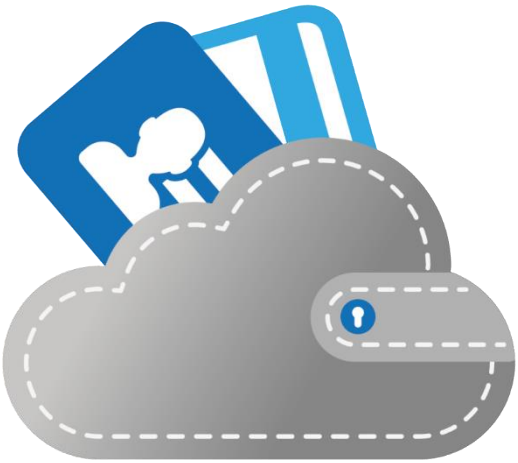
Project number: 653454
H2020-DS-2014-1

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



D2.3
Cloud Identity Wallet Requirements

Document Identification	
Due date	March 31, 2017
Submission date	March 31, 2017
Revision	1.0

Related WP	WP6	Dissemination Level	PU
Lead Participant	FOKUS	Lead Author	Florian Thiemer (FOKUS)
Contributing Beneficiaries	FOKUS, GUF, TUG, OTE, ICERT, KAU, KGH, LISPA, AIT, ATOS	Related Deliverables	D2.1, D2.2, D2.5, D6.1

Abstract: The CREDENTIAL Wallet provides cloud services and an infrastructure for sharing identity data across user and services. Demonstrating the practicability of these services will be performed in three different pilots across the domains eGovernment, eHealth and eBusiness. Generic and pilot specific use cases were already defined in past deliverables. Moving to the next steps which includes a definition of a component architecture, UI prototyping and developing – the requirements have to be defined. This document describes all the identified requirements on the functional, legal, organizational and technical level.

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

The CREDENTIAL Wallet hosts a set of security and applications services to enable user-friendly authentication and privacy-aware identity-data sharing within web services and with other users. It is doing so by using novel cryptographic algorithms like proxy re-encryption[1] and malleable signatures[2]. To demonstrate the CREDENTIAL Wallet and showcase its capabilities, three different pilot were defined in the domains eGovernment, eHealth and eBusiness.
As a prerequisite before the pilots can be implemented and executed, a well-defined set of requirements has to be established to support the forthcoming development processes. The foundation for this work has already be done in previous deliverables D2.1 "Use Cases" and D6.1 "Pilot use case specification" by defining multiple use cases for the CREDENTIAL Wallet and its pilot domains. Requirements are elaborated from these artifacts and defined in this document. The requirements are divided into the functional, legal, organizational and technical requirements of the CREDENTIAL Wallet.
This document introduces a framework for a unified way to represent each requirement. A requirement is characterized by multiple attributes, which helps to identify them in the forthcoming development process, relate them to previously defined artifacts and categorize them into different clusters.
These requirements will drive and support the forthcoming work regarding UI development, architecture design, software development and pilot execution for the CREDENTIAL project.

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

[2] 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

Document information

Contributors

Name	Partner
Andreas Happe	AIT
Stephan Krenn	AIT
Miryam Villegas Jimenez	ATOS
Juan Carlos Pérez Baún	ATOS
Florian Thiemer	FOKUS
Welderufael Tesfay	GUF
Luigi Rizzo	ICERT
Tobias Pulls	KAU
Alberto Zanini	LISPA
Andrea Migliavacca	LISPA
Silvana Mura	LISPA
Alexandros Kostopoulos	OTE
Andreas Abraham	TUG
Felix Hörandner	TUG

Reviewers

Name	Partner
Stephan Krenn	AIT
Welderufael Tesfay	GUF
Tobias Pulls	KAU
Felix Hörandner	TUG

History

0.01	2016-05-23	Florian Thiemer	1st Draft
0.02	2016-06-13	Tobias Pulls	Add assigned requirements in redmine.
0.03	2016-06-16	Andreas Abraham	Add assigned requirements in redmine.
0.04	2016-06-28	Alberto Zanini	Add assigned requirements in redmine
0.05	2016-06-29	Luigi Rizzo	Add assigned requirements in redmine
0.06	2017-01-11	Florian Thiemer	Change to new template
0.07	2017-01-26	Andreas Happe Stephan Krenn	Start service provider centric requirements
0.08	2017-01-31	Andreas Abraham	Add Administration requirement cluster
0.09	2017-02-01	Miryam Villegas Jiménez Juan Carlos Pérez Baún	Add Account requirement cluster. Feedback on Methodology section
0.10	2017-02-02	Stephan Krenn	Extended SP centric requirements, added first issuer specific requirements
0.11	2017-02-15	Andrea Migliavacca	Add Introduction chapter

0.12	2017-02-19	Florian Thiemer	Address high-level review feedback.
0.13	2017-02-28	Florian Thiemer	Address first round of reviewer's feedback
0.14	2017-03-03	Anna Klughammer	Add Conclusion chapter
0.15	2017-03-10	Alberto Zanini	Add references to requirements in description chapter.
0.16	2017-03-10	Andrea Migliavacca Silvana Mura	Address reviewers comments
0.17	2017-03-12	Alexandros Kostopoulos	Add data sharing requirements. Correct editing and spelling errors.
0.18	2017-03-24	Florian Thiemer	Address second round of reviewer's feedback
0.19	2017-03-29	Florian Thimer	Polishing
1.0	2017-03-31	Stephan Krenn Agi Karyda	Final copy-editing for submission

List of Contents

List of Figures

List of Acronyms

BUC	Business Use Case
eID	Electronic Identification
eIDAS	Electronic Identification and trust services for electronic transactions
GDPR	General Data Protection Regulation
IdP	Identity Provider
LUC	Logical Use Case
SAML	Security Assertion Markup Language
SP	Service Provider
SQL	Structured Query Language

Glossary of Terms

CREDENTIAL Wallet

The CREDENTIAL Wallet is cloud-based identity data sharing platform. It allows users to store and share identity data in a privacy-aware way by using novel cryptographic mechanisms like proxy-re-encryption and redactable signature.

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.

User's Cold Storage

Place where the user's recovery keys are safely stored. For example, USB Stick, QR Code, Smartcard, etc.

1 Introduction

The work carried out in the first part of the project has led to define the functional, technical and organizational requirements of technologies relevant to CREDENTIAL.
The main objective of this deliverable is to showcase/describe the requirements in a way useful for being an input for the following design, implementation, deployment and evaluation steps of the project.
The methodology adopted to elicit requirements, described in Chapter 2, is based on the requirements engineering process model that foresees an iterative process, performed taking into account activities such as design and first stages of coding. The methodology foresees the use of a common structure to describe each identified requirement and to group similar requirements into clusters, identified during the elicitation process, to ease understanding.
The requirements identified are analysed in the following chapters:

- Chapter 3 - CREDENTIAL Wallet Requirements
- Chapter 4 - CREDENTIAL App Requirements
- Chapter 5 - External Service Provider Requirements

1.1 CREDENTIAL Project Highlight

The goal of CREDENTIAL is to develop, test and showcase innovative cloud-based services for storing, managing, and sharing digital identity information and other critical personal data. The security of these services relies on the combination of strong hardware-based multi-factor authentication with end-to-end encryption representing a significant advantage over current password-based authentication schemes.
The use of sophisticated proxy cryptography schemes, such as proxy re-encryption and redactable signatures, will enable a secure and privacy preserving information sharing network for cloud-based identity information in which even the identity provider cannot access the data in plain-text and hence protect access to identity data.
CREDENTIAL's basic architecture integrates cryptographic mechanisms into three key actors: user, CREDENTIAL Wallet, and data receiver, as shown in the following Figure 1.
The **User** owns data that may be securely stored or shared with other members. In the user's domain, a client application is deployed to handle operations such as signing or generating a re-encryption key.
The **Wallet** is a cloud-based data storage and sharing service characterized by important advantages such as constant availability, scalability, and cost effectiveness. The Identity and Access Management system implements multi-factor authentication and authorizes access to stored data. With proxy re-encryption, the confidentiality of the stored and shared data is ensured even when deploying the wallet at a cloud provider, as no plain data is exposed. Moreover, once a re-encryption key is available, data can be shared with other users even if the user or his/her client application is not available.
The **Data Receiver,** which can be another CREDENTIAL user or a service provider, relies on data stored in or authentication assertions issued by the CREDENTIAL Wallet. With this information, the data receiver reaches authorization decisions and performs arbitrary data processing.

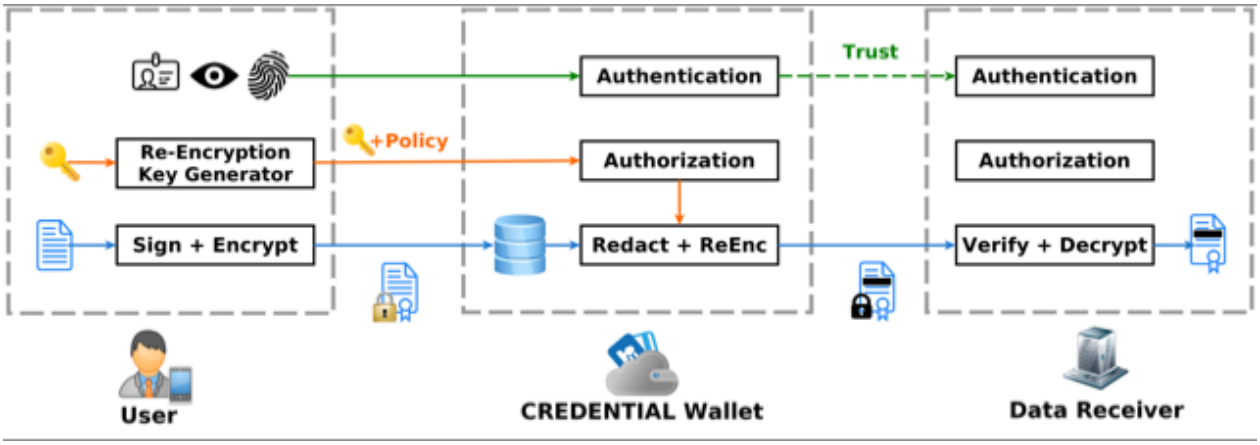


Figure 1: CREDENTIAL's basic architecture

Data sharing process is based on the following steps: the user authenticates at the CREDENTIAL Wallet to get permission to upload signed and encrypted data, data is encrypted for the user herself to keep maximum control, the Wallet re-encrypts data towards a selected data receiver without getting knowledge about the encrypted data. A re-encryption key generation is performed on the user domain and a policy defining which data may be disclosed is transmitted to the CREDENTIAL Wallet.

Then, the user's cipher text is transformed into encrypted data for the data receiver by using the re-encryption key. Finally, the data receiver decrypts the data and verifies the signature on the disclosed parts.

To showcase the functionality of the CREDENTIAL Wallet, three different pilots in the domains eGovernment, eHealth and eBusiness are performed by the project.

- **eGovernment**: the pilot focuses on identity management to authenticate citizens and assess their eligibility for a service, based on sensitive identity attributes.
  Standardized identity protocols such as SAML or OpenID Connect should be used in CREDENTIAL's identity management data sharing process. Within this protocol, the service provider (i.e., the data receiver) triggers the process by requesting authentication and identity attributes from the identity provider (i.e., the CREDENTIAL Wallet). The pilot will concern not only enabling authentication for national eID solutions but also cross-border authentication according to the eIDAS regulation. The CREDENTIAL Wallet prompts the user for consent as well as a re-encryption key, and then selectively discloses re-encrypted attributes to the service provider.
- **eHealth**: The pilot focuses on secure data sharing between patients, doctors, and further parties, in the field of Type 2 diabetes. In particular, the pilot applies to patients, which can use mobile devices to record their health data, those data are collected by a CREDENTIAL e-Health mobile app which remotely stores them in the CREDENTIAL Wallet. The user can decide who is allowed to access medical data and which specific parts, thus allowing authorized people to prepare and send advices back to the user. The fact of disclosing a minimal part of data brings several advantages to user such as saving time and money for personal visits and having a continuous control of health data.
- **eBusiness**: The pilot focuses on the integration of modular libraries implementing CREDENTIAL's technologies to increase the privacy offered by existing solutions.
  In particular, it tackles the issue of encrypted mails, which are nowadays increasingly used by companies to protect data and products but raise important challenges when employees are not at work. In fact, according the current legislation, workers have to provide their private

keys to access company e-mail to give the possibility to other colleagues to still read and eventually take over incoming mail.
Thanks to proxy re-encryption system, a worker can generate a re-encryption key and deliver it to an authorized colleague before leaving. The new person does not manage the key but the mail server is able to decode incoming mail during the worker absence.
Other aspects of the eBusiness pilot is the login and registration to Legalmail services by using strong authentication features offered by the CREDENTIAL Wallet and automatic contract form filling by using personal identity data from the CREDENTIAL Wallet.

1.2 Objectives

Requirements engineering is a systematic process to collect, identify and manage requirements during the software development process. During the software development, many changes can occur but we need a strong point of reference also to base the evaluation activity. To avoid inconsistency between elicited requirements, software architecture and implementations, the requirement engineering process will document all elicited requirements from the use case analysis and link them to architecture and implementation parts of the other work packages. This method will allow to detect missing requirements, superfluous requirements and unnecessary implementations.
The main goals of requirements engineering process are the following:

- To enable communications between software developers, stakeholders and end users about the software that needs to be delivered;
- To agree on acceptance criteria which determine if and how a software can get an approval;
- To derive constraints and understanding to be reflected by the software architecture;
- To document the relations between existing systems and the software under development.

This deliverable provides a comprehensive description of each requirement by using a common structure as explained in Chapter 2 “Methodology”.
The deliverable addresses four main types of requirements: **functional** requirements that reflect the end-user and business user needs; **technical** requirements, considering both mandatory and optional functionalities and related to existing components’ interfaces; **organizational** requirements that reflect the experience of the industrial partners offering secure cloud provider solutions in a production environment; **legal** requirements.

1.3 Scope and Connection with Other Deliverables

The Cloud Identity Wallet requirements makes a description of the functional requirements to be used as an input to design the CREDENTIAL architecture, as will be later on described in D5.1 Functional Design (Deliverable in preparation for the same period).
The deliverable takes as a starting point the findings of previously released deliverables (D2.1, D2.2, D2.5, and D6.1). D2.1 elaborates the use cases for the CREDENTIAL Wallet and builds the foundation for all upcoming work and analyses upon the CREDENTIAL Wallet and its functionalities. D2.2 describes the elicited system security requirements in the 1st and 2nd iteration. D6.1 describes the adaption of the use cases for each of the three pilots in the eGovernment, eHealth and eBusiness domain. The use cases are described in more detail as in D2.1. This deliverable takes these deliverables as input and aims to identify functional, technical,

legal and organizational requirements. The privacy and usability requirements are addressed in D2.6.
Each of the described requirements needs to be checked if it is fulfilled during the project or not. These checks are performed in D5.7 and guarantees that the developed software aligns with the requirements defined in this deliverable.

1.4 Outline

The deliverable is structured as follows:

- *Chapter 1 Introduction*: outlines project activities focusing on objectives of the analysis, describes the relation with other project deliverables and gives an overview of the deliverable contents.
- *Chapter 2 Methodology*: makes a detailed description of the requirements analysis and outlines the methodology applied. The steps followed to the definition of the requirements and the clustering criteria are also described in a formal way, in order to ease reading the deliverable.
- *Chapter 3 Generic CREDENTIAL Wallet Requirements:* describes through detailed tables the requirements collected during the elicitation process, clustered by category.
- *Chapter 4 Generic CREDENTIAL App Requirement*: describes requirements towards the CREDENTIAL App which is used by the users to access the CREDENTIAL Wallet.
- *Chapter 5 External Service Provider*: describes requirements towards external service providers who registered at the CREDENTIAL Wallet in order to offer its services to users of the CREDENTIAL Wallet.
- *Chapter 6 Conclusion*: concludes the results of the requirement elicitation process and gives and outlook of the forthcoming work.

2 Methodology

The **functional requirements** used for the development of the Cloud Identity Wallet architecture are derived from the use cases and the storyboards provided in D2.1 Scenarios and use cases document [1], reflecting the end-user and business user needs. We are focusing on requirements related to:

- user and service authentication;
- authenticity, exchange and recovery of data;
- secure data re-encryption;
- exchange and recovery of keys.

Moreover, **technical requirements** are defined, fundamentally:

- mandatory and optional functionalities;
- existing components' interfaces in both secure cloud storage solutions and service providers.

Organizational requirements reflect the experience of the industrial partners offering secure cloud solutions in a production environment. Finally, **legal requirements** affecting the user data management and the General Data Protection Regulation (GDPR) also have been collected.
The procedure followed to the definition of the requirements is described in a formal way later in Chapter 2.2, in order to ease reading the deliverable.

2.1 Requirement Engineering Process

The requirement engineering process is one of the most critical activities which influence the software implementation. As the development of the CREDENTIAL Wallet components is a complex task the requirements engineering process model followed is based on an iterative process [4], performed taking into account activities such as design and even first stages of coding, which is shown in Figure 2. With this approach, different viewpoints are considered with the aim of collecting a well-defined defined set of requirements from different sources and finally a good quality final product.

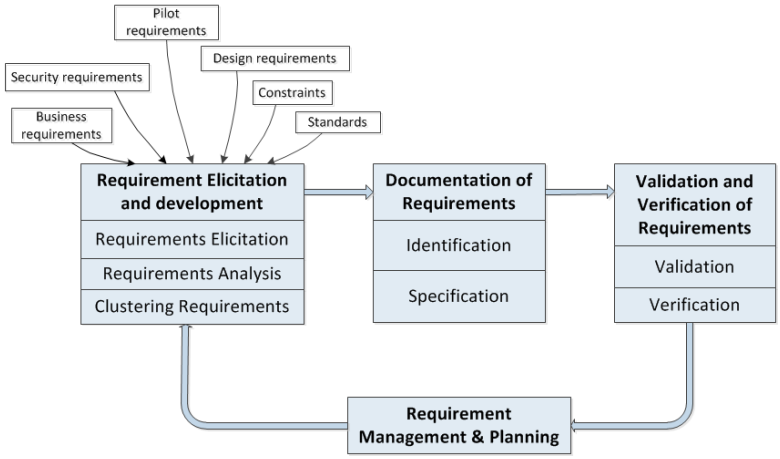


Figure 2: Requirement engineering process model [4]

The process followed for describing the above-mentioned requirements is based on the information provided by the different stakeholders and sources such as the pilot partners and the partners participating during the architecture reference design [2], which has been developed in parallel.
As can be seen in Figure 2 the activities developed by the suggested model maps with the activities the requirements engineering process comprises [5], [6]:

- Requirements elicitation;
- Requirements analysis;
- Requirements specification;
- Requirements validation;
- Requirements management.

Accordingly, with the proposed requirement engineering model four phases can be described with the aim to produce a set of high quality CREDENTIAL requirements.

2.1.1 Requirement Elicitation and Analysis

The main goal of the requirement elicitation phase is to refine the raw requirements previously identified by the different stakeholders. Figure 3 shows the iterative process which is described next:

- These raw requirements are extracted from the already defined Logical Use Cases (LUCs) derived from the business use cases.
- A detailed analysis is performed on these raw requirements taking into account the business requirements, security requirements, related standards, and system constraints. It must be also considered if the requirements collide with other identified requirements. In this way, a variety of viewpoints and different perspectives are contemplated. A polished requirement is derived after this process.
- Once the raw requirements have been refined the derived requirements are grouped in clusters (the list of clusters is described in section 2.3). This grouping in clusters facilitates an additional refinement step combining similar requirements and abstracting to a higher-level requirement.
- The retrieved requirements are refined again after reviewing the proposed CREDENTIAL Functional Design document [2].

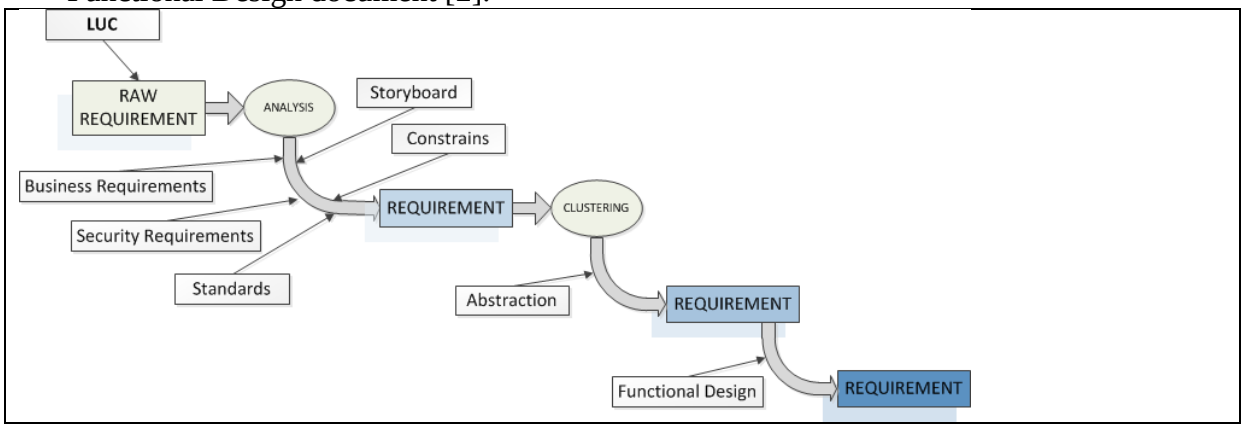


Figure 3: Iterative requirement elicitation process

2.1.2 Documentation of the Requirements

The detailed description of each refined requirement is included in a structure described in Section 2.2. This structure contains among other information a full description of the requirement, the acceptance criteria, the requirement motivation and also an identifier. This information eases the later implementation work and the requirement management.

2.1.3 Validation and Verification of the Requirements

Once the requirements descriptions are obtained, the requirements are validated ensuring that meet the stakeholder needs and it is verified whether the requirements are stated correctly.
This validation and verification phase provides a set of requirements valid for the implementation phase.

2.1.4 Requirements Management and Mapping

The requirements not only may change, but new ones can emerge during the process. Moreover, the requirements are the basis for the implementation phase. For these reasons, it is necessary to control the requirement's changes and keep track the requirement's relationship. In spite of the scope of this deliverable D2.3 is not focused in the requirement management, but providing the pillars for the rest of management activities such as the requirement's traceability.

2.1.5 CREDENTIAL Terminology

With the aim to facilitate the following requirements sections reading and clarify the actors the requirements are referring to, a definition of the relevant involved actors is extracted, from D2.1[1], and included next.

- **CREDENTIAL App:** The smartphone application with which a user access the CREDENTIAL Wallet and uses its functionality.
- **User**: A person who uses the CREDENTIAL Wallet. She 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.
- **CREDENTIAL Wallet**: Is the central platform where data storage, data exchange and authentication occur. The CREDENTIAL Wallet can be both a portal offering service to users and other service provider or be a collection of libraries which supports the integration of CREDENTIAL technology in existing systems.
- **Service Provider**: Is an external service which offers some functionality and can be used by users of the CREDENTIAL Wallet with the additional benefit to share directly data from the CREDENTIAL Wallet with the service provider.
- **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 another Service Provider to identify and authorize the user. Attributes may be encrypted.

- **Data Owner:** A user of the CREDENTIAL Wallet who possesses a certain set of data. The term is mostly used when a description needs to refer to the owner of the data.

2.2 Requirement Structure Description

Requirements have the main goal to specify what developers have to realize in order to deliver a correct product to the customer. To keep track about the set of all requirements a well-defined structure needs to be elaborated for them. This section describes the structure and fields for each requirement that is defined in this deliverable. Due to the use cases and the storyboards were managed and stored using Redmine tool, the initial retrieved requirements were stored in the same tool. With the aim to create a requirement's structure that facilitates the understanding, management and traceability of the elicited requirements, the attributes that will define and describe the requirements has been agreed. Therefore, the requirements will be collected and documented in the following structure:

ID	
Title	
Area	
Type	
Cluster	
Contradicts	
Description	
Motivation	
Acceptance Criteria	
Comments	

The individual fields of a requirement are described as follows:

- **ID**: The ID of the requirement with the following structure:
    - TYPE can be FUNC/ORG/LEG/TECH and describes the type of the requirement.
    - AREA can be APP/CW/SP describes the area the requirement belongs to, CREDENTIAL Application, CREDENTIAL Wallet and Service Provider respectively.
    - CLUSTER indicates the cluster to which the requirement belongs to, and can beACCESS/AUTHN/ADMIN/ACCOUNT/DATA/SERV/GEN.
    - NN will be a numerical value iterated for each cluster.
    - An example requirement might by: R-ORG-CW-DATA-01
- **Title**: The title of the requirement. It establishes the related action at high level, using nouns, adjectives, etc., but not verbs.
- **Area**: Defines if the requirement targets either the App, the CREDENTIAL Wallet or a Service Provider
- **Type**: One of the following types
    - Functional
    - Organizational
    - Legal
    - Technical

    - Security
- **Cluster**: Indicates the set of requirements, the requirement belongs to. Each requirement category
- **Contradicts**: If the requirement may contradict another requirement, it is referenced in this section.
- **Description**: A concise description of the requirement. Use the following key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" following the RFC 2119 standard for describing requirements of a specification [3].**Motivation**: The motivation should motivate the existence of the requirement in as simple terms as possible, ideally without the need for the reader to be familiar with the area or specific technologies. Include references to use cases if needed.
- **Acceptance Criteria**: Statements about this requirement, which have to be fulfilled in order to realize this requirement.
- **Comments**: A detailed description of the requirement when necessary.

2.3 Requirement Clusters

During the requirements elicitation and analysis process the requirements have been classified and organized in clusters, which are used in order to group requirements into similar ones. Thus, we aim to have a better understanding about the requirements. The three main sections for the requirements of the CREDENTIAL Wallet, the CREDENTIAL App and external service providers introduce their defined requirements and describe them before the requirements are listed. For example, a cluster might define anything related to an authentication process.
Clusters can be introduced in more than one section but may contain totally different requirements. It is not necessary, that each cluster have to be present in every section.

3 Generic CREDENTIAL Wallet Requirements

The chapter describes the Generic CREDENTIAL Wallet requirements. All of these requirements are focusing on the backend side of the CREDENTIAL Wallet. Thus, addressing the functional, technical, legal and organizational requirements in a cloud based environment.
During the elicitation process we identified the following main clusters:

- Granting Access Rights
- Authentication
- Administration
- Account Management
- Data Sharing
- Services
- Generic

The clusters and their requirements are described in the following chapters.

3.1 Granting Access Rights

The cluster Granting Access Rights describes the requirements related to the processes in the CREDENTIAL Wallet that are triggered or necessary to enable access to a user's related data set for other users of the CREDENTIAL Wallet.
In particular, the processes are:

- User requests list of access rights (R-FUNC-CW-ACCESS-01)
- Associate re-encryption key with user (R-FUNC-CW-ACCESS-02)
- Search re-encryption keys by identifier (R-FUNC-CW-ACCESS-03)
- Data sharing with service providers (R-FUNC-CW-ACCESS-04)
- Delegation of access rights (R-FUNC-CW-ACCESS-05)

This cluster is build up exclusively with functional requirements towards the CREDENTIAL Wallet. It defines four requirements that can be extracted into unique services from the CREDENTIAL Wallet. Two of those services can be characterized as functionalities for a user, where the user can view a list of all users who have access to her personal data and where she can request access rights towards another user's personal data. The other two services can be characterized as functionalities for the underlying components. Because proxy-re-encryption mechanisms are used for defining access rules and re-encrypting data, the CREDENTIAL Wallet has to offer services for searching of re-encryption keys by a given identifier. The fifth requirement is more a characterization of how the re-encryption keys are stored. Since no information about the associated entities is given inside a re-encryption key, proper meta-information has to be stored.

The following tables describe the detailed requirements that were collected during the requirements elicitation process regarding the Granting Access Rights cluster.

ID	R-FUNC-CW-ACCESS-01
Title	User requests list of access rights
Area	CREDENTIAL Wallet
Type	Functional

Cluster	Granting Access Rights
Contradicts	-
Description	A user SHOULD be able to request a list containing the granted access rights.
Motivation	CREDENTIAL will be utilized in different areas such as eGovernment, eHealth and eBusiness. Furthermore, CREDENTIAL will be used in different countries of the European union. This creates a variety of different use cases involving different entities. This amount of use cases creates a huge number of possible accesses which increases the demand on "knowing who has access to parts of my wallet".
Acceptance Criteria	1. The user has to have permission to request the access rights list. 2. An error is displayed if the access list cannot be created.
Comments	The user might be interested to know who has access rights to parts of his/her CREDENTIAL Wallet. Therefore, the user should be able to request a list which is containing the granted access rights related to her/his CREDENTIAL Wallet. If the user has the rights to request this list it will be send to him/her.

ID	**R-FUNC-CW-ACCESS-02**
Title	Associate re-encryption key with user
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Granting Access Rights
Contradicts	-
Description	A re-encryption key MUST be associated with a user from whom the data is encrypted and a user to whom the data should be re-encrypted.
Motivation	Assign users to re-encryption keys.
Acceptance Criteria	1. The Authorization Service stores one re-encryption in a relation with the associated user's identifier.
Comments	Re-Encryption has the goal to transform a cipher text, encrypted for entity A, in a cipher text that is encrypted for entity B. Entities in the context of CREDENTIAL Wallet are considered to be users and therefore are associated to a public/private key pair. The re-encryption key is therefore associated to these entities.

ID	**R-FUNC-CW-ACCESS-03**
Title	Search re-encryption keys by identifier
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Granting Access Rights
Contradicts	-
Description	The CREDENTIAL Wallet MUST implement an interface to search for re-encryption keys based on user’s identifier only for CREDENTIAL Wallet internal use.
Motivation	Search re-encryption keys based on user’s identifiers.
Acceptance Criteria	1. The interface is queried with two user’s identifiers. The CREDENTIAL Wallet responds with the associated re-encryption key. If no key can be

	found an error is returned.
Comments	The CREDENTIAL Wallet stores the re-encryption keys and their associated user's identifier. In order to perform re-encryption, the re-encryption keys have to be querried through the search interface.

ID	**R-FUNC-CW-ACCESS-04**
Title	Data sharing with service providers
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Granting Access Rights
Contradicts	-
Description	Service providers MUST be able to access user data after being properly authorized by the user.
Motivation	-
Acceptance Criteria	1. Service provider gets access.
Comments	The Service Providers need access to data from the user from her CREDENTIAL Wallet. The Service Provider reads her public key from her Personal Trust Store. The Service Provider suggests a policy with the access rights she wants to have. The Public Key and the Access Rights are compiled in a request for access rights and signed by the Service Provider. In a Request Access Rights the Service Provider requests access to the data in the CREDENTIAL Wallet. The Request Access Rights object is send back to the CREDENTIAL Wallet which distributes it towards the user's smartphone.

ID	**R-FUNC-CW-ACCESS-05**
Title	Delegation of access rights
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST provide a service that allows a user to give another user access rights to certain data for a user-specified time frame.
Motivation	When a user A is to be out of the office, it could be necessary to give another user B access to the user A's CREDENTIAL Wallet, to help with the user A's electronic mail, for example.
Acceptance Criteria	1. On success, the delegated user accesses to the CREDENTIAL Wallet with the CREDENTIAL ID of the delegating user.
Comments	

3.2 Authentication

The cluster Authentication describes the requirements related to the processes in the CREDENTIAL Wallet that are triggered or necessary for user authentication in the cloud.

In particular, the processes are:

- Authentication using external IdP (ID R-FUNC-CW-AUTHN-01)
- Support IdM functionality (ID R-FUNC-CW-AUTHN-02)
- Receive an Identity Assertion request (ID R-FUNC-CW-AUTHN-03)
- Sign an Identity Assertion (ID R-FUNC-CW-AUTHN-04)
- Unique IdP identifier (ID R-FUNC-CW-AUTHN-05)
- Query IdP address (ID R-FUNC-CW-AUTHN-06)
- Easiness of use of identification token (ID R-FUNC-CW-AUTHN-07)
- IdP community (ID R-FUNC-CW-AUTHN-08)

This cluster is made up only of functional requirements towards the CREDENTIAL Wallet, which mainly refers to two main processes: user or service that authenticates against an IdP and verification of identity assertion. The following tables describe more in detail each functional requirement focusing on motivation and the acceptance criteria against CREDENTIAL Wallet.

ID	R-FUNC-CW-AUTHN-01
Title	User Authentication using external IdP
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication
Contradicts	-
Description	CREDENTIAL Wallet SHOULD be able to utilize for user authentication additional external IdPs. External IdPs are describing the IdPs which are not the CREDENTIAL Wallet but the CREDENTIAL Wallet MAY use this IdPs to authenticate users.
Motivation	The usage of additional IdPs for user authentication can make the authentication process more flexible.
Acceptance Criteria	1. An external IdP can be plugged into CREDENTIAL Wallet. User can choose that IdP and gain authentication.
Comments	The integration and implementation of the connection to Stork 2.0/eIDAS authentication service using eIDs could be demonstrated in this requirement.

ID	R-FUNC-CW-AUTHN-02
Title	Support IdM Functionality
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication
Contradicts	-
Description	The CREDENTIAL Wallet MUST have a dedicated functionality for sharing identity data in form of an IdM component.
Motivation	This is needed for authenticated users towards CREDENTIAL enabled service providers.
Acceptance Criteria	1. IdM functionality is available
Comments	-

ID	R-FUNC-CW-AUTHN-03
Title	Receive an Identity Assertion request
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication
Contradicts	-
Description	The CREDENTIAL Wallet MUST be able to receive a well-formed and valid identity assertion request
Motivation	When a service provider needs to identify and authenticate a user, it needs the credentials from the CREDENTIAL Wallet.
Acceptance Criteria	1. CREDENTIAL Wallet releases a user authentication if (and only if) a valid authentication request is produced by the service provider. The request is expected to include some information about the service provider. The request should be signed by the service provider. The signature of authentication request must be verified by CREDENTIAL Wallet.
Comments	The authentication request must be well formed, typically signed by service provider. No specific protocol is specified (i.e. the requirement should be covered by a SAML authentication request or any other standard authentication protocol).

ID	R-FUNC-CW-AUTHN-04
Title	Sign an Identity Assertion
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication
Contradicts	-
Description	The CREDENTIAL Wallet MUST be able to sign an identity assertion needed to be sent.
Motivation	Any identity assertion must have the corresponding signature to be authenticated.
Acceptance Criteria	1. Every identity assertion released by CREDENTIAL Wallet is signed. The certificate used is valid (not revoked, not expired). The root certificate that has issued the certificate used for signing process is known and trusted by service providers.
Comments	Acceptance criteria could also be shifted to service provider: any SP must reject an identity assertion released by CREDENTIAL Wallet if it is signed with a certificate no more valid or issued by an unknown certification authority.

ID	R-FUNC-CW-AUTHN-05
Title	Unique IdP identifier
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication

Contradicts	-
Description	Each Identity Provider MUST be identified through a unique identifier. Thus, further processing components know which entity is meant. A URI MUST be used as identifier.
Motivation	Processing systems should know which Identity Provider is meant.
Acceptance Criteria	1. An Identity Provider is uniquely identifiable by an URI.
Comments	-

ID	**R-FUNC-CW-AUTHN-06**
Title	Query IdP address
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication
Contradicts	-
Description	Each Identity Provider MUST have at least one corresponding endpoint address. Given a unique identifier the IdP selector MUST be capable to resolve it to its endpoint address.
Motivation	A user is redirected through an authentication process to the corresponding Identity Provider.
Acceptance Criteria	1. Given a unique identifier of an Identity Provider the IdP selector resolve this identifier to the endpoint URL of the Identity Provider. If the identifier is not known an error is returned to the user.
Comments	-

ID	**R-FUNC-CW-AUTHN-07**
Title	Easiness of use of a hardware identification token
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication
Contradicts	-
Description	It SHALL be assured that the selected hardware identification token is easy to use for CREDENTIAL user.
Motivation	CREDENTIAL project involves use of several modern, state-of-art cryptography algorithms. Nonetheless, identification token must be easy to use.
Acceptance Criteria	1. Hardware id token must be easy to use and user friendly. Usage of "simple" devices or authentication systems is encouraged.
Comments	Mobile devices are typically easy to use and should be used.

ID	**R-FUNC-CW-AUTHN-08**
Title	IdP community
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Authentication
Contradicts	-

Description	Any CREDENTIAL IdP which offers its service to CREDENTIAL users MUST be known to the CREDENTIAL network and must be added in "IdP list".
Motivation	User can be asked to choose from an IdP list an appropriate or preferred Identity Provider. This can be done if the IdP list is maintained and always up-to-date, in order to present all IdPs available.
Acceptance Criteria	1. An IdP can be used in CREDENTIAL if it is known and listed in "IdP list".
Comments	-

ID	**R-FUNC-CW-AUTHN-09**
Title	CREDENTIAL Authentication landing page
Area	App
Type	Functional
Cluster	Registration
Contradicts	-
Description	CREDENTIAL SHOULD have an authentication landing page
Motivation	A service provider needs to redirect the CREDENTIAL user to where can be authenticated.
Acceptance Criteria	1. An authentication landing page is available.
Comments	In order to process an authentication, CREDENTIAL should have an authentication web page. This page is usually rendered in the smartphone of the user.

3.3 Administration

The cluster Administration describes the requirements related to the administration process in the CREDENTIAL Wallet, which are necessary to administer users together with their related data. In particular, the identified administration processes are listed as follows:

- Ban User (ID R-FUNC-CW-ADMIN-01)
- Unban User (ID R-FUNC-CW-ADMIN-02)
- Access Restriction to Log (ID R-FUNC-CW-ADMIN-03)
- Log Users Access Attempts (ID R-FUNC-CW-ADMIN-04)

The administration requirements are detailed in the following tables.

ID	**R-FUNC-CW-ADMIN-01**
Title	Ban User
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Administration
Contradicts	-
Description	The CREDENTIAL Wallet MUST provide the functionality to ban users. This action SHOULD only be performed by authorized users.
Motivation	Ban users from the CREDENTIAL Wallet.
Acceptance	1. The CREDENTIAL Wallet must support the ban user functionality.

Criteria	2. Only authorized user can perform ban user action. These authorized users have to have the Administrator role. 3. After a ban user operation, the access to the CREDENTIAL Wallet is not allowed for this user
Comments	A user can be banned if actions are performed, which are not following the terms and conditions of the CREDENTIAL as well as its pilots. Additionally, user can send a ban user request to the CREDENTIAL Wallet.

ID	**R-FUNC-CW-ADMIN-02**
Title	Unban User
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Administration
Contradicts	-
Description	The CREDENTIAL Wallet MUST provide the functionality to unban banned users. This action SHOULD only be performed by authorized users.
Motivation	It should be possible to unban banned users.
Acceptance Criteria	1. The CREDENTIAL Wallet must support the ban user functionality. 2. Only authorized user can perform ban user action. These authorized users have to have the Administrator role. 3. The user has to be banned to perform an unban action.
Comments	If a user has been banned, it should be possible to unban the user. The unban reason could be that the user has been banned because of a mistake or the ban reason does not exist anymore. User can send an unban request to the CREDENTIAL Wallet.

ID	**R-FUNC-CW-ADMIN-03**
Title	Log Access Restriction
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Administration
Contradicts	-
Description	CREDENTIAL Wallet MUST provide mechanisms to avoid access of unauthorized persons to the log files.
Motivation	Access restriction to log files of the CREDENTIAL Wallet.
Acceptance Criteria	1. Only restricted access to the log files is available.
Comments	Log files can contain sensitive data or meta information, which can create additional privacy issues. To prevent this privacy leakage, the access to the log files must be restricted.

ID	**R-FUNC-CW- ADMIN-04**
Title	Log users' login attempts
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Administration

Contradicts	-
Description	CREDENTIAL Wallet MUST log all successful or unsuccessful login attempts related to a user account.
Motivation	All login attempts, successful or not, related to a user account should be logged.
Acceptance Criteria	1. Every login attempt is logged in an encrypted form.
Comments	The users should be able to see their login history; therefore, all login attempts have to be logged. Additionally, the log could disclose if someone unsuccessfully tried to login, which can emerge security issues.

3.4 Account Management

The cluster Account Management describes the requirements related to the processes that are triggered or necessary to manage the user's account in the CREDENTIAL Wallet.
In particular, the identified processes are listed next:

- Registration of user (R-FUNC-CW-ACCOUNT-01)
- Association of a new key-pair (R-FUNC-CW-ACCOUNT-02)
- Removal of user (R-FUNC-CW-ACCOUNT-03)
- Updating a re-encryption key (R-FUNC-CW-ACCOUNT-04)
- Recovery of CREDENTIAL Wallet data (R-FUNC-CW-ACCOUNT-05)
- Request for a recovery process (R-FUNC-CW-ACCOUNT-06)
- Verification of recovery request (R-FUNC-CW-ACCOUNT-07)
- User identification in recovery request (R-FUNC-CW-ACCOUNT-08)
- Storage of a linked devices' list (R-FUNC-CW-ACCOUNT-09)
- Unlinking devices (R-FUNC-CW-ACCOUNT-10)

This cluster comprises exclusively functional requirements towards the CREDENTIAL Wallet and covers the full lifecycle of an account of a CREDENTIAL Wallet user. These account requirements can be grouped in those requirements related to functionalities for the creation/removal of user accounts, updating data and delegating access rights; the requirements matching functionalities related to the account recovery process; the requirements associated with the creation and association of account's key-pair and the re-encryption keys; and those requirements for linked devices to the account.

In order to verify the requirement's fulfilment during the unit-testing phase, the acceptance criteria, included in the following tables describing the detailed requirements, must be accomplished.

ID	**R-FUNC-CW-ACCOUNT-01**
Title	Registration of user
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST provide a service for registering new users.
Motivation	It is the basic functionality of the CREDENTIAL Wallet: add new users to the

ID	R-FUNC-CW-ACCOUNT-01
	CREDENTIAL Wallet.
Acceptance Criteria	1. A CREDENTIAL ID is provided after registering into the CREDENTIAL Wallet, if success. Check the CREDENTIAL ID is valid by using any service.
Comments	

ID	R-FUNC-CW-ACCOUNT-02
Title	Association of a new key-pair
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	-
Description	The CREDENTIAL Wallet MUST provide a service for associating a new generated key pair to a given user.
Motivation	After a user, has generated a new key pair, it has to be associated to him/her. There are different reasons why a user would generate a new key pair such as losing a device or starting using a new one. This new key pair must be associated to him/her to be able to access the CREDENTIAL Wallet.
Acceptance Criteria	1. The user will receive an error if the key pair does not fulfill required security standards. 2. On success, the user will receive a success message.
Comments	Only the public key is sent to the Wallet. The private key does not leave the mobile.

ID	R-FUNC-CW-ACCOUNT-03
Title	Removal of user
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST provide a service for removing a given user.
Motivation	It is another basic functionality of the CREDENTIAL Wallet: remove user from the CREDENTIAL Wallet.
Acceptance Criteria	A success message is generated if the removal of the user was successful. Check the CREDENTIAL ID is not valid anymore. Otherwise, an error is generated if the action fails.
Comments	

ID	R-FUNC-CW-ACCOUNT-04
Title	Updating a re-encryption key
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management

ID	R-FUNC-CW-ACCOUNT-04
Contradicts	
Description	The CREDENTIAL Wallet MUST provide a service to *store* the re-encryption key.
Motivation	A re-encryption key update has to be possible to be able to use the CREDENTIAL Wallet on new devices after for example loss of the old one, or using additional devices.
Acceptance Criteria	A new re-encryption key, related to a user, will be created.
Comments	The re-encryption key is created in the App, but it is stored in the Wallet.

ID	R-FUNC-CW-ACCOUNT-05
Title	Recovery of CREDENTIAL Wallet *data*.
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST provide a service to recover CREDENTIAL Wallet data of a user.
Motivation	If a user is only using one device, the so-called primary device the user must be able to restore his/her data stored in the CREDENTIAL Wallet. Users must be able to recover data stored in the CREDENTIAL Wallet for example after primary device loss. This recovery process includes encrypted data as well as not encrypted data. Encrypted data have to be re-encrypted for the new device used by the related user.
Acceptance Criteria	1. A recovery key for each user exists: one cannot recover the Wallet data of other account but hers. 2. The recovery key is only available for the user itself 3. A user can recover her personal data by using the recovery key
Comments	A user is able to recover her Wallet data by providing the related recovery key kept by her.

ID	R-FUNC-CW-ACCOUNT-06
Title	Import of the Recovery Account
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST provide a service to request a recovery process. Such process will re-encrypt all the data of the user and re-generate all the re-encryption keys of the users sharing data with.
Motivation	The stored data have to be re-encrypted and new re-encryption keys for the related users generated, since the private key of the user has changed.
Acceptance Criteria	1. All the documents kept by the user are now decrypted with the new private key.

ID	R-FUNC-CW-ACCOUNT-06
	2. All the documents shared with other user are now decrypted with the new re-encryption keys.
Comments	The recovery request is sent from the CREDENTIAL App directly to the CREDENTIAL Wallet.

ID	R-FUNC-CW-ACCOUNT-07
Title	Verification of recovery request
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST pass verification checks in order to begin to manage the request for the recovery of the user involved.
Motivation	This requirement is a *must* for security reasons.
Acceptance Criteria	1. Since a user must only be allowed to change the key if the associated recovery key in the request matches a mapping between this id and the user's identification, try to change the key with several recovery keys: only with the right key, the operation will be successful.
Comments	This must be checked by querying the Authorization Service, and if this checking succeeds the signature of the request is verified.

ID	R-FUNC-CW-ACCOUNT-08
Title	User identification in recovery request
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST demand user information when managing a recovery request.
Motivation	The recovery request is a mechanism to recover a user's identity after losing his/her private key. A proof of the ownership of the private counterpart of the recovery key has to be provided in order to identify him/her at the CREDENTIAL Wallet.
Acceptance Criteria	1. The recovery request contains at least the user's CREDENTIAL ID.
Comments	

ID	R-FUNC-CW-ACCOUNT-09
Title	Storage of the list of the linked devices
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST store the device just linked.
Motivation	A list of linked devices associated with an account has to be available at the

ID	R-FUNC-CW-ACCOUNT-09
	CREDENTIAL Wallet.
Acceptance Criteria	1. A user attempts to access a CREDENTIAL service from a device just linked. No authorization error is generated. 2. A user attempts to access a CREDENTIAL service from an unlinked device. An error message is generated.
Comments	The Authorization Service takes care of validating if an attempt from a certain device is valid or not.

ID	R-FUNC-CW-ACCOUNT-10
Title	Unlinking devices
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL Wallet MUST unlink the device after a user successfully requested an unlink device operation.
Motivation	The user can only access the CREDENTIAL Wallet with linked devices. If the user is not going to use a certain device never more, it must be unlinked.
Acceptance Criteria	1. After the device is unlinked, a request to any CREDENTIAL services using that device is prohibited by the CREDENTIAL Wallet.
Comments	

3.5 Data Sharing

This cluster defines all requirements that are relevant for the data sharing aspect of the CREDENTIAL Wallet. In particular, the following aspects are covered by these requirements:

1. Storage of encrypted data (R-FUNC-CW-DATA-01)
2. Deny access (R-FUNC-CW-DATA-02)
3. Access to attributes (R-FUNC-CW-DATA-03 & R-FUNC-CW-DATA-04)
4. Disclose attributes (R-FUNC-CW-DATA-05)
5. Edit documents (R-FUNC-CW-DATA-06)
6. User's data updating (R-FUNC-CW-DATA-07)

By sharing data with other users, private and personal information are exchanged and needs to be protected against data disclosure. Therefore, encryption of the data enforced by the CREDENTIAL Wallet needs to be made. Documents of a user are characterized by attributes. Thus, data sharing involves denying and granting access to these attributes and select which attributes can be read for which entity. Finally, documents need to be editable by adding or removing certain attributes.

ID	R-FUNC-CW-DATA-01
Title	Storage of encrypted data
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Data Sharing

ID	R-FUNC-CW-DATA-01
Contradicts	-
Description	The CREDENTIAL Wallet MUST store the user data in an encrypted manner.
Motivation	The CREDENTIAL Wallet is a cloud wallet which is utilizing data encryption to maintain data confidentiality and integrity. Even if a thief steals data he/she is not able to read this data.
Acceptance Criteria	1. Specific set of data used by the CREDENTIAL Wallet can be encrypted
Comments	The CREDENTIAL Wallet must be able to ensure the data integrity and confidentiality.

ID	R-FUNC-CW-DATA-02
Title	CREDENTIAL Wallet Deny Access
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Data Sharing
Contradicts	-
Description	CREDENTIAL Wallet MUST be able to deny access to users.
Motivation	CREDENTIAL stores personal and private identity data for each user who is willing to join the CREDENTIAL Wallet. Therefore, it is crucial to guarantee only eligible access to someone's data.
Acceptance Criteria	1. An error message is displayed if the access is denied.
Comments	CREDENTIAL Wallet must be able to deny access to users for different reasons such as the certificate is invalid or the credentials are incorrect.

ID	R-FUNC-CW-DATA-03
Title	Access to user's attributes for users
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Data Sharing
Contradicts	-
Description	CREDENTIAL Wallet MUST provide access to user´s attributes for users with given permissions.
Motivation	The CREDENTIAL Wallet offers functionality to share the user's attributes. In order to guarantee the user's privacy, only user with valid permissions will be able to access the user's attributes.
Acceptance Criteria	1. The attributes can be accessed by users with given permissions.
Comments	The CREDENTIAL Wallet grants access to a user´s attributes, or any part of them, without accessing the content of these attributes. User attributes are propagated to identity assertions or shared with other users.

ID	R-FUNC-CW-DATA-04
Title	Access to user's attributes
Area	CREDENTIAL Wallet

ID	R-FUNC-CW-DATA-04
Type	Functional
Cluster	Data Sharing
Contradicts	-
Description	CREDENTIAL Wallet MUST NOT have access to user´s attributes
Motivation	The user's attributes are always encrypted in the CREDENTIAL Wallet. The CREDENTIAL Wallet has never access to the decrypted values of the attributes.
Acceptance Criteria	1. After providing the attributes to a user, the CREDENTIAL Wallet has no knowledge about the content of the attributes.
Comments	The CREDENTIAL Wallet must have access to a user´s attributes, or any part of them, without however accessing the content of these attributes. User attributes are propagated to identity assertions or shared with other users.

ID	R-FUNC-CW-DATA-05
Title	Disclose partial data
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Data Sharing
Contradicts	-
Description	The CREDENTIAL Wallet MUST redact attributes in a given Identity Assertion if the user wants to expose only a subset of the contained attributes.
Motivation	Identity assertions shares identifying personal data of the attested entity in the assertion. However, there are cases where the identity assertion holder does not want to expose every content of the identity assertion to a second user. Especially if the other user does not need every information from the identity assertion. Therefore, a user can disclose certain attributes within the identity assertion.
Acceptance Criteria	1. The attributes of the Identity Assertion are redacted according to the request from the user's IT-System
Comments	The CREDENTIAL Wallet processes incoming redact requests. It is able to disclose attributes within an Identity Assertion without changing the original signature over the attributes.

ID	R-FUNC-CW-DATA-06
Title	Edit attributes in a document
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Data Sharing
Contradicts	-
Description	The user MUST be able to edit attributes in a document
Motivation	Documents are defined by their contained attributes. A user might want to add more attributes to a document and thus edit it. In addition, in order to verify the identity of the user who owns the document, a signature must be able to be

ID	R-FUNC-CW-DATA-06
	added to a document which can be interpreted as an attribute.
Acceptance Criteria	1. Attributes are added to a document
Comments	The user must be able to edit data in a document, specifically the signature. Edit also contains the add new attributes functionality.

ID	R-FUNC-CW-DATA-07
Title	User's data updating
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Data Sharing
Contradicts	-
Description	The CREDENTIAL Wallet MUST provide services for updating user's data. These data comprise both encrypted data and metadata (e.g., usernames, credentials …) to be stored.
Motivation	
Acceptance Criteria	1. The user will receive an error if the update fails. 2. On success, the user will receive a success message.
Comments	Both encrypted data and metadata are sent to the Data Service.

3.6 Services

The cluster "Services" describes the requirements related to the services offered by the CREDENTIAL Wallet to realize certain functionalities extracted from the processes defined by the use cases.
The processes can be characterized as follow:

- Signing a link account request (R-FUNC-CW-SERV-01)
- User directory (R-FUNC-CW-SERV-02)
- Secure deletion (R-FUNC-CW-SERV-03)
- Handle notifications (R-FUNC-CW-SERV-04-05)
- Register link account request (R-FUNC-CW-SERV-06)
- Receive link account request (R-FUNC-CW-SERV-07)

All of the above-mentioned processes can be directly mapped onto CREDENTIAL services or a specific function of a service. With the search engine, a service is introduced that can be directly used by CREDENTIAL users. The remaining services describe functionalities which can be used from components either outside of CREDENTIAL or from within the CREDENTIAL Wallet. Special attention need to be made with the services which handle notifications. Often external service providers, for example Google or Apple, have own solutions for notification mechanisms towards smartphones and apps. Thus, privacy issues may arise which need to be taken carefully in account.

The following tables describe the detailed requirements that were collected during the requirements elicitation process regarding this cluster.

ID	R-FUNC-CW-SERV-01
Title	Signing a link account request
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Services
Contradicts	-
Description	CREDENTIAL MUST have the capability to sign a link account request
Motivation	As a part of the sign service included in the CREDENTIAL, the request to link a CREDENTIAL account to another account of the same user in a service provider must be signed.
Acceptance Criteria	1. The request is successfully signed
Comments	Any link account request must be possible to be signed by CREDENTIAL in order to be processed.

ID	R-FUNC-CW-SERV-02
Title	User directory
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Services
Contradicts	-
Description	CREDENTIAL Wallet MUST create a User directory.
Motivation	In order to facilitate the user search and user identity attributes it will be necessary to create a user directory.
Acceptance Criteria	1. A user directory is available at the CREDENTIAL Wallet 2. The user directory has a lookup option
Comments	The user directory contains the identifying data like the user's ID and the user's public key information. It offers a lookup function in order to search for a particular user.

ID	R-FUNC-CW-SERV-03
Title	Secure deletion
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Services
Contradicts	-
Description	Secure deletion of data MUST be available for a user.
Motivation	If a user decides to delete data or to de-register from CREDENTIAL, he shall be ensured that all his data is indeed removed from the CREDENTIAL Wallet.
Acceptance Criteria	1. All user's data is deleted after he decides to delete his account
Comments	It must be possible for the user to securely erase data from the CREDENTIAL Wallet. It must be infeasible to reconstruct deleted data after deletion.

ID	R-FUNC-CW-SERV-04
Title	Define notification triggers
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Services
Contradicts	-
Description	The CREDENTIAL Wallet MUST support the definition of notification-triggering events.
Motivation	For instance, a user wants to be informed when another user writes data to her personal wallet.
Acceptance Criteria	1. Notifications can be defined by the user.
Comments	User shall be able to define upon which actions they want to be notified.

ID	R-FUNC-CW-SERV-05
Title	Send notification upon triggering event
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Services
Contradicts	-
Description	The CREDENTIAL Wallet MUST be able to send notifications to users upon predefined events.
Motivation	For instance, a patient may want to be notified every time a doctor writes data to his data set. Or a user might want to be notified once his data has been read by a contractor. He thus sets up the corresponding trigger, and shall then be notified.
Acceptance Criteria	1. User receives notifications if a predefined event happened.
Comments	The CREDENTIAL Wallet shall notify the user as soon as a predefined trigger (i.e., event) happens.

ID	R-FUNC-CW-SERV-06
Title	Register link account request
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Services
Contradicts	-
Description	CREDENTIAL SHOULD register a link account request
Motivation	The user should have the possibility to link both accounts in service provider and CREDENTIAL, in order to access service provider with the same authentication as in the CREDENTIAL Wallet.
Acceptance Criteria	1. The CREDENTIAL Wallet stores a relation from the service provider user's identity and the CREDENTIAL Wallet user's identity.
Comments	CRENDENTIAL should be able to register a link account request sent by a Service provider

ID	R-FUNC-CW-SERV-07
Title	Receive link account request
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Services
Contradicts	-
Description	A request to link CREDENTIAL account with another service provider account of the same SHOULD be possible to be received.
Motivation	In order to have the capability to process a request of linking a CREDENTIAL account with another service provider account of the same user, the CREDENTIAL Wallet should be able to receive the request and manage it.
Acceptance Criteria	- The request is successfully received
Comments	A request to link CREDENTIAL account with another service provider account of the same SHOULD be possible to be received.

3.7 Generic

The cluster Generic describes the requirements related to all the processes and functionalities offered by the CREDENTIAL Wallet which did not fit in the introduced clusters before. The requirements in this cluster can be described as:

- Exception handling (R-FUNC-CW-GEN-01)
- Availability (R-TECH-CW-GEN-02, R-TECH-CW-GEN-07)
- Logging (R-TECH-CW-GEN-03, R-TECH-CW-GEN-04)
- Database management (R-TECH-CW-GEN-05, R-TECH-CW-GEN-06, R-TECH-CW-GEN-08, R-TECH-CW-GEN-09)
- Integration (R-TECH-CW-GEN-10, R-TECH-CW-GEN-11, R-TECH-CW-GEN-14)
- SAML interoperability (R-TECH-CW-GEN-12, R-TECH-CW-GEN-13)
- Legal (R-LEG-CW-GEN-15 to R-LEG-CW-GEN-29)

The exception handling requirements are there to enforce a unique behaviour across the CREDENTIAL Wallet in case an error happens. The availability requirements describe a certain level of service quality. The logging related requirements address the need for the safety of the user's data at the CREDENTIAL Wallet as well as the organizational duty of the hosting provider. The database related requirements describing the technical aspects that a database system has to realize for the CREDENTIAL Wallet. The integration related requirements targeting the inclusion of external systems together with CREDENTIAL Wallet services and interfaces. Thus, a certain set of standards, protocols and programming languages are proposed.
In addition, a large set of legal requirements towards the responsibility of the CREDENTIAL Wallet provider are made. They are focussing mainly on the privacy aspects and the legal rights of the user about how her personal data can be processed and how she can limit the use of the data without giving up her sovereignty of the data.

The following tables describe the detailed requirements that were collected during the requirements elicitation process regarding the service cluster.

ID	R-FUNC-CW-GEN-01

Title	Respond Exception
Area	CREDENTIAL Wallet
Type	Functional
Cluster	Generic
Contradicts	-
Description	A process or functional flow in the CREDENTIAL Wallet MUST propagate an exception to the caller if an error occurred.
Motivation	Provide enough information on an exception. Thus, a caller can decide how he proceeds.
Acceptance Criteria	1. An exception occurred during a progress in the CREDENTIAL Wallet. The initiator involved in this process receives an exception. 2. Only sanitized errors are returned to an external caller.
Comments	Errors occurred during the process of the CREDENTIAL Wallet are propagated through exceptions or sanitized errors to any caller of this process. This can be a component inside CREDENTIAL or an external caller.

ID	**R-TECH-CW-GEN-02**
Title	Availability of CREDENTIAL Wallet
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	The CREDENTIAL Wallet SHOULD support high availability and fault tolerance
Motivation	The CREDENTIAL Wallet gains its strength by providing a cloud based storage solution for personal and identity data. Thus, it is crucial to have a high availability for the CREDENTIAL Wallet since most of the use cases rely on a continuous availability of CREDENTIAL services.
Acceptance Criteria	1. CREDENTIAL services have an availability of 99,9% (Downtime per year around 8 hours)
Comments	The availability characterizes how often CREDENTIAL services are available during the time of a year. Each time a CREDENTIAL service is not available it lowers the percentage of the availability.

ID	**R-TECH-CW-GEN-03**
Title	Database access trail
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	Access to database SHOULD be audited.
Motivation	Control of the access and modifications made in database.
Acceptance Criteria	1. After the database was accessed, a log entry is written to the log trail
Comments	The log files have the purpose to help the process of intrusion or possible attacks on CREDENTIAL services.

ID	R-TECH-CW-GEN-04
Title	Database access trail content
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	Who and what modifications on a database access are performed SHOULD be logged in the database audit trail.
Motivation	Intrusion detection might need the information in order to conclude certain decisions.
Acceptance Criteria	1. Log files for the database access contain the identifier of the requester 2. Log files for the database access contain the action of the requester 3. Log files for the database access contain the resource to be accessed
Comments	The log files have the purpose to help the process of intrusion or possible attacks on CREDENTIAL services.

ID	R-TECH-CW-GEN-05
Title	Existence of database
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	The CREDENTIAL Wallet SHOULD provide a database.
Motivation	The CREDENTIAL Wallet offers services to store, share and update in a privacy and secure way personal data. Therefore, an own database is needed.
Acceptance Criteria	1. A database in the CREDENTIAL Wallet is integrated
Comments	

ID	R-TECH-CW-GEN-06
Title	SQL standard support
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	The request to a database SHOULD follow the current SQL standard allowing the use of different SQL-based databases.
Motivation	Many different vendors offer implementations for the most used query language for databases SQL. Therefore, by using a standard like SQL it offers great flexibility when choosing a most fitting solution.

Acceptance Criteria	1. The installed database supports at least the SQL-92[3]standard
Comments	If a SQL-like database is used it should be compatible with the SQL standard in order to ease the integration with the components of the CREDENTIAL Wallet. Otherwise, it is not a must to include a SQL database. Thus, NoSQL and object stores are still valid choices for the database solution.

ID	**R-TECH-CW-GEN-07**
Title	Database availability
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	The availability of the database MUST be 24x7.
Motivation	The CREDENTIAL Wallet gains its strength by providing a cloud based storage solution for personal and identity data. Thus, it is crucial to have a high availability for the database since most of the use cases rely on a continuous availability of CREDENTIAL services.
Acceptance Criteria	1. CREDENTIAL database has an availability of 99,9% (Downtime per year around 8 hours)
Comments	The availability characterizes how often CREDENTIAL databases available during the time of a year. Each time the CREDENTIAL database is not available it lowers the percentage of the availability.

ID	**R-TECH-CW-GEN-08**
Title	Database backups
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	Back up of this database SHOULD be made periodically.
Motivation	The database builds the backbone of the service functionality of the CREDENTIAL Wallet. Without the database, no sharing and storing of personal or identity data can be made. To prevent data loss, a backup of the data is mandatory.
Acceptance Criteria	1. The CREDENTIAL Wallet creates each day a full backup of the database.
Comments	

ID	**R-TECH-CW-GEN-09**
Title	Database synchronization

[3]http://www.contrib.andrew.cmu.edu/~shadow/sql/sql1992.txt

Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	Synchronization of Database SHOULD be assured if multiple are used.
Motivation	The CREDENTIAL Wallet may offer multiple databases for huge database content in order to optimize the data access. Therefore, synchronization between multiple databases have to be made.
Acceptance Criteria	1. Synchronization between multiple databases is performed on a regularly basis
Comments	

ID	**R-TECH-CW-GEN-10**
Title	Limited impact on existing service providers
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	Service provider who migrates into CREDENTIAL network SHOULD benefit of limited impact on its architecture and configuration.
Motivation	The services don't need to be heavily modified in order to be interfaced with CREDENTIAL; the integration will impact only the security components that give access to SP's. Looking at e-Gov pilot, for example, the candidate SP is SIAGE, a service that widely uses a particular identification data of the citizen, named "codice fiscale" (or "fiscal code"). Any IdP usable by citizen to access SIAGE *shall* insert fiscal code into the SAML assertion. This data could also be contained in CREDENTIAL Wallet if not directly managed by IdP during user authentication.
Acceptance Criteria	1. CREDENTIAL architecture should be designed to guarantee low integration effort for SP joining the CREDENTIAL Wallet.
Comments	In some pilot, it should be possible to candidate as a CREDENTIAL service provider an already existing SP. This SP is required to join CREDENTIAL network and a value added of the project will be, without any doubt, the capability to ensure low impact on this SP. For example, the SP might be required to change IdPs integration: this kind of operation should be realized with minor changes on SP itself.

ID	**R-TECH-CW-GEN-12**
Title	State of the art identity protocol interoperability
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	Any CREDENTIAL IdP SHOULD support state of the art identity assertions (such as SAML).
Motivation	As specified in another requirement, existing SP joining the CREDENTIAL

	Wallet should not be heavily modified. To do so, CREDENTIAL IdPs must guarantee a complete SAML 2.0 adoption. Translation between attributes released by IdP and legacy attributes can be done natively (on IdP) or just before release attributes to SP (i.e. Shibboleth attribute map).
Acceptance Criteria	1. An IdP can be used if it is fully compliant with state of the art identity assertions (such as SAML 2.0 standard)
Comments	A CREDENTIAL IdP shall use SAML 2.0 authentication scheme. Interoperability between attributes released by third party IdP and CREDENTIAL IdP have to be assured.

ID	**R-TECH-CW-GEN-13**
Title	SAML assertion consumer component
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	A SP MAY integrate an efficient SAML requester/consumer component, i.e. Shibboleth
Motivation	Usage of standard and well-known component to produce SAML request and perform SAML verification is highly recommended because it avoids technical difficulty for the SP.
Acceptance Criteria	1. SP may use SAML requester/consumer component 2. Open source components are recommended
Comments	Every SP which delegates user authentication to a SAML IdP must be capable of produces, receives, correctly understand and validates a SAML response. This task is efficiently performed by standard, open-source component, like Shibboleth.

ID	**R-TECH-CW-GEN-14**
Title	CREDENTIAL Wallet integration
Area	CREDENTIAL Wallet
Type	Technical
Cluster	Generic
Contradicts	-
Description	CREDENTIAL Wallet SHOULD be accessible by at least two different technologies (e.g. REST web services and JAVA API)
Motivation	In CREDENTIAL project, we'll probably gather different component made with different technologies, and lets CREDENTIAL Wallet accessible by different technologies should be a good idea to enhance project success.
Acceptance Criteria	1. CREDENTIAL Wallet integration is performed with REST API calls and Java interface integration.
Comments	CREDENTIAL Wallet offers integration services for several tasks, i.e. apply proxy re-encryption. Several components into CREDENTIAL network will integrate CREDENTIAL Wallet and the more the integration technologies are different, the more is the value added by the project.

ID	R-LEG-CW-GE N-15
Title	Privacy by design
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	The CREDENTIAL project MUST consider privacy of users from the onset by implementing technical solutions such as providing users the possibility to access the CREDENTIAL service with pseudonymous identities.
Motivation	Privacy by design guarantees that the system has considered privacy of the users early on and at consequent processes and implementations.
Acceptance Criteria	1. Privacy by design methods were used by defining and developing the CREDENTIAL Wallet
Comments	

ID	R-LEG-CW-GEN-16
Title	Privacy by default
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	The CREDENTIAL project MUST provide the strictest possible privacy settings of the system at the time the user starts to use it.
Motivation	Setting privacy preferences is a cumbersome task for users. Majority of users fail to appropriately configure optimal privacy settings. Moreover, typical settings, e.g., those set by social media networks, don't fully fulfil the expectations of users. Therefore, CREDENTIAL MUST consider user-centred default privacy settings.
Acceptance Criteria	1. The default settings for a new user are set to the privacy friendliest way possible
Comments	

ID	R-LEG-CW-GEN-17
Title	Purpose limitation
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	Personal data SHALL be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.
Motivation	The ‘why’ of the personal data collection has to properly be communicated to the data subject. Furthermore, data collected for one purpose, e.g., personal health collected for diabetes follow up, shouldn't be used for a different objective than the initial intentions.
Acceptance Criteria	1. Personal data is only processed for the purpose it was collected.

Comments	

ID	**R-LEG-CW-GEN-18**
Title	Lawfulness, fairness and transparency
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	Personal data SHALL be processed lawfully, fairly and in a transparent manner in relation to the user.
Motivation	Data subjects have the rights that their data is processed in accordance with the data protection regulations. Likewise, pilot users in CREDENTIAL have such fundamental rights.
Acceptance Criteria	1. Personal data is processed lawfully, fairly and transparent to the user.
Comments	

ID	**R.LEG-CW-GEN-19**
Title	Data minimisation
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	Personal data MUST be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
Motivation	Users must have the possibility to, e.g., authenticate to CREDENTIAL system with only those credentials essentially required for authentication.
Acceptance Criteria	1. Personal data is limited to what is necessary in relation to the purpose for which it is processed.
Comments	

ID	**R-LEG-CW-GEN-20**
Title	Accuracy
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	User’s data MUST be accurate and, where necessary, kept up to date.
Motivation	Every reasonable step must be taken to ensure that user's data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
Acceptance Criteria	1. User’s data is kept up to date
Comments	

ID	R-LEG-CW-GEN-21
Title	Storage time limitation
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	Personal data MUST be kept in a form which permits identification of the user for no longer than is necessary for the purposes for which the personal data are processed.
Motivation	Storage limitation, like other rights, is an essential requirement for users. When users sign consents, it must clearly be stated as to how long their data will be retained for processing. When this time expires, the data must be permanently deleted and users have the right to get notified about it.
Acceptance Criteria	1. User can only be identified as long the personal data is processed.
Comments	

ID	R-LEG-CW-GEN-22
Title	Integrity and confidentiality of user's data
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	User's data MUST be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
Motivation	Users should be given with the assurance that intruders do not have access to their personal data. High level integrity and confidentiality measurements MUST be put.
Acceptance Criteria	1. Mechanisms to protect unauthorized access on personal data are implemented
Comments	

ID	R-LEG-CW-GEN-23
Title	Right to be forgotten
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	The user SHALL HAVE the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay.
Motivation	In the middle of the project (or after termination of project, and before

	retention period expires), the user might request for erasure of part or all of her personal data.
Acceptance Criteria	1. Personal data can be deleted without any delay after the request of a user.
Comments	

ID	**R-LEG-CW-GEN-24**
Title	Restriction of processing
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	The user SHALL HAVE the right to obtain from the controller (pilot hosts) the restriction of the processing of her personal data.
Motivation	Similar to erasure, the user has the right to withhold the processing of her personal data by the controller, e.g., a patient in the e-Health CREDENTIAL pilot may request that her doctor or another health personnel should not process her data.
Acceptance Criteria	1. The user can stop at any time the processing of her personal data
Comments	

ID	**R-LEG-CW-GEN-25**
Title	Data breach notification
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	Whenever a data breach happens, especially one that threatens the privacy of the users, the pilot host MUST communicate this risk to the users and entities responsible for data protection.
Motivation	In the event that a data breach is detected, the user has the right to get notified of the incidence, and the possible remedies have to be communicated. Furthermore, the ethics board as well as the affected users have to be notified about incidents of data breach.
Acceptance Criteria	1. The users can be informed about a data breach
Comments	

ID	**R-LEG-CW-GEN-26**
Title	Trustworthy storage
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	The cloud service from CREDENTIAL SHALL provide a trustworthy storage

	where only authorized persons would be allowed to make changes and new entries. Furthermore, the data should able to meet authenticity checks.
Motivation	
Acceptance Criteria	1. Only authorized persons can make changed to data entries
Comments	

ID	**R-LEG-CW-GEN-27**
Title	Recognizing legal representatives
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Generic
Contradicts	-
Description	When a user is unable to digitally sign or transfer data (e.g., patient data), a legal representative SHOULD have the authentication credentials and equivalent level of authorization to perform the transaction.
Motivation	
Acceptance Criteria	1. Transactions regarding personal data can be performed by legal representatives of the user
Comments	

ID	**R-LEG-CW-GEN-29**
Title	Minimize processed data
Area	CREDENTIAL Wallet
Type	Legal
Cluster	Administration
Contradicts	-
Description	Only necessary user data MUST be processed by the CREDENTIAL Wallet.
Motivation	The amount of processed user data by the CREDENTIAL Wallet should be minimized.
Acceptance Criteria	1. The processed user data must be minimized.
Comments	The processed user data should be minimized according to technical and legal reasons.

4 Generic CREDENTIAL App Requirements

This chapter describes the requirement for the CREDENTIAL App. The following clusters have been identified for the CREDENTIAL App requirements:

- Registration
- Account Management
- Services

All clusters and their requirements are described in the following three subchapters.

4.1 Registration

The cluster registration describes the requirements related to the registration process of a user at the CREDENTIAL Wallet. It covers all the aspects an App and the smartphone has to fulfil in order to enable the registration process successfully for a user. The requirements collected in these clusters are:

- Submit registration form (R-FUNC-APP-REG-01)
- Provide Username (R-FUNC-APP-REG-02)
- Register with fingerprint (R-FUNC-APP-REG-03)

All requirements are pure functional requirements. The last two requirements focusing on the initial registration process of a single user on the CREDENTIAL Wallet by providing at least a username and start the registration process by using her fingerprint. The first two requirements address the cases that a user has already a CREDENTIAL account and wants to use these data to register to a third-party service provider by using the CREDENTIAL App. Thus, a navigation to the authentication screen needs to be performed and a way to submit a registration form from the CREDENTIAL App to the service.
The registration requirements are described in the following tables:

ID	R-FUNC-APP-REG-01
Title	Submit registration form
Area	CREDENTIAL App
Type	Functional
Cluster	Registration
Contradicts	-
Description	A user SHOULD be able to submit a registration form
Motivation	If a service provider needs to receive personal data in a registration form. This personal data must be provided encrypted by CREDENTIAL Wallet to ensure the privacy.
Acceptance Criteria	1. The registration form has been submitted with the information of the user.
Comments	A user should be able to submit a registration form in a secure way with personal data to a service provider.

ID	R-FUNC-APP-REG-02
Title	Provide Username
Area	CREDENTIAL App
Type	Functional

Cluster	Registration
Contradicts	-
Description	The CREDENTIAL App MUST collect a unique username during the registration process.
Motivation	The username is used by the user to identify him- or herself and easily find other users in order to share data.
Acceptance Criteria	1. The registration page contains the form field for enter a username
Comments	The CREDENTIAL services check in the background if the given username may have already been taken.

ID	**R-FUNC-APP-REG-03**
Title	Register with fingerprint
Area	CREDENTIAL App
Type	Functional
Cluster	Registration
Contradicts	-
Description	The CREDENTIAL App SHOULD provide a function to let a user register with his fingerprint.
Motivation	The access to CREDENTIAL services should be made easier for user if they can unlock the CREDENTIAL App and access to their data by using a fingerprint function.
Acceptance Criteria	1. The registration page contains the form field for fingerprint recognition
Comments	The CREDENTIAL App verifies a successful read from the fingerprint and in case of success give the user some feedback.

4.2 Account Management

The cluster Account Management describes the requirements related to the managing tasks around the account of a user. The requirements are:

- Unlink device functionality (R-FUNC-APP-ACCOUNT-01)
- Select disclosed attributes (R-FUNC-APP-ACCOUNT-02)
- Storage of CREDENTIAL Keys (R-FUNC-APP-ACCOUNT-03)
- Availability of cryptographic material (R-FUNC-APP-ACCOUNT-04)
- Key-pair re-generation (R-FUNC-APP-ACCOUNT-05, R-FUNC-APP-ACCOUNT-06)

The requirements are all functional. The unlink device functionality addresses the cases where an external device is coupled with the CREDENTIAL App on the user's smartphone. The select disclosed attributes requirement describes a requirement which allows the user to select which attributes should be disclosed during the authentication process against another service. The last three requirements focusing on the general cryptographic functions a user can perform for his key material.

The requirements are described in the following tables:

ID	**R-FUNC-APP-ACCOUNT-01**

Title	Unlink device functionality
Area	CREDENTIAL App
Type	Functional
Cluster	Account Management
Contradicts	-
Description	The CREDENTIAL App MUST render a webpage with a list of unlinkable devices
Motivation	The user is able to view all linked devices to his account and their settings.
Acceptance Criteria	1. A list of the user's linked devices is rendered to the user. Each entry has an unlink option.
Comments	The user receives the option to select which device he/she wants to unlink.

ID	**R-FUNC-APP-ACCOUNT-02**
Title	Select disclosed attributes
Area	CREDENTIAL App
Type	Functional
Cluster	Account Management
Contradicts	-
Description	The user SHOULD be able to select attributes he/she wants to be disclosed.
Motivation	Disclose Identity Attributes without resign the attributes from the vouching entity.
Acceptance Criteria	1. The attributes can be selected to be disclosed or non-disclosed.
Comments	The Identity Assertion contains of its attributes and at least one signature vouching for the attributes. The user is able to select which attributes should be disclosed for further processing without attempting to resign the attributes.

ID	**R-FUNC-APP-ACCOUNT-03**
Title	Store CREDENTIAL key in personal trust store
Area	CREDENTIAL App
Type	Functional
Cluster	Account Management
Contradicts	-
Description	The CREDENTIAL App MUST store his private key in a Personal Trust Store.
Motivation	Store Private Key on User's device.
Acceptance Criteria	1. The CREDENTIAL App is configured with a Personal Trust Store holding the CREDENTIAL Private Key.
Comments	The Private Key allows a user to access his CREDENTIAL resources. Each CREDENTIAL App maintains a Personal Trust Store where the private key is stored.

ID	**R-FUNC-APP-ACCOUNT-04**
Title	Availability of cryptographic material for signing access control policies
Area	CREDENTIAL App
Type	Functional

Cluster	Account Management
Contradicts	-
Description	The Smartphone MUST store cryptographic material that can be used to electronically sign data
Motivation	CREDENTIAL aims for having user-friendly authentication mechanisms with the focus on mobile devices. Since cryptographic algorithms play a large role in the authentication and authorization process, the smartphone has to be capable of using cryptographic material.
Acceptance Criteria	1. Cryptographic material for signing is available at the smartphone
Comments	

ID	**R-FUNC-APP-ACCOUNT-05**
Title	Generation of a new key-pair
Area	CREDENTIAL App
Type	Functional
Cluster	Account Management
Contradicts	-
Description	The CREDENTIAL App MUST provide a service to generate new key-pair.
Motivation	The user requires a new public key/pair, for instance, when registering for the first time in CREDENTIAL, or to replace his/her old one.
Acceptance Criteria	1. New key-pair is generated.
Comments	-

ID	**R-FUNC-APP-ACCOUNT-06**
Title	Generation of a recovery key
Area	CREDENTIAL App
Type	Functional
Cluster	Account Management
Contradicts	
Description	The CREDENTIAL App MUST provide a service for creating a recovery key.
Motivation	A basic functionality of the CREDENTIAL project is to offer the user a possibility to recover his account just in case his/her CREDENTIAL account is threatened, the smartphone was stolen or the password is lost.
Acceptance Criteria	1. After sending the recovery request, a new key pair for his/her account and a re-encryption key are available.
Comments	The generation of the key is performed by the user. The recovery key needs to be generated before the device is lost. She should export the generation key and save it to a cold storage (e.g. a USB stick, etc…)

4.3 Services

The cluster services describe the requirements for services or functionalities that have to be available on or are part of the CREDENTIAL App. In particular, the cluster can be broken down in the following parts:

- Signature service (R-FUNC-APP-SERV-01)

- Encryption service (R-FUNC-APP-SERV-02 to R-FUNC-APP-SERV-05)
- Key-Generation service (R-FUNC-APP-SERV-06 to R-FUNC-APP-SERV-08)

All requirements are pure functional requirements. They describe basically the need of at least three different services at the CREDENTIAL App that enables the signature over a given data set, the encryption of a given data set, and the generation of the appropriate key material.
The requirements are listed in the following tables:

ID	R-FUNC-APP-SERV-01
Title	Signature service
Area	CREDENTIAL App
Type	Functional
Cluster	Service
Contradicts	-
Description	The CREDENTIAL App MUST contain a Signature Service.
Motivation	The signatures are needed to enforce data and message integrity. Moreover, redactable signature functionality should be provided by this service.
Acceptance Criteria	1. A signature service is available for the CREDENTIAL App.
Comments	The signature service of the CREDENTIAL App.

ID	R-FUNC-APP-SERV-02
Title	Signature service functions
Area	CREDENTIAL App
Type	Functional
Cluster	Service
Contradicts	-
Description	This signature service MUST be able to create, receive and submit signature requests.
Motivation	The signature is performed on the user's device.
Acceptance Criteria	1. The signature service can process, receive and submit encryption and decryption requests.
Comments	The functionality of the signature service of the CREDENTIAL App.

ID	R-FUNC-APP-SERV-03
Title	Encryption service
Area	CREDENTIAL App
Type	Functional
Cluster	Service
Contradicts	-
Description	The CREDENTIAL App MUST contain an Encryption Service.
Motivation	The encryption is performed on the data before it is uploaded to the CREDENTIAL Wallet. Decryption is performed after the App receives data from the CREDENTIAL Wallet.
Acceptance Criteria	1. An encryption service is available for the CREDENTIAL App.

Comments	The encryption service of the CREDENTIAL App.

ID	**R-FUNC-APP-SERV-04**
Title	Encryption service functions
Area	CREDENTIAL App
Type	Functional
Cluster	Service
Contradicts	-
Description	This encryption service MUST be able to process, receive and submit encryption and decryption requests.
Motivation	The encryption is performed on the user's device.
Acceptance Criteria	1. The encryption service can process, receive and submit encryption and decryption requests.
Comments	The functionality of the encryption service of the CREDENTIAL App.

ID	**R-FUNC-APP-SERV-05**
Title	Key generation service
Area	CREDENTIAL App
Type	Functional
Cluster	Service
Contradicts	-
Description	The CREDENTIAL App MUST contain a Key Generation Service.
Motivation	The key material for the general public/private key pair as well as the re-encryption keys have to be created on the user's device.
Acceptance Criteria	1. A key generation service is available for the CREDENTIAL App.
Comments	The key generation service of the CREDENTIAL App.

ID	**R-FUNC-APP-SERV-06**
Title	Key Generation service functions
Area	CREDENTIAL App
Type	Functional
Cluster	Service
Contradicts	-
Description	This encryption service MUST be able to process, receive and submit key generation requests.
Motivation	The encryption is performed on the user's device.
Acceptance Criteria	• The key generation service can process, receive and submit key generation requests.
Comments	The functionality of the key generation service of the CREDENTIAL App.

ID	**R-FUNC-APP-SERV-07**
Title	Request creation of re-encryption key
Area	CREDENTIAL App
Type	Functional
Cluster	Services

Contradicts	-
Description	A user MUST be able to request a re-encryption key creation.
Motivation	A new re-encryption key is required if the user starts using a new device for different reasons.
Acceptance Criteria	1. A request for a new re-encryption key is propagated to the re-encryption generation service.
Comments	A user must be able to request a re-encryption key creation.

5 External Service Requirements

In this chapter, all requirements towards an external service provider are documented. Service Providers are able to connect to the CREDENTIAL Wallet. Users are able to use these services by providing their identity data from the CREDENTIAL Wallet for authentication and application purposes of the service. Thus, special consideration towards the service provider requirements has to be made and is discussed in the following subchapters.

5.1 Service Provider Requirements

This cluster focuses on the functional and technical requirements towards an external service provider who wants to participate in CREDENTIAL. The requirements identified for a service provider covering the following aspects:

- Definition of required authentication attributes (R-FUNC-SP-SERV-01)
- Access to plaintext attributes (R-FUNC-SP-SERV-02)
- Detection of multiple usage (R-TECH-SP-SERV-03)

The first two requirements describe the functional need of a service provider to publish the attributes he needs from users in order to provide his service as well the ability to read those attributes in plaintext. The third requirement describes a technical improvement of the service quality by detecting the usage of the service provider by the same identity attributes across multiple devices or users. Thus, he might be able to shut down the service for abuse.

ID	R-FUNC-SP-SERV-01
Title	Definition of required disclosed fields for authentication
Area	Service Provider
Type	Functional
Cluster	Services
Contradicts	-
Description	SP MUST be able to define required data fields and accepted issuers
Motivation	A service provider must be able to define which attributes (e.g., first name, date of birth, etc.) a user has to reveal for authentication. Also, the service provider must be able to choose which issuers (e.g., self-signed, governmental agency, etc.) may have certified this information. This information is contained in the presentation policy presented to the user before the protocol starts.
Acceptance Criteria	1. As part of the authentication policy, the SP can define accepted issuers and tags of required information. If not all those fields are revealed, or another issuer certified the data, the authentication protocol fails.
Comments	

ID	R-FUNC-SP-SERV-02
Title	Access to plaintext attributes for disclosed attributes
Area	Service Provider
Type	Functional
Cluster	Services
Contradicts	-
Description	SP MUST be able to access the requested attributes in the clear
Motivation	At the end of the authentication protocol, the service provider must have access

	to the plaintext attributes contained in the requested data fields, certified by (one of) the requested issuer(s). This information can then be used for further processing.
Acceptance Criteria	1. The SP can access at least all requested data fields in the clear.
Comments	

ID	**R-TECH-SP-SERV-03**
Title	Detection of multiple usage
Area	Service Provider
Type	Technical
Cluster	Services
Contradicts	*Potential partial contradictions to privacy requirements defined in D2.6.*
Description	A SP MAY be able to detect parallel usage of credentials
Motivation	For instance, for streaming services, the SP may need means to detect that a subscription is shared by physical entities without permission.
Acceptance Criteria	1. If a credential is used more than a threshold number of times within a predefined time interval, the SP is alerted.
Comments	

5.2 Administration

This cluster defines the administration needs and functionalities of a service provider towards the CREDENTIAL Wallet. In particular, the following administration tasks and requirements have been identified:

- Anonymity Revocation (R-TECH-SP-ADMIN-01)
- List of Supported Issuers (R-ORG-SP-ADMIN-02)
- Registration as Service Provider (R-FUNC-SP-ADMIN-03)
- Listing User Logins (R-FUNC-SP-ADMIN-04)
- Manage Service Provider Information (R-FUNC-SP-ADMIN-05)

These requirements are a mix of technical, functional and organizational requirements. The first requirement describes a technical requirement in the case of abuse. Thus, a service provider is able to identify the identity who abuses the service. The second requirement is an organizational requirement and describes the possibility to publish a list of trustworthy issuers across all service provider, thus that they can configure their validation and verification services. The last two requirements describe functional aspects during the registration of a service provider towards the CREDENTIAL Wallet as well that the service provider has to provide a list of all devices with which a user is logged-in to its services. Finally, the service provider has the possibility to manage their attributes and contact information at the CREDENTIAL Wallet. The CREDENTIAL Wallet later on uses the information to register the service properly within the CREDENTIAL Wallet.

ID	**R-TECH-SP-ADMIN-01**
Title	Anonymity revocation
Area	Service Provider
Type	Technical
Cluster	Administration

Contradicts	*Potential partial contradictions to privacy requirements defined in D2.6.*
Description	User's anonymity MAY be revocable
Motivation	In case of abuse (e.g., a user posts criminal content in an anonymous forum), a pre-defined external party (e.g., a judge) can be contacted to reveal the identity of the otherwise anonymous user.
Acceptance Criteria	1. The external party can unambiguously identify the identity of the user, solely based on the information held by the SP.
Comments	

ID	**R-ORG-SP-ADMIN-02**
Title	List of supported issuers
Area	Service Provider
Type	Organizational
Cluster	Administration
Contradicts	-
Description	There SHOULD exist a list of registered issuers, which SHOULD be grouped.
Motivation	As a SP may accept multiple issuers (e.g., passport offices from any country), the issuer index should also offer predefined groups/clusters of issuers. One specific cluster (potentially per legislation) should be "trustworthy issuers" which are allowed to certify data in a legally binding way.
Acceptance Criteria	1. SPs can access an index containing all issuers and (hashes of) their public keys for which credentials have been uploaded to the CREDENTIAL Wallet. 2. The issuers in the index are grouped, e.g., by country, trust level, etc.
Comments	Without this requirement, every service provider would have to keep a local list of accepted issuers, their keys, etc. This may be a viable solution for small deployments or if the service provider only accepts a very limited number of issuers (e.g., if it only accepts credentials that it issued itself, or that were issued by a specific governmental agency). In larger settings, offloading this work to the central CREDENTIAL Wallet could positively contribute to market adoption and the willingness of SPs to use CREDENTIAL technologies.

ID	**R-FUNC-SP-ADMIN-03**
Title	Registration as service provider
Area	Service Provider
Type	Functional
Cluster	Administration
Contradicts	-
Description	SPs MUST be able to register themselves at the CREDENTIAL Wallet.
Motivation	To allow users to link their accounts at the service provider to their CREDENTIAL account, the service provider needs to be able to register itself as a CREDENTIAL-supporting service at the CREDENTIAL Wallet.
Acceptance Criteria	1. A new SP can join the CREDENTIAL universe and register at the CREDENTIAL Wallet.
Comments	

ID	R-FUNC-SP-ADMIN-04
Title	Listing current user logins
Area	Service Provider
Type	Functional
Cluster	Administration
Contradicts	*Potential partial contradictions to privacy requirements defined in D2.6.*
Description	User SHOULD be able to list all current logins to a specific service
Motivation	It is required that a user is able to list all his current connections (from potentially different devices) to a service. For privacy reasons, this may not always be possible in CREDENTIAL, as the SP may not be able to link multiple sessions of a specific user. Thus, the CREDENTIAL Wallet should provide means to let users list all recent or currently active sessions.
Acceptance Criteria	1. The CREDENTIAL App allows the user to list all devices that are currently logged in to a specific service.
Comments	

ID	R-ORG-SP-ADMIN-05
Title	Updating service provider information
Area	Service Provider
Type	Organizational
Cluster	Account Management
Contradicts	-
Description	SP MUST be able to update its information in the CREDENTIAL Wallet
Motivation	A service provider must be able to update its identifying information at the CREDENTIAL Wallet. This may, e.g., include contact information, but also cryptographic values such as the public re-encryption key of the SP.
Acceptance Criteria	1. A SP can request its information to be updated. 2. If cryptographic values are updated, users are notified and requested to upload fresh re-encryption keys.
Comments	

5.3 Services

This cluster defines requirements towards services within the CREDENTIAL Wallet eco-system that can be used by external service providers. In particular, these requirements are:

- Single sign-out (R-FUNC-SP-SERV-01)
- Ease of integration (R-FUNC-SP-SERV-02)
- OAuth 2.0 compatibility (R-FUNC-SP-SERV-03)

A single sign-out functionality for the user enables her to log-out from any service provider she is currently logged in with CREDENTIAL Wallet capabilities. Furthermore, service providers are more willing to cooperate with CREDENTIAL Wallet capabilities if the integration of these services is easy to perform. The last service requirement is the compatibility with certain well-established authentication and authorization standards, which OAuth 2.0 delivers.

ID	R-FUNC-SP-SERV-01
Title	Single sign-out

Area	Service Provider
Type	Functional
Cluster	Services
Contradicts	*Potential partial contradictions to privacy requirements defined in D2.6.*
Description	A single sign-out functionality SHOULD be provided to the user
Motivation	A single sign-out functionality is required so that a user can terminate all his current sessions (potentially across devices) to a service. As the SP may not be able to link sessions to a user, this functionality should be provided by the CREDENTIAL Wallet.
Acceptance Criteria	1. The CREDENTIAL App lets the user terminate all sessions to a specific service across multiple devices.
Comments	

ID	**R-ORG-SP-SERV-02**
Title	Ease of integration into service provider architecture
Area	Service Provider
Type	Organizational
Cluster	Services
Contradicts	-
Description	CREDENTIAL components MUST be easy to integrate for the SP
Motivation	Integrating CREDENTIAL into the existing SP's software stack must be efficient and convenient.
Acceptance Criteria	1. Availability of a well-document and easy-to-deploy software bundle that is compatible with the most commonly used SP software stacks.
Comments	

ID	**R-TECH-SP-SERV-03**
Title	OAuth2 compatibility
Area	Service Provider
Type	Technical
Cluster	Services
Contradicts	-
Description	CREDENTIAL components SHOULD be compatible with OAuth 2
Motivation	To increase market adoption, the SP's components of CREDENTIAL should be available as a standard OAuth2 service provider plugin.
Acceptance Criteria	1. Availability of an OAuth2 service provider plugin for integrating CREDENTIAL into existing SP architectures.
Comments	

5.4 Issuer Requirements

This cluster defines requirements towards issuer of identity attributes and data. The requirements can be grouped into:

- Issuer-driven revocation (R-FUNC-SP-ISSUER-01)
- Disclosure of attributes at issuance (R-FUNC-SP-ISSUER-02)

- Issuer registration (R-FUNC-SP-ISSUER-03)
- Key update and revocation (R-FUNC-SP-ISSUER-04)
- Expiration dates on credentials (R-FUNC-SP-ISSUER-05)

All of these requirements are pure functional requirements. The first one describes the requirement that issuers are capable to revoke certain user credentials, which in turn denies a user to successfully authenticate herself towards any service provider. While issuing a certain set of attributes the issuer needs to be able to read those attributes in plaintext. Issuer registration describes the capability of an issuing entity to register themselves at the CREDENTIAL Wallet. While providing his own keys, an issuer needs to be able to update and revoke their registration information towards the CREDENTIAL Wallet. Finally, an issuer is able to add expiration date to user's credentials which limits the time of use of these credentials.

ID	R-FUNC-SP-ISSUER-01
Title	Issuer-driven revocation of user credentials
Area	Issuer
Type	Functional
Cluster	Services
Contradicts	-
Description	Issuers SHOULD be able to revoke credentials
Motivation	In the case of abuse, but also, e.g., when an employee leaves a company, the issuer of a credential should be able to invalidate this without compromising the revoked user's privacy.
Acceptance Criteria	1. An issuer can define the credential to be revoked. 2. After revocation, the owner of the credential is no longer able to successfully authenticate to SPs using this credential.
Comments	With credentials, some form of issued cryptographic material, for example a signed certificate, is meant. The issuer is able to provide a revocation list service or similar mechanisms, where the validity of the credentials can be verified.

ID	R-FUNC-SP-ISSUER-02
Title	Disclosure of attributes at issuance
Area	Issuer
Type	Functional
Cluster	Services
Contradicts	-
Description	Issuers MUST be able to define which attributes they need to verify
Motivation	Depending on the scenario, issuers may be willing to sign certain user attributes (e.g., revocation handles or key material) without seeing the data in the plain, while other information (e.g., name, date of birth) may be required and validated before signing the attributes. The issuer must be able to define this policy upon issuance.
Acceptance Criteria	1. The issuer is able to define a policy containing the data fields to be revealed. 2. In case of non-conformity, i.e., if the requested data fields are not revealed, the issuance protocol fails.
Comments	

ID	R-FUNC-SP-ISSUER-03
Title	Issuer registration
Area	Issuer
Type	Functional
Cluster	Services
Contradicts	-
Description	Issuers SHOULD be able to register themselves at the CREDENTIAL Wallet.
Motivation	If the CREDENTIAL Wallet maintains and offers a list of issuers, an issuer must be able to join this list.
Acceptance Criteria	1. The issuer is able to register itself at the CREDENTIAL Wallet. 2. After registration, the issuer is listed in the issuer index.
Comments	

ID	R-FUNC-SP-ISSUER-04
Title	Issuer key update and revocation
Area	Issuer
Type	Functional
Cluster	Services
Contradicts	-
Description	Issuers SHOULD be able to update and revoke their registration information.
Motivation	If the CREDENTIAL Wallet maintains and offers a list of issuers, issuers need to be able to update their information (e.g., public key material). Furthermore, they shall be able to revoke their keys (thereby invalidating all issued credentials) in case their secret issuance keys are found to be compromised.
Acceptance Criteria	1. The issuer is able to update its registration information 2. After revocation, the issuer's key is no longer listed in the issuer index. As a consequence, no SP will accept certificates issued under this key any longer.
Comments	

ID	R-FUNC-SP-ISSUER-05
Title	Adding expiration dates to credentials
Area	Issuer
Type	Functional
Cluster	Services
Contradicts	-
Description	Issuers MAY be able to encode expiration dates into credentials.
Motivation	In many situations, certificates automatically expire after a predefined time period, e.g., ten years in case of passports. The issuer may thus be able to also define such expiration periods into electronic certificates.
Acceptance Criteria	1. At issuance, the issuer can define an expiration date for a credential. 2. The user is not able to perform a valid presentation of the credential after the defined expiration date.
Comments	If this feature is not supported, the issuer can alternatively keep state of all issued credentials locally. When a credential expired, it can then revoke it.

	However, the typically needed revocation information (e.g., blacklist of all revoked credentials) would be smaller if expiration dates are supported.

6 Conclusion

This document describes the Cloud Identity Wallet requirements. These requirements are necessary to develop its architecture and to define the scope of the Cloud Identity Wallet. The requirements covering the authentication of users and services, secure data re-encryption, data authenticity and data exchange of the CREDENTIAL Wallet. The strength of the CREDENTIAL Wallet is gained by providing a cloud based storage solution for personal and identity data. The CREDENTIAL Wallet will provide innovative cloud-based services for storing, managing and sharing digital identity information and other critical personal data.

This document describes the functional, legal, organizational and technical requirements of the CREDENTIAL Wallet. These requirements are elicited by analysing the pre-defined use cases and storyboards. Cryptographic mechanisms involving key components such as user, CREDENTIAL Wallet, and data receiver provide a solution for a secure storage of personal data which complies with the state-of-the-art end-user and business user needs. Security is guaranteed by the user and service authentication, the authenticity, exchange and recovery of data, the secure data re-encryption and the exchange and recovery of keys. The document points out the generic CREDENTIAL Wallet requirements which are divided into the granting access rights, the authentication, the administration, the account management, the data sharing, the services and the generic cluster.

CREDENTIAL App and external service provider requirements play also important roles within the CREDENTIAL Wallet. For those requirements, it is important to implement registration forms, an authentication page, the possibility of providing the username and the registration with fingerprints. For the external service provider, the requirements are described in the document. The document also includes the administration needs and functionalities, the account management and the services within the CREDENTIAL wallet.

The user part is described in the document. It takes into consideration the experience of the industrial partners offering secure cloud provider solutions in a production environment. A verification for all requirements will be realized in upcoming development tasks of the CREDENTIAL Wallet project. This guarantees that only the developed functionality from this work package will be tested. In addition to the results of this document, a knowledge database which stores all those requirements has been established. The storage will allow one to keep track about the change process of requirements and how they affect the resulting software architecture, implementation and operation of the Cloud Identity Wallet. Applications like eBusiness, eCommerce and eHealth will benefit from the security and functionality of the CREDENTIAL Wallet.

References

[1] - CREDENTIAL - D2.1 Scenarios and use cases document. Editor: Florian Thiemer (Fokus). 2016.
[2] - CREDENTIAL - D5.1 CREDENTIAL Functional Design. Editor: Nicolas Notario McDonnell (Atos). 2017.
[3] - RFC keywords for requirements: https://www.ietf.org/rfc/rfc2119.txt
[4] - D. Pandey, U. Suman, and A.K. Ramani. "An Effective Requirement Engineering Process Model for Software Development and Requirements", in Management 2010 International Conference on Advances in Recent Technologies in Communication and Computing. pp. 288-291.
[5] - J. Siddiqi, "Requirement Engineering: The Emerging Wisdom", in IEEE Software, 1996, pp.15- 19.
[6] - Sommerville, Ian. Software Engineering" (9th ed.). Addison-Wesley.2009.