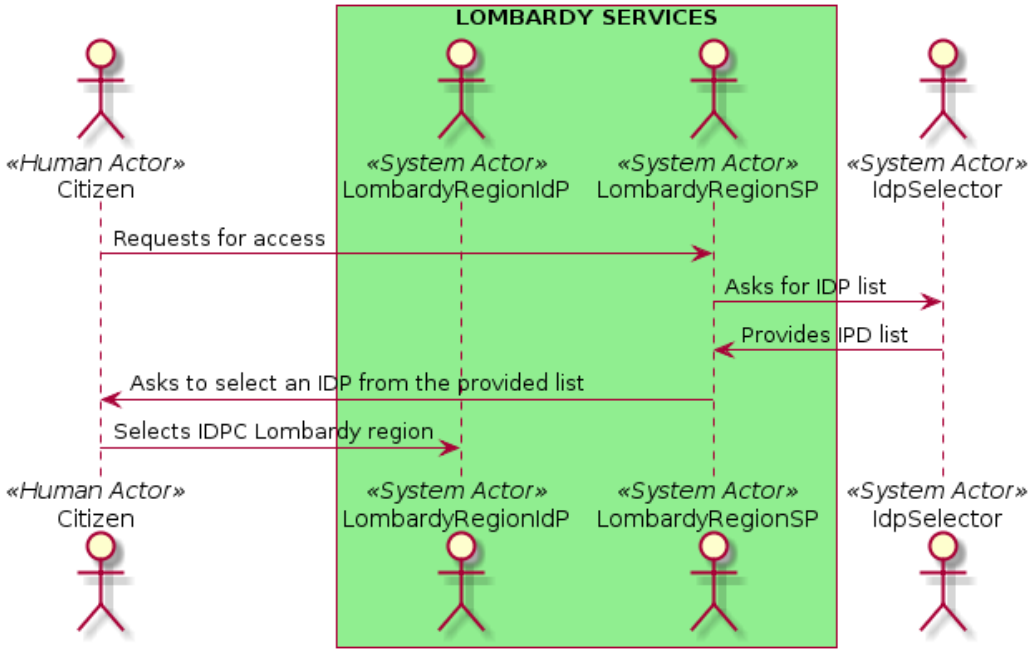
A.2.4.37 Import Private Key

Use Case Name	Import Private Key
ID	G-LUC-IMPPRIVKEY
LUC_in	Register new device for accessing CREDENTIAL Wallet
Main Actor	- CREDENTIAL Participant's IT-System
Secondary Actors	- CREDENTIAL Personal Trust Store
Pre-conditions	- Participant has a imported a private key on his IT-System
Post-conditions	- Private key is imported in CREDENTIAL Personal Trust Store
Description	In order to use the CREDENTIAL Wallet credentials a user has to provide them in his Personal Trust Store.
Image	

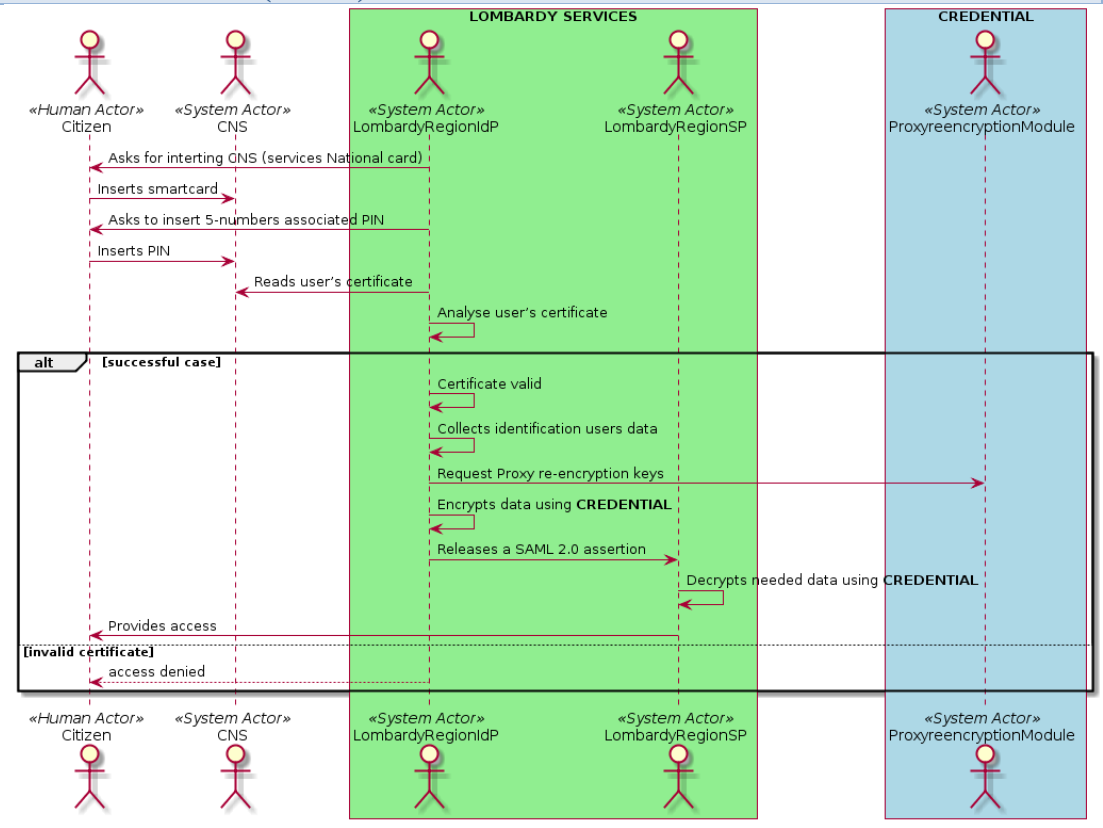
A.3 Pilot domains: eGovernment, eHealth, eBusiness

A.3.1 eGovernment

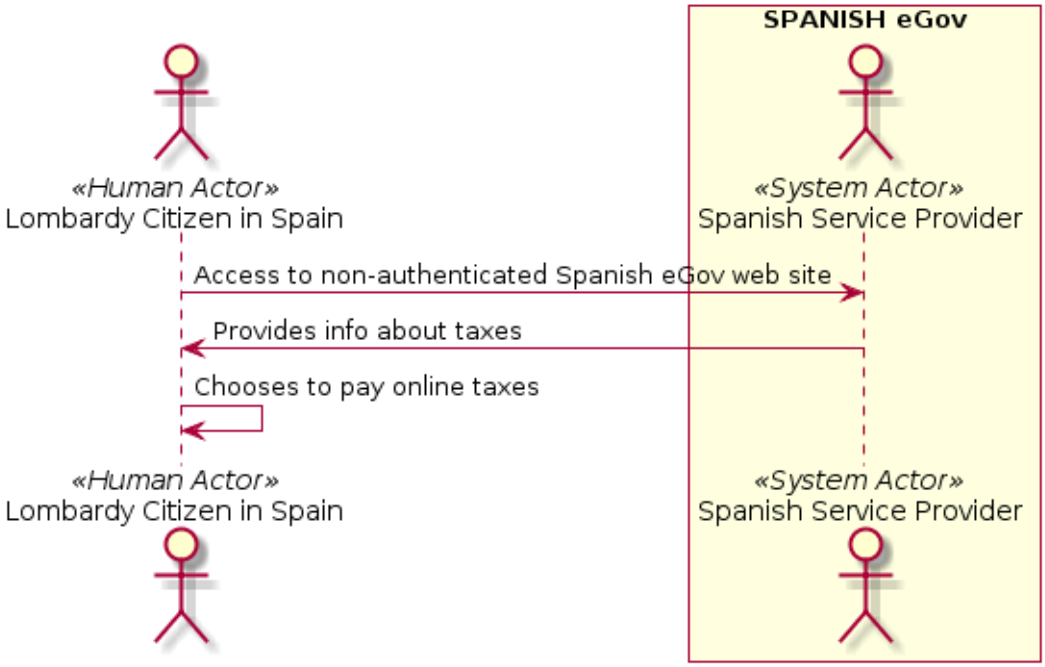
A.3.1.1 Citizen asks for a contribution from Lombardy Region

Use Case Name	Citizen asks for a contribution from Lombardy Region
ID	E-GOV-BUC-ASKLOMBCONTRIB #250
Related Generic Use Case	None
Main Actor	- Citizen
Secondary Actors	- Lombardy Region - IdP selector - Lombardy Region IdP (IdPC)
Pre-conditions	- Antonio needs some service offered by SIAGE web site, and has his CNS smartcard and PIN
Post-conditions	- Antonio selects IdPC from IdP list
Description	A citizen, called Antonio in the related story, needs to ask for a contribution from Lombardy Region.
Image	

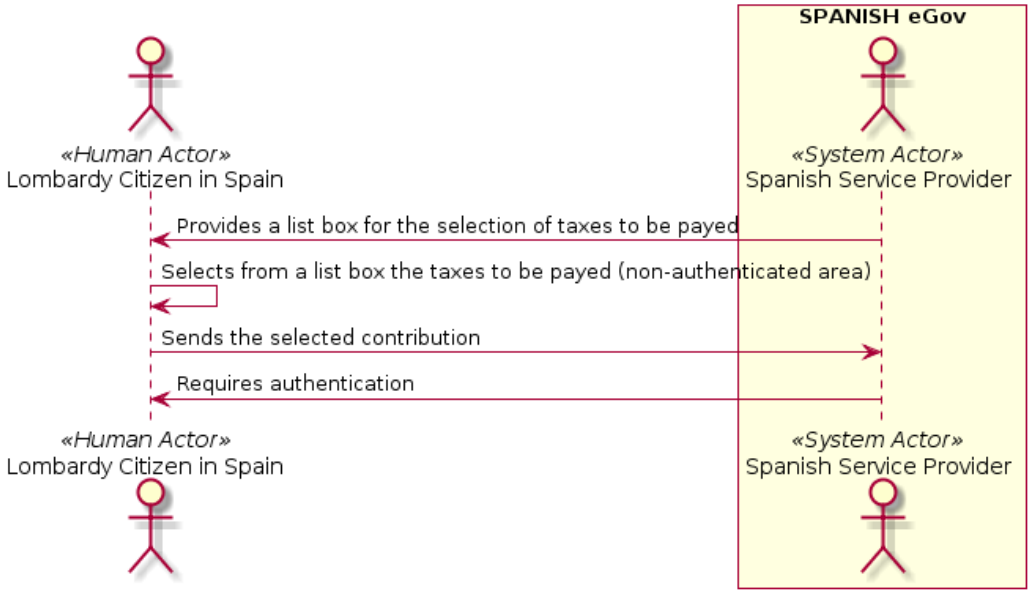
A.3.1.2 Citizen authenticates and access to SP

Use Case Name	Citizen authenticates and access to SP
ID	E-GOV-BUC-AUTHSP #251
Related Generic Use Case	- Authenticate towards a CREDENTIAL SP using CREDENTIAL Wallet and a CREDENTIAL-enabled IdP
Main Actor	- Citizen
Secondary Actors	- Lombardy Region IdP (IdPC) - Lombardy Region Region Service Provider - CNS - CREDENTIAL proxy re-encryptio Module
Pre-conditions	- User has previously inserted his CNS in smartcard reader
Post-conditions	- User successfully access to SP
Description	- A citizen, called Antonio in the related story, gains an authentication from Lombardy Region IdP (IdPC) using his CNS and successfully access to the Lombardy Region Service Provider (SIAGE).
Image	

A.3.1.3 Citizen pays some taxes using a Spain eGovernment website

Use Case Name	Citizen pays some taxes using a Spain eGovernment website
ID	E-GOV-BUC-PAYTAX #252
Related Generic Use Case	None
Main Actor	- Citizen
Secondary Actors	- Spain - CREDENTIAL Service Provider
Pre-conditions	- User has the needs to pay online some taxes
Post-conditions	- User chooses taxes to pay online
Description	An Italian citizen, named Danilo in the related story, needs to pay some taxes using a Spain eGovernment website.
Image	

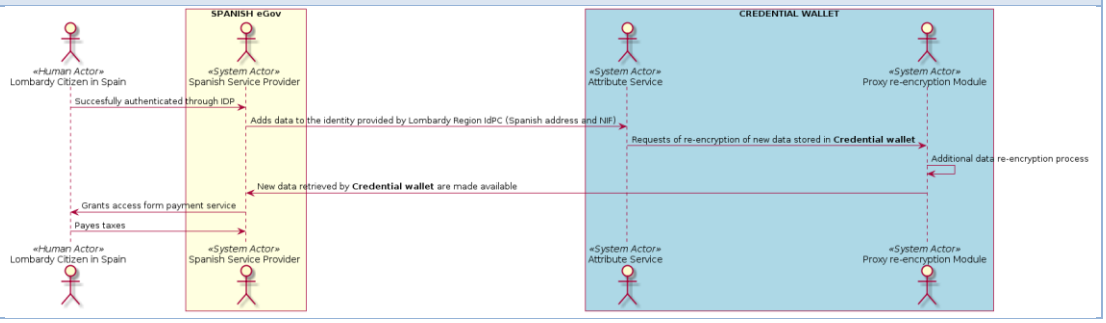
A.3.1.4 Citizen chooses taxes to pay and try to access to SP

Use Case Name	Citizen chooses taxes to pay and try to access to SP
ID	E-GOV-BUC-ACCSP #262
Related Generic Use Case	none
Main Actor	- Citizen
Secondary Actors	- CREDENTIAL Service Provider
Pre-conditions	- User has identified the tax to be paid
Post-conditions	- User is challenged to perform a strong authentication
Description	Danilo chooses the right taxes to pay and prepare to access to an authenticated area of the Spanish web site.
Image	

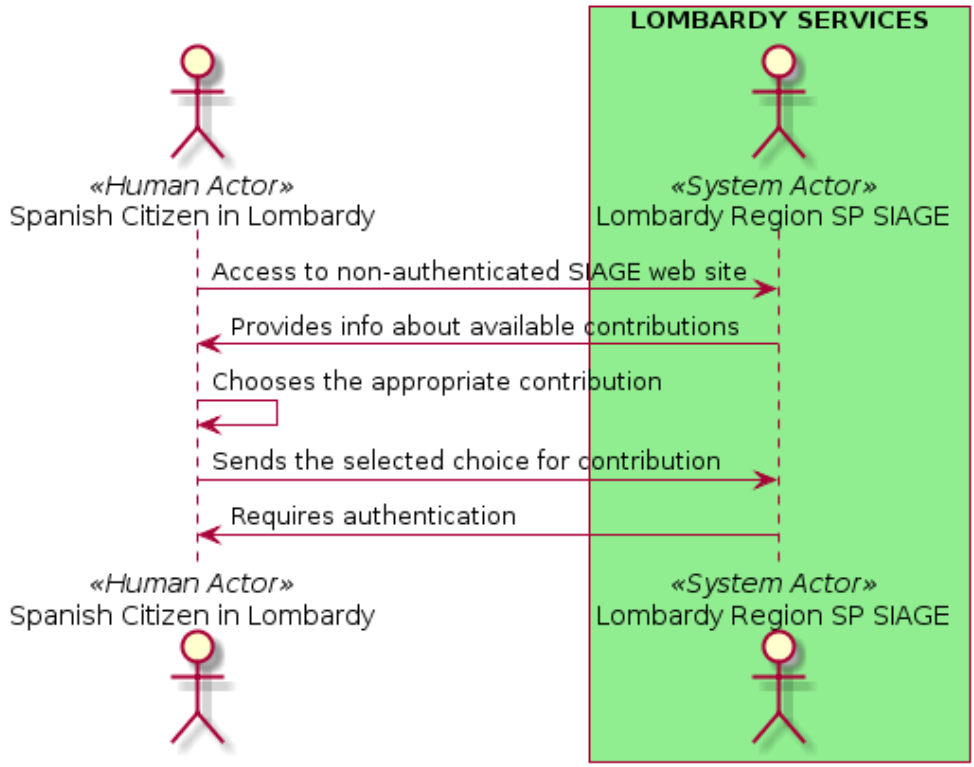
A.3.1.5 Citizen performs authentication

Use Case Name	Citizen performs authentication
ID	E-GOV-BUC-AUTHENT #263
Related Generic Use Case	none
Main Actor	- Citizen
Secondary Actors	- CREDENTIAL Service Provider - IdP selector - Lombardy Region IdP (IdPC) - CNS - CREDENTIAL proxy re-encryption Module - STORK adapter
Pre-conditions	- User has at least one token suitable for at least one CREDENTIAL IdP
Post-conditions	- IdPC releases an authentication token for the user
Description	Danilo performs authentication using his domestic IdP.
Image	

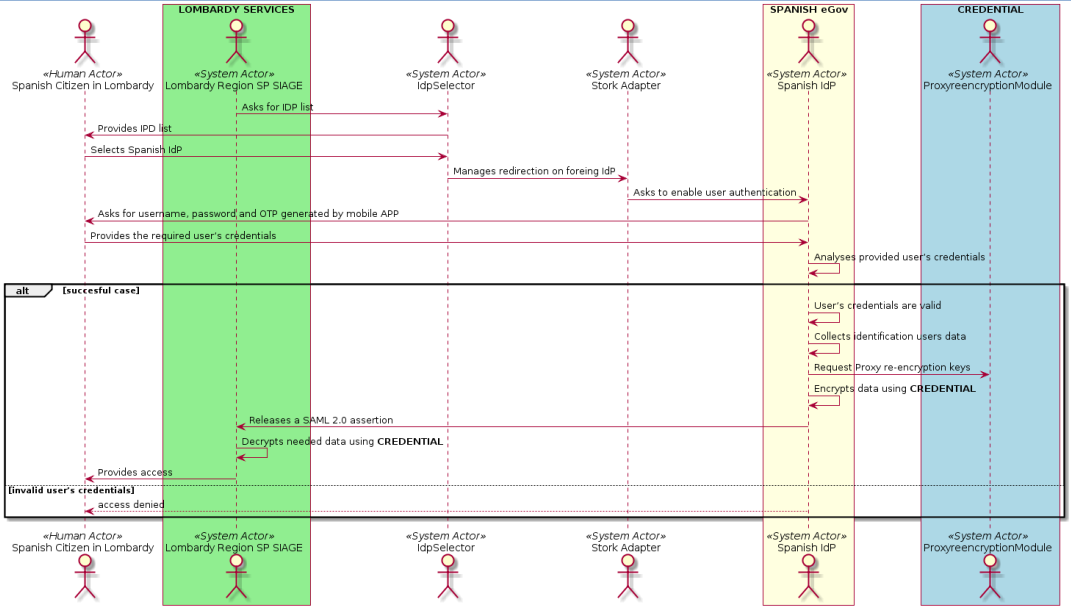
A.3.1.6 Citizen pays taxes on Spanish eGovernment website

Use Case Name	Citizen pays taxes on Spanish eGovernment website
ID	E-GOV-BUC-COMPLETEPAYM #264
Related Generic Use Case	- Proxy Re-Encryption
Main Actor	- Citizen
Secondary Actors	- CREDENTIAL Service Provider - CREDENTIAL Wallet - CREDENTIAL proxy re-encryption Module
Pre-conditions	- User has been successfully authenticated by an IdP
Post-conditions	- User successfully access to SP
Description	After a successful authentication, Italian citizen is ready to pay taxes in the Spanish eGovernment website.
Image	

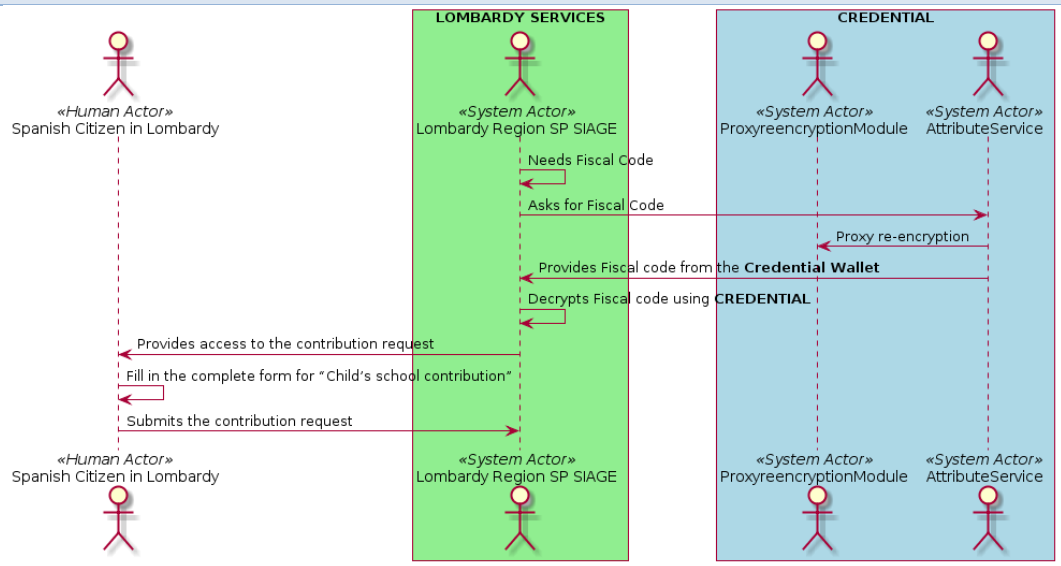
A.3.1.7 Foreign citizen looks for a contribution from Lombardy Region

Use Case Name	Foreign citizen looks for a contribution from Lombardy Region
ID	E-GOV-BUC-FOREIGNASKCONTRIB #265
Related Generic Use Case	
Main Actor	- Citizen
Secondary Actors	- Lombardy Region Service Provider - Lombardy Region
Pre-conditions	- User has a contribution need
Post-conditions	- User finds an appropriate contribution on SIAGE
Description	A foreign citizen living in Italy, named Cristiano in the related story, needs a contribution from Lombardy Region.
Image	

A.3.1.8 Citizen gains on-line authentication

Use Case Name	Citizen gains on-line authentication
ID	E-GOV-BUC-FOREIGNAUTH #284
Related Generic Use Case	- Authentication towards a CREDENTIAL SP using CREDENTIAL Wallet and a IdP
Main Actor	- Citizen
Secondary Actors	- IdP selector - Spanish IdP - CREDENTIAL proxy re-encryptio Module - STORK adapter
Pre-conditions	- User has previously choose a contribution request on SIAGE
Post-conditions	- User gets authentication from Spanish IdP
Description	A strong authentication is required from SIAGE prior to the request is submitted by the user.
Image	

A.3.1.9 Citizen completes online request to SIAGE

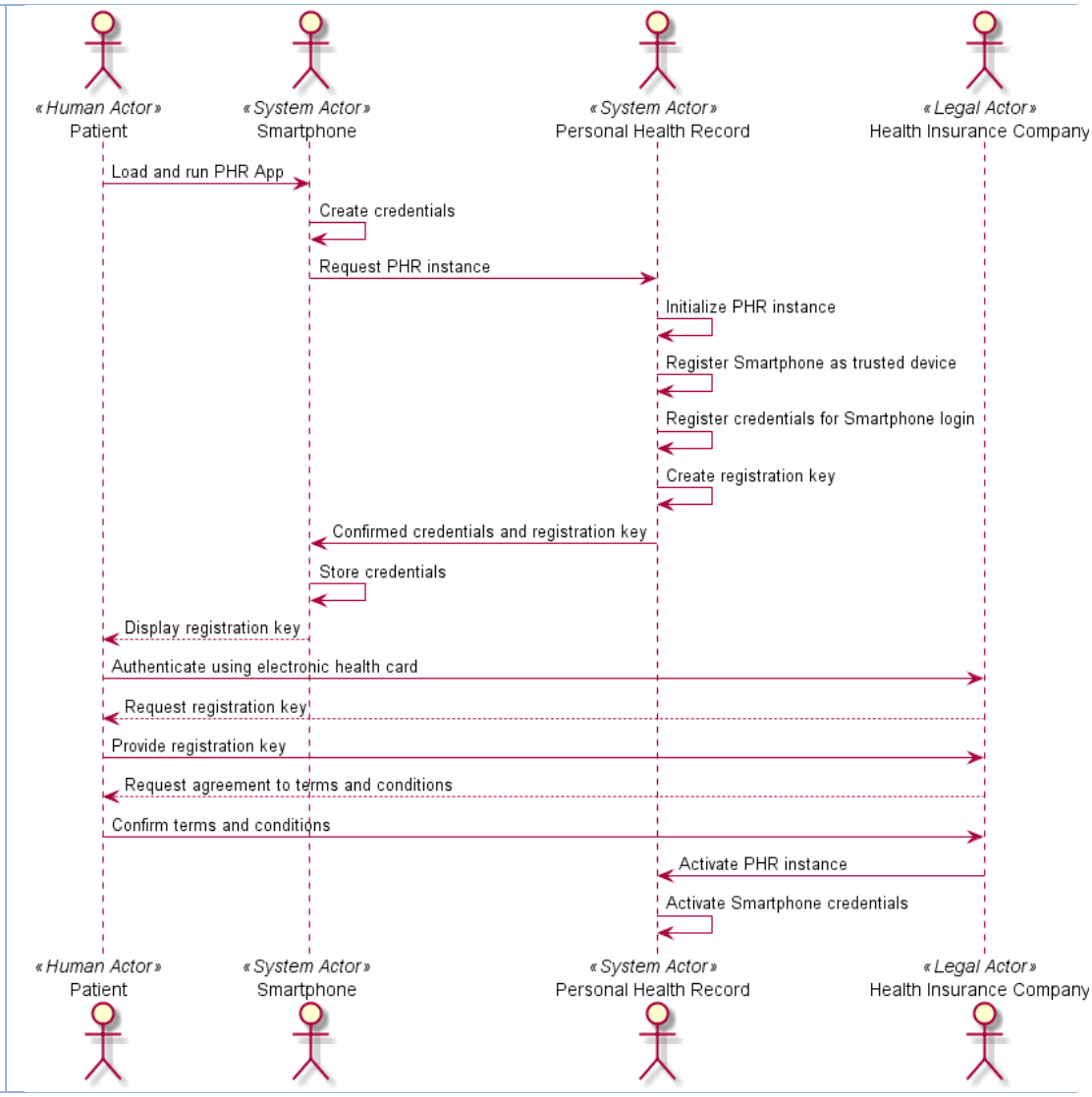
Use Case Name	Citizen completes online request to SIAGE
ID	E-GOV-BUC-FOREIGNCOMPLCONTRIB #287
Related Generic Use Case	- Selective Disclosure - Proxy re-encryption
Main Actor	- Citizen
Secondary Actors	- Lombardy Region Service Provider - CREDENTIAL Wallet - CREDENTIAL proxy re-encryption Module
Pre-conditions	- User has been successfully authenticated by IdP
Post-conditions	- User is logged into SP
Description	Adriano can now access to SIAGE in order to submit the needed contribution request.
Image	

A.3.2 eHealth

A.3.2.1 Setup and Configure PHR

Use Case Name	Setup and Configure PHR
ID	E-HEA-BUC-SETUPCONFPHR
Related Generic Use Case	none
Main Actor	- Personal Health Record (PHR)
Secondary Actors	- Patient - Health Insurance Company - Smartphone
Pre-conditions	- The patient's statutory health insurance is operating a PHR platform for its customers/members. - The patient fulfills the health insurance's conditions for subscribing to the PHR platform. - The patient holds credentials that allow the health insurance company to univocally identify him and securely authenticate him.
Post-conditions	- A shared Personal Health record (PHR) has been set up and is ready for collecting and sharing medical data about the patient. - The patient has signed the PHR provider's terms and conditions and is aware about how to use the various services the PHR platform offers. - As the owner of his PHR the patient is given all tokens/credentials he needs for securely interacting with the PHR and for granting permissions to other actors. - The patient's Smartphone is registered as a trusted device with the PHR.
Description	The patient downloads the PHR App and installs it on his Smartphone. Through a handshake between the PHR and the Smartphone, his Smartphone gets registered as a trusted device for interacting with the PHR. The patient identifies and authenticates himself with his health insurance company through the company's web portal. He provides a link to his newly created PHR instance and requests the health insurance company for accepting all related costs within a specific patient compliance program. After agreeing to the terms and conditions for using a PHR and for participating in the compliance program, the previously set up PHR instance is activated through the health insurance company.

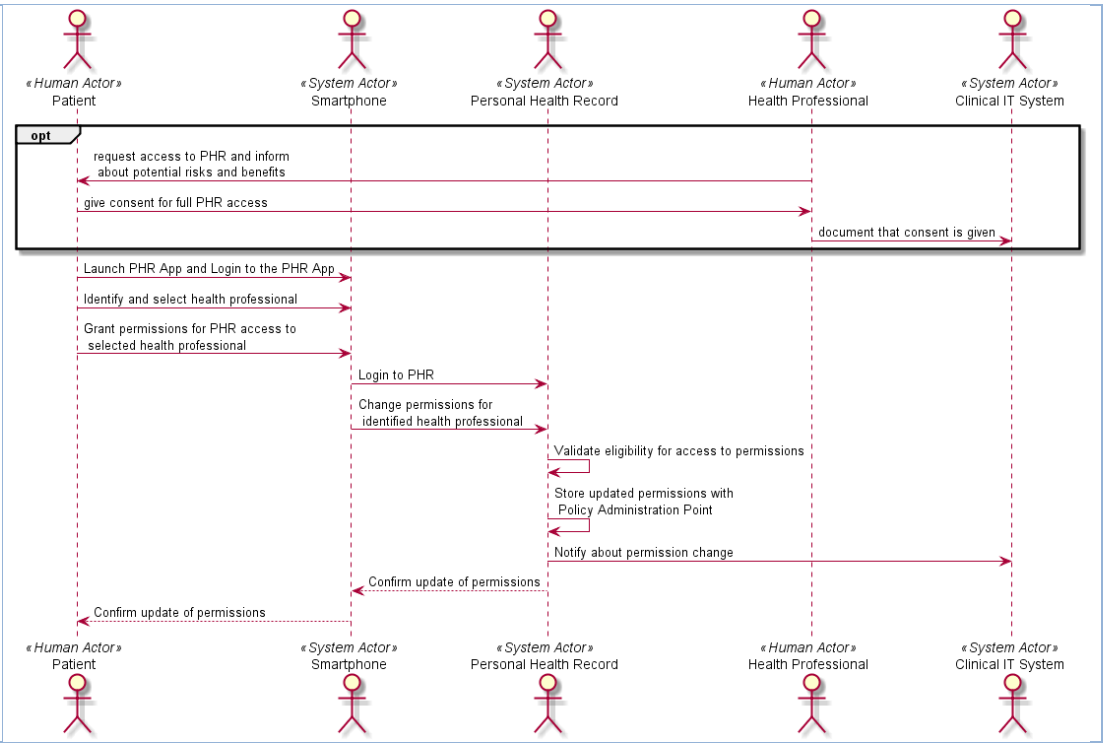
Image


«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record
«Legal Actor»
Health Insurance Company
Load and run PHR App
Create credentials
Request PHR instance
Initialize PHR instance
Register Smartphone as trusted device
Register credentials for Smartphone login
Create registration key
Confirmed credentials and registration key
Store credentials
Display registration key
Authenticate using electronic health card
Request registration key
Provide registration key
Request agreement to terms and conditions
Confirm terms and conditions
Activate PHR instance
Activate Smartphone credentials
«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record
«Legal Actor»
Health Insurance Company

A.3.2.2 Grant Permission

Use Case Name	Grant Permission
ID	E-HEA-BUC-GRANDPERM
Related Generic Use Case	Grant Access Rights
Main Actor	- Personal Health Record (PHR)
Secondary Actors	- Patient - Health Professional - Smartphone
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data - The patient is equipped with a Smartphone that has been registered as a trusted device with the PHR - The patient has been advised and trained in interacting with the PHR - The patient is able to identify the health professional he wants to authorize for accessing his PHR
Post-conditions	- A health professional is granted CRUD (create, read, update, delete) permissions for accessing the patient's PHR - The health professional is informed about the authorization and provided with all information he needs for securely connecting to the patient's PHR.
Description	The patient gives informed consent to a health professional for accessing his PHR. Depending on national legislation this consent may either be given on paper, orally or implicitly by granting permissions for PHR access to the physician. In any case the patient needs to register the permissions given through the consent with the PHR using his smartphone: - The patient launches the PHR app on his smartphone and connects to the PHR - The patient identifies the health professional by using respective directory services which are provided through the PHR app on his smartphone - The patient states that the selected health professional is allowed to provide data to the PHR and to read data from the PHR. A default value for the validity time of the permission is set which can be overwritten by the patient during this step. After the authorization of the health professional is registered with the PHR, the PHR sends a respective notification to the health professional.

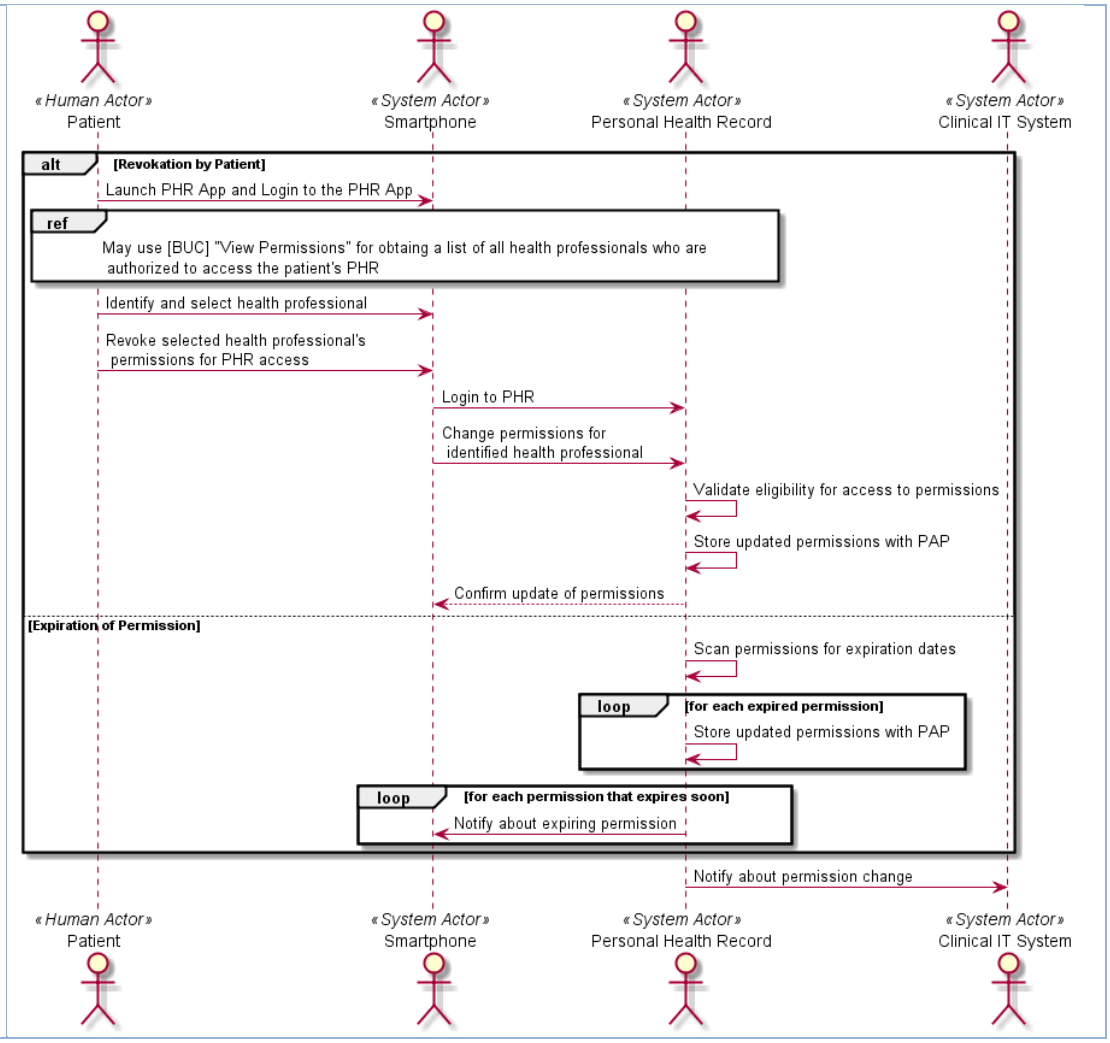
Image


«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record
«Human Actor»
Health Professional
«System Actor»
Clinical IT System
opt
request access to PHR and inform about potential risks and benefits
give consent for full PHR access
document that consent is given
Launch PHR App and Login to the PHR App
Identify and select health professional
Grant permissions for PHR access to selected health professional
Login to PHR
Change permissions for identified health professional
Validate eligibility for access to permissions
Store updated permissions with Policy Administration Point
Notify about permission change
Confirm update of permissions
Confirm update of permissions
«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record
«Human Actor»
Health Professional
«System Actor»
Clinical IT System

A.3.2.3 Revoke Permission

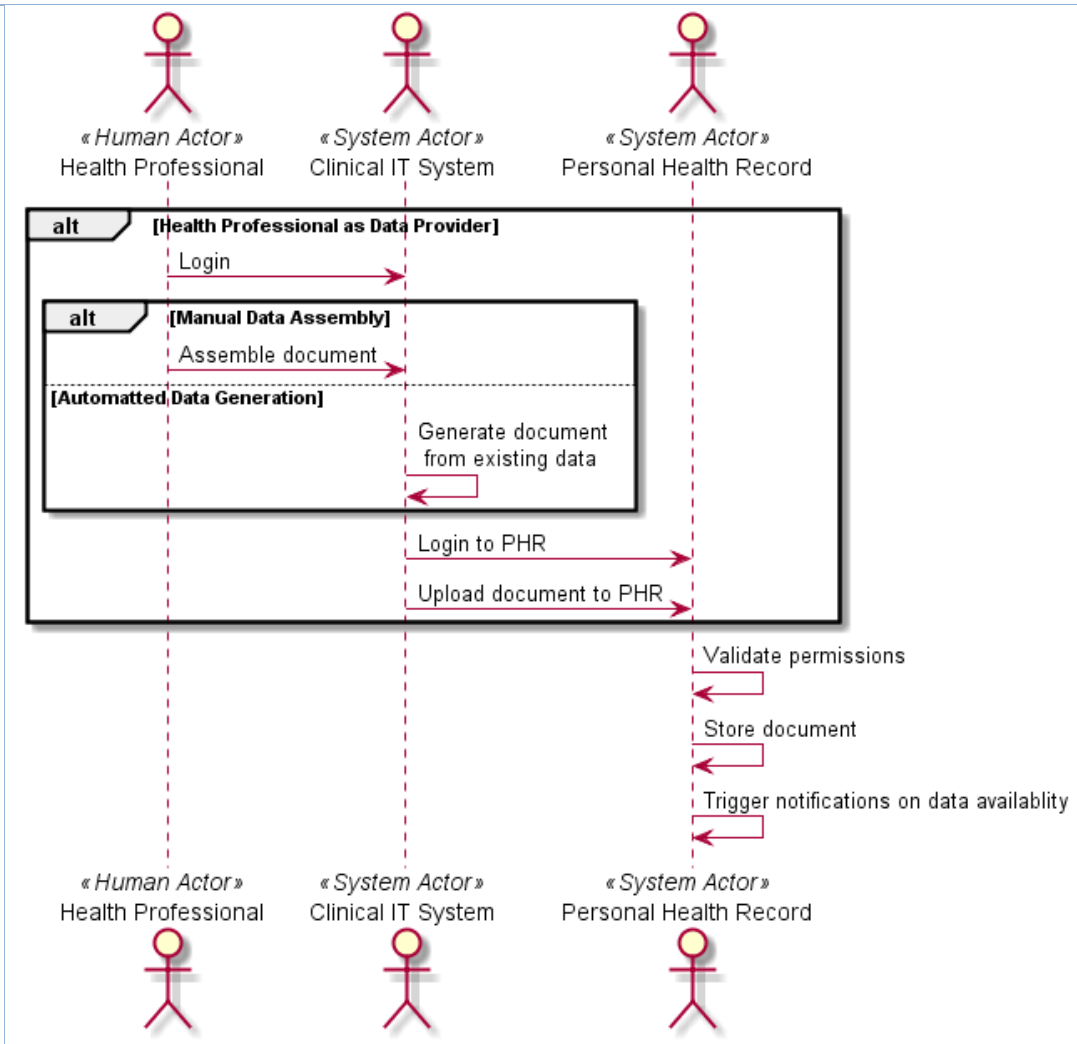
Use Case Name	Revoke Permission
ID	E-HEA-BUC-REVOKEPERM
Related Generic Use Case	Grant Access Rights
Main Actor	- Personal Health Record (PHR)
Secondary Actors	- Patient - Health Professional - Smartphone
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data - The patient is equipped with a Smartphone that has been registered as a trusted device with the PHR - The patient has been advised and trained in interacting with the PHR - The Health professional has been granted access rights to the PHR by the patient
Post-conditions	- Formerly granted permissions to a health professional are revoked. The health professional is no longer able to access the patient's PHR - The health professional is informed about the revocation of permissions.
Description	Granted permissions can get revoked either explicitly by the patient or implicitly by reaching their expiration date. Explicit Revocation: - The patient launches the PHR app on his smartphone and connects to the PHR. - The patient identifies the health professional whose permissions are to be revoked. - The patient states that the selected health professional is no longer allowed to provide data to the PHR or to read data from the PHR. - The affected health professional gets informed about the revocation of permissions. Implicit Revocation: - The PHR regularly scans all permissions for their expiration dates. - If an expired permission is detected, the respective access rights are revoked and a notification is sent to the patient and the affected health professional

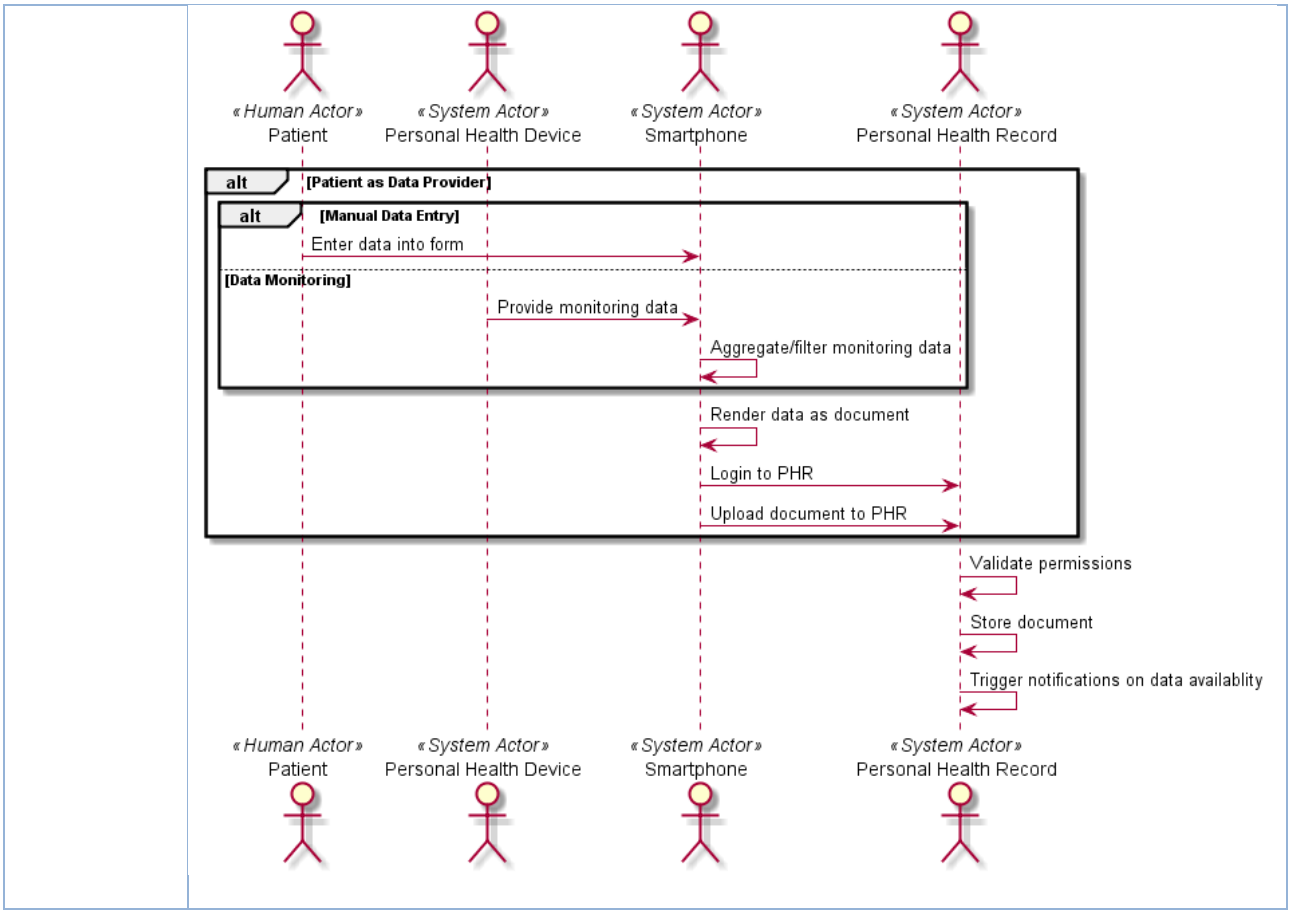
Image


«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record
«System Actor»
Clinical IT System
alt
[Revokation by Patient]
Launch PHR App and Login to the PHR App
ref
May use [BUC] "View Permissions" for obtaing a list of all health professionals who are authorized to access the patient's PHR
Identify and select health professional
Revoke selected health professional's permissions for PHR access
Login to PHR
Change permissions for identified health professional
Validate eligibility for access to permissions
Store updated permissions with PAP
Confirm update of permissions
[Expiration of Permission]
Scan permissions for expiration dates
loop
[for each expired permission]
Store updated permissions with PAP
loop
[for each permission that expires soon]
Notify about expiring permission
Notify about permission change
«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record
«System Actor»
Clinical IT System

A.3.2.4 Send (Medical) Data

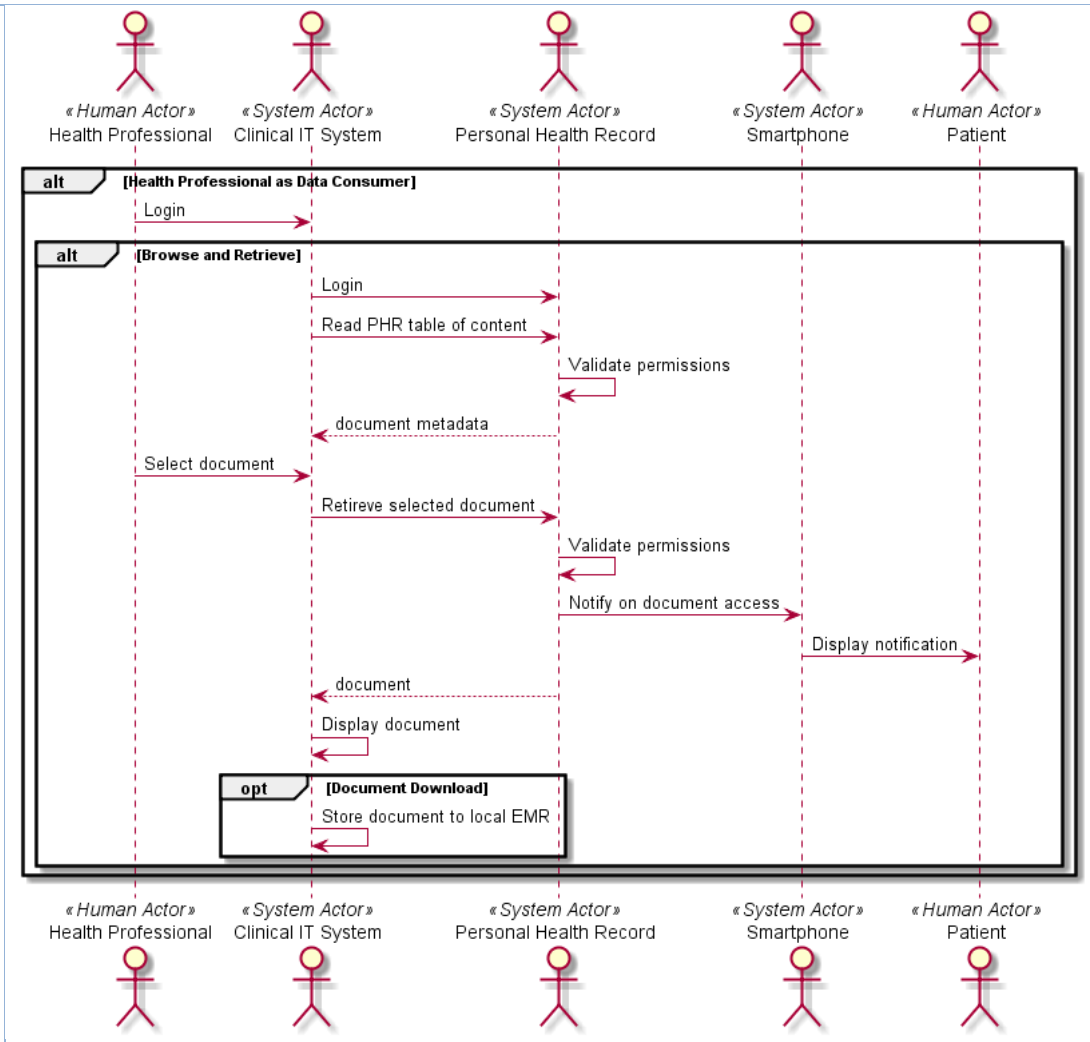
Use Case Name	Send (Medical) Data
ID	E-HEA-BUC-SENDMEDDATA
Related Generic Use Case	Send Data
Main Actor	- Personal Health Record (PHR)
Secondary Actors	- Patient - Health Professional - Personal Health Device - Smartphone - Clinical IT System
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data - The patient is equipped with a smartphone that has been registered as a trusted device with the PHR - The patient has been advised and trained in interacting with the PHR - If data is to be provided by a health professional: The health professional has been granted access rights to the PHR by the patient - If data is to be provided through a personal health device: The personal health device is paired with the patient's smartphone
Post-conditions	- New data is stored in the patient's PHR - Authorized PHR users are able to access this data - Notifications on data availability are triggered
Description	New data can be stored in a PHR from four different sources: 1. A healthcare professional assembles a new document at his clinical IT system and provides it to the patient's PHR 2. The healthcare professional's clinical IT system regularly and automatically renders a document from existing data and uploads it to the patient's PHR 3. The patient provides data to the PHR through an interactive form or any other data capturing service on his smartphone 4. A personal health device regularly monitors data of the patient. The patient's smartphone accepts this data, aggregates/filters it through an app that came with the personal health device and upload the data to the patient's PHR All alternatives require that the data sender is authenticated and authorized with the PHR. Ideally authentication relies on the principle of brokered trust so that the PHR accepts a formerly done authentication to a trusted device/environment. Whenever new data is uploaded to the PHR a notification is triggered and send to all authorized users (see BUC "Read (Medical) Data" on how this is processed).
Image	For reasons of readability alternatives 1+2 and 3+4 are shown in separate figures.

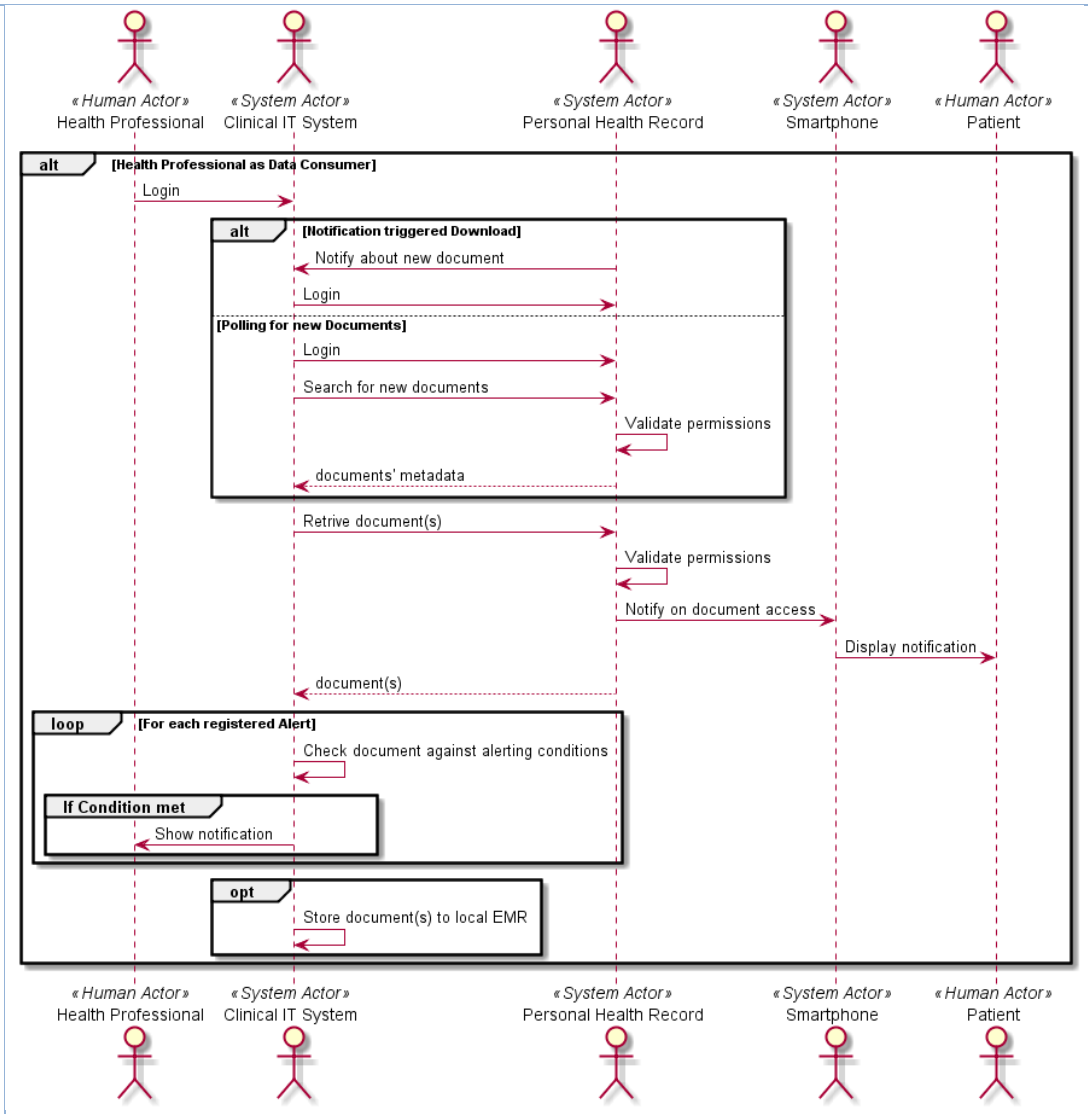

«Human Actor»
Health Professional
«System Actor»
Clinical IT System
«System Actor»
Personal Health Record
alt
[Health Professional as Data Provider]
Login
alt
[Manual Data Assembly]
Assemble document
[Automatted Data Generation]
Generate document from existing data
Login to PHR
Upload document to PHR
Validate permissions
Store document
Trigger notifications on data availablity
«Human Actor»
Health Professional
«System Actor»
Clinical IT System
«System Actor»
Personal Health Record

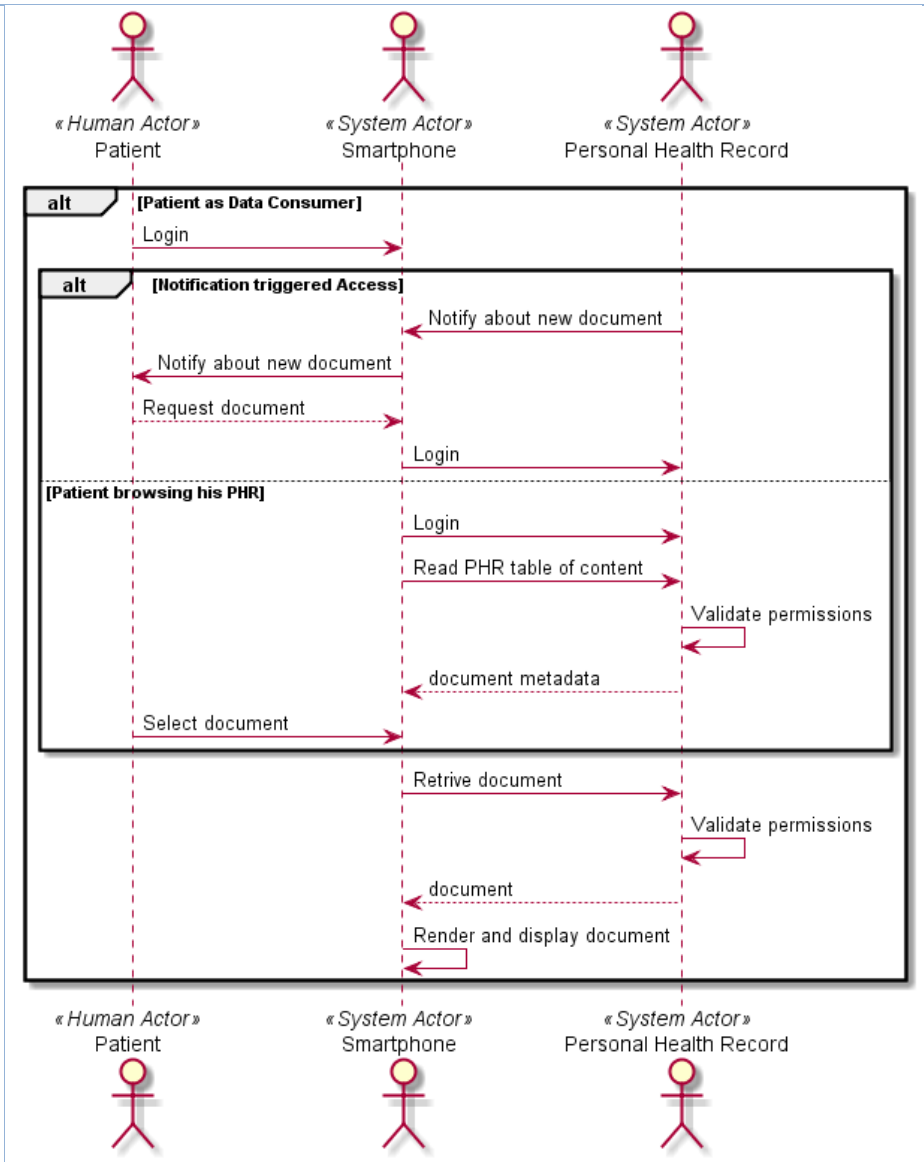

«Human Actor»
Patient
«System Actor»
Personal Health Device
«System Actor»
Smartphone
«System Actor»
Personal Health Record
alt
[Patient as Data Provider]
alt
[Manual Data Entry]
Enter data into form
[Data Monitoring]
Provide monitoring data
Aggregate/filter monitoring data
Render data as document
Login to PHR
Upload document to PHR
Validate permissions
Store document
Trigger notifications on data availablity
«Human Actor»
Patient
«System Actor»
Personal Health Device
«System Actor»
Smartphone
«System Actor»
Personal Health Record

A.3.2.5 Read (Medical) Data

Use Case Name	Read (Medical) Data
ID	E-HEA-BUC-READMEDDATA
Related Generic Use Case	Read Data
Main Actor	- Personal Health Record (PHR)
Secondary Actors	- Patient - Health Professional - Personal Health Device - Smartphone - Clinical IT System
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data - The patient is equipped with a smartphone that has been registered as a trusted device with the PHR - The patient has been advised and trained in interacting with the PHR - If data is to be accessed by a health professional: The health professional has been granted access rights to the PHR by the patient
Post-conditions	- Data is read from the patient's PHR and may be stored by the user for further processing - A notification has been sent to the patient that a health professional accessed his medical data
Description	Data can be read from a PHR in five different ways: 1. A healthcare professional browses the patient's PHR and opens selected documents. These documents may then be downloaded into the health professional's clinical IT system. 2. A healthcare professional's IT system receives a notification about new data available and downloads the document for local visualization and processing. 3. The healthcare professional's clinical IT system regularly polls the patient's PHR for new data and automatically downloads the document for local visualization and processing. 4. The patient logs into his own PHR via his smartphone and oversees the data available. He visualizes selected documents. 5. The patient's smartphone receives a notification about new data available and notifies the patient about this. The patient oversees the document on his smartphone. All alternatives require that the data user is authenticated and authorized with the PHR. Ideally authentication relies on the principle of brokered trust so that the PHR accepts a formerly done authentication to a trusted device/environment. Alternatives 2 and 3 may be used in conjunction with registered alerts (see BUC "Register Alert"). In this case each new document is assessed if it matches specific rules which were defined as alerting conditions. If an alerting condition is met, a respective notification is shown to the healthcare professional. In each scenario where a health professional accesses a patient's PHR data, a respective notification is send to the patient via his smartphone.
Image	For reasons of readability alternatives 1, 2+3 and 4+5 are shown in separate figures.


«Human Actor»
Health Professional
«System Actor»
Clinical IT System
«System Actor»
Personal Health Record
«System Actor»
Smartphone
«Human Actor»
Patient
alt
[Health Professional as Data Consumer]
Login
alt
[Browse and Retrieve]
Login
Read PHR table of content
Validate permissions
document metadata
Select document
Retireve selected document
Validate permissions
Notify on document access
Display notification
document
Display document
opt
[Document Download]
Store document to local EMR
«Human Actor»
Health Professional
«System Actor»
Clinical IT System
«System Actor»
Personal Health Record
«System Actor»
Smartphone
«Human Actor»
Patient

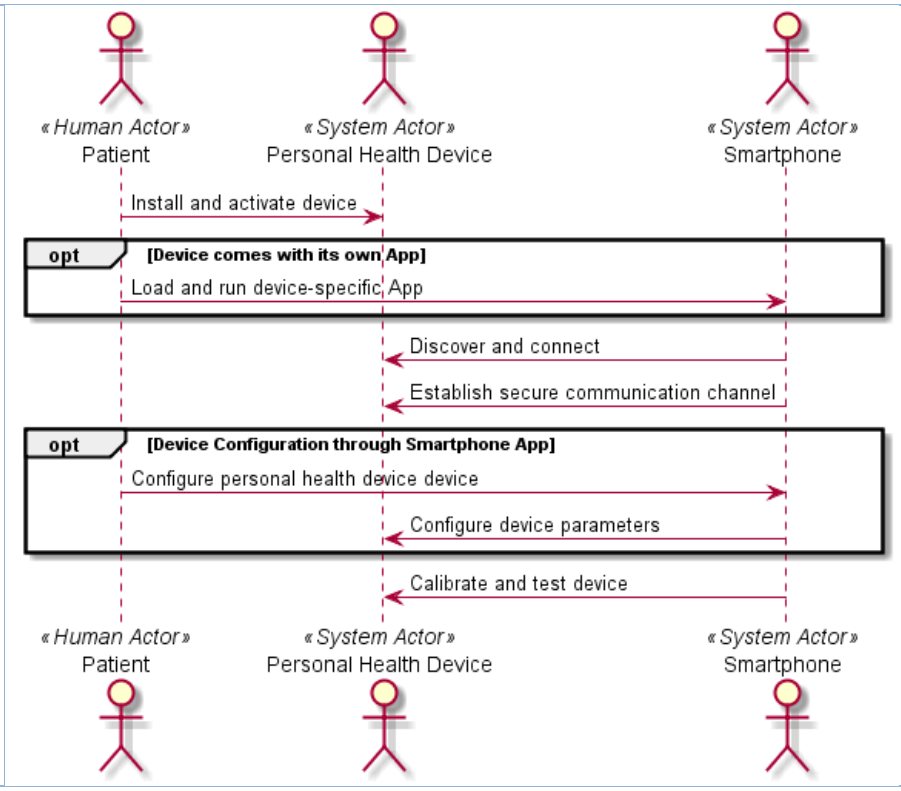

«Human Actor»
Health Professional
«System Actor»
Clinical IT System
«System Actor»
Personal Health Record
«System Actor»
Smartphone
«Human Actor»
Patient
alt
[Health Professional as Data Consumer]
Login
alt
[Notification triggered Download]
Notify about new document
Login
[Polling for new Documents]
Login
Search for new documents
Validate permissions
documents' metadata
Retrive document(s)
Validate permissions
Notify on document access
Display notification
document(s)
loop
[For each registered Alert]
Check document against alerting conditions
If Condition met
Show notification
opt
Store document(s) to local EMR
«Human Actor»
Health Professional
«System Actor»
Clinical IT System
«System Actor»
Personal Health Record
«System Actor»
Smartphone
«Human Actor»
Patient


«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record
alt
[Patient as Data Consumer]
Login
alt
[Notification triggered Access]
Notify about new document
Notify about new document
Request document
Login
[Patient browsing his PHR]
Login
Read PHR table of content
Validate permissions
document metadata
Select document
Retrive document
Validate permissions
document
Render and display document
«Human Actor»
Patient
«System Actor»
Smartphone
«System Actor»
Personal Health Record

A.3.2.6 Personal Health Device Pairing

Use Case Name	Personal Health Device Pairing
ID	E-HEA-BUC-PERSHEALTHDEVPAIR
Related Generic Use Case	none
Main Actor	- Patient's IT-System
Secondary Actors	- Patient - Personal Health Device
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data - The patient is equipped with a Smartphone that has been registered as a trusted device with the PHR - The patient has been advised and trained in interacting with the PHR - The patient is given one or more personal health devices that shall provide monitoring data to the PHR
Post-conditions	- A personal health device is paired with the patient's smartphone such that both devices can securely share data - The smartphone is equipped and configured to forward (filtered and aggregated) monitoring data to the PHR
Description	Each personal health device given to the patient (e. g. glucometer) needs to be paired with the patient's smartphone which takes the roles of - an application hosting device that runs a service (App) for administrating the personal health device and for securely accepting monitoring data that was collected by this device - a personal hub that securely transmits monitoring data to the patient's PHR. For CREDENTIAL we assume that each personal health device either comes with a dedicated smartphone app or can be connected to an existing health app (e. g. Apple Health or Google Fit). This app provides all means for discovering the device, connecting to the device and accepting data from the device. Additional functionality such as local data processing and data visualization may be provided by this App but will not be considered for CREDENTIAL. By this pairing of a personal health device and a smartphone almost only consists of downloading the device-specific App and then using the configuration means of this App for establishing a secure connection between the health device and the smartphone.

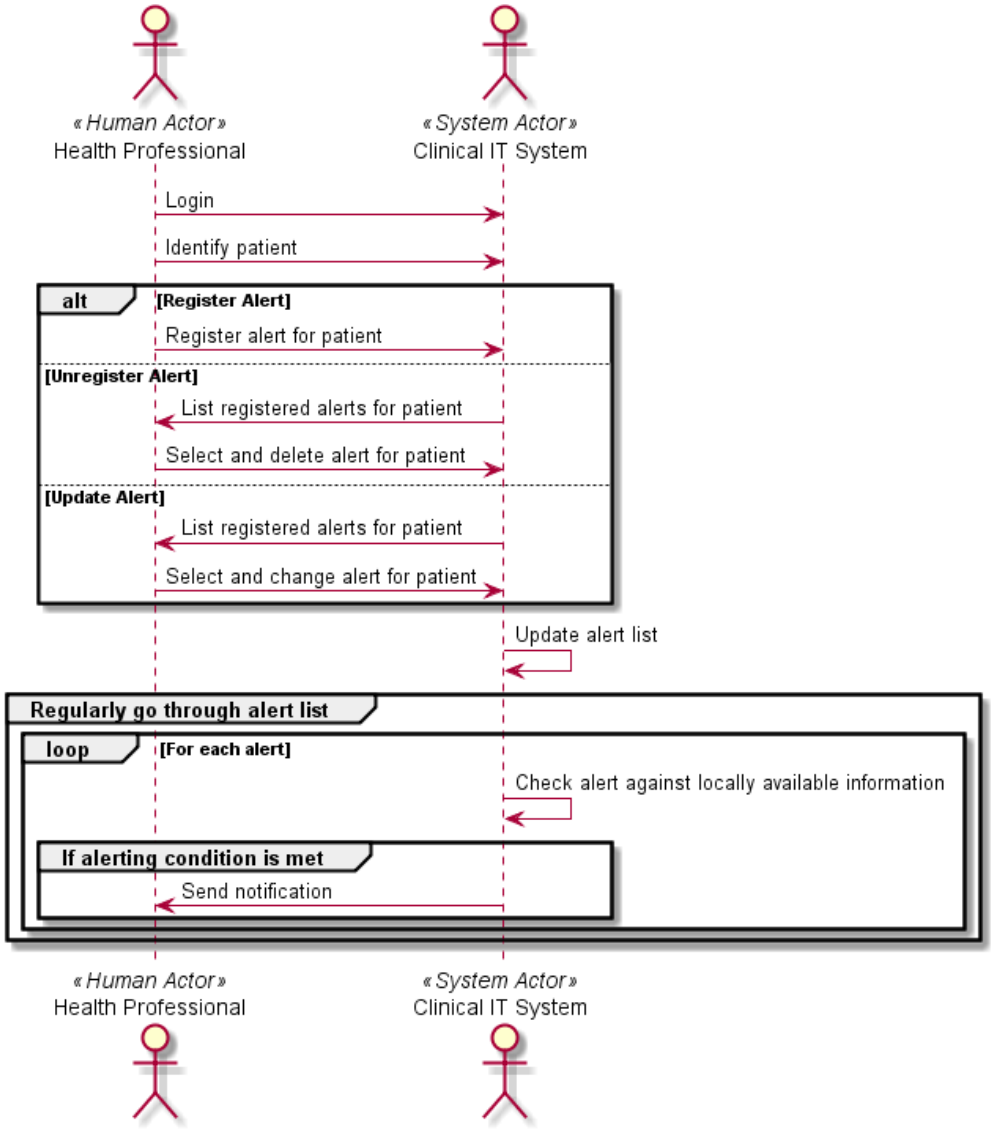
Image


«Human Actor»
Patient
«System Actor»
Personal Health Device
«System Actor»
Smartphone
Install and activate device
opt
[Device comes with its own App]
Load and run device-specific App
Discover and connect
Establish secure communication channel
opt
[Device Configuration through Smartphone App]
Configure personal health device device
Configure device parameters
Calibrate and test device
«Human Actor»
Patient
«System Actor»
Personal Health Device
«System Actor»
Smartphone

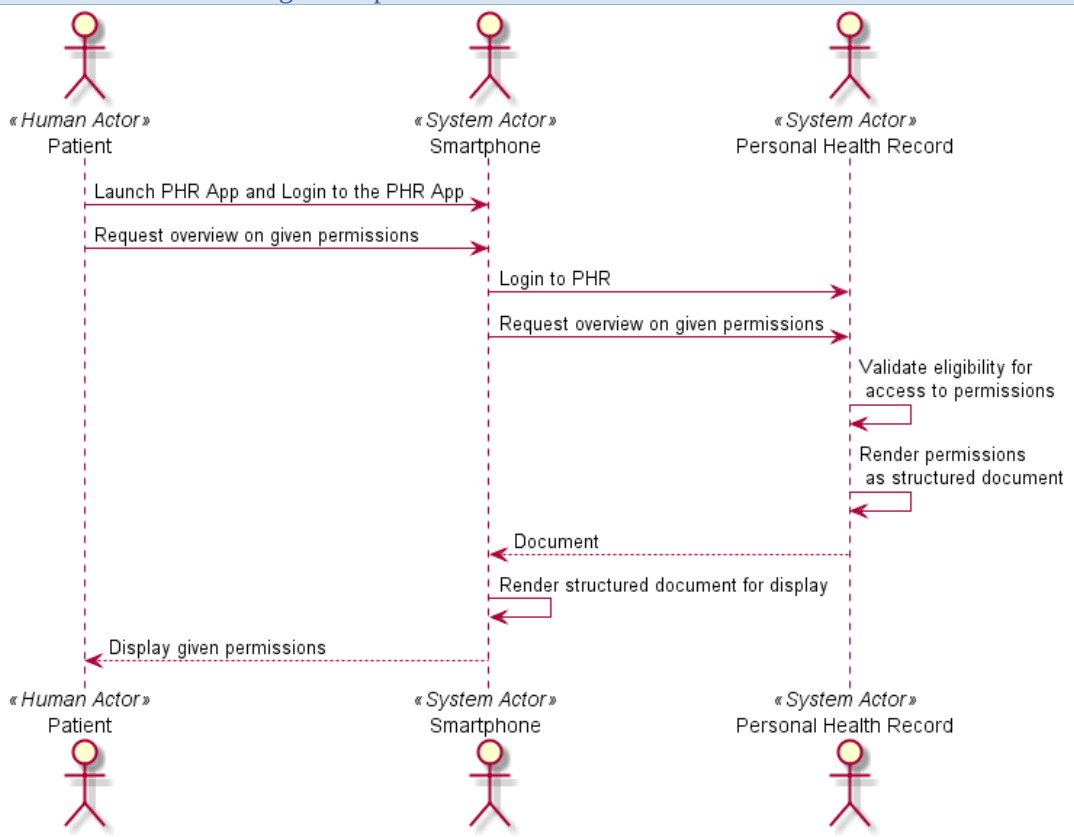
A.3.2.7 Register Alert

Use Case Name	Register Alert
ID	E-HEA-BUC-REGALERT
Related Generic Use Case	none
Main Actor	- Clinical IT System
Secondary Actors	- Health Professional
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data - The health professional has been granted access rights to the PHR by the patient
Post-conditions	- An alert is registered, unregistered or updated with the health professional's clinical IT system - A notification is send to the health professional whenever a new document provided to the PHR meets the defined alerting condition
Description	A health professional may register alerts with his clinical IT system for triggering a notification whenever a document newly provided to a patient's PHR meets a defined condition. As alerts may as well be registered for the absence of expected events (e. g. a requested lab report is not available within a defined time frame) the health professional's clinical IT system will regularly go through all defined alerts in order to catch such conditions, too.

Image

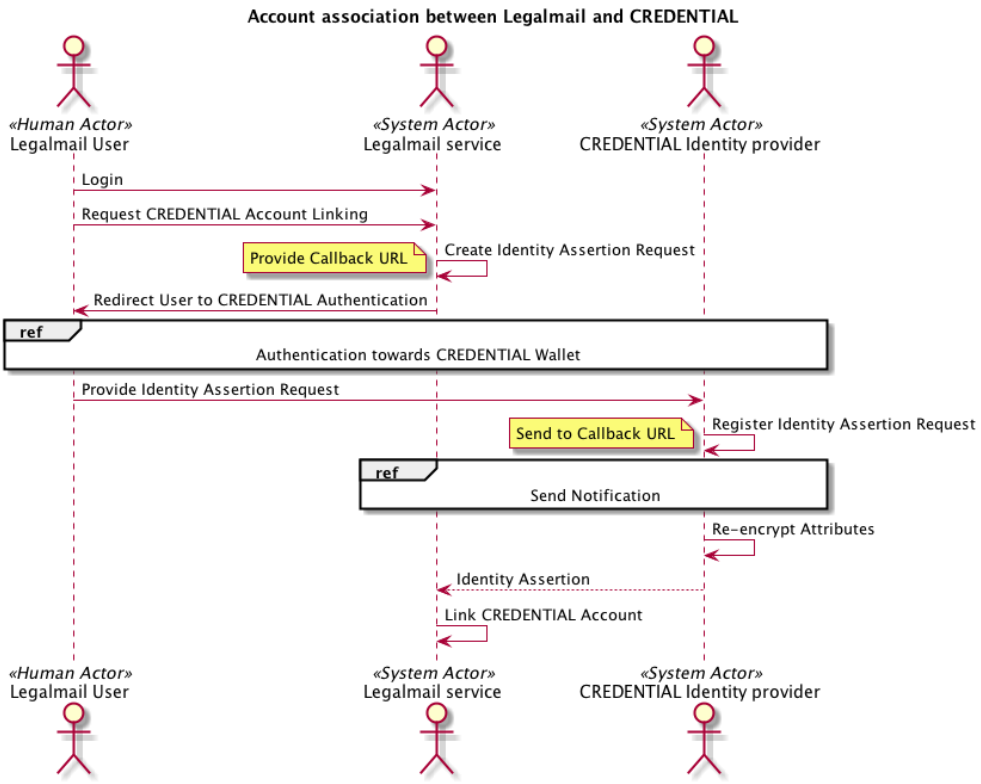

«Human Actor»
Health Professional
«System Actor»
Clinical IT System
Login
Identify patient
alt
[Register Alert]
Register alert for patient
[Unregister Alert]
List registered alerts for patient
Select and delete alert for patient
[Update Alert]
List registered alerts for patient
Select and change alert for patient
Update alert list
Regularly go through alert list
loop
[For each alert]
Check alert against locally available information
If alerting condition is met
Send notification
«Human Actor»
Health Professional
«System Actor»
Clinical IT System

A.3.2.8 View Permissions

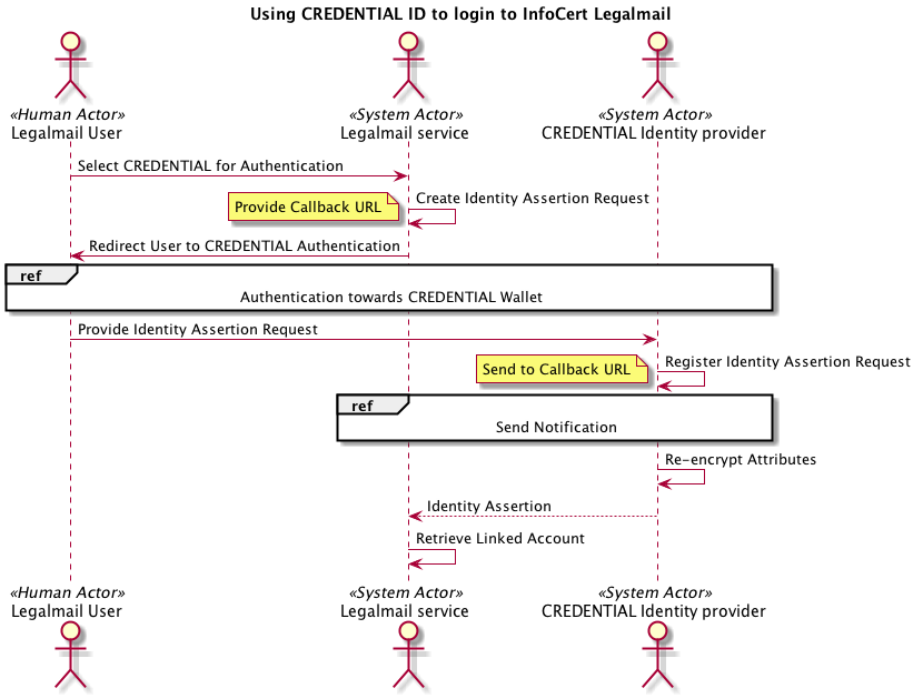
Use Case Name	View Permissions
ID	E-HEA-BUC-VIEWPERM
Related Generic Use Case	none
Main Actor	- Personal Health Record (PHR)
Secondary Actors	- Patient - Smartphone
Pre-conditions	- A shared Personal Health record (PHR) has been set up for collecting and sharing medical data - The patient is equipped with a Smartphone that has been registered as a trusted device with the PHR - The patient has been advised and trained in interacting with the PHR
Post-conditions	-
Description	In order to properly manage his PHR the patient shall be able to oversee what permissions had been granted to which health professionals. As the patient's PHR is the single source of truth for managing all permissions, the patient needs to login to the PHR through his smartphone. The smartphone receives a structured document from the PHR that provides full information on all granted permissions.
Image	

A.3.3 eBusiness

A.3.3.1 Set up login to Legalmail by using CREDENTIAL

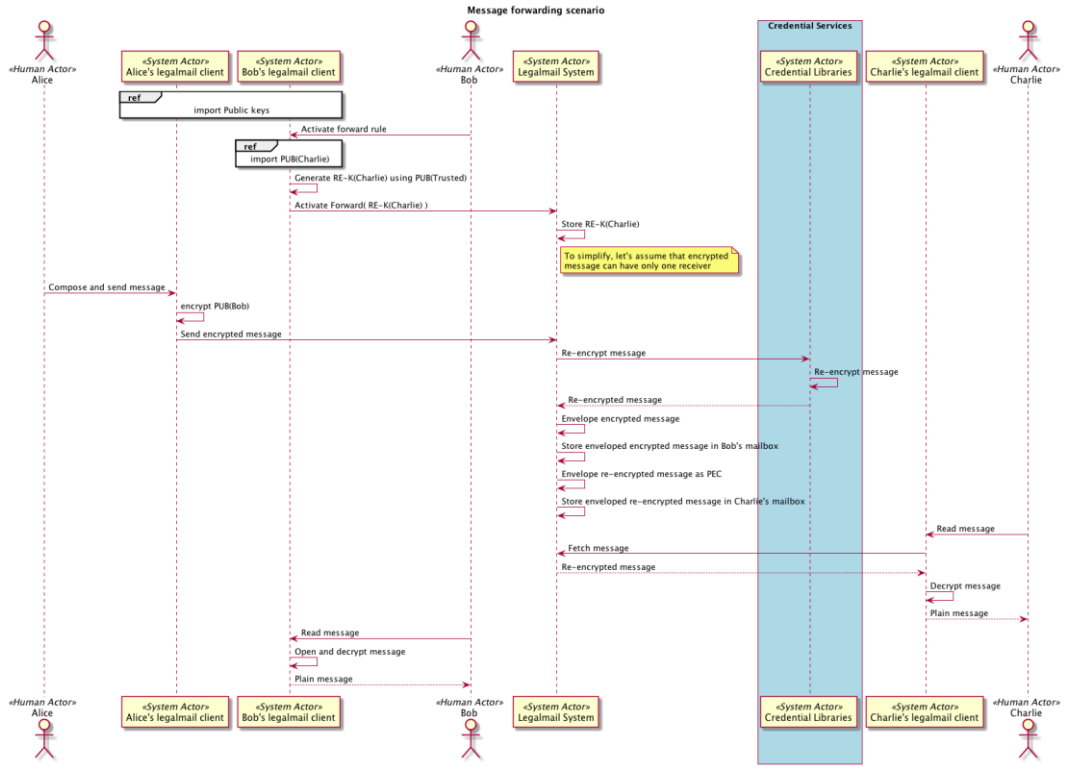
Use Case Name	Account association between Legalmail and CREDENTIAL
ID	E-BUS-1-LMAIL-A
Related Generic Use Case	Link Service Provider account with CREDENTIAL account
Main Actor	- Legalmail User
Secondary Actors	- Legalmail Service - CREDENTIAL Identity provider
Pre-conditions	- The user has a Legalmail account. The user has a CREDENTIAL account.
Post-conditions	- The user associates his Legalmail account to his CREDENTIAL ID.
Description	- The Legalmail account and the CREDENTIAL ID are associated
Image	

A.3.3.2 Using CREDENTIAL ID to login to InfoCert Legalmail

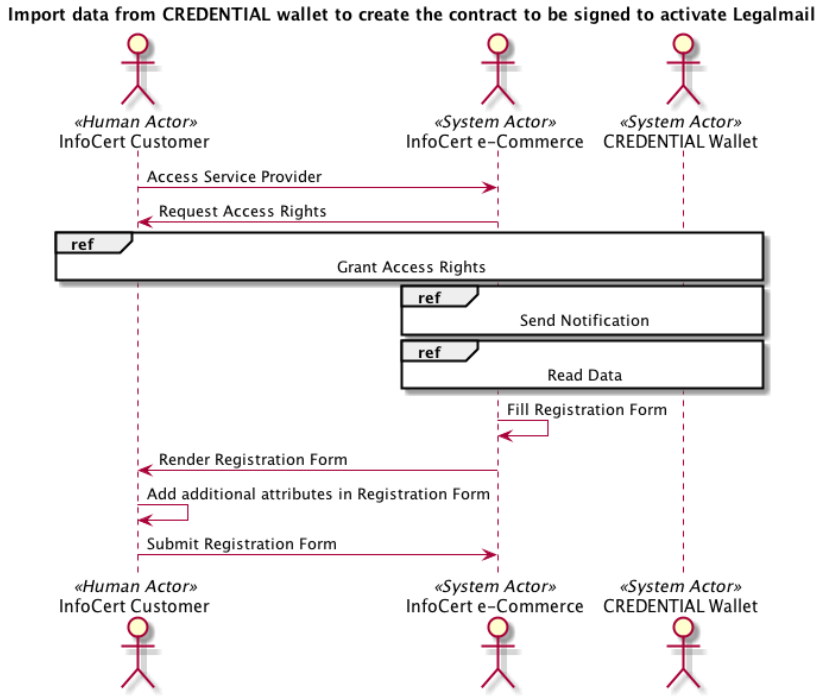
Use Case Name	Using CREDENTIAL ID to login to InfoCert Legalmail
ID	E-BUS-1-LMAIL-B
Related Generic Use Case	none
Main Actor	- Legalmail User
Secondary Actors	- Legalmail Service - CREDENTIAL Identity provider
Pre-conditions	- Having a CREDENTIAL account
Post-conditions	- The CREDENTIAL participant can login to InfoCert Legalmail service
Description	- The Legalmail User can login to Legalmail Service by using CREDENTIAL Identity Provider
Image	

grw

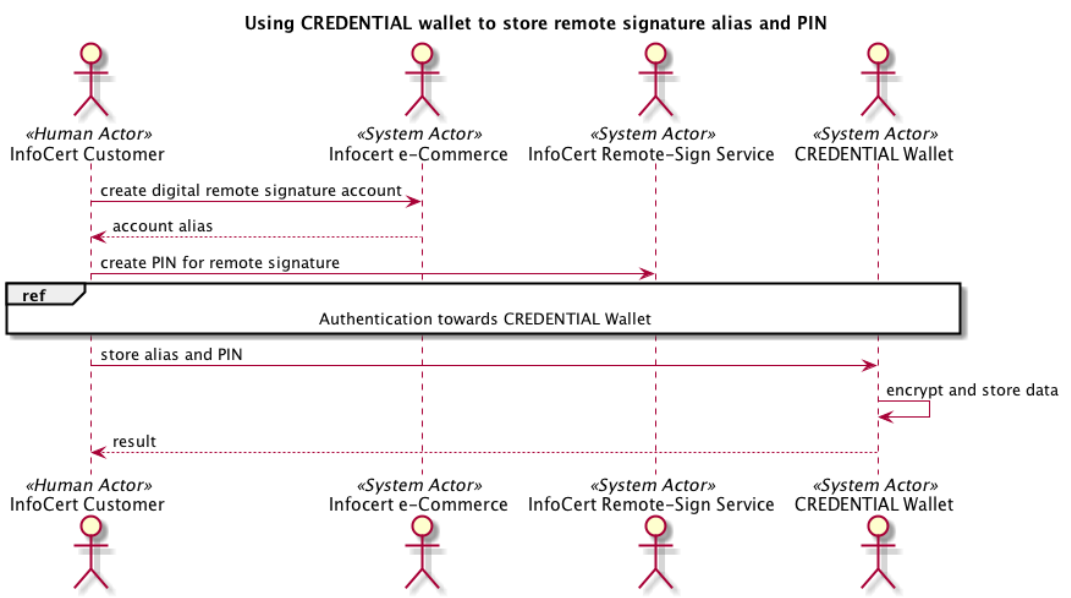
A.3.3.3 Activate encrypted Legalmail forward

Use Case Name	Activating message forward for encrypted Legalmail
ID	E-BUS-2-LMAIL
Related Generic Use Case	Link Service Provider account with CREDENTIAL account
Main Actor	- Legalmail User
Secondary Actors	- Legalmail Service - CREDENTIAL re-encryption libraries
Pre-conditions	- Users have an encryption service configured in their Legalmail account
Post-conditions	- Users are sending registered mails with legalmail client software
Description	- A Legalmail user that enable message encryption with other users want to temporary forward the messages he receives to one or more trusted users. The trusted users should be able to read the encrypted messages
Image	

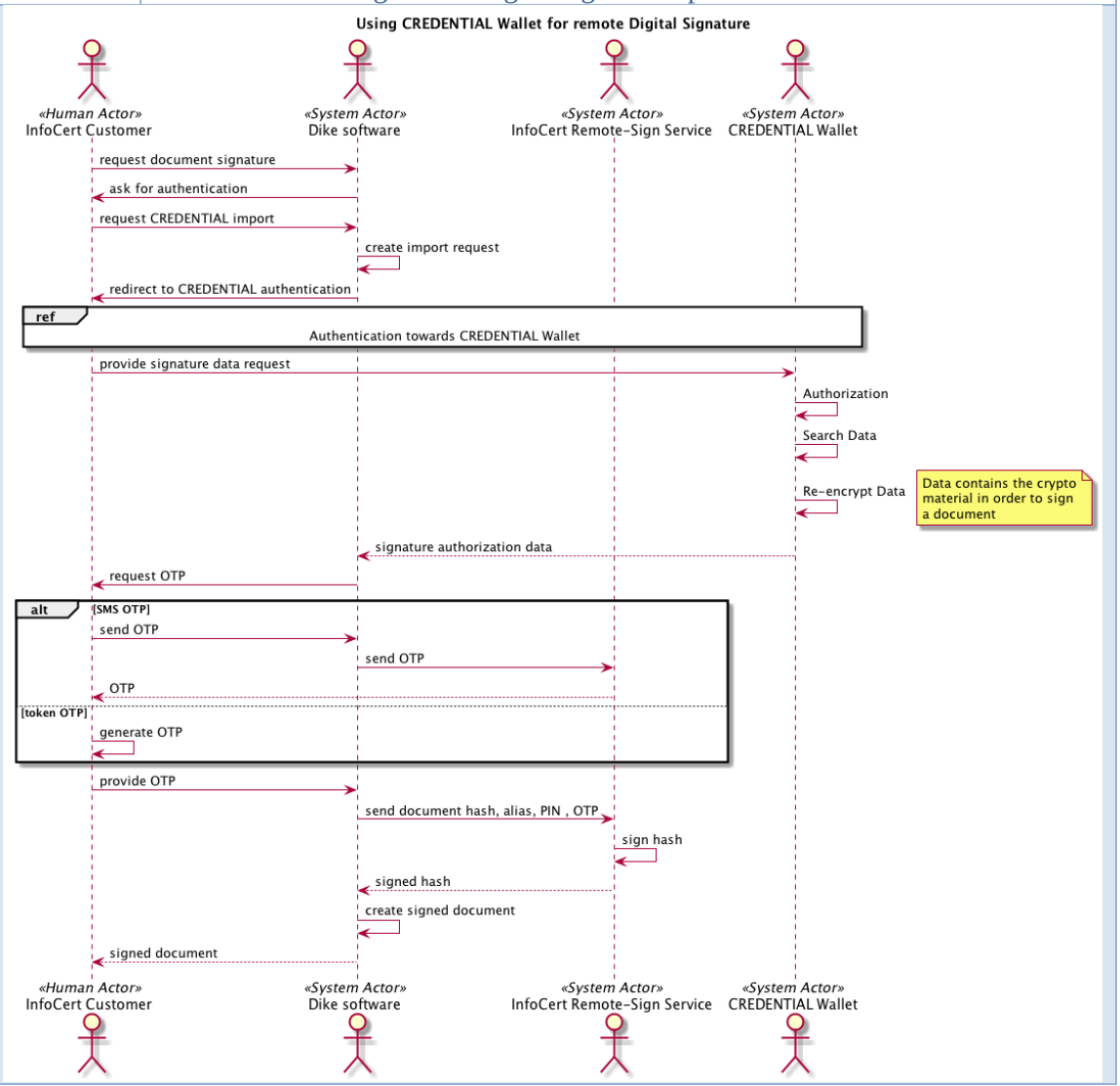
A.3.3.4 Import data into Legalmail subscription form. Choose CREDENTIAL for authentication

Use Case Name	**Import data from CREDENTIAL Wallet to create the contract to be signed to activate Legalmail**
ID	E-BUS-3-SHOP
Related Generic Use Case	none
Main Actor	- InfoCert Customer
Secondary Actors	- InfoCert e-commerce - CREDENTIAL Wallet
Pre-conditions	- The InfoCert Customer has a CREDENTIAL account. The InfoCert Customer has registered in CREDENTIAL Wallet the data needed to complete the Legalmail contract.
Post-conditions	- The Legalmail contract is created and confirmed/accepted. A new Legalmail account is created for the InfoCert_customer and linked to InfoCert_customer CREDENTIAL ID.
Description	- Having completed the purchase on InfoCert e-commerce, Customer has to fulfill the contract to be signed for the legalmail account creation. To proceed, customer authorizes CREDENTIAL Wallet to disclose information needed to complete the task.
Image	

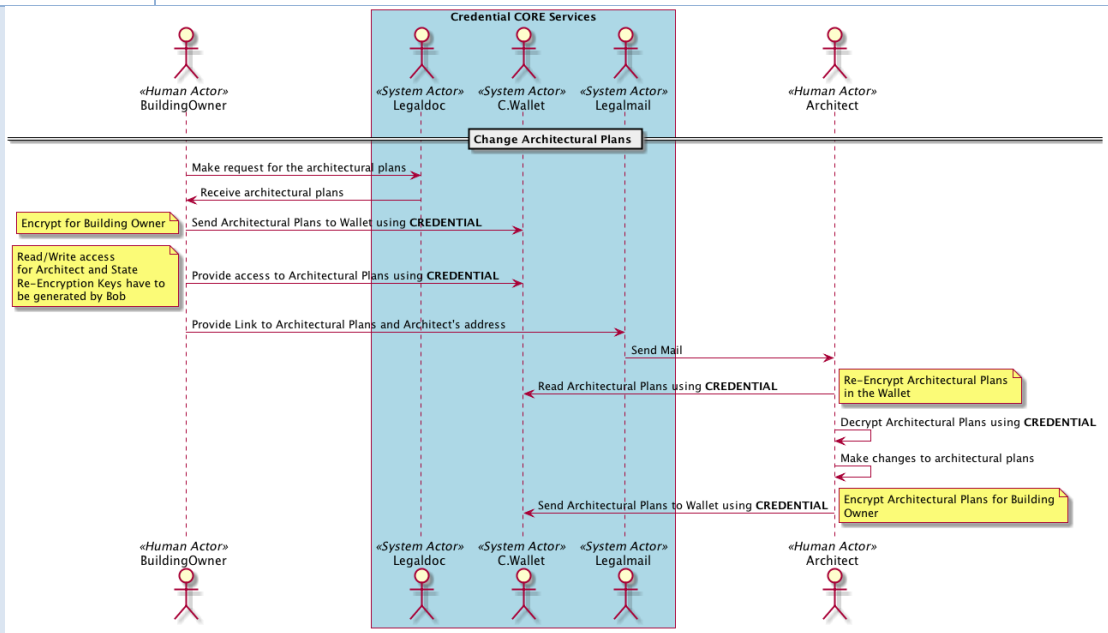
A.3.3.5 Signing a document by using a remote digital signature credential stored in a HSM

Use Case Name	Using CREDENTIAL Wallet to store remote signature alias and PIN
ID	E-BUS-4-SIGN-A
Main Actor	- InfoCert Customer
Secondary Actors	- Infocert e-Commerce - CREDENTIAL Wallet - InfoCert Remote Sign Service
Pre-conditions	- The InfoCert customer has a CREDENTIAL account. The InfoCert customer create a remote digital signature account in InfoCert remote-sign service.
Post-conditions	- The InfoCert Customer personal data needed for remote digital signature operations are stored in CREDENTIAL Wallet in encrypted format. The encryption keys needed to encipher alias and PIN when provided to requesting applications can be chosen by the InfoCert Customer
Description	- The InfoCert Customer, after creating a remote digital signature account, stores in CREDENTIAL Wallet the personal data (alias and PIN) needed to execute remote digital signature operations. The data are stored in encrypted format. The data can be provided to requesting applications only in encrypted format. The encryption keys needed to encrypt the data when provided to requesting applications can be chosen by the InfoCert Customer.
Image	

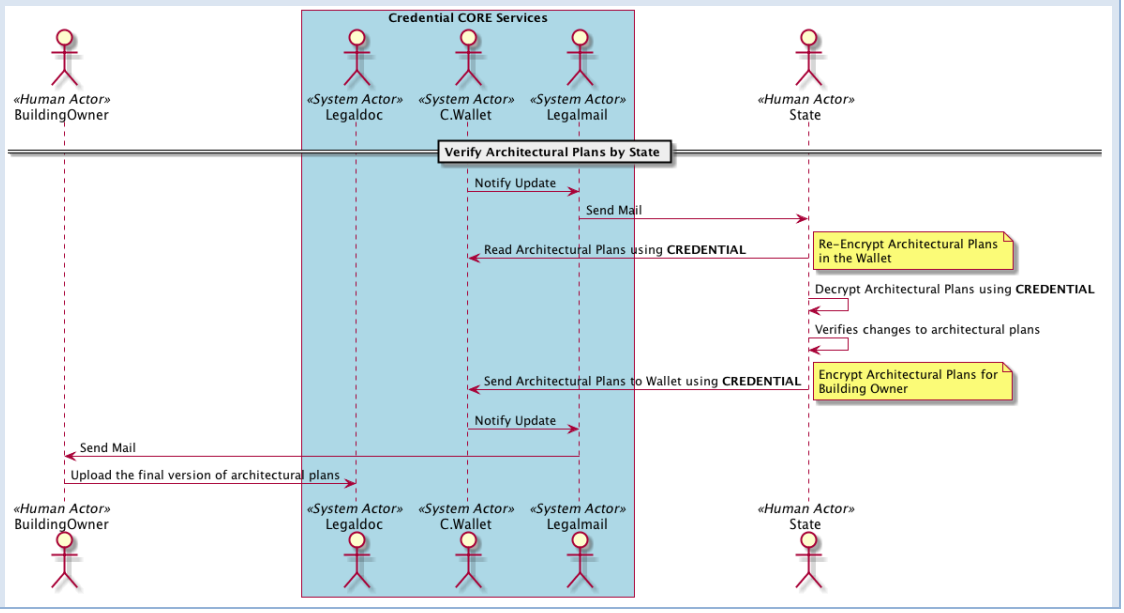
A.3.3.6 Using CREDENTIAL Wallet for remote digital signature

Use Case Name	Using CREDENTIAL Wallet for remote digital signature
ID	E-BUS-4-SIGN-B
Main Actor	- InfoCert Customer
Secondary Actors	- CREDENTIAL Wallet - InfoCert Remote-Sign Service - Dike software
Pre-conditions	- The InfoCert Customer has a CREDENTIAL account. The InfoCert Customer has a remote digital signature account in InfoCert Remote-sign service. The InfoCert Customer personal data needed for remote digital signature operations are stored in CREDENTIAL Wallet in encrypted format.
Post-conditions	- The InfoCert Customer completes the needed remote digital signature operations.
Description	- The InfoCert Customer can use personal data stored in CREDENTIAL Wallet when executing remote digital signature operations.
Image	

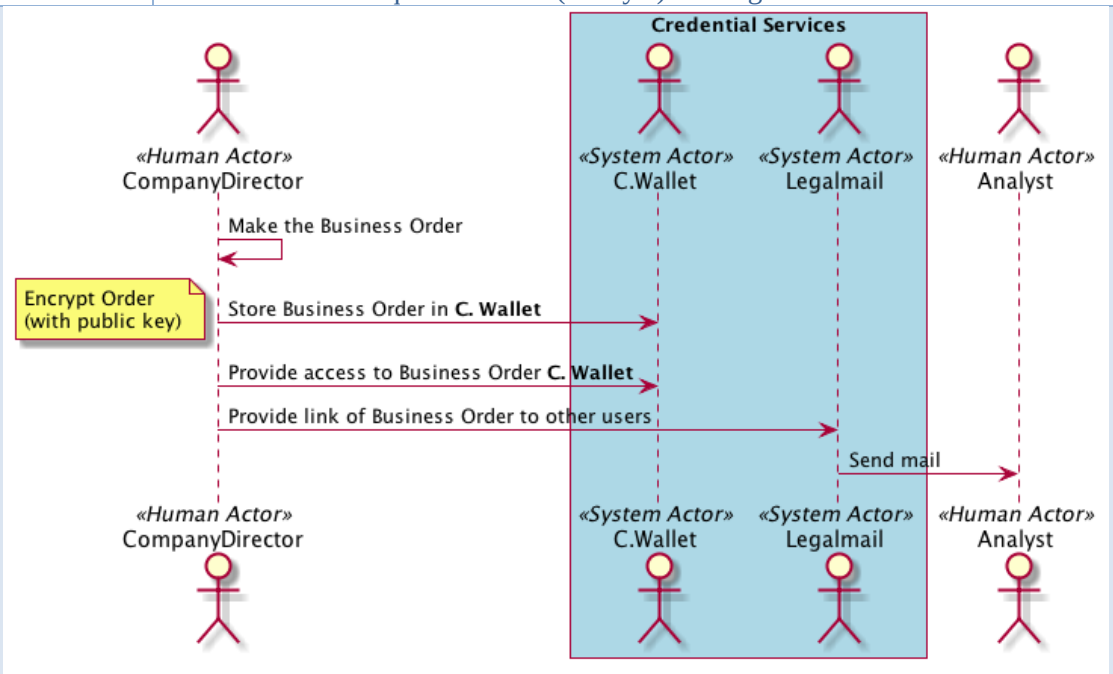
A.3.3.7 Editing Architectural Plans

Use Case Name	Change Architectural Plan
ID	E-BUS-5-AP-A
Main Actor	- Building Owner
Secondary Actors	- CREDENTIAL Wallet - Legaldoc - LegalMail - Architect
Pre-conditions	- Bob (Building Owner) and Archi (Architect) have CREDENTIAL account. - Bob and Archi have LegalMail account. - Bob has Legaldoc account.
Post-conditions	The architectural plans are ready for the verification procedure.
Description	- Building owner (Bob) makes changes on architectural plans. - Bob retrieves the architectural plans from Legaldoc using CREDENTIAL Wallet as Identity provider. After getting the plans from Legaldoc, he encrypts and uploads into the CREDENTIAL Wallet. Subsequently Bob creates proxy-re-encryption keys for Archi (Architect). Then Bob sends an email to Archi (Architect), using Legalmail as mail service. So from now on, Bob could be offline until he receives the confirmation email of the procedure termination. - Archi receives email from the Bob to apply the changes on architectural plans. Archi downloads the plans using the proxy-re-encryption key. Archi decrypts the architectural plans using CREDENTIAL and makes the changes on plans. In the end, he saves the re-encrypted plans and uploads them into CREDENTIAL Wallet.
Image	

A.3.3.8 Verify Architectural Plans

Use Case Name	Verify Architectural Plans
ID	E-BUS-5-AP-B
Main Actor	- State Engineer
Secondary Actors	- Credential Wallet - Legaldoc - LegalMail - Building Owner
Pre-conditions	- Bob (Building Owner) and Sam (State Engineer) have CREDENTIAL account. - Bob and Archi have LegalMail account. - Bob has Legaldoc account. - Sam has received email for the verification procedure.
Post-conditions	The architectural plans are stored in Legal doc.
Description	- After the changes on architectural plans, CREDENTIAL Wallet sends a notification to Sam (State engineer) to inform him about the architecture plans. Sam receives the plans from CREDENTIAL Wallet using the proxy-re-encryption key and acts as follow. Decrypts the plans with CREDENTIAL technology and verifies the changes on the architectural plans. Encrypts and finally uploads the architectural plans into Credential Wallet. - Finally, CREDENTIAL Wallet receives the architectural plans and notifies the offline Building Owner to check the architectural plans. - Bob stores the architectural plans in Legaldoc.
Image	

A.3.3.9 Business Report Ordering by Company

Use Case Name	Business Report Request
ID	E-BUS-6-BR-A
Main Actor	- Company Director
Secondary Actors	- CREDENTIAL Wallet - LegalMail - Analyst
Pre-conditions	- Codie (Company Director) and Anna (Analyst) have CREDENTIAL account. - Codie and Anna have LegalMail account. - Codie User has stored his signature alias, public key in C. Wallet.
Post-conditions	Business report is ready for the verification procedure.
Description	- Codie (Company director) decides to make an order for his Company. - Codie makes the order for his company. he uses C. Wallet (with his public key) to encrypt the order. He stores the order in C. Wallet and sends a notification request to Anna (Analyst) via Legalmail.
Image	

A.3.3.10 Business Report Response

Use Case Name	Business Report Response
ID	E-BUS-6-BR-B
Main Actor	- Analyst
Secondary Actors	- CREDENTIAL Wallet - Legaldoc - LegalMail - Company Director
Pre-conditions	- Codie (Company Director) and Anna (Analyst) have CREDENTIAL account. - Codie and Anna have LegalMail account. - Codie User has stored his signature alias, public key in C. Wallet. - Anna has received email for the verification procedure.
Post-conditions	Business report is verified and stored in Legaldoc.
Description	- Anna decrypts the business order and checks/verifies it. After the verification step he creates the business report. Encrypts and stores business report into C. Wallet. Then he sends a notification back to Codie. Codie decrypts with C. Wallet, reads and it. - The process stops when he stores the business report in Legaldoc.
Image