Digital Security: Cybersecurity, Privacy and Trust
DS-02-2014 Access Control

European Commission | Horizon 2020 European Union funding for Research & Innovation

From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control

WP2 – Requirements, Business Cases and Architecture

Deliverable D2.6 "Business and Technical Requirements (revised)"

Editor(s):	Charalambos Chrysostomou (CUT), Antonis Hatzikonstantinou (EXUS)
Author(s):	Savvas Zannettou (CUT), Michael Sirivianos (CUT), Georgios Fakas (CUT), Dimitris Katsaros (EXUS), Evangelos Kotsifakos (WEDIA)
Dissemination Level:	Public
Nature:	Report
Version:	1.7

ReCRED Project Profile

Contract Number	653417
Acronym	ReCRED
Title	From Real-world Identities to Privacy-preserving and Attribute-based CREDentials for Device-centric Access Control
Start Date	May 1st, 2015
Duration	36 Months

Partners

University of Piraeus	University of Piraeus research center	Greece
Telefónica Investigación y Desarrollo	Telefonica Investigacion Y Desarrollo Sa	Spain
verizon	Verizon Nederland B.V.	The Netherlands
certSIGN BY UTI	Certsign SA	Romania
wedia	Wedia Limited	Greece
EXUS	EXUS Software Ltd	U.K.
upcom Bringing business and IT together	Upcom Bvba (sme)	Belgium
The Productizers	De Productizers B.V.	The Netherlands
	Cyprus University of Technology	Cyprus
	Universidad Carlos III de Madrid	Spain
cnit	Consorzio Nazionale Interuniversitario per le Telecomunicazioni	Italy
Baker & McKenzie	Studio Professionale Associato a Baker & Mckenzie	Italy

Document History

Version	Date	Author	Remarks
0.1	21.6.2016	Antonis Hatzikonstantinou (EXUS)	
0.2-0.4	01/10/2016	Charalambos Chrysostomou (CUT)	Restructuring
0.5-0.6	31/10/2016	Charalambos Chrysostomou (CUT)	User Stories
0.6-09	04/11/2016	Charalambos Chrysostomou, Savvas Zannettou (CUT)	
0.9-1.5	10/11/2016	ReCRED Consortium	Document restructuring
1.6	15/11/2016	Charalambos Chrysostomou, Savvas Zannettou (CUT)	Minor Corrections
1.7	26/07/2017	Spyros Evangelatos (EXUS)	Revised version as per PO’s comments and suggestions

Executive Summary

Deliverable 2.6 “Business and Technical Requirements (revised)” is a revision of Deliverable 2.2. It includes a refined list of a) scenarios grouped by use case, and b) technical user requirements.

The user stories are the natural next step in the use case based requirements engineering methodology that ReCRED has opted for. User stories transform the use cases that were described in D2.1 into first person narrative stories that essentially provide another level of detail, addressing each user role individually and from a first person perspective. The user stories are more detailed since they do not provide the generic narrative of the use cases but take each requirement of every role and describe it in a format that is technically agnostic. The approach has the benefit of producing accurate technical requirements without taking into consideration the limitations imposed by the technology at hand. The user stories are a detailed description of what all users expect from the platform.

This document relies on the user stories in order to produce a list of specific technical requirements. The requirements are classified according to the six components and services that will together form the ReCRED platform. These are:

1. User Device
2. Identity consolidator
3. Service Providers
4. Behavioural Authentication Authorities
5. Identity Providers
6. Privacy Preserving Access Control

The requirements description for each component is then subdivided into Functional Requirements, Security & Privacy Requirements and Operational Requirements.

The document begins with a short introduction to the current stage of the requirements engineering methodology within ReCRED (see Section 1). Subsequently, Sections 2-9 include the scenarios for every use case subdivided into the specific scenarios, Section 10 contains the usability requirements, Section 11 lists all the technical user requirements per major architectural component of the ReCRED platform and Section 12 gives a conclusion for the entire document.

Table of Contents

List of Figures

1. Introduction

1.1. User Stories Methodology

The User Stories Methodology follows the requirements engineering methodology that was adapted for ReCRED and was initially described in D2.1 and D2.5 Business Cases deliverables. D2.2 and now D2.6 continues with the process of requirements elicitation by gradually transforming the user scenarios into user stories. The approach follows the traditional route Requirements Elicitation → Requirements Analysis → Requirements Specification → Requirements Validation. D2.2 and D2.6 covers the second and third stages of the process.

According to William C. Wake author of "Extreme Programming Explored[1,2] good user stories should follow the INVEST acronym:

- **I**ndependent: User stories need to overlap as little as possible in order to be able to be independently implementable
- **N**egotiable: User stories need to be flexible in order to allow for small customisations that will be decided upon between the user and implementer
- **V**aluable: Every user story needs to have a certain value to the end user and a lack thereof would essentially mean that some of the user needs are not met
- **E**stimable: User stories need to be understandable to both customers and implementers at a level such that a fairly good estimation of effort and scheduling can be agreed upon by both parties
- **S**mall: User stories need not be massively complex or large. Good user stories should be equivalent to a few person-weeks of work.
- **T**estable: The user stories need to be easily testable in order to provide a validation mechanism for requirements.

User stories for ReCRED are written based on these ground rules. Based on the user scenarios and user stories, a set of technical requirements is then provided. Those are categorized according to the six envisaged main architectural components of the ReCRED platform and then subdivided to three major categories: Functional requirements, Security and Privacy Requirements and Operational Requirements.

1.2. User Story template

To provide a structured User Story description, a template is defined as follows:

Code Number	**Coded Identification of every user story**
Title	**User story title**
Description	User story text in the following format **As a** … **I want to** … **so that …**
Acceptance Criteria	Criteria based upon which the successful implementation of the user story will be established - Criterion 1

[1] William C. Wake, "Extreme Programming Explored", 804-934-8194, 2000
[2] http://xp123.com/articles/invest-in-good-stories-and-smart-tasks/

	- Criterion 2 . . . - Criterion n

2. Horizontal Use Cases

In order to cover for parts of the ReCRED functionality that are not described in the domain-specific scenarios, the consortium has decided that it would be suitable to list a set of use cases that involve the basic actions within the ReCRED platform that are horizontal to all vertical use cases.

2.1. Horizontal Use Case A – User interactions with Identity Consolidator service

This section presents user stories for user interactions with the Identity Consolidator service use case. The purpose of this use case is to demonstrate how end users interact with the various components of the architecture and how they can use the Identity Consolidator to manage and control their identity attributes and online identity accounts.

2.1.1. Scenario 1: "Registration to Identity Consolidator service" Use case

Code Number	**H_RCS_1**
Title	**Registration to the Identity Consolidator**
Description	**As a** user **I want to** be able to easily create an account to the ReCRED's Identity Consolidator **so that** I can bind my online accounts, my physical identity, issue credentials etc.
Acceptance Criteria	1. The Identity Consolidator must check that the user that wants to register is unique and there is no registered user with the same personal information. 2. The service must verify that an email confirmation has been sent to the email address that the user declared. 3. The service must verify that all the declared identity information of the included passport and user's photos are valid.

Code Number	**H_RCS_2**
Title	**Delete my account from the ID consolidation service**
Description	**As a** user **I want to** be able to easily delete my account from the ReCRED's ID consolidation service **So that** I do not have to worry about the privacy of my personal identity information when I will stop using the platform.
Acceptance Criteria	1. The Identity Consolidator must verify that the user who requests the deletion is the holder of the account. 2. The service must verify that all the personal identity information of the user (such as identity attributes, cryptographic credentials, etc.) has been successfully deleted from the ReCRED platform. 3. The service should allow the user to create an account after the deletion when he desires so.

Code Number	**H_RCS_3**
Title	**Verify my age**
Description	**As a** user

	I want to be able to easily declare and verify my age to the Identity Consolidator **So that** I can prove to other users or service providers that I am over a particular age (e.g., over 18 years old).
Acceptance Criteria	1. The Identity Consolidator must request from the user to upload a photo of his identity (or a similar document) and crop the region where his date of birth is shown. 2. The service must verify that the declared date of birth matches the information that is shown on the cropped region using optical character recognition (OCR). 3. The service should assign audits (whether the declared date of birth matches the information on the uploaded cropped region) to randomly selected users. This procedure should be as privacy-preserving as possible and should only reveal minimal information to auditors about the identity of the user to be audited. 4. The service should be able to calculate a confidence score about the age of the user and store it to the Identity Consolidation Service.

Code Number	**H_RCS_4**
Title	**Prove the ownership of an online account**
Description	**As a** user, **I want to** be able to prove to the consolidator the ownership of an online account **so that** I consolidate all my online accounts under a single profile.
Acceptance Criteria	1. The Identity Consolidator should request from the user to connect to the online account that he wants to verify. 2. The Identity Consolidator should be able to create a proof of account ownership to the user for his verified account. This proof will be transferred to the user device and can be used in the future by the user in order to prove that he is the owner of the account to 3rd Parties.

2.1.2. Scenario 2: "Issuing cryptographic credentials to the mobile device" Use case

Code Number	**H_CCM_1**
Title	**Prove that I am a student**
Description	**As a** user **I want to** be able to prove to the Identity Consolidator that I am a student **So that** I can prove to a service provider that I am a student.
Acceptance Criteria	1. The Identity Consolidator should request from the user to provide a photo of his student card. 2. The Identity Consolidator should be able to verify that the student card is valid and it should also collect the expiration date from the photo. 3. After the verification of the identity attribute (that the user is a student until the expiration date), the Identity Consolidator should be able to store these identity attributes to the user's account.

Code Number	**H_CCM_2**
Title	**Issue cryptographic credential to mobile device from Identity Consolidator**
Description	**As a** user **I want to** be able to issue cryptographic credential directly to my mobile device from the Identity Consolidator **So that** I can use it to access service provider that require to provide a particular identity attribute (e.g., that the user is from the UK)
Acceptance Criteria	1. The Identity Consolidator should be able to verify that the cryptographic credential has been issued and sent to the mobile device of the user. 2. The cryptographic credentials should be stored securely to the mobile device of the user. 3. The Identity Consolidator should only maintain a back-up of the credential if the user desires. In all other cases the Identity Consolidator should make sure that the issued credential has been deleted from the Identity Consolidator.

Code Number	**H_CCM_3**
Title	**Prove to a service provider that you are a student**
Description	**As a** user **I want to** be able to use the cryptographic credentials to the mobile devices of the user **So that** I can prove to a service provider that I am student.
Acceptance Criteria	1. The cryptographic credential must be used as a proof that you are a student and get access to the service. 2. The user is able to prove to the service that he is a student without revealing any other identity information. 3. The credential must be presented securely from the device to the service provider.

Code Number	**H_CCM_4**
Title	**Issue cryptographic credential to a user's mobile device from Identity Provider**
Description	**As an employee** of the university's student services **I want to** be able to issue cryptographic credentials to the mobile devices of the user **so that** the user can prove to a service provider that he is a student.
Acceptance Criteria	1. The cryptographic credential must be issued and stored only to the device of the user. 2. The cryptographic credential must be securely stored to the user's device.

Code Number	**H_CCM_5**
Title	**Grant access only to students**
Description	**As a** service provider administrator **I want to** be able to be presented with cryptographic credentials from the users **so that** I can verify that they are students and grant them access.
Acceptance Criteria	1. The service provider can receive and decrypt the cryptographic credentials and verify that the user is a student. 2. The service provider must store the verified user so he does not have to prove every time that he is a student. 3. If the user does not want to share any personal information with the service provider or he doesn't have any credential that he is a student, he must not be granted access.

2.2. Horizontal Use Case B – Identity Consolidator interactions with ID providers

2.2.1. Scenario 1: "Proving the ownership of an online account" Use case

Code Number	**H_PO_1**
Title	**Manage identity attributes from the Identity Consolidator**
Description	**As a** user **I want to** be able to manage my identity attributes from the Identity Consolidator **so that** I can have a global view of what the Identity Consolidator and ID Providers know about my identity and also perform various operations with my identity attributes
Acceptance Criteria	1. The Identity Consolidator should present to the user an interface that will depicts the identity attributes and which entity (ID provider or Identity Consolidator) have it. 2. The user should be able to perform various operations on his identity attributes such as transfer them across entities, delete them from the Identity Consolidator if stored, etc.

Code Number	**H_PO_2**
Title	**Verify multiple online accounts to Identity Consolidator**
Description	**As a** user **I want to** be able to easily prove the ownership of an account to the ReCRED identity consolidation service **so that** I can prove to other users or services the ownership of the account
Acceptance Criteria	1. The Identity Consolidator must establish an OpenID Connect/OAuth connection with the identity provider that maintains the user account. 2. The service must verify that all the declared identity information of the user matches the information obtained from the online account of the user. 3. The Identity Consolidator should be able to generate a proof of ownership of the account the user has verified.

Code Number	**H_PO_3**
Title	**Transfer reputation among online accounts using the Identity Consolidator**
Description	**As a** user **I want to** be able to transfer identity information (e.g., sales reputation) among online accounts **So that** I can update the information of my accounts faster and securely.
Acceptance Criteria	1. The Identity Consolidator must establish an OpenID Connect/OAuth connection with the service that the user wants to obtain from, or transfer to, the identity information. 2. Verify that the identity information has been transferred or obtained successfully.

Code Number	**H_PO_4**
Title	**Transfer identity attribute (e.g., student) from Identity provider (university) to the Identity Consolidator**
Description	**As a user** **I want to** be able to initiate an OpenID Connect/OAuth transfer of attributes from the university to the Identity Consolidator **So that** I can enrich my Identity Consolidator account with additional identity attributes
Acceptance Criteria	1. Verify that an OpenID Connect/OAuth connection has been initiated between the university (ID provider) and the Identity Consolidator (acts as Relying Party) and that the identity attributes of the user has been successfully transferred to the Identity Consolidator.

2.3. Horizontal Use Case C –Second-factor authentication using behavioral profiles

This section presents user stories for the second-factor authentication using behavioral profiles use case. The purpose of this use case is to demonstrate how behavioral profiles can be used as second-factor authentication, either for security or recovery reasons.

2.3.1. Scenario 1: "Two-factor authentication in online banking" use case

Code Number	**H_TFA_1**
Title	**Fast and secure access to an online bank account**
Description	**As a user** **I want to** be able to easily and securely access my bank account from my mobile device **So that** I don't have to remember passwords and at the same time not have to worry

	about my security and privacy.
Acceptance Criteria	1. The device must request from the user a local device authentication using biometrics and verify that is valid. 2. The ReCRED daemon must ensure the secure transfer of the cryptographic authentication data token for the FIDO remote authentication along with an optional ABAC credential to the online banking service for the device-to-service authentication.

Code Number	**H_TFA_2**
Title	**Perform FIDO remote authentication**
Description	**As an online banking service provider** **I want to** be able to perform FIDO remote authentication **So that** I can verify and grant access to users.
Acceptance Criteria	1. The ReCRED daemon receives the FIDO authentication data token and performs the authentication. 2. The ReCRED daemon must ensure that the FIDO authentication is successful before requesting any second-factor authentication.

Code Number	**H_TFA_3**
Title	**Request second-factor authentication**
Description	**As an online banking service provider** **I want to** be able to request a second-factor authentication from the user **So that** I can secure access to my accounts.
Acceptance Criteria	1. When requesting a second-factor authentication, the ReCRED daemon must ensure that it receives an authorization key and a unique identifier for the device of the user. 2. The ReCRED daemon contacts the Identity Consolidator through an OpenID Connect/OAuth connection and decides which of the available second-factor authentications it wants to perform. 3. If there is no second-factor authentication available then the bank can stop the authentication procedure and refrain from granting access to the user.

Code Number	**H_TFA_4**
Title	**Perform behavioral profile verification**
Description	**As a** service provider **I want to** be able to request a second-factor authentication from the user **So that** I can increase the security and prevent malicious attacks.
Acceptance Criteria	1. The Service Provider contacts the Identity Consolidator to get the information of the Behavioral Authentication Authority that will be responsible to undertake the behavioral authentication. 2. The behavioral authentication authority must verify that the user has the same behavior as usual (according to the stored behavioral profiles). 3. After the verification has been completed the behavioral authentication authority has to report to the Service Provider the result of the behavioral authentication.

Code Number	**H_TFA_5**
Title	**Activate/De-activate Account Locks**
Description	**As the Identity Consolidator** **I want to** be able to lock a user's account **So that** I can prevent unwanted access in case of failed authentication.
Acceptance Criteria	1. The behavioral authentication authority should inform the Identity Consolidator regarding failed authentication attempts 2. The Identity Consolidator, after receiving multiple authentication failures for a particular user from the behavioral authentication authorities should be able to perform account locks.

	3. The account locks/unlocks will be performed by using a Latch-like software that will run on the Identity Consolidator.

2.4. Horizontal Use Case D – Privacy and consent management

This section presents the user stories for the use case where users determining the degree of their desired privacy. The purpose of this use case is to demonstrate how the identity management service of the ReCRED platform empowers users to control what attributes of their identity each identity provider and service provider knows.

2.4.1. Scenario 1: "Maintaining different degrees of privacy against the Identity Consolidator" use case

Code Number	**H_DDP_1**
Title	**Maintain the least degree of privacy**
Description	**As a user** **I want to** be able to maintain the degree of privacy against the Identity Consolidator **so that** I can choose to fully trust the Identity Consolidator
Acceptance Criteria	1. The Identity Consolidator cannot be compromised and it won't misuse the user's personal information. 2. The Identity Consolidator holds the cryptographic credentials of the user in plain text and knows all his consolidated attributes. 3. Verify that the failure recovery is easy and it offers highly usable authentication to service providers. 4. Verify that as soon as the user has access to the Identity Consolidator can recover his credential in any device.

Code Number	**H_DDP_2**
Title	**Maintain the highest degree of privacy**
Description	**As a** user **I want to** be able to choose the degree of privacy against the Identity Consolidator **so that** I can choose the highest degree of privacy against the Identity Consolidator
Acceptance Criteria	1. The Identity Consolidator holds the credentials of the user encrypted, and the master key is maintained by the user. 2. Verify that the Identity Consolidator service does not store any identity attributes. 3. Verify that the authentication process happens cryptographically through the mobile device. 4. The consolidator does not have the ability to see what the identity attributes of the user are. 5. Verify that the Identity Consolidator knows where the ID providers of the user are and what types of identity attributes the user has proven to each ID provider.

2.4.2. Scenario 2: "Privacy management with respect to which ID attributes are known to verifiers" use case

Code Number	**H_PMA_1**
Title	**Track what Service Providers know about me**
Description	**As a user** **I want to** track at any time what Service Providers know about me by using the identity management application within the Identity Consolidator **so that** I can preserve my privacy
Acceptance Criteria	1. The ReCRED identity management application and the Identity Consolidator must have the user's authorization to access his service provider. 2. The application should be able to initiate an OpenID Connect/OAuth connection with the Service Providers of the user. 3. The identity management application should be able to track which Service

	Providers know an attribute of the user's identity that he will specify. 4. The application should be able to tell to the user what identity attributes are maintained by a particular Service Provider.

Code Number	**H_PMA_2**
Title	**Receive privacy risk indicators**
Description	**As a user** **I want to** get privacy risk indicators from the ReCRED's identity management application **so that** I can get the appropriate measures to protect my privacy
Acceptance Criteria	1. The identity management application should be able to present the user with privacy risk indicators that define the risk of involuntary de-anonymization. 2. The identity management application should be able to present the user with privacy risk indicators that define the identity attribute inference by Service Providers that the user has not explicitly shown a specific attribute. 3. The user should have the option to enable or disable this functionality.

2.4.3. Scenario 3: "Privacy and consent management with respect to which ID attributes are known to ID providers and the consolidator" use case

Code Number	**H_PCM_1**
Title	**Track what identity attributes each ID provider knows**
Description	**As a** user **I want to** be able to track what identity attributes each of my ID providers know **so that** I take measures to preserve my privacy and prevent unwanted disclosure of my identity information
Acceptance Criteria	1. The user should provide authorization to the identity management application to access the ID providers that he wants to track. 2. The identity management application should be able to inform the user at any time what identity attributes, an ID provider that he specifies, know. 3. The application can learn this information from the Identity Consolidator, who has acquired the identity attributes of the user from the ID providers, using OpenID Connect/ OAuth 4. The application should be able to contact directly an ID provider and learn what Identity attributes are maintained about the user.

Code Number	**H_PCM_2**
Title	**Transfer identity attributes between ID providers**
Description	**As a** user **I want to** be able to transfer identity attributes between ID providers **so that** I can save time and don't have to verify the same identity attribute to all my ID providers separately
Acceptance Criteria	1. The identity management application should be able to establish OpenID Connection/OAuth connections with the identity consolidator and the ID providers. 2. The user should be able to transfer identity attributes to ID providers through the Identity Consolidator. 3. The user should be able to transfer identity attributes by directly copying the identity information from one ID provider to the other.

Code Number	**H_PCM_3**
Title	**Issue requests for identity attributes deletion from ID providers**
Description	**As a** user **I want to** be able to issue requests for identity attributes deletion from ID providers

	So that I can ensure that a particular ID provider does not know my identity attributes
Acceptance Criteria	1. The user can issue requests for identity attributes deletion using the identity management application. 2. Verify that the issued requests are obeyed by both the Identity Consolidator and the ID providers. 3. The user has the ability to request the deletion of a specific identity attribute from a specific identity provider. 4. The user has the ability to request the deletion of specific identity attributes from the Identity Consolidator. 5. The user has the ability to request the deletion of specific or multiple identity attributes from a set of ID providers.

2.4.4. Scenario 4: "Privacy and consent management with respect to deletion of account from ID Providers

Code Number	**H_PCD_1**
Title	**Issue requests for account deletion from ID providers**
Description	**As a** user **I want to** be able to issue requests for account deletion from ID providers **So that** I maintain the privacy of my personal identity information when I will stop using the Identity Provider's services.
Acceptance Criteria	1. The Identity Consolidator must verify that the user who requests the deletion is the holder of the account. 2. The service must verify that all the personal identity information of the user has been successfully deleted from the selected Identity Providers.

2.5. Horizontal Use case E - Mobile Device Data Protection

This section describes user stories for use case of Mobile Device data protection. Three scenarios are considered:

- Stolen Mobile Phone
- Misused Mobile Phone
- Damaged or lost Mobile Phone

2.5.1. Scenario 1: "Stolen Mobile Phone"

Code Number	**MMDP_SMP_1**
Title	**Check accounts**
Description	**As a** user **I want to** have access to some webpage with information of my accounts **So that** I can check what is the status them
Acceptance Criteria	1. The user can access a webpage with information about his accounts. 2. The user sees which accounts are enabled, which are disabled. 3. The login to the webpage is secure.

Code Number	**MMDP_SMP_2**
Title	**Latch/unlatch accounts**
Description	**As a** user **I want to** switch on and off the latch on my accounts **So that** I have full control of my accounts.
Acceptance Criteria	1. The user can securely login to a webpage with info about his accounts. 2. The user can switch services protection on an off.

	3. The user can latch off (unlock) all services at once.

Code Number	**MMDP_SMP_3**
Title	**History of latch changes**
Description	**As a** user **I want to** have a place to see history of all accounts latched on and off **So that** I know if some suspicious behavior happened.
Acceptance Criteria	1. The user can access a history of accounts latched off and on. 2. The user can see where and when such changes happened.

Code Number	**MMDP_SMP_4**
Title	**Behavioral Authentication failure information**
Description	**As a** user **I want to** know when and where an authentication failure happened and which modality caused such failure **So that** I can have better understanding on when and where someone tried to compromise my mobile phone.
Acceptance Criteria	1. The user can see a history of behavioral authentication failures. 2. Each failure is described by place, time and modality/modalities that caused the behavioral authentication failure.

Code Number	**MMDP_SMP_5**
Title	**Behavioral Authentication modalities selection**
Description	**As a** user **I want to** select which authentication modalities to use to authenticate me to my services **So that** I can avoid those that don't work well for me or those I don't trust or those I don't want to use.
Acceptance Criteria	1. User can see which behavioral authentication modalities can be used for the authentication process of a particular service. 2. User can switch on/off behavioral authentication modalities (e.g. typing patterns ON, local phone mobility patterns ON, remote mobility authentication OFF) 3. User can see which modalities are supported by his mobile phone, which are supported by his Behavioral Authentication Authorities (e.g., Telcos)

Code Number	**MMDP_SMP_6**
Title	**Authentication failure or Latch off information**
Description	**As a** user **I want to** be notified about authentication failures of latch off events **So that** I know that those events happened.
Acceptance Criteria	1. After authentication failure or latch off event a user receives a text message or e-mail.

Code Number	**MMDP_SMP_7**
Title	**Communication channel selection**
Description	**As a** user **I want to** have the option to select which communication channel the ReCRED Authentication will use to inform me about any events **So that** I can be sure that such important information reaches me.

Acceptance Criteria	1. User can select a mobile phone number(s) and e-mail(s) which will be used to communicate important ReCRED events.

2.5.2. Scenario 2: "Misused Mobile Phone"

For this scenario, all previous user stories apply too. In addition, requirements about fast service logoff apply.

Code Number	**MMDP_MMP_1**
Title	**Immediate Latch off**
Description	**As a** user **I want to** be sure that even when my mobile phone is unlocked, my accounts will be blocked when someone else is operating my mobile phone **So that** my accounts are safe.
Acceptance Criteria	1. Demonstrate accounts latch off when service in use. 2. Demonstrate that non-registered accounts are not affected. For example, that user's GPS navigation still works when his friend during driving enters new destination, but his e-banking is latched-off.

2.5.3. Scenario 3: "Damaged or lost Mobile Phone"

Code Number	**MMDP_LMP_1**
Title	**Multiple devices use-case**
Description	**As a** user **I want to** have the possibility to use two mobile devices with one ReCRED account **So that** I'm not limited in case I lost or damaged one of the phones.
Acceptance Criteria	1. The user can access services from more mobile devices and those are independent. 2. A service can recognize type/kind of a mobile device and adjust the authentication procedure according to the particular type. 3. If one of the devices is damaged, all the services must be accessible from the other authorized device.

Code Number	**MMDP_LMP_2**
Title	**Damaged device does not give away any ReCRED-related credentials**
Description	**As a** user **I want to** be sure that during repair of my mobile device nobody in the service shop can access my ReCRED credentials **So that** I can trust the whole ReCRED principle.
Acceptance Criteria	1. Demonstrate and verify that all ReCRED related credentials are secured by the TEE of the mobile phone, so that even direct access to the mobile phone's hardware cannot compromise the credentials.

Code Number	**MMDP_LMP_3**
Title	**ReCRED installation**
Description	**As a** user **I want to** easily install all ReCRED-related software components to my mobile phone **so that** I don't waste my time and have immediately access to all my services
Acceptance Criteria	1. There exists a clear and easy way to install ReCRED-related software to a new mobile phone. 2. The user's credentials are available only through a secured webpage. 3. There exists a bypassing way to authenticate to a mobile phone during the installation of ReCRED software. 4. Behavioral device-to-service authentication will work immediately after installation if there were previously collected samples of user's behavior (for

	example from a different mobile phone). If user is new to ReCRED, there will be a learning period during which the user's behavior will be collected and analyzed. 5. The user will be informed (on a webpage, his ReCRED profile) which device-to-service authentication mechanisms are in their learning phase and are not working yet. 6. In case of different mobile device type, such change is registered and related behavioral signatures are collected again, and the old ones are invalidated.

Code Number	**MMDP_LMP_4**
Title	**ReCRED backup service**
Description	**As a** user **I want to** configure again access to all my services in case I lost my mobile phone **So that** the re-installation process is simpler and I'm not lost in all configurations.
Acceptance Criteria	1. The user's device-to-service mappings will be stored in the ReCRED credential management server (the Identity Consolidator) so that the user does not have to setup particular services one by one when he loses his mobile phone.

3. Use case A – Support to Financial Services

This section describes user stories for use case on Financial Services. Two scenarios are considered:

- Loan Origination Application
- Online banking

3.1. Scenario 1: "Loan Origination Application"

Code Number	**FS_LA_1**
Title	**Proof of Specified Attributes**
Description	**As an** applicant **I want to** provide proof of only the credentials that the application form requests for **so that** I don't give away information that the lender does need to process the application
Acceptance Criteria	1. Fewer requests for additional paperwork to verify ones identity. Companies tend to resort to paperwork if online checks fail or insufficient information is available from Credit Reference Agencies (CRAs) and Fraud Prevention Agencies (FPAs). 2. Replace altogether some of the requested paperwork to be sent by an online query at the ReCRED service 3. Match specific identity attributes to specific DCA-enabled identity proof services.

Code Number	**FS_LA_2**
Title	**Increased speed of attribute checking and response**
Description	**As an** applicant **I want to** get a faster response on my application **so that** crediting of the loaned amount on my bank account takes place faster
Acceptance Criteria	1. Reduce current processing time when compared to industry standards for cases where online credit and identity check is not sufficient and additional documentation is required. 2. Replace the documentation verification via document checking with the ReCRED service for proof of identity

Code Number	**FS_LA_3**
Title	**Control over provided personal information**
Description	**As an** applicant **I want to** be sure that my data is used only for the verification of my credit history and not for any other purpose **so that** I am confident that my personal data and proof of credentials is not mis-used by third parties
Acceptance Criteria	1. Make sure that the interaction with the ReCRED service has minimal (if at all) data exchange with the loan provider other than the request for proof of identity 2. Make sure that the user provides proof of identity once and only to the ReCRED service 3. Provide the necessary legal framework for the data protection to take place.

Code Number	**FS_LA_4**
Title	**Ubiquity and mobility in ability to prove specific attributes**
Description	**As an** applicant **I want to** be able to apply for a loan anywhere and from my mobile device **so that** I don't have to retrieve various proof of identity documents, employment status, annual income, permanent address etc.
Acceptance Criteria	1. For the cases where additional documentation is required by the loan provider these will gradually fade out and a query to the ReCRED service will replace the need for additional documentation to be sent by the applicant, allowing an application process to be completed from a mobile phone

Code Number	**FS_LA_5**
Title	**Reduce average time of response to loan application**
Description	**As a** microloan advisor **I want to** be able to respond to applicants quickly **so that** I can process more applications
Acceptance Criteria	1. Replace some of the requested paperwork to be sent, by an online query at the RECRED service 2. Considerably reduce the time required for an entire application to be filed, especially for the cases where additional documents are required for the proof of specific attributes

Code Number	**FS_LA_6**
Title	**Reliability of Identity Verification Mechanisms**
Description	**As a** microloan advisor **I want to** make sure that verification services are reliable and up to date **so that** I can provide accurate credential verification and reduce my risk
Acceptance Criteria	1. If we are to replace some of the manual verification cases where online credentials are not sufficient then the loan providers need to be sure about the credibility and reliability of the verification mechanism 2. Transparent, reliable and robust verification process with very low error probability especially for all DCA related functionality.

Code Number	**FS_LA_7**
Title	**Verification of legitimate mobile phone owner**
Description	**As a** microloan advisor **I want to** be make sure that my mobile customers are the legitimate owners of the phone **so that** I can prevent identity theft and fraud

Acceptance Criteria	1. Robust and reliable DCA mechanism (human-to-device) with very low error probability 2. Robust and reliable DCA mechanism (device-to-service) with very low error probability

Code Number	**FS_LA_8**
Title	**Reduce amount of information required in the application form**
Description	**As a** microloan advisor **I want to** reduce the amount of information that my customers provide on the online loan application form **so that** I can make the process easier for my customers
Acceptance Criteria	1. The ReCRED authentication mechanism replaces some of the text fields in the application forms 2. The ReCRED authentication mechanism replaces some of the queries to the FPA and CRA agencies.

3.2. Scenario 2: "Online Credit Card Purchase"

Code Number	**FS_CC_1**
Title	**Online credit card purchase using additional biometric authentication**
Description	**As an** applicant **I want to** be biometrically authenticated when using my credit card for online purchases **So that** a thief that has stolen my credit card will definitely not be able to use it online.
Acceptance Criteria	1. The Credit Card authentication service asks for additional biometric authentication. 2. The credit card owner must authenticate to the mobile device which will then exchange crypto keys with the online service to confirm the biometric authentication 3. The online Credit Card service will reject all attempts to execute a transaction if the biometric authentication fails.

Code Number	**FS_CC_2**
Title	**Online credit card purchase using additional behavioral authentication**
Description	**As an** applicant **I want to** be behaviorally authenticated when using my credit card for online purchases **So that** the thief that has stolen my credit card will not be able to use it online because of behavioral authentication failure.
Acceptance Criteria	1. The Credit Card authentication service should ask for additional behavioral authentication. 2. The Behavioral Authentication Authority communicates with the service provider and confirms the credit card owner's identity. 3. The online Credit Card service will reject all attempts to execute a transaction if the Behavioral Authentication Authority indicates that the credit card user is not the credit card owner.

3.3. Scenario 3: "Online Banking and Mobile Payments"

Code Number	**FS_OB_1**
Title	**Quick and robust connection to e-banking services**
Description	**As an** online banking user **I want to** have one simple way of connecting to all my e-banking accounts

	So that I can quickly and easily connect and perform transactions from my various e-banking accounts without the possibility to lock myself out.
Acceptance Criteria	1. Login to different e-banking accounts without the need to provide extra passwords to each one. At most using a short and easy to remember pin. 2. No need for the user to change a hard to generate and hard to remember password for every e-banking account very often.

Code Number	**FS_OB_2**
Title	**Secure e-banking accounts**
Description	**As an** online banking user **I want to** have a sophisticated/secure access mechanism for my bank services **so that** I can be confident that my account cannot be easily compromised
Acceptance Criteria	1. No one else can login to user's account from another device, even if he/she can guess the pin. 2. Even if the device is stolen, the thief should not be able to login to user's e-banking accounts.

Code Number	**FS_OB_3**
Title	**Available e-banking services anytime/anywhere**
Description	**As an** online banking user **I want to** be able to easily access my e-banking accounts from another device as well **So that** I can use my e-banking services anytime/anywhere, even if I have not my mobile device with me, or it is stolen or damaged.
Acceptance Criteria	1. User could still use his/hers e-banking services from another device using an extra password or other credential 2. User account is not locked or limited if he/she is logging-in from a different device or location.

Code Number	**FS_OB_4**
Title	**Synchronized user data across different accounts**
Description	**As an** online banking user **I want to** have a centralized profile that I can manage (change personal data) for my banking services **so that** I do not have to access every single e-banking account to change my address, phone, email, job, marital and family status etc.
Acceptance Criteria	1. The user accesses his ReCRED platform profile and edits his personal data. After a short period of time, all of his/hers e-banking accounts have been updated with the new data (if no proof is required). 2. E-banking services "trust" the ReCRED platform and accept profile changes that are requested through the platform. 3. If the bank needs proof for the new data (as in the case of physical address or job status) user should be able to provide related documents online, through the ReCRED platform, without having to send hard copies to every bank. In that case the update of the corresponding e-banking accounts will be done after the bank has accepted the documents.

Code Number	**FS_OB_5**
Title	**Secure centralized ReCRED user profile management**
Description	**As an** online banking user **I want to** have a secure way to access my centralized ReCRED profile **so that** I am confident that no one can access it and change my personal data across my e-banking services or have access to personal documents

Acceptance Criteria	1. The login to ReCRED platform should be secure itself as well, incorporating all the security features that ReCRED platform provides. 2. The documents that the user provides to the platform as a proof for the bank institutes, should have an expiration date and be automatically deleted after that date. Alternatively, these documents could be deleted right after bank institutes have accepted them as a proof of profile data change.

Code Number	**FS_OB_6**
Title	**Trusted ReCRED platform and bank institute connection**
Description	**As a** bank institute management officer **I want to** have a secure connection to the ReCRED platform **so that** I am confident that access to e-banking services and changes to user profile requested by the ReCRED platform are performed only by the certified user/client
Acceptance Criteria	1. Use of specialized secure protocols to connect the ReCRED platform with all the bank institutes 2. Connection/interfaces with the various bank institutes should meet the standards and requirements of each institute. 3. A universal ReCRED interconnection protocol should be defined and accepted by all interested parties.

3.4. Scenario 4: "Automated Teller Machine (ATM) Cash Withdrawals"

Code Number	**FS_AT_1**
Title	**ATM Cash withdrawal**
Description	**As a** ReCRED user **I want to** withdraw cash from an ATM using ReCRED authentication (biometric and/or behavioral) and a one-time authentication key. **So that** I don't have to remember and/or store PIN numbers.
Acceptance Criteria	1. The user authenticates to the device. 2. The user starts the appropriate ReCRED application, selects bank, account and amount. 3. The bank service issues a one-time authentication key i.e. a four digit number, valid only for a limited time. 4. The user enters the authentication key at the ATM, the transaction is approved and the ATM dispenses the money. 5. The bank service will not issue an authentication key if user-to-device authentication fails. 6. The ATM will reject all transaction attempts if authentication key is invalid or has expired.

4. Use case B - Age Verification

This section presents user stories for Age Verification use-case. The purpose of this use case is to demonstrate how service providers and end users can benefit from the ReCRED platform, using the Age Gate product in situations where content is age-restricted.

4.1. Scenario 1: "Age Gate Service" Use Case

Code Number	**AV_AG_1**
Title	**Register website with the ReCRED platform**
Description	**As a** web site owner **I want to** be able to receive age-related information about visitors **so that** I can grant them access to my web site
Acceptance Criteria	1. The website owner may request from the ReCRED platform access to age-related information; the request must contain the exact information

	requested, as well as full identification information for his web site and acceptance of the relevant license agreement 2. A ReCRED operator will assess and grant or deny access to this information and – if approved – enable this information exchange in the platform 3. The ReCRED platform should prohibit unjustified requests from web site owners 4. The exchange of the age-related identity attributes will be performed by using OpenID Connect/OAuth.

Code Number	**AV_AG_2**
Title	**Unregister website from the ReCRED platform**
Description	**As a** web site owner or ReCRED operator **I want to** stop receiving/sending age-related information about visitors **so that** I clean-up previous requests
Acceptance Criteria	1. The owner may request from the ReCRED platform to revoke access to age-related information; the ReCRED operator acts immediately, after verifying the validity of the request 2. The ReCRED operator may revoke access from a web-site for numerous reasons, primarily related to the violation of the relevant license agreement by the web site owner.

Code Number	**AV_AG_3**
Title	**Modify the website configuration with the ReCRED platform**
Description	**As a** web site owner **I want to** modify the age-related information received about visitors **so that** I can maintain my site, even after own modifications
Acceptance Criteria	1. The owner may request from the ReCRED platform to modify access to age-related information 2. A ReCRED operator will assess and grant or deny access to this request for modification of transmitted information and – if approved – enable the updated information exchange in the platform 3. The ReCRED platform should prohibit unjustified requests from web site owners

Code Number	**AV_AG_4**
Title	**The user proves his age**
Description	**As a** website user **I want to** prove my age without revealing other personal information **so that** I am granted access to an age-restricted website
Acceptance Criteria	1. When a user requests access to an age-restricted site, the site asks him to prove his age, via his identity 2. The user must be able to prove his identity, via a supported authentication process (using an Identity Provider) 3. The Identity Provider should respond to the website only with respect to the age-related question asked (e.g. user older than 18 years old, or user in age-range 25-35 or exact age, etc.) 4. The website should not have access to other information other than the requested and agreed information 5. The user should not prove his age-related information every time, but he should prove his identity whenever requested; the first time, the user must confirm this; otherwise, ReCRED should always ask the user for the specific information to share with the website 6. If the user does not want to share the age-related information with the web site or his age is outside the expected range, he must not be granted access

Code Number	**AV_AG_5**
Title	**The user wants to view the sharing of age-related information**
Description	**As a** website user **I want to** view all age-related information about me shared with web sites **so that** I can protect myself
Acceptance Criteria	1. The user verifies his profile information in ReCRED after successful authentication 2. The system shows all accesses to websites and every single request from the websites; for each request, the timestamp and the response of ReCRED will be shown

Code Number	**AV_AG_6**
Title	**The user no longer wants to share age-related information with a website**
Description	**As a** website user **I want to** restrict access to age-related information about me **so that** I can protect myself from unsolicited contacts
Acceptance Criteria	1. The user verifies his profile information in ReCRED and views all permissions to websites and the relevant information shared with them 2. The user revokes access to age-related information for one or more websites 3. ReCRED informs the website about this revocation; any relevant information for this user cached by the web-site MUST be removed immediately; if the end user tries again to connect to the web site, it should be like it is the first time it connects to it

Code Number	**AV_AG_7**
Title	**Audit access to personal information**
Description	**As a** personal data auditor **I want to** sample audit records related to age-related information **so that** I can make sure access is in line with the regulations
Acceptance Criteria	1. The auditor should be able to search for audit records randomly or with predefined filters in the legally defined date range 2. For each advised record, the system should provide information such as: request from the website, interaction with the user, response to the web site

Code Number	**AV_AG_8**
Title	**Reporting on age-related information**
Description	**As a** ReCRED administrator **I want to** create a report on age-related information **so that** I can invoice website owners
Acceptance Criteria	1. The ReCRED administrator should be able to generate recurrent reports (every X days, months, etc.) or ad-hoc reports related to age-related information 2. The reports should be both detailed and aggregated; the aggregated per website owner should provide totals necessary for the relevant invoicing; the detailed reports should be made available whenever disputes pop-up between ReCRED and the web-site owners 3. Recurrent reports should be generated in PDF format (or other non-changeable format) and emailed to website owners and ReCRED administrators

5. Use case C – Campus Wi-Fi and campus-restricted web-services

This section presents user stories for the Campus Wi-Fi and campus-restricted web-services use case. The purpose of the use case is to demonstrate how the ReCRED platform can simplify access to the Wi-Fi network for students, professors and staff and how they can grant access, based on their credentials and attributes, to the same network, for other users.

Actors:

- **Registration officer**: the person responsible to verify user identity and provide credentials
- **Network administrator**: the person responsible to configure access rights of the users based on their credentials
- **Registered user**: the person willing to access the service by presenting his attributes
- **Guest**: a person without credentials that wants to access the service

Two scenarios are considered:

- Campus Network Access
- Guest Campus Wi-Fi Access

5.1. Scenario 1: "Campus Network Access"

Code Number	**CW_CA_1**
Title	**Provide credentials**
Description	**As a** registration officer **I want to** provide credentials to users **so that** they can use only specific attributes to access the Wi-Fi network
Acceptance Criteria	1. A user is physically present to the Registration office and prove his identity attributes 2. The registration officer should be able to provide the credentials to the user 3. The registration officer should define the validity period for the credentials 4. A mobile device is used to store the credentials and the access application

Code Number	**CW_CA_2**
Title	**Revoke credentials**
Description	**As a** registration officer **I want to** be able to revoke user credentials **so that** they cannot access the Wi-Fi network
Acceptance Criteria	1. I revoke the credentials of the user 2. Next time the user tries to use the Wi-Fi using these credentials his access is denied.

Code Number	**CW_CA_3**
Title	**Define access control policies**
Description	**As a** network administrator **I want to** define control access policies **so that a** registered user can connect to the Wi-Fi under certain conditions
Acceptance Criteria	1. I can define access control policies depending on the category of users (student/ professor/staff/guest) 2. I can define access control policies depending on the attributes presented by a user

	3. I can define the minimum set of attributes required for Wi-Fi access 4. I can define the number of devices a user can use to access the Wi-Fi 5. I can define the number of guests for a user

Code Number	**CW_CA_4**
Title	**Refresh user credentials**
Description	**As a** network administrator **I want** the system verifying the user credentials each time he tries to authenticate **So that** I am sure he is not using revoked, expired or outdated credentials.
Acceptance Criteria	1. The user request access the Wi-Fi 2. The authentication service should verify the user attribute with the ReCRED platform and should decide if it grants access.

Code Number	**CW_CA_5**
Title	**Obtain credentials**
Description	**As a** registered user **I want to** obtain my credentials **so that** I can use only specific attributes in order to connect to the Wi-Fi
Acceptance Criteria	1. I present to the Registration office and prove my status and identity attributes 2. A mobile device is used to store the credentials and the access application

Code Number	**CW_CA_6**
Title	**Connect to the Wi-Fi network and campus-restricted web-services**
Description	**As a** registered user **I want to** connect to the Wi-Fi by presenting my attributes **so that** I can access the Internet
Acceptance Criteria	1. Access to Wi-Fi is granted by providing information about my identity attributes that I want to reveal 2. The authentication is performed by using the application from the mobile device 3. The Wi-Fi network does not require any other information from the user 4. Depending on the set of attributes that I present, I can have varying access rights 5. I have the ability to access the Wi-Fi network and campus-restricted web-services from multiple devices

5.2. Scenario 2: "Guest Campus Wi-Fi Access"

Code Number	**CW_GA_1**
Title	**Issue credentials to a guest**
Description	**As a** registered user **I want to** be able to enroll a new user as my guest **so that** he can access the Wi-Fi network of the campus
Acceptance Criteria	1. Generate credentials for a visitor that allow him to access the Wi-Fi only by providing his status (guest) 2. Transfer credentials to the guest's device 3. The guest authenticates to the Wi-Fi by installing the application on his mobile device and using the credentials provided 4. Wi-Fi does not require any other information from the guest 5. The guest can access Wi-Fi from multiple devices 6. The guest is not allowed to grant access to other users

Code Number	CW_GA_2
Title	**Grant access to the Wi-Fi network to a guest**
Description	**As a** registered user **I want to** be able to grant access to the Wi-Fi for a guest as my guest **so that** he can access the Wi-Fi network of the campus
Acceptance Criteria	1. When a visitor tries to connect to the Wi-Fi I am able to use my credentials to grant him access 2. When authenticating to the system I can specify that I am doing it for a guest 3. The guest's device is associated with my account 4. Authentication is performed by using the application from the mobile device 5. Wi-Fi does not require any other information from the guest 6. The guest can access the Wi-Fi only from the device for which I granted him access

Code Number	CW_GA_3
Title	**Obtain credentials from a registered user**
Description	**As a** visitor **I want to** obtain my credentials **so that** I can use only specific attributes in order to connect to the Wi-Fi network
Acceptance Criteria	1. I receive credentials from a registered user that allow me to access the Wi-Fi network only by providing my status (guest of a student/ professor) 2. A mobile device is used to store the credentials and the access application 3. After obtaining credentials and the access application I am able to authenticate to the Wi-Fi network as a registered user

Code Number	CW_GA_4
Title	**Obtain access to the Wi-Fi network from a registered user**
Description	**As a** visitor, **I want to** receive access to the Wi-Fi network from a registered user, as his guest, **so that** I can access the Internet
Acceptance Criteria	1. When I try to connect to the Wi-Fi network, a registered user can use his credentials to grant me access 2. When authenticating, the registered user specifies that I am his guest 3. I am not required any other information to grant me access 4. I can access the Wi-Fi network from the device for which I was granted access

6. Use case D - Student Authentication and Offers

This section presents user stories for the Simple Student Discount offer and Complex student discount offers scenarios.

Some basic scenario specific definitions include:

- ReCRED platform: identity and attribute validation
- offers platform: offer creation, targeting, and reporting

- mobile offers application: offer selection and purchase, agent for real world identity and attribute verification
- issuer: the user of the ReCRED platform who is the provider of the offers platform to the merchant and the mobile offers application to the student
- student: the user of the mobile offers application who uses offers created by merchants
- merchant: the user of the ReCRED platform and the offers platform, provides offers to students (includes the role of marketing manager)

6.1. Scenario 1: "Simple Student discount Offers"

Code Number	**SA_SO_1**
Title	**Evaluate a student registration request**
Description	**As an** issuer **I want to** receive verified identity and student status information from students who are registering **so that** I can grant them an online identity
Acceptance Criteria	1. The issuer may request from the ReCRED platform access to verified identity and student status information 2. A ReCRED operator will assess and grant or deny access to this information and – if approved – enable this information exchange in the platform 3. The ReCRED platform should prohibit unjustified requests from issuers

Code Number	**SA_SO_2**
Title	**Evaluate a merchant connection request**
Description	**As an issuer** **I want to** receive verified identity and business registration information from merchants who are connecting to the offers platform **so that** I can give them connection credentials
Acceptance Criteria	1. The issuer may request from the ReCRED platform access to verified identity and business registration information; hereby we assume a national chamber of commerce as a trusted source 2. A ReCRED operator will assess and grant or deny access to this information and – if approved – enable this information exchange in the platform 3. The ReCRED platform should prohibit unjustified requests from issuers 4. The offers platform should deny unjust registrations from merchants 5. The contracting process will be manually executed by the issuer.

Code Number	**SA_SO_3**
Title	**Provisioning credentials to a student**
Description	**As a student** **I want to** register **so that** I can access their mobile offers application
Acceptance Criteria	1. The student registers for an online identity 2. The student gives consent to the issuer for the verification of his identity and student status 3. The issuer provides the credentials to the user 4. The issuer defines the validity period for the credentials 5. The credentials allow the user to access the mobile offers application 6. A mobile device is used to store the credentials and access the application 7. The user uses ReCRED functionality for authentication

Code Number	**SA_SO_4**
Title	**Create usage reports per merchant**
Description	**As an issuer** **I want to** create usage reports per merchant **so that** I can use this for a transaction-based business model and settlement of disputes
Acceptance Criteria	1. The issuer should be able to generate recurrent reports (every X days, months, etc.) or ad-hoc reports related to the offers platform usage and to the ReCRED platform information exchange 2. The reports should be both detailed and aggregated; the aggregated per merchant should provide totals necessary for the relevant invoicing; the detailed reports should be made available whenever disputes pop-up between the issuer and the merchant

Code Number	**SA_SO_5**
Title	**Create usage reports per student**
Description	**As an issuer** **I want to** create usage reports per student **so that** I can use this for a transaction-based business model and settlement of disputes
Acceptance Criteria	1. The issuer should be able to generate recurrent reports (every X days, months, etc.) or ad-hoc reports related to the offers application usage and to the ReCRED platform information exchange 2. The reports should be both detailed and aggregated; the aggregated per student should provide totals necessary for the business model refinement; the detailed reports should be made available whenever disputes pop-up between the issuer and the student

Code Number	**SA_SO_6**
Title	**Register to the offers platform and the ReCRED platform**
Description	**As a merchant** **I want to** register to the offers platform and the ReCRED platform **so that** I can use only specific attributes to gain access to the platforms
Acceptance Criteria	1. A merchant registers for an online identity 2. The merchant gives consent to the issuer for the verification of his identity and business registration 3. The merchant receives the credentials and their validity period 4. The credentials allow the user access to the offers platform and the ReCRED platform 5. A mobile device is used to store the credentials and access the offers platform and ReCRED platform

Code Number	**SA_SO_7**
Title	**Creating an offer**
Description	**As a** merchant **I want to** receive aggregated attribute information **so that** I can create targeted offers for students
Acceptance Criteria	1. The merchant may request from the ReCRED platform access to verified identity 2. A ReCRED operator will assess and grant or deny access to this information and – if approved – enable this information exchange in the platform 3. The ReCRED platform should prohibit unjustified requests from issuers

Code Number	**SA_SO_8**
Title	**Receive proof of identity or an attribute**
Description	**As the offers application** **I want to** receive proof of identity or an attribute (i.e. verified student status or computer science student) **so that** I can grant the user access to an offer
Acceptance Criteria	1. The merchant may request from the ReCRED platform access to a verified attribute 2. A ReCRED operator will assess and grant or deny access to this information and – if approved – enable this information exchange in the platform 3. The ReCRED platform should prohibit unjustified requests from issuers

Code Number	**SA_SO_9**
Title	**Purchase an offer from mobile device**
Description	**As a student** **I want to** be able to prove my identity and student status online **so that** I can select and purchase an offer from my mobile
Acceptance Criteria	1. The student selects an offer to purchase from his mobile 2. If the student has not given his consent to provide proof of identity and student status through his consent management then he is prompted to do so before continuing with the purchase 3. The merchant receives proof of identity and student status 4. If the identity and attributes match the criteria of the offer then the student is able to continue with the purchase

Code Number	**SA_SO_10**
Title	**Purchase a deal in store**
Description	**As a student** **I want to** be able to prove my identity in the real world using my mobile **so that** I can purchase an offer in store
Acceptance Criteria	1. The student selects an offer to purchase on his mobile 2. If the student has not given his consent to provide proof of identity and student status through his consent management then he is prompted to do so before continuing with the purchase 3. The merchant receives proof of identity and student status 4. If the identity and attributes match the criteria of the offer then the student receives a QR code to present in store 5. In store, the merchant scans the QR code at the time of purchase and the student receives the offer

Code Number	**SA_SO_11**
Title	**Unsubscribe from the service**
Description	**As a student** **I want to** unsubscribe myself from the offers service **so that** I can be assured that my personal data is no longer used
Acceptance Criteria	1. The user verifies his profile information in ReCRED and views all permissions to the issuer and the relevant information shared with him 2. The student can see the history of identity and attribute usage by the issuer 3. If unsubscribed, ReCRED informs the issuer about this termination; any relevant information for this user cached by the issuer MUST be removed immediately; if the end user tries again to interact with the

	issuer, it should be like it is the first time

Code Number	**SA_SO_12**
Title	**Create reports of offers usage per attribute**
Description	**As a merchant** **I want to** create reports of offers usage per attribute **so that** I can refine the offers that I create for subscribed students
Acceptance Criteria	1. The merchant should be able to generate recurrent reports (every X days, months, etc.) or ad-hoc reports related to the offers platform usage and to the ReCRED platform information exchange 2. The reports should be both detailed and aggregated; the aggregated per student should provide totals necessary for the refinement of offers; the detailed reports should be made available whenever disputes pop-up between the merchant and the student

6.2. Scenario 2: Use case "More complex student discount offers"

Code Number	**SA_CO_1**
Title	**Verification of multiple aspects of a student's identity**
Description	**As a** merchant **I want to** verify multiple ID attributes of the student **so that** I can ensure that the offers are used by genuine students and that the student has the particular characteristics of my target group
Acceptance Criteria	1. The student presents the digital identity card from the mobile app to the merchant and merchant scans that ID and verifies the student ID on the fly. 2. The student can present multiple ID attributes that ensure the merchant that she is the type of the student targeted by the offer.

Code Number	**SA_CO_2**
Title	**Control identity**
Description	**As a**n Issuer **I want to** control the flow of identity information **so that** both students and merchants trust the service, thereby increase the revenue and brand
Acceptance Criteria	1. The issuer stores the user attributes and consent information. 2. This information is shared with merchants based on the user consent.

7. Use case E – Request for a Public Service

This section contains the user stories for scenarios focusing on the user requesting a public service. The two scenarios presented are "Request for a resident's parking card" and "Access in a pedestrian zone".

7.1. Scenario 1: "Request for a public service – resident's parking card"

Code Number	**PS_PC_1**
Title	**Registration for a resident's parking card**
Description	**As a** ReCRED user **I want to** register for a resident's parking card using the ReCRED services **so that** I will be issued a parking card for my residence area quickly and easily avoiding the bureaucracy and the paperwork.
Acceptance Criteria	1. The online Parking Registration service requires ReCRED credentials that verify the user's residence.

	2. The requested credentials are issued and cryptographically signed by the local municipality office. 3. The Parking Registration service registers the user upon verification of the credentials. 4. The Parking Registration service rejects all attempts to register if the credentials are invalid, or contain a residence area other that the requested.

Code Number	**PS_PC_2**
Title	**Verification of a parking card’s validity**
Description	**As a** Parking owner **I want to** verify that my resident’s parking card is still valid **so that** I will know whether I can still use it.
Acceptance Criteria	1. The user must authenticate to the mobile device and supply the parking card number to the Parking Registration service. 2. The Parking Registration service exchanges cryptographic keys with the ReCRED mobile application and associates the user with the registered parking card. 3. The Parking Registration service returns the requested information (valid or invalid) to the user. 4. The Parking Registration service rejects any invalid attempts i.e. user did not authenticate or user is not associated with the registered parking card.

7.2. Scenario 2: “Request for a public service – access in a pedestrian zone”

Code Number	**PS_PZ_1**
Title	**Issuing of a Permit to drive in a Pedestrian Zone**
Description	**As a** ReCRED user **I want to** be issued a pedestrian zone access permit **so that** I am able to drive my car in the pedestrian zone.
Acceptance Criteria	1. The Permits office requests ReCRED credentials that verify that the user is either a resident or a business owner and should be allowed entry with his car. 2. The requested credentials are issued and signed by the appropriate authority such as Municipality and/or Shop owners Association. 3. The Permits Office issues a signed electronic credential that contains the Permit in the pedestrian zone. 4. The Permits Office rejects all registration attempts that do not involve valid and eligible credentials.

Code Number	**PS_PZ_2**
Title	**Use a Permit to drive in a Pedestrian Zone**
Description	**As a** Permit holder **I want to** use my permit **so that** I am able to drive my car in the pedestrian zone.
Acceptance Criteria	1. The Permit holder uses the mobile device’s NFC sensor to initiate communication to the Access Control Device. 2. The mobile application requests biometric authentication in order to exchange credentials with the Access Control Device. 3. The Access Control Device transfers the credentials to the central computing center and the credentials are validated. 4. Access is allowed (e.g. bars are lifted) if the credentials are valid. 5. Access is denied when credentials are not eligible or invalid.

8. Use Case F – Share Sensitive Documents

This section contains a scenario about sharing sensitive documents e.g. medical records, and aims to show how ReCRED can offer the necessary security and controlled access to such documents.

8.1. Scenario 1: “Share Sensitive Medical Documents”

Code Number	**SD_MD_1**
Title	**Sharing Medical Documents**
Description	**As a** ReCRED user **I want to** be able to use ReCRED to share medical documents **so that** I can securely and easily allow a third party, such as my insurance company, to access personal sensitive information.
Acceptance Criteria	1. The user connects to the ReCRED server and saves medical information as identity attributes. 2. The insurance company acts as a Relying Party that is registered in the ReCRED server so that a ReCRED user can transfer attributes to it. 3. The user allows transfers a selection of the medical attributes, to the insurance company server.

9. Usability principles

In addition to functional and operational requirements, the design of the Graphic User Interface (GUI) of the ReCRED platform will follow some usability principles, which are defined according to the heuristics proposed by Jacob Nielsen[3] and to some standard conventions[4].

9.1. Usability requirements

In the following tables, the main usability heuristics are translated into requirements, which will be applied to the entire ReCRED platform and to the different users’ roles.

Code Number	**USR_1**
Title	**Visibility of the system status**
Description	**As a** user **I want to** be informed about the system status in each moment **so that** I can understand the possible actions I can perform, and the consequences of the actions once performed
Acceptance Criteria	1. The system should provide appropriate feedback within reasonable time, and a clear vision of the system current status

Code Number	**USR_2**
Title	**Error prevention**
Description	**As a** user **I want to** be able to undo an unintended action **so that** I can avoid mistakes
Acceptance Criteria	1. The system should provide a clearly marked "emergency exit" to leave the unwanted state or undo an action performed by mistake.

[3] Nielsen, J. “10 Usability Heuristics for User Interface Design”, available at https://www.nngroup.com/articles/ten-usability-heuristics/

[4] Lidwell, W., Holden, K., & Butler, J. (2010). *Universal principles of design, revised and updated: 125 ways to enhance usability, influence perception, increase appeal, make better design decisions, and teach through design*. Rockport Pub.

	2. The system should present users with a confirmation option before they commit to critical actions (i.e. delete account from Identity Consolidator service, transfer identity information among online accounts etc.), in order to prevent unintended actions by requiring verification of the actions before they are performed. It should be done through a dialog box (“Are you sure you want to …?”) or through a two-steps operation that involves a preliminary step that occurs prior to the actual command or input.

Code Number	**USR_3**
Title	**Error diagnosis**
Description	**As a** user **I want to** be informed about errors occurred **so that** I can recognize, diagnose and recover from errors
Acceptance Criteria	1. The system should present error messages expressed in a clear and understandable way, precisely indicate the problem and constructively suggest a solution.

Code Number	**USR_4**
Title	**Consistency**
Description	**As a** user **I want to** perceive the consistency of the system **so that** I can easily understand and use it
Acceptance Criteria	1. The system should have internal consistency related to its aesthetic (consistency of style and appearance), and to the controls and functions among the different components and features.

	2. The system should have external consistency, applying common standards and conventions to icons, symbols and labels.

Code Number	**USR_5**
Title	**Documentation**
Description	**As a** user **I want to** have a clear documentation **so that** I can be assisted in basic operations, troubleshooting and error recovery
Acceptance Criteria	1. The system should provide a documentation including information and guidelines which are easy to search, focused on the user's task and list concrete steps to be carried out.

9.2. General recommendations for the Graphic User Interface Design

This section describes some general recommendations for the organization of the layout and the compositions of the different elements (icons, texts, figures etc.) within the GUI.

9.2.1. Fitts' Law

Fitts' Law states that the time required to move to a target is a function of the target size and distance to the target. According to Fitts' Law, the smaller and more distant a target, the longer it will take to move to a resting position over the target. In addition, the faster the required movement and the smaller the target, the greater the error rate due to a speed-accuracy tradeoff. This rule is applicable only for rapid, pointing movements, not for more continuous movements, such as writing or drawing. It suggests to design near or large controls when rapid movements are required and accuracy is important; distant and smaller controls when they should not be frequently used, or when they will cause problems if accidentally activated.

9.2.2. Gutenberg rule

Gutenberg rule describes the general pattern followed by the eyes when looking at evenly distributed, homogeneous information, providing advice for where to place important information, commands or a call to action. Beside this pattern applies to text-heavy content, it can be useful also to design a layout that doesn't include so much text.

The Gutenberg diagram (Figure 1) divides a display medium into four quadrants: Western readers naturally begin at the primary optical area and move across and down the display medium in a series of sweeps to the terminal area. Each sweep begins along an *axis of orientation*–a horizontal line created by aligned elements, text lines, or explicit segments–and proceeds in a left-to right direction.

The strong and weak fallow areas lie outside this path and receive minimal attention unless visually emphasized. The tendency to follow this path is metaphorically attributed to *reading gravity*–the left-right, top-bottom habit formed from reading.

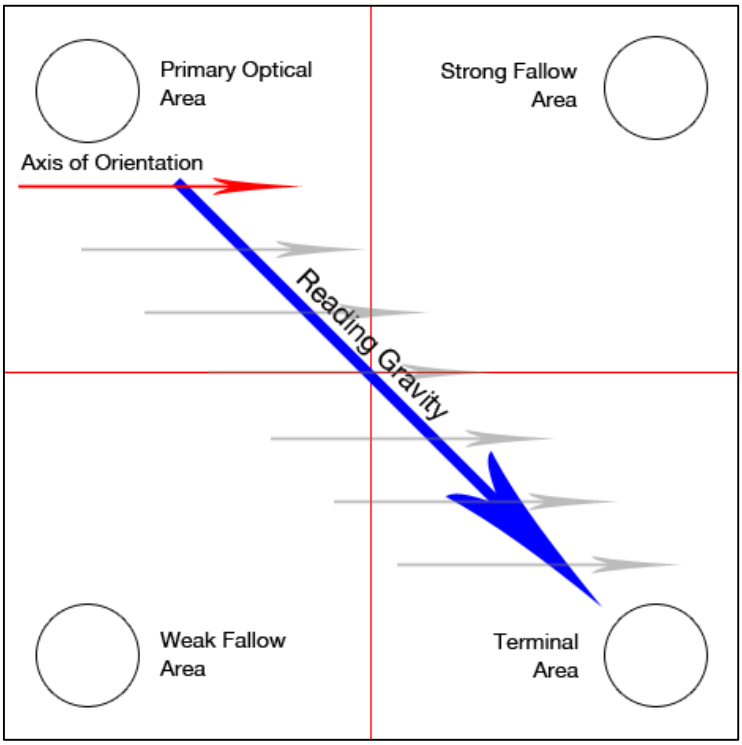


Figure 1 - Gutenberg diagram

9.2.3. Verbal and visual language

Because the ReCRED platform is addressed to different kinds of users[5], who are experts and non-experts, the labels and the information presented to the user need to be well designed, so to be clearly understandable and correctly interpreted. As well as texts and labels, the use of colors should be properly used to attract attention, organize the elements within the interface and communicate meanings. In order to design the GUI in the best way, it is recommended to limit the palette to what the eye can process at one glance (about five colors) and create a good combination of the colors.

9.3. Usability Assessment

The ReCRED project includes the assessment of the User Experience within the WP7 “Large Scale Pilots and End User Experience Assessment”. Because the objective of ReCRED is to design a “usable” device-centric authentication, it is essential to evaluate the GUI and the entire process of interaction between ReCRED and the users, according to the use cases and the user stories described in the previous paragraphs.

The usability evaluation will be performed as a preliminary investigation using wireframes, so to early collect users’ feedback and make the proper adjustments. Then, after the implementation in each pilot site, the assessment will be carried out on the final version of ReCRED.

[5] ReCRED target users were defined as Personas in the Deliverable 7.5 “HCI concept testing on user groups”.

The goal is to evaluate whether the users clearly understand the system and easily accomplish every task along with its consequences, within a secure and reliable framework that meets users’ needs.
The usability evaluation will be performed through a mixed method that includes different procedures:

- Heuristic evaluation by experts, who evaluate ReCRED according to the usability heuristics and provide a list of issues to fix;
- Test sessions with users, during which some participants who are representative of the target audience, are invited to perform tasks within one or more scenarios, thinking out loud so to explain what they are doing, thinking and feeling in each moment;
- Online survey, through which users can install the app on their own, try it out and then complete a questionnaire to provide their opinions.

The questionnaire will be created by integrating the items of the System Usability Scale[6] with other items more focused on the specific ReCRED features. The detailed report of the assessment will be included in Deliverable 7.4 “All pilots in operation and end user assessment report”.

[6] https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html

10. Technical Requirements

This section contains the technical requirements as they were extracted from the use cases and user stories. The technical requirements of each of the six major architectural components of the ReCRED platform are listed and categorised according to Functional, Security & Privacy and Operational. Below we list a non-exhaustive list of requirements that are written in the form of user stories. Note that in each user story we list the corresponding code number (and our Phabricator task number where applicable). Also, note that due to the fact that we are employing an Agile methodology to the development of the ReCRED platform, the below list can be refined/updated during the course of the development.

The technical requirements together with the architecture deliverable are going to be the two major inputs that will initiate the platform delivery process.

10.1. User Device

The mobile device of the user plays a major role within the ReCRED platform as is the main component for the users perform device- centric authentication. Below we list the functional requirements, security & privacy requirements and operational requirements with regard to the user device component.

10.1.1. Functional Requirements

ReCRED mobile application for user-device and device-service authentication

This section is about the ReCRED application that will run on the user's device. Specifically, on the user device we will implement, modify and deploy the following components:

- FIDO Universal Authentication Framework (UAF) client
- ABAC schemes such as Idemix and U-Prove
- OpenID connect
- Cryptographic Credentials Storage by utilizing Trusted Execution Environments
- User-to-device authentication schemes such as face recognition

ReCRED daemon on user's device

This daemon is a logical placeholder for the functionalities that ReCRED will introduce to the user's device. Specifically, we will deploy a behavioral profile capturing module which acquires all behavioral attributes of the user, such as typing pattern, network activity, location, interaction with the UI, etc. Those captured behavioral profiles are transferred securely and stored to the Behavioral Authentication Authorities (BAA). Moreover, we will implement and deploy a cryptographic credentials storage which allows the device to store the cryptographic credentials it receives from the ID consolidation service and from multiple ID providers. The device runs federated login protocols with the ID providers and Service Providers (aka, relying parties) for the cases where the authentication does not take place with cryptographic credentials (RSA, ABAC) but through passwords and cookies.

The aforementioned functionalities will be deployed on the android phone either as mobile applications or background services.

Deployment of FIDO stack on user's device

The FIDO UAF Client implements the client side of FIDO and transports the underlying protocol specific authentication and registration messages. It is responsible for:

- Communicating with the FIDO server, not directly but through a user agent (an application that runs on the user device that can be either a mobile application or a standard internet browser). Therefore the FIDO client will interface with the user agent and will deliver and receive messages from it. The user agent forwards FIDO protocol specific messages to the FIDO server through the relying party web application. The user agent contains a FIDO-specific implementation (e.g. a browser plugin) that handles the FIDO messages.
- Communicating with the FIDO UAF Authenticator, exchanging protocol specific cryptographic messages (e.g. U-Prove or Idemix). The FIDO Client communicates with the FIDO Authenticator using a standardized interface: the Authenticator Specific Module, which provides a uniform interface between the client and the hardware.

The Authenticator Specific Module (ASM) is an abstraction layer that provides a uniform API between the authenticator hardware and the FIDO Client. The FIDO Client uses the ASM API calls in order to delegate cryptographic operations to the Authenticator module. Also, the ASM interface allows the use of different authenticator modules and ensures the compatibility between the authenticator and the client.

The FIDO UAF Authenticator is the secure element connected to all or part of the user device (mobile phone) that is responsible for the creation of the cryptographic key material, storage and secure usage of the private keys used in the authentication protocol. In case the device contains and uses a Trusted Execution Environment (e.g., ARM Trust Zone), the authenticator can use this safe storage and execution memory/CPU to obtain a higher level of security.

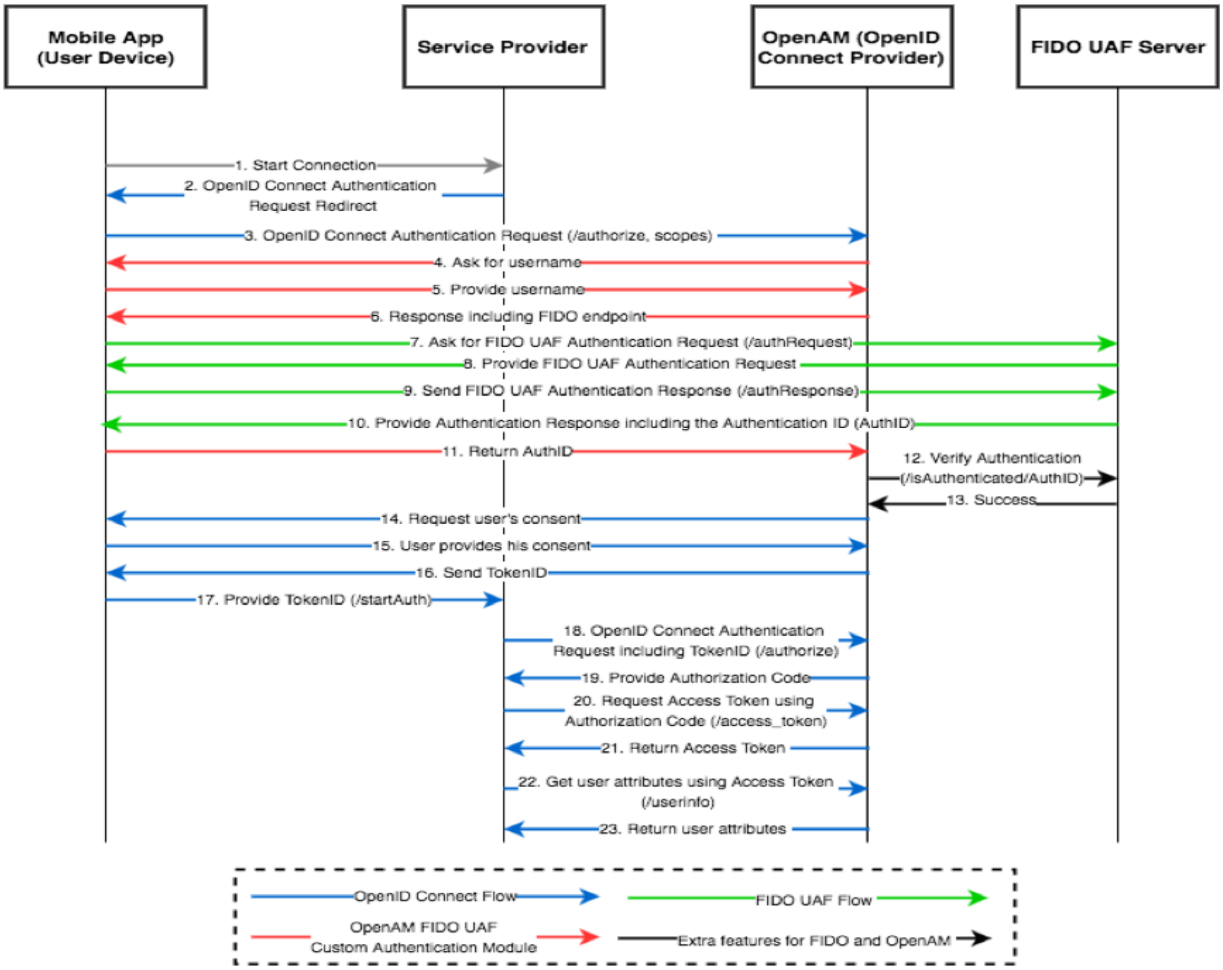


Figure 2: Implementation of secure OpenID Connect and FIDO integration

Code Number	**D3.2.2.1 - T128**
Business Value	**High**
Title	**Deployment of FIDO stack on user's device**
Description	**As a** user **I want to** be able to authenticate to Identity Providers using the FIDO UAF specification **so that** the Identity Provider can authenticate me and verify my identity
Acceptance Criteria	1. The user can authenticate to Identity providers using the FIDO UAF specification.

	2. The stack should support all the common authenticators such as fingerprint, pin etc.

Deployment of FIDO stack in user’s device: Integrate FIDO component with the authenticators

Code Number	**D3.2.2.1.3 - T504**
Business Value	**High**
Title	**Deployment of FIDO stack in user’s device: Integrate FIDO component with the authenticators**
Description	**As a** user **I want to** be able to use the common authenticators such as fingerprint etc. **so that** I can login to Identity Providers that support the FIDO Universal Authentication Framework (UAF) specification
Acceptance Criteria	1. The user should be immediately re-authenticated to his device upon every login attempt to an online service, using one of the common authenticators (fingerprint, pin, etc.) 2. The TEE should handle the FIDO private key and execute the FIDO UAF authentication process on the user’s behalf

Key generation and secure key storage for FIDO using the TEE

Code Number	**D3.2.2.1.4 - T505**
Business Value	**High**
Title	**Implementation of key generation and secure key storage for FIDO using the TEE**
Description	**As a** user **I want to** be able to generate and secure my FIDO keys using the TEE

	so that the security of my authentication process is guaranteed
Acceptance Criteria	1. The FIDO stack should use the TEE key pair generation function 2. The generated private key should be always handled and secured by the TEE

Signing and verifying operations for FIDO using the TEE

Code Number	**D3.2.2.1.5 - T506**
Business Value	**High**
Title	**Implementation of signing and verifying operations for FIDO using the TEE**
Description	**As a** user **I want to** be able to perform the signing and verifying operations for FIDO using the TEE **so that** the security of my authentication process is guaranteed
Acceptance Criteria	1. The FIDO stack should use the TEE signing and verifying functions 2. The FIDO private key should be always handled and secured by the TEE

User-to-device authentication using biometrics

Code Number	**D3.2.2.2.4.1.1 - T175**
Business Value	**High**
Title	**Authenticate to Device Using Face Recognition**
Description	**As a** user **I want to** periodically authenticate to my device using face recognition

	so that I can then authenticate to a particular service provider that require face recognition as an authentication factor
Acceptance Criteria	1. The application tries to seamlessly verify the user each time he unlocks his phone or after certain predefined time interval. 2. Each face recognition attempt begins with a face detection attempt, which lasts for a predefined amount of time (in seconds). If no face is detected during that time, the application informs the user through a “face detection failed” notification on the user’s device. 3. The user can instantly trigger a face recognition attempt after interacting with a “face detection failed” notification. 4. After a face is detected, the application takes a series of user photos and proceeds with face recognition, producing a verification probability (a number between 0 and 1 - the higher the number, the most confident the application is of the user’s identity). 5. The application doesn’t store any photos acquired during face recognition.

Code Number	**D3.2.2.2.4.1.2 - T174**
Business Value	**High**
Title	Train the Face Recognition Engine
Description	**As a** user **I want to** be able to train the recognition engine, by providing various photos of me **so that** I can then authenticate to my device using face recognition
Acceptance Criteria	1. The user can train the application’s recognition engine, by taking a series of photos (templates) through his device’s camera.

	2. The application doesn’t store any template unless a face is detected on the acquired photo. 3. The user can preview and accept or reject each acquired photo. 4. The user can retrain the recognition engine, by adding or removing photos at any time (after providing a previously chosen PIN / password). 5. The application generates and stores a hash value from the acquired user photos. 6. The user can decide whether or not the acquired photos will be deleted from the device, after their hash value has been created. 7. The user can grant (or revoke) camera access to the application. 8. The application displays an error message in case there is no camera on the device or no camera access has been granted.

Code Number	**D3.2.2.2.4.1.3 - T507**
Business Value	**High**
Title	**Secure storage of Facial Templates using the Trusted Execution Environment (TEE)**
Description	**As a** user **I want to** securely store my facial templates **so that** they can’t be accessed from unauthorized entities
Acceptance Criteria	1. The facial templates created by the facial recognition module should be encrypted by the TEE 2. The encryption key should always reside inside the TEE

Cryptographic Credentials storage on user's device ReCRED daemon

The ReCRED daemon has a Cryptographic Credentials Storage (CCS) where the device stores in a secure fashion the cryptographic credentials it receives from the ID consolidation service and from multiple ID providers. Keys stored in the CCS should not be exported even in the event that the OS get compromised. This can be achieved by using a Secure OS (also referred as Trusted OS) along with hardware to set a Trusted Execution Environment (TEE). A TEE is an isolated secondary environment that can be used for security-sensitive functions and data storage, and it can be implemented in a separate processor such as Secure Element (SE) or isolated in a shared processor, by using, for example, the ARM Trustzone technology.

Code Number	**D3.2.2.2.2 - T127**
Business Value	**High**
Title	Implementation of Cryptographic Credentials storage on user's device ReCRED daemon
Description	**As a** user **I want to** I want to securely store my cryptographic credentials **so that** my online identity stays protected if my device gets compromised (e.g. by a malware)
Acceptance Criteria	1. All ReCRED-issued cryptographic credentials should be encrypted by the TEE 2. The encryption keys should always reside inside the TEE

Integration of OpenID connect in ReCRED daemon on user's device

The device should run the OpenID connect protocol with the ID providers and Service Providers.

Code Number	**D3.2.2.2.3 - T150**
Business Value	**High**
Title	**Integration of OpenID connect in ReCRED daemon on user's device**
Description	**As a** user's device application

	I want to be able retrieve user attributes from Identity Providers **so that** I can use user's identity attributes for various procedures that are supported by the ReCRED platform
Acceptance Criteria	1. The app should be compatible with OpenAM's OpenID connect provider. 2. The procedure will follow the OpenID Connect's Authorization Code flow 3. The app should be able to maintain access tokens in order to be able to re-use them multiple times. 4. The user's authentication will be based on the FIDO UAF protocol.

FIDO Universal Authentication Framework (UAF) Client

The FIDO UAF Client should implement an HTTP/HTTPS client required for the communication with FIDO UAF Server through the REST interface and process/create the messages received/sent according to the FIDO UAF protocol specification.

Code Number	**D3.3.1.2.1 - T586**
Business Value	**High**
Title	**Implementation of policy processing for the registration function on the FIDO UAF Client**
Description	**As a** user **I want** to rely on the FIDO UAF client to correctly process FIDO UAF server policies **So that** I can securely register to an Identity Provider through the FIDO UAF protocol.
Acceptance Criteria	1. The registration process will accept a policy from the server 2. The registration process will match the server policy

Code Number	**D3.3.1.2.2 – T587**
Business Value	**High**
Title	**Implementation of the messages required for the registration functionality on the FIDO UAF Client**
Description	**As a** user **I want** to rely on the FIDO UAF client to recognize the messages required for the registration functionality **So that** I can securely register to an Identity Provider through the FIDO UAF protocol.
Acceptance Criteria	1.The FIDO client will accept a registration request from the server which will have the following form: username, challenge, application ID, authenticator policy (described in FIDO UAF protocol section 3.4) 2. The FIDO client will decode a JSON registration request which is described in FIDO UAF protocol section 3.4.1 and 3.4.2 3. For the registration process the FIDO client will send to the server a registration response message as described in FIDO UAF protocol section 3.4.5

Code Number	**D3.3.1.2.3 - T588**
Business Value	**High**
Title	**Implementation of the processes required for the registration functionality on the FIDO UAF Client**
Description	**As a** user **I want** to rely on the FIDO UAF client to correctly process the structures required **So that** I can securely register to an Identity Provider through the FIDO UAF protocol.

Acceptance Criteria	1. The FIDO client will compute the Final Challenge Params from the Server Challenge and some other values and sends the AppID, FinalChallengeParams (FCH) and the username to the authenticator 2. For the registration process the FIDO client will filter the available authenticators and present the suitable authenticators to the user. 3. For the registration process the FIDO client will obtain the FacetID of the requesting application (ReCRED) and will verify if the FacetID is authorized for the AppID as described in FIDO AppID and Facet Specification. 4. For the registration process the FIDO Client must send ASM Request only to the authenticator selected by the user as specified in the FIDO UAF Authenticator-Specific Module API. 5. The FIDO Client should implement TLS binding

Code Number	**D3.3.1.2.4 - T589**
Business Value	**High**
Title	**Implement the recognition of FIDO UAF authenticators specified by the FIDO UAF server**
Description	**As a** user **I want** the FIDO UAF client to recognize the authenticators specified by the FIDO UAF server **so that** I can authenticate to FIDO UAF Identity Providers
Acceptance Criteria	1. Based on the server metadata information, the FIDO Client API should expose only the supported authenticator types 2. The FIDO Client should implement the FIDO UAF protocol version negotiation 3. The FIDO Client application should authenticate with all the Authenticators that the server requires

Code Number	**D3.3.1.2.5 - T590**
Business Value	**High**
Title	**Implementation of the processing required for the authentication function on the FIDO UAF client**
Description	**As a** user **I want** the FIDO UAF client to process the data required **so that** I can authenticate to FIDO UAF Identity Providers
Acceptance Criteria	1. Implement client authentication messages: Request, Response, ProcessingRules 2. The FIDO client will compute the FinalChallengeParams (FCH) from the Server Challenge and some other values and sends the AppID, FCH and the username to the authenticator (the processing is described in FIDO UAF protocol section 3.4) 3. The FIDO client will decode a JSON registration request which is described in FIDO UAF protocol section 3.4.1 and 3.4.2 4. The FIDO Client should implement TLS binding

Code Number	**D3.3.1.2.6 - T591**
Business Value	**High – Medium - Low**
Title	**Implementation of the deregistration function on the FIDO UAF Client**
Description	**As a** user **I want** the FIDO UAF client to tell the other modules to remove the registration data

	So that I can clear my FIDO UAF identity information from both my smartphones.
Acceptance Criteria	1. The Deregistration process will allow an Identity Provider to tell the authenticator to forget a locally managed key 2. The FIDO client will check the integrity of the deregistration request and if it does not follow the specifications from the FIDO UAF protocol section 3.4.6.2 will reject it. 4. The FIDO client will parse the deregistration request and will send the appropriate ASM request to the authenticator.

User-Device Quick Response (QR) Authentication Module

The QR Device Client scans the QR code presented by the QR Web Client, processes it and sends authentication data to the QR Server.

Code Number	**D3.2.17.2 – T599**
Business Value	**High**
Title	**QR code parsing**
Description	**As a** QR Web Client/QR Authentication Server **I want** the device client to be able to decode QR codes **so that** communication between entities can flow without errors
Acceptance Criteria	1. Use a QR code interpretation library (zxing/zbar/etc) 2. Processing should not be bigger than the QR code expiration gap.

Quick Response (QR) Web Client

The QR Web client is responsible for fetching and displaying the QR code from the QR Authentication Server, plus polling the server for authentication on the current QR code.

Code Number	**D3.2.17.1 – T599**

Business Value	**High**
Title	**QR Authentication Server polling**
Description	**As a** QR Authentication Server **I want** the web client to detect device authentication as fast as possible **so that** communication between entities can be established as fast as possible
Acceptance Criteria	1. This should be implemented as a JavaScript polling service

Authenticator Specific Module (ASM)

The FIDO UAF authenticator specific module (ASM) allows the FIDO UAF Client to talk to any trusted FIDO UAF Authenticator connected or bound to the device.

Code Number	**D3.3.1.3.1 - T594**
Business Value	**High**
Title	**Implementation of the Registration function on the FIDO UAF ASM**
Description	**As a** FIDO UAF Client **I want** to not depend on a certain authenticator device manufacturer **So that** I can register to an Identity Provider through the FIDO UAF protocol.
Acceptance Criteria	1. The procedure should support the register request method as described in “FIDO UAF Authenticator-Specific Module API section 3.6” 2. The procedure should support the GetRegistrations request method as described in "FIDO UAF Authenticator-Specific Module API section 3.9"

Code Number	**D3.3.1.3.2 - T595**

Business Value	**High**
Title	**Implement the support operation of FIDO UAF Authenticators using FIDO UAF ASM authentication function**
Description	**As a** FIDO UAF Client **I want** the FIDO UAF ASM to extend FIDO UAF authenticators **So** that I can authenticate to a FIDO UAF Identity Provider in case the FIDO UAF authenticator doesn’t support it.
Acceptance Criteria	1. Use ASM to implement operations not supported by authenticators (e.g. KeyID in case authenticator does not support it)

Code Number	**D3.3.1.3.3 - T596**
Business Value	**High**
Title	**Implementation of the authentication function on the FIDO ASM**
Description	**As a** FIDO UAF Client **I want** the authentication function to be conformant to the specification **So that** I can authenticate to a FIDO UAF Identity Provider.
Acceptance Criteria	1. The procedure should support the authenticate request method as described in "FIDO UAF Authenticator-Specific Module API section 3.7" 2. The procedure should support some of the request types described in "FIDO UAF Authenticator-Specific Module API section 3.1" 3. The procedure should be able to verify the integrity of a request as described in “FIDO UAF Authenticator-Specific Module API section 3.3” 4. The procedure should deliver the FIDO UAF responses as described in "FIDO UAF Authenticator-Specific Module API section 3.4" 5. Implement an Android-based ASM API as described in "FIDO UAF Authenticator-Specific Module API section 5.1"

Code Number	**D3.3.1.3.4 - T597**
Business Value	**High**
Title	**Implementation of the deregistration function on the FIDO UAF ASM**
Description	**As a** FIDO UAF Client **I want** to have a possibility to unregister myself **So that** I clear my FIDO identity information from my hardware authenticator device.
Acceptance Criteria	1. The procedure should support the deregister request method as described in "FIDO UAF Authenticator-Specific Module API section 3.8" 2. Implement an Android-based ASM API as described in "FIDO UAF Authenticator-Specific Module API section 5.1"

FIDO Universal Authentication Framework (UAF) Authenticator

The FIDO UAF Authenticator should handle key generation/usage in a TEE and communicate with FIDO UAF ASM according to the FIDO UAF specification.

Code Number	**D3.3.1.1.1 - T580**
Business Value	**High**
Title	**Implementation of key generation for the registration function on the FIDO UAF Authenticator**
Description	**As an** ASM API **I want** to rely on secure cryptographic protocols and on the Android secure key generation features **So that** I can register to a particular Identity Provider according to the FIDO UAF protocol.

Acceptance Criteria	1. The FIDO cryptographic keys will be generated using the Android Java Security interface (KeyStore) 2. The FIDO cryptographic keys will be stored in the Android KeyStore 3. Allows a user to generate and associate new key material with an account at the relying party server

Code Number	**D3.3.1.1.1 - T581**
Business Value	**High**
Title	**Implementation of the attestation signatures for registration function on the FIDO UAF Authenticator**
Description	**As an** ASM API **I want** to rely on secure implementation of the cryptographic protocols **So that** I can register to an Identity Provider through the FIDO UAF protocol.
Acceptance Criteria	1. For the registration process the authenticator will generate a Key Registration Object: hash of the FCH, the generated public key and some other values. These values will be signed by the attestation key. (the detailed structure of this message is described in FIDO UAF protocol section 3.4) 2. For the registration process the authenticator will respond with a message described in FIDO UAF protocol section 3.4.3 3.The authenticator will provide attestation during the registration methods using PKI (X.509 certificates)

Code Number	**D3.3.1.1.2 - T583**
Business Value	**High**
Title	**Implementation of the authentication functionality on the FIDO UAF Authenticator**

Description	**As an** ASM API **I want** the FIDO UAF authenticator to attest the authentication response **So that** I can be protected against impersonation attacks by securing my identity data.
Acceptance Criteria	1. The Authenticators should not allow key access in case the user authentication fails 2. The Authenticator should detect and reject malicious authentication attempts 3. Implement SignAssertion for client authentication messages 4. Implement attestation credential(X509)/Authenticator Attestation ID 5. Implement Authentication Request Processing Rules for FIDO Authenticator

Code Number	**D3.3.1.1.4 - T583**
Business Value	**High**
Title	**Implementation of the FIDO UAF Authenticator using fingerprint key authentication**
Description	**As an** ASM API **want to** be able to generate a FIDO UAF key pair that can only be used after I authenticate with my fingerprint, **So that** I can prove login to service providers.
Acceptance Criteria	1. Authenticator must be conformant with the FIDO UAF protocol specification.

Code Number	**D3.3.1.1.5 - T584**

Business Value	**High**
Title	**Implementation of the deregistration function on the FIDO UAF Authenticator**
Description	**As an** ASM API **I want** the FIDO UAF Authenticator to delete the keys **so that** I can deregister from a FIDO UAF Identity provider
Acceptance Criteria	**1. The keys should be deleted from the Android KeyStore**

FIDO Universal Authentication Framework (UAF) Extensions

Code Number	**D3.3.1.1 – T541**
Business Value	**High**
Title	**Implementation of authentication id access for the last successful authentication function**
Description	**As an Identity Provider** **I want to verify that a user authenticated against** the FIDO UAF Server with a particular authentication id number **so** that I can verify that access is only provided to authenticated users.
Acceptance Criteria	1. The output should be accessible through the REST API of the FIDO UAF server. 2. The timestamp should be either an integer that represent the last authentication time or -1 if the authentication isn't valid.

10.1.2. Security & Privacy Requirements

#	Security & Privacy Requirements	Rational / Comments	Mandatory or Not
S&P1.1	The human to device authentication mechanism should detect and reject malicious authentication attempts.	-	Yes

S&P1.2	Secret data (e.g., the fingerprint template of a user) should be securely stored. Its secrecy should be guaranteed as long as the trusted computing components of the platform remain uncompromised.	It should be hard for an adversary to learn the secret information required for authentication.	Yes
S&P1.3	Secret information of S&P1.2 should never leave the device.	-	Yes
S&P1.4	The personal or other information stored on the device related to the user must be cryptographically encoded	In case of theft or loss, the device may not be used by an unauthorized user	Yes
S&P1.5	Cryptographic credentials should be stored on user device and must be protected by eavesdropping/leakage	-	Yes
S&P1.6	Biometric credentials used to authenticate the user to the device must not leave the device.	-	Yes
S&P1.7	Information about the user stored on his device must be securely protected. Anyone else apart from the user of the device must not be able to have access to this information. Similarly, third parties requesting access to user’s information must only have access to the agreed set of information	If the device is broken or stolen, personal information in it must not be made available to unauthorized users	Yes
S&P1.8	The application generates and stores a facial feature vector from the acquired user photos.	The actual user photos should not be stored in the device.	Yes
S&P1.9	The facial feature vectors are encrypted in the TEE.	The facial feature vectors should not be accessible by unauthorized entities.	Yes
S&P1.10	Information about the user stored on his device must be securely protected.	Only the legitimate device owner should have access to this info.	Yes
S&P1.11	The mobile application must obtain explicit consent from the end-user to collect and process its personal data.	Compliance with GDPR	Yes
S&P1.12	The system must obtain explicit consent from the end-user to transfer its personal data between ReCRED consortium members.	Compliance with GDPR	Yes
S&P1.13	All communication must occur over a secure channel	SSL through gateSAFE	Yes
S&P1.14	The TEE must protect its assets from the Rich Execution Environment (REE).	This is achieved through hardware mechanisms that the REE cannot control.	Yes
S&P1.15	The Trusted Storage must be bound to the device such that no unauthorized internal or external attacker may access, copy or modify the data contained.	The strength of this protection must be at least equal to that of the TEE environment.	Yes

S&P1.16	The TEE must be protected against a range of physical attacks.	This protection is a level less than that found to dedicated tamper resistant technology.	Yes
S&P1.17	All TEE primary trusted resources must be implemented in-package and not be accessible by the REE.	The resources must be protected from physical attacks by the processor packaging.	Yes
S&P1.18	The TEE code must be kept at minimum size.	The reduction of the amount of code running leads to the reduction of the attack surface.	Yes
S&P1.19	Secret/private keys should never leave the TEE.	-	Yes
S&P1.20	Software in the REE must be able to call directly TEE Functions only through secure and dedicated APIs (TEE Client API, TEE Internal API).	The REE software must go through protocols such as the Trusted OS or the Trusted Application that performs the verification of the acceptability of the operation that the REE software has requested.	Yes
S&P1.21	User I/O to TEE must be through trusted interfaces.	Trusted interfaces must communicate directly with TEE without any interference from REE.	Yes
S&P1.22	The TEE must be GlobalPlatform compliant.	GlobalPlatform is responsible for establishing the TEE specifications.	Yes
S&P1.25	The Authenticators should not allow key access in case the user authentication fails	-	Yes
S&P1.26	The Authenticators should detect and reject malicious authentication attempts	-	Yes
S&P1.27	Implement attestation credential(X509)/Authenticator Attestation ID	-	Yes
S&P1.28	Verify the integrity of a request as described in "FIDO UAF Authenticator-Specific Module API section 3.3"	Compliance with the FIDO UAF specification	Yes
S&P1.29	The FIDO cryptographic keys will be generated using Android Keystore	Android Keystore provides security guarantees	Yes
S&P1.30	The FIDO cryptographic keys will be stored in the Android KeyStore	-	Yes
S&P1.31	For the registration process the authenticator will generate a Key Registration Object: hash of the FCH, the generated public key and some other values. These values will be signed by the attestation key. (the detailed structure of	-	Yes

	this message is described in FIDO UAF protocol section 3.4)		
S&P1.32	For the registration process the FIDO client will obtain the FacetID of the requesting application (ReCRED) and will verify if the FacetID is authorized for the AppID as described in FIDO AppID and Facet Specification.	Compliance with the FIDO UAF specification	Yes
S&P1.33	The FIDO Client should implement TLS binding	-	Yes
S&P1.34	The FIDO client will check the integrity of the deregistration request and if it does not follow the specifications from the FIDO UAF protocol section 3.4.6.2 will reject it.	Compliance with the FIDO UAF specification	Yes
S&P1.35	For the registration process the FIDO Client must send ASM Request only to the authenticator selected by the user as specified in the FIDO UAF Authenticator-Specific Module API.	Compliance with the FIDO UAF specification	Yes
S&P1.36	The mobile application must ensure that only credentials of the same owner are restored in the mobile device (prevent "planting" of false credentials)	-	Yes
S&P1.37	All information sharing from the device to third parties must be monitored and audited.	Increased accountability.	Yes
S&P1.38	The debug facilities of a production TEE must either be disabled, or be controlled by an element that itself meets, or exceeds, the security requirements of the TEE.	This requirement places no restrictions on debug capabilities for system components (including the REE) that cannot access assets of the TEE.	Yes
S&P1.39	The TEE must be instantiated through a secure boot process using assets bound to the System-on-Chip and isolated from the REE.	The integrity and authenticity, gained through secure boot, must extend throughout the lifetime of the TEE and retained through any state transitions in the system, such as power transitions or core migration.	Yes

10.1.3. Operational Requirements

#	Operational Requirements	Rational / Comments	Mandatory or Not
O1.1	The user must register her identity to the device.	-	Yes

O1.2	User registration must happen when the trusted computing base of the device is not compromised	-	Yes
O1.3	Authentication should be fast (e.g., < 1 second)	-	Not
O1.4	The user device shall collect the passive behavioral patterns without the user's interaction.	Behavioral factors may be passive or active: Active behavioral factors need user's interaction (e.g. typing pattern). Patterns for Passive behavioral factors, such as mobility are collected over time during a non-transparent process for the user.	Yes
O1.5	The behavioral profiles acquisition shall be optimized in the manner of battery and bandwidth consumption.	-	Yes
O1.6	The identity attributes are grouped in homogenous tabs (e.g. personal details, contact details, job details).	Better UX since the user won't have to scroll through a big list of identity attributes.	Yes
O1.7	The device must have Android 4.4+	Security issues with previous Android versions.	Yes
O1.8	The TEE operations must be optimized in the manner of resources consumption.	E.g. power/battery consumption.	Yes
O1.9	The TEE operations are transparent to user.	User shall not be able to identify the exact interference of the TEE due to the smooth user experience provided by the ReCRED app menu.	Not
O1.10	The TEE must deliver high performance and availability.	The TEE operations must be executed fast in a secure and accurate way, at any given time.	Yes

10.2. Identity Consolidator

The Identity Consolidator is the most important component within the ReCRED ecosystem. It is responsible to provide a wide variety of features to end-users and other entities. As documented in D4.1 the Identity Consolidator consists of the following components:

- Physical Identity Acquisition Module
- Online Identity Acquisition Module

- Account Management Module
- Credential Management Module
- Identity Management Module (includes the identity profile management and the consent management modules)
- Storage API and Identity Repository
- 3rd Party API

These components alongside with their functional requirements, security & privacy requirements and operational requirements are described in distinct subsections below.

10.2.1. Functional Requirements

Physical Identity Acquisition Module

The Physical Identity Acquisition Module performs vertical identity binding. It is responsible for binding the real-world identity of a user to verifiable identity attributes. This module will be implemented as an application on smart trusted-computing-enabled devices and as a web application.

Physical Identity Acquisition Process

The acquisition process will be implemented as a web and mobile application. The acquisition process involves the acquirement of physical identity documentation of the user. The user has to capture, through his device's camera, images of his real-world identity and his face. Afterwards, the process enables the extraction and verification of the user's desired identity attributes (such as identity number, full name, date of birth, etc.). This is achieved, by requiring from the user to crop the corresponding parts from the captured image of his identity. Furthermore, this module enables the acquirement of additional physical characteristics of the users (e.g., his address).

Code Number	**D4.2.2.1.1 -T243**
Business Value	**High**
Title	**Implementation of document submission for the Physical Identity Acquisition Process**
Description	**As a** user **I want** to be able to submit a physical document **so that** I can verify my real-world identity
Acceptance Criteria	1. The process should support a wide variety of documentation types such as ID, Passport, Student Card, etc.

	2. The process should support differences in the documentation structure. For instance an ID from Cyprus might be completely different from an ID from another European country. The process should be transparent to such differences. 3. After the successful submission and verification, the identity attributes will be stored to the IDC's repository by using the Storage API.

Code Number	**D4.2.2.1.2 -T244**
Business Value	**High**
Title	**Implementation of listing documents on the Physical Identity Acquisition Process**
Description	**As a** user **I want to** be able to see my document submissions **so that** I can see the acquired data and the verification status
Acceptance Criteria	1. All of the user's document submissions should list with adequate details 2. The user should be presented with the option to withdraw a submitted document.

Code Number	**D4.2.2.1.3 - T245**
Business Value	**High**
Title	**Implementation of viewing/managing documents on the Physical Identity Acquisition Process**
Description	**As a user** **I want** to be able to see my document submissions **so that** I can see the acquired data and the verification status
Acceptance Criteria	1. The user should be given with the option to update documents, thus triggering a new acquisition and verification process

	2. The user should be given with the option to delete submitted documents 3. The procedure should make use of the Storage API in order to access information from the IDC's repository.

Code Number	**D4.2.2.1.4 - T489**
Business Value	**High**
Title	**RFID (NFC) Identity card reading**
Description	**As a** user **I want** to be able to scan my RFID identity card **so that** I can verify my identity in an easy way
Acceptance Criteria	1. The whole procedure should be as easy as possible. 2. The user should be able to scan his RFID-enabled card using a mobile device that has NFC functionality.

Code Number	**D4.2.2.1.5 - T490**
Business Value	**High**
Title	**Real-time video presentation of ID documents using WebRTC**
Description	**As a** user **I want** to be able to present my ID documents through real-time video presentation **So that I** can prove my identity to another user in the web.
Acceptance Criteria	1. The video and sound quality of the conversation should be as high as possible so that the verifier can clearly see the Identity documents that the other user is showing to him.

	2. In order for a communication to be initiated the verifier should also have an account to our platform and has already proved his identity.

Physical Identity Verification Process

The physical identity acquisition module uses smart trusted-computing-enabled devices (e.g., mobile device) which will acquire the physical characteristics and identity documentation of the users. The devices also use trusted software paths in order to securely and verifiably capture through the device’s camera images of a user and his documentation. Additionally, the physical characteristics of a user (such as location) will be extracted. All this information is then transferred into the identity verification sub-module. This sub-module contains processes that verify the collected identity information of the user. These processes include automated verification (such as OCR) or peer-to-peer (crowdsourced) verification. Automated verification (such as face recognition and optical character recognition) is established on the acquired photos of the user. Peer-to-peer verification (such as crowdsourcing techniques) also takes place to verify that the information on the acquired photos matches the declared personal ID information and physical characteristics. As soon as the verification is completed, all the verified independent identity attributes are stored in the Identity Repository of the ID consolidator.

Code Number	**D4.2.2.2.1 -T91**
Business Value	**Medium**
Title	**Implementation of Peer-to-Peer verification**
Description	**As a** ReCRED administrator/user **I want to** be able to perform audits **so that** I can verify parts of user's identity attributes
Acceptance Criteria	1. The system will assign audits of partial identity attributes of a user, to other users of the system or to dedicated ReCRED administrators. For example, it will require from the auditor to verify whether the cropped photo that contains the name (or part of) on the identity document matches the name (or part of) that the user declared. 2. The whole procedure should be as privacy-preserving as possible. A peer-to-peer auditor should not be able to infer a user's identity by the peer audits that he will undertake.

	3. According to all the audits, the IDC should be able to decide on whether should trust a specific identity attribute. If yes, then the IDC will make use of the storage API in order to store the identity attributes to the identity Repository. 4. This process should be done in a way that will provide incentives for the users to undertake audits.

Code Number	**D4.2.2.2.2 - T92**
Business Value	**High**
Title	**Implementation of Automated Verification Process**
Description	**As the** Identity Consolidator **I want** to be able to automatically verify the user’s identity **so that** I can speed-up the process for my users and also provide verification guarantees
Acceptance Criteria	1. The user should be able to submit documents in an image format, and the Physical Identity Acquisition Module will identify the document and extract the text, using optical character recognition (OCR). 2. The Physical Identity Acquisition Module should be able to automatically verify that a face is included in the acquired user photos by using face detection techniques. 3. The Physical Identity Acquisition Module should make use of face recognition techniques so that it can automatically determine whether the face on the provided documents matches the face of the user.

Code Number	**D4.2.2.2.3 - T221**
Business Value	**High**
Title	**Implementation of address/location verification process**
Description	**As the** Identity Consolidator

	I want to be able to capture user's locations **so that** I can verify his address/location
Acceptance Criteria	1. The system should periodically capture user’s location so that it can compare it with the defined address. 2. The system should be able to provide a trust score of how likely a location is the actual address of a user. 3. This process can be turned off if the user desires so (privacy-preserving option) 4. The administrator should be able to see the status of the location verification process 5. Upon successful verification of an address the Physical Identity Acquisition module should make use of the Storage API in order to store the verified address to the Identity Repository.

Code Number	**D4.2.6.6.5 - T491**
Business Value	**High**
Title	**Face-to-face ID verification by trained (f2f) auditors**
Description	**As a** trained (f2f) auditor **I want** to have a verification form/console **so that** I can declare the details and the result of a face-to-face verification
Acceptance Criteria	1. This form should allow the trained auditor to easily search and find the profile of the user with his declared physical identity information in our system. 2. In the case when a f2f is not successful the trained auditor should be able to declare the reason. 3. The verification form should clear and easy to be filled.

	4. The verification form should let the auditor know of all the identity documents that the user has submitted to our platform so that he will request to see them from the user.

Online Identity Acquisition Module

The Online Identity Acquisition module obtains identity information from various ID Providers, such as online social networks like Facebook or Twitter, using Facebook Connect or OpenID Connect/OAuth2. The main challenge in developing this module is to acquire user information integrated from a user’s online accounts that user wishes to connect to the IDC. Once the IDC obtains access, it can collect the identity from the various ID Providers and it processes this information using the identity integration module to determine their validity. We envision the use of an automated and a user-assisted way of binding online accounts. These 2 ways are described below.

User-assisted online binding tool

Code Number	**D4.2.3.1.1 -T416**
Business Value	**High**
Title	**Implementation of operation for connecting an online account to the IDC**
Description	**As a** user **I want to** be able to connect an existing online account to the IDC **so that** the account can be horizontally binded
Acceptance Criteria	1. In order to bind a user's account, the IDC will act as a Service Provider and the Service Provider will act as the Identity Provider. The IDC will retrieve the user's attributes using the OpenID Connect specification. 2. The user should provide his consent to the Service Provider (which acts as the IdP in this case) and the IDC will retrieve the user's identity attributes from the Service Provider that the user has the account. 3. Optionally the user can transfer other identity attributes to the IDC if the user has declared that he trusts the IDC to holds its information. These information will be normalized by using the Identity Integration module 4. Upon the successful connection of the account, the user should be notified by the IDC. Once the IDC, has the user's username (for the specific Service Provider) then the account is binded to the IDC and the user can perform various operations (e.g., providing proof of account ownership)

	5. The procedure should not allow the connection of the same online account to multiple IDC users.

Code Number	**D4.2.1.8 - T628**
Business Value	**High**
Title	Transfer Identity Attribute Values from a Mobile Connect Identity provider to the Identity Consolidator
Description	**As a** user **I want** to able to transfer the values of identity attributes from an Mobile Connect Identity Provider to the Identity Consolidator **So that** I can be issued credentials for those attributes, directly from the Identity Consolidator
Acceptance Criteria	1. By using Mobile connect the user attributes can be labeled with LoA 4 to the IDC given that the user authenticates via an enhanced with TEE capabilities FIDO UAF authentication. 2. The user can select one or more attribute values maintained by an Identity Provider and transfer them to the Identity Consolidator. This will be achieved by using Mobile Connect/OpenID Connect. In this case, the Identity Consolidator acts as the Service Provider (Relying Party) for the Mobile Connect Identity Provider. This will be performed by invoking the Online Identity Acquisition module. 3. The application asks the user to authenticate to the selected Mobile Connect Identity Provider and authorize the transfer of data to the Identity Consolidator. It displays error messages in case of authentication or authorization failure. 4. Upon successful completion, the application displays a success message to the user. 5. The application doesn’t transfer any attribute values if the user doesn’t trust the Identity Consolidator (highest degree of privacy). The user will need to provide at-least proof his real life name, surname and Identity document number.

	6. In case of any other error, the application displays a comprehensible error message to the user.

Code Number	**D4.2.2.1.1 - T420**
Business Value	**High**
Title	**Implementation of operation for providing a proof of account ownership**
Description	**As a** user **I want to** be able to create a proof of account ownership **so that** I can use it to verify the possession of my account to 3rd parties
Acceptance Criteria	1. The account should be connected to the Identity Consolidator (see T416) 2. The process should call the Credential's Management Module internal API in order to issue a credential that should be used to prove account ownership 3. The credential should be able to be transferred secured to the user's device. Additionally, the credential will be securely stored to the user device's credential storage module.

Code Number	**D4.2.3.1.4 - T419**
Business Value	**Medium**
Title	**Implementation of operation for disconnecting an account from the IDC**
Description	**As a** user **I want to** be able to disconnect an account from the IDC **so that** I can no longer use it for my consolidated IDC account

Acceptance Criteria	1. Any identity attributes related to the specific account should be deleted from the consolidator's repository 2. Any credentials that were issued about proving account ownership for this particular account should be revoked. To achieve this, the procedure will call the credential management module's internal API.

Code Number	**D4.2.3.1.3 - T418**
Business Value	**High**
Title	**Implementation of operation for transferring user data to the IDC**
Description	**As a** user **I want to** be able to transfer identity attributes from an already connected account to the IDC **so that** I can enhance my IDC account
Acceptance Criteria	1. The whole procedure should follow the OpenID Connect specification. In this case the Identity Consolidator will act as the Service Provider and the online service will act as the Identity Provider. 2. The process should make use of the Storage API in order to store the identity attributes to the consolidator. If the user does not trust the consolidator then the actual data will not be stored to the identity repository 3. The identity attributes will be normalized according to the specification of the Identity Integration Module 4. After the successful transfer of identity attributes the user will be notified about the operation's outcome.

Code Number	**D4.2.3.1.2 - T417**

Business Value	**Low**
Title	**Implementation of operation for viewing connected accounts**
Description	**As a** user **I want** to be able to view my connected accounts **so that** I can have a better overview of my IDC account status
Acceptance Criteria	1. The user should be presented with a highly intuitive interface that can clearly depict the different accounts that the user has binded to the consolidator 2. The user should be able to view which attributes are contributed to the IDC by which account. 3. The process should utilize the Storage API in order to retrieve the required data from the Identity Consolidator's Repository

Non-assisted online identity binding tool

Code Number	**D4.2.3.2 - T81**
Business Value	**Medium**
Title	**Implementation of non-assisted online identity binding tool**
Description	**As** the Identity Consolidator **I want** to be able to automatically match different accounts that belong to the same user **so that** I can automatically perform horizontal online identity binding
Acceptance Criteria	1. The whole procedure should make use of web techniques (e.g., crawling techniques, social network analysis techniques, etc.) in order to detect with certain probability that two different accounts belong to the same user. 2. The whole procedure should take into consideration the terms-of-use of the online account providers. The crawler avoid attracting the attention of the online account providers service (e.g., facebook)

Identity Integration Module

The Integration module is responsible for verifying, standardizing and normalizing user information. It manages the spectrum of information elements that a user has on various online social networks. A typical user has to deal with multiple online identities, which usually are stored in online social networks and managed independently of one another. Identity Integration is the process of providing a unified view of the data spread across different sources.

We have to recognize that existing online identity systems might be around for a long time, which leads us to find other solutions for resolving three key issues arising from managing data across disparate online identity systems:

1. **Duplication of information**. Identity information is often duplicated in multiple Identity Providers.
2. **Lack of integration**. The complete view of a given user's attributes, credentials and privileges are often distributed across multiple identity providers, using heterogeneous protocols and technologies.
3. **Lack of veracity assessment and inference of missing attributes**. It is hard to determine the confidence in the veracity of identity information from a multitude of heterogeneous Identity sources.

The identity integration module is responsible for aggregating and connecting the acquired online and physical user attributes, as well as for inferring the veracity of the claimed identity attributes via means of statistical data analysis techniques. The identity integration module is also responsible for assigning confidence scores for the veracity of the attributes and for labeling identity attributes based on their origin. Additionally, the confidence score should be accompanied by a Level of Assurance Score (LoA) 1-4 for identity attributes based on their origin and the LoA of the user session. For example, the Identity consolidator should be able to tell Service Providers that user A is more than 18 years old with confidence 90%, and LoA 4. Alternatively, the IDC should be able to tell Service Providers that it has acquired the age information of user A through a named Identity provider and let the Service Provider determine how much it trusts the identity information of that provider.

Identity Integration Capture Module

Code Number	**D4.2.9.1.1 – (T478 and T481)**
Business Value	**Medium**
Title	**Direct information Retrieval from Physical and Online Identity Acquisition Module for the Identity Integration Module**
Description	**As an** Identity Integration Module

	I want to be able retrieve information from the Physical and Online Identity Acquisition Module **so that** I normalize, assign confidence score and store the user information
Acceptance Criteria	1. The Identity Integration module should be able to successfully connect to the Physical and Online Identity Acquisition Module in order to retrieve information that were captured either by online account or after verification of physical documents. 2. The communication between these module should happen using a REST Interface. All the calls should require authentication in order to avoid unauthorized use.

Identity Integration and Normalization Module

Code Number	**D4.2.9.2.1 – T476**
Business Value	**Medium**
Title	**Data Transformation for the Identity Integration Module**
Description	**As the** Identity Consolidator **I want** to be able to transform collected information **so that** I can store them to a unified and normalized schema
Acceptance Criteria	1. The normalized schema should contain the origin of the information. 2. The normalized schema should take into account the schema of the underlying Identity Repository on the IDC so that they are compatible.

Confidence Score Generator and Level of Assurance Module

Code Number	**D4.2.9.4 – T482**
Business Value	**High**
Title	**Labeling identity attributes and assigning confidence scores and Level of Assurance (LoA) for the identity integration module**

Description	**As the** Identity Consolidator **I want to** be able to calculate a confidence score for each identity attribute and assign a LoA 1-4 **so that** I know which attributes are more likely to be legit and verified
Acceptance Criteria	1 The LoA for a specific attribute is assigned based on the method the user verified the attributes. For example an attribute verified physically by the user will have LoA 4 2. The confidence score will take into account information from multiple IDC components such as the Physical and Online Identity Acquisition. 3. The whole procedure will be based on statistical analysis in order to calculate a confidence score for each identity attributes. 4. The confidence scores for each identity attributes should be stored to the Identity Repository of the IDC using the Storage API.

Account Management Module

The Account Management Module within the ID Consolidator is responsible to manage the status of online accounts and to expose this information to authorized parties within the ReCRED framework.

Degree of Privacy Selection and Enforcement

Users should be able to configure their account with the Identity Consolidator. An example is when a user wants to increase/decrease the levels of privacy within the IDC service. A user will have the option to choose between highest and lowest degree of privacy.

Highest degree of privacy: In this case, the consolidator acts as a discovery service under a Federated Identity model. Specifically, with the exception of the user’s real life name, surname and Identity document number, the consolidator can only store the information that a user has an attribute and the respective Identity provider that holds it. When a Service Provider needs an attribute, the consolidator redirects him to the respective Identity Provider. In such way, the Service Provider obtains the attributes without the need of revealing any attributes to the ID consolidation service thus providing a more privacy-preserving solution.

Least degree of privacy: In this case, the consolidator will store a user's attributes on his service as well as credentials to access external service providers. For this feature, the Account Management Module interfaces with the Identity Profile Management and the Credential Management module.

Code Number	D4.2.1.3.1 – T218

Business Value	**High**
Title	Implementation of operation for providing the highest degree of privacy
Description	**As a** user **I want to** be able to choose the degree of privacy against the ID consolidator **so that** I can choose not to trust the consolidator and get a privacy preserving solution.
Acceptance Criteria	1. The ID consolidator holds the credential back-ups of the user encrypted, and the master key is maintained by the user. 2. The ID consolidator does not store any identity attributes within its Identity Repository. Instead, it stores information that specifies which Identity Providers know which attributes for the users. In that way, the IDC can act as an IdP discovery service. 3. In case that the user has previously selected the least degree of privacy option, then the IDC should delete all the stored identity attributes from its Identity Repository. 4. The user should authenticate with the highest LoA with the IDC in order to perform this action

Code Number	D4.2.1.3.2 – T219
Business Value	**High**
Title	Implementation of operation for providing the least degree of privacy
Description	**As a** user **I want to** be able to maintain the least degree of privacy against the ID consolidator **so that** I can choose to fully trust the ID consolidator
Acceptance Criteria	1. The ID consolidator cannot be compromised and it won’t misuse the user’s personal information.

	2. The ID consolidator holds the user’s identity attributes in its Identity Repository. 3. In this mode, the IDC can act as an Identity Provider and provide identity attributes to Service Providers by using the OpenID Connect specification. 4. The user should authenticate with the highest LoA with the IDC in order to perform this action

Operations for managing behavioral profiles

A user should be able to fully control the behavioral profiles they will provide to the ReCRED platform. They will be able to configure their settings depending on their needs, through this configuration interface. Note that the content of the behavioral profiles will not be stored on the IDC. Instead, the Account Management Module will redirect the user to the BAA where he will perform view and manage operations.

Code Number	**D4.2.6.6.1 - T226**
Business Value	**Low**
Title	**Implementation of operations for viewing behavioral profiles**
Description	**As a** user **I want** to know what behavioral profiles are available in the ReCRED platform **so that** I can decide which one I should use for each online service
Acceptance Criteria	1. The user should be able to view all the available by ReCRED behavioral profiles (e.g. gait, typing, location etc.) and their main characteristics with information related to their security and privacy, efficiency and availability as well as about the attributes they require and the time needed for them to be working (i.e. if they need training time)

Code Number	**D4.2.6.6.2 - T227**
Business Value	**Medium**

Title	**Implementation of operations for activating/deactivating behavioral profiles**
Description	**As a** user **I want** to be able to either activate or deactivate a particular behavioral profile **so that** a specific behavioral profile can be used or not be used by service providers
Acceptance Criteria	1. The activation and deactivation process should be in the granularity of Service Provider-specific behavioral profile. For example, a user should be able to deactivate a behavioral profile so that is not be used for a specific Service Provider within the ReCRED platform 2. The user should be able to activate/deactivate behavioral profiles as much times as he wants 3. After the activation/deactivation of the behavioral profile, the change should be applied immediately and the behavioral profile should be or not be used for all subsequent second factor authentication attempts.

Code Number	**D4.2.6.6.3 - T228**
Business Value	**Medium**
Title	**Implementation of operations for selecting behavioral profile for specific service provider**
Description	**As a** user **I want** to be able to select a specific behavioral profile for a specific service provider **so that** I can use the behavioral profile in order to perform second factor authentication to Service provider
Acceptance Criteria	1. The user should be able to select multiple behavioral profiles for a specific service provider 2. A specific behavioral profile should be able to be selected by multiple service providers

Code Number	**D4.2.6.6.4 - T229**
Business Value	**Low**
Title	**Implementation of operations for viewing history of behavioral profiles accesses**
Description	**As a** user **I want** to be able to view a history of the behavioral profile accesses **so that** I can verify that everything is ok with regard to the behavioral profiles
Acceptance Criteria	1. The user should be presented with a highly intuitive user interface that will contain the following: i) service provider that wants to use the behavioral profile,; ii) time and date of the access; and iii) outcome of the second factor authentication 2. The user should be able to filter and sort this history according to : i) date; ii) specific service provider and iii) specific behavioral profile, iv) outcome of the request

Code Number	**D4.2.6.6.5 - T230**
Business Value	**Medium**
Title	**Implementation of operations for deleting a behavioral profile**
Description	**As a** user **I want to** be able to completely delete a behavioral profile **so that** it will not be used by the ReCRED platform
Acceptance Criteria	1. The deletion method should ensure that all entities of the ReCRED platform are aware of the deletion of the behavioral profile. Specifically, the Behavioral Authentication Authorities and the Identity Consolidator 2. The deletion method should ensure that the behavioral profile that is about to be deleted will be removed from all the active behavioral profiles for a specific Service Provider that is currently used for second factor authentication.

Identity Provider Registration

Code Number	**D4.2.6.2 - T190**
Business Value	**High**
Title	**Implementation of ID provider registration**
Description	**As an** Identity provider Administrator **I want to** be able to easily create an account to the ReCRED’s ID consolidation service for the Identity Provider **so that** I can use the ReCRED system
Acceptance Criteria	1. The ID consolidator must check and verify the Identity Provider before completing the registration. 2. The ID consolidator must receive a list of supported IdP attributes during the registration and store this information to its repository. 3. During the registration of the IdP to the IDC, the consolidator should store all the necessary endpoints for the Identity Provider. For instance, the IDC should store the OpenID Connect endpoints, the FIDO server endpoints etc. These endpoints will be stored to the Identity Repository by using the Storage API.

Behavioral Authentication Authority registration

Code Number	**D4.2.6.3 - T191**
Business Value	**High**
Title	**Implementation of Behavioral Authentication Authority registration**
Description	**As a** Behavioral Authentication Authority Administrator **I want** to be able to easily create an account to the ReCRED’s ID consolidation service **so that** I can use the ReCRED system to provide second factor behavioral authentication services to ReCRED users
Acceptance Criteria	1. The ID consolidator must check and verify the Behavioral Authentication Authority before completing the registration.

	2. The ID consolidator must receive a list of Behavioral Authentication Authority attributes during the registration and store this information to its Identity repository. Such information will include the type of the behavioral profile that the Behavioral Authentication Authority supports. This information will be stored by utilizing the consolidator's Storage API. 3. The exchange of information between the BAAs and the Identity Consolidator will make use of the OpenID Connect protocol.

User to ID provider and Behavioral Authentication Authority mapping

Code Number	**D4.2.6.4 -T192**
Business Value	**High**
Title	**Implementation of user to ID provider and BAA mapping**
Description	**As** the Identity Consolidator **I want** to be able to maintain user to ID provider and user to BAA mappings **so that** I can redirect Service Providers to ID providers for acquiring identity attributes and to BAA’s for performing behavioral authentication
Acceptance Criteria	1. The mappings should be stored in the Identity Repository of the Identity Consolidator. 2. This information will be accessed by calling the IDC’s Storage API.

Operations for viewing history of account locking changes

Code Number	**D4.2.6.5 - T220**
Business Value	**Low**
Title	**Implementation of operations for viewing history of account locking changes**
Description	**As a** user **I want** to have a place to see history of all services latched on and off **So that** I know if some suspicious behavior happened.

Acceptance Criteria	1. The user can access a history of services latched off and on. The user should be presented with adequate information regarding the latch on or off. For example, this should include when, where and other statistics regarding the latched on or off operation.

Account recovery mechanisms

The user is presented with a list of the accounts that he has and from there he is able to recover the secret keys (e.g., private keys) to a new device (e.g., after a device failure). If the user loses his device, it is the Account Management Module that is responsible for guiding the user through the recovery process. To this end, it needs to interface with the Credential Management Module.

Code Number	**D4.2.6.7 - T290**
Business Value	**High**
Title	**Recover credentials**
Description	**As a** User **I want** to be able to perform a credential recovery **so that** I have my credentials to my mobile phone
Acceptance Criteria	1. User recovers credentials through the account management module (AMM) of the IDC 2. AMM lists the user all his accounts and guides him to the process of recovery 3. AMM uses credential management module (CMM) if it backed the credentials, else it redirects user to the ID provider recovery site

Deletion of user's account from the ID Consolidator

Code Number	**D4.2.6.8 - T194**
Business Value	**High**
Title	**Implementation of deletion of user's account from the ID Consolidator**

Description	**As a** user **I want** to be able to easily delete my account from the ReCRED’s ID consolidation service **So that** I do not have to worry about the privacy of my personal identity information when I will stop using the platform.
Acceptance Criteria	1. The ID consolidator must verify that the user who requests the deletion is the holder of the account. 2. The service must verify that all the personal identity information of the user (such as identity attributes, cryptographic credentials, etc.) has been successfully deleted from the ReCRED platform. 3. The service should allow the user to create an account after the deletion when he desires so 4. The user should authenticate with the highest LoA against the Identity Consolidator in order to perform this action.

User Account Management console

Code Number	**D4.2.6.11 - T324**
Business Value	**High**
Title	**User Account Management Console**
Description	**As a** user **I want** to have access to my account information in an easy and friendly way **so that** I can configure my preferences and edit my information related to my profile
Acceptance Criteria	1. The user should be able to access a user friendly interface where all the related functions to his account and profile will be available and configurable in a straightforward way 2. The user should be able to control how a BAA tracks him (typing/location etc.)

3. The user should be able to control how often he sends behavioral info

4. The user should be able to control whether the BAA can lock him out if he behaves weirdly

5. The user should be able to control whitelists/blacklists of service providers that can query the BAA (whether the user behaves as usual, via openid connect)

6. The user should be able to view, delete, activate/deactivate behavioral profiles

7. The user should be able to view history of behavioral profiles accesses

8. The user should be able to manage his Behavioral profile for specific online service. Users will have the ability to choose which of their behavioral profiles will be accessed or not by each online service.

9. The user should be able to select from a list of the accounts. in order to recover the secret keys to a new device

10. The user should be able to view all the connected online accounts and the status of each account (latched/unlatched).

11. The user should be able to manually latch / unlatched accounts

12. The user should be able to set policies to automatically latch / unlatched accounts.

13. The user should be able to view history of latch / unlatched accounts changes

14. The user should be able to delete the user account from the ID Consolidator and the BAA.

Identity Federation Sub-module

The Account Management Module works together with the ID Profile Management module to provide Federated ID services by enabling ID providers to query the IDC for certain attributes that the Service Providers have requested, and they do not maintain themselves. The IDC either responds with the attribute value in case it stores it, or redirects the requesting Service Provider to the appropriate ID provider who maintains that attribute. In other words, this module acts as an attribute discovery service to instantiate a Federated Identity solution.
The Identity Federation is used when a Service Provider asks an Identity provider for a proof of identity, and the Identity Provider does not know that identity. In this case, the Identity provider redirects the user to the IDC for further actions. Subsequently, the IDC either responds with the

identity attributes (if he has the attributes, and the user trusts the consolidator) or redirects the Service Provider to the appropriate Identity Provider who maintains the requested attributes. The Identity Consolidator acts as an Identity provider discovery service, for the Identity Federation.
The Identity Consolidator has a complete list of attributes for each Identity Provider. In the case the Identity Consolidator does not know the value to the user's attribute, it will notify the primary Identity Provider to identify other Identity Providers the Service Provider should contact.
The Identity Federation will be the only way that the IDC interacts with the user and the IDPs in case of the highest degree of privacy. However, the Identity Federation will also be used in less than the highest degree of privacy modes, as it will not always be the case that the user has transferred all his attributes from the IDPs to the IDC.

Code Number	**D4.3.6.13 - T492**
Business Value	**High**
Title	**Implementation of Identity Federation Submodule**
Description	**As the** Identity Consolidator **I want to** be able to redirect Service Providers to the appropriate Identity Providers **so that** the Service providers can acquire data from Identity Providers that the IDC is unaware of
Acceptance Criteria	1. The Identity Consolidator should initially check if the required identity attributes are stored in its Identity Repository. If yes, then the IDC can decide to provide the requested identity attributes by itself and not delegate the request to others Identity Providers. In the case where the user does not trust the consolidator or the consolidator does not maintain the requested attributes the other acceptance criteria apply. 2. The Identity Consolidator should query the Identity Repository in order to find the appropriate Identity provider and its OpenID connect endpoints. In case that the endpoints are not stored in the ID consolidator, the IDC should query the Identity Provider and retrieve the OpenID Connect endpoints. This should be according to the OpenID Connect discovery service. 3. The OpenID Connect endpoints will be returned to the Service provider so that it can query the respective Identity Provider and acquire the identity attributes by using the OpenID Connect specification.

Continuous Authentication using BAAs and Latch

In addition to on-demand behavioral authentication where the BAA acts as an ID provider, the BAA also performs continuous authentication (i.e., using the browsing behavior), while having an open session with the IDC (account management module), and proactively Latches out the accounts when needed.

Code Number	**D4.2.6.14 - T468**
Business Value	**High**
Title	**Continuous Authentication and Latch**
Description	**As a BAA** **I want to** continuously monitor user behavior **So that** the ID Consolidator can trigger account locking upon detection of suspicious activity
Acceptance Criteria	1. The BAA continuously monitors user behavior and sends signs of unusual behavior to the Identity Consolidator. 2. The IDC should be able to decide whether to lock/unlock specific accounts according the received data and the pre-defined locking policies that are defined within the Account Management Module. 3. Communication between the BAA and the ID Consolidator should be performed by utilizing the IDC's 3rd Party API

Account locking functionality in Account Management Module

Code Number	**D4.3.6.1 - T25**
Business Value	**High**
Title	**Account Locking on Account Management Module**
Description	**As an** Identity Consolidator **I want** to be able to keep the status (looked/unlocked) of user accounts

	So that I can expose this information to Service Providers.
Acceptance Criteria	1. Service providers should be able to query for the status (locked/unlocked) of a user account. This information will be exposed through the 3rd Party API of the IDC that will call the Account Management’s Module Internal API. 2. Users should be able to query for/set the status of their accounts 3. The user or the ID Consolidator should be able to set the status of a user account. 4. The Authentication Management module should make use of the Latch clone software in order to perform the accounts locks and unlock. This functionality should be also provided as a REST API

Account Locking Policies

A user may define arbitrary policies to automatically lock or unlock an account. For example, a user may define a policy to lock his corporate email account over weekends and to lock his e-banking account at night. ReCRED also allows the ID Consolidator to act on behalf of the user and lock his online accounts if the ID Consolidator detects a high risk of account compromise. For example, if the ID consolidator learns of a number of failed login attempts at U's e-banking account, it may decide to lock that account and also other accounts belonging to the same user. The ID consolidator may learn of failed login attempts via the Behavioral Authentication Authorities. The parameters to trigger account locking (e.g., number of failed authentication attempts, their frequencies, which other accounts to lock, etc.) may be chosen by the user.

Code Number	**D4.2.6.15.1 - T524**
Business Value	**Medium**
Title	**Implementation of the user-defined Account Locking Policies**
Description	**As a** user **I want** to be able define policies for locking/unlocking an account **so that** I can decide when my accounts should be locked/unlocked
Acceptance Criteria	1. The user should be able to define policies for specific accounts or accounts of specific risk level.

	2. The IDC should allow the user to define a wide variety of policies for each account. For instance an account may have multiple lock policies (e.g., lock on weekends and on weekdays after midnight). 3. The user should be able to remove/modify/add locking policies at any time. These policies will be stored to the Identity Repository by utilizing the IDC's Storage API. 4. The policies should support an action field which can be either lock or unlock. 5. The policies should have a field that sets them as active or inactive. 6. The user will be able to view policies suggested by the IDC admin and enabling them, after editing them to fit their specific needs. 7. The policies should allow the inclusion of BAA results. For instance, a policy should specify that a specific account will be locked after a particular behavioral authentication failure.

Code Number	**D4.2.6.15.2 - T522**
Business Value	**Medium**
Title	**Implementation of IDC-defined suggested Account Locking Policies**
Description	**As an** IDC administrator **I want** to be able to suggest to the IDC users policies for locking/unlocking accounts that are essential for the account security **so that** I can provide adequate security to my users' accounts
Acceptance Criteria	1. The defined policies can be generic, based mainly on the risk level of the account and they should not be account/user - specific. 2. The administrator should be able to remove/modify/add locking policies at any time. These policies will be stored to the Identity Repository by utilizing the IDC's Storage API. 3. The policies should support an action field which can be either lock or unlock.

4. The policies should allow the inclusion of BAA results at a Behavioral Type level. For instance, a policy should specify that a specific account will be locked after a particular behavioral authentication failure.

Mobile Connect Proxy Service

For this module, the Service Provider will only trust the Identity Consolidator as the contact point to the Mobile Connect Telco providers federation that determines the Telco Provider for a given identifier. Additionally, the Identity Consolidator will act as an OpenID Connect ID Provider that stores attributes retrieved via Mobile Connect sessions.

The Identity Consolidator invokes the GSMA apigee API Exchange-enabled discovery service on a trusted Mobile Connect Telco provider. The API Exchange is used as the federation mechanism for Mobile Connect. It ensures that Service Providers (in this case the IDC) only need to connect to one operator of a federation to get access to customers of all connected operators. Therefore, the Identiy Consolidator as a Service Provider, uses the GSMA APIGEE API Exchange Discovery Service of the trusted Mobile Connect provider to ask for the Telco Provider for a given phone number or IP or MSISDN, etc. The Identity Consolidator will call the APIGEE API of the discovered Telco provider to initiate a Mobile Connect session between the user and the Telco Provider.

The next steps will be for the user to authorize the transfer of attributes between the Mobile Connect Provider and the Identity Consolidator, and the IDC will store those Mobile Connect-retrieved attributes. Finally, the IDC then continues to act as the ID Provider for the OpenID Connect session with the non-Mobile Connect enables Service Provider.

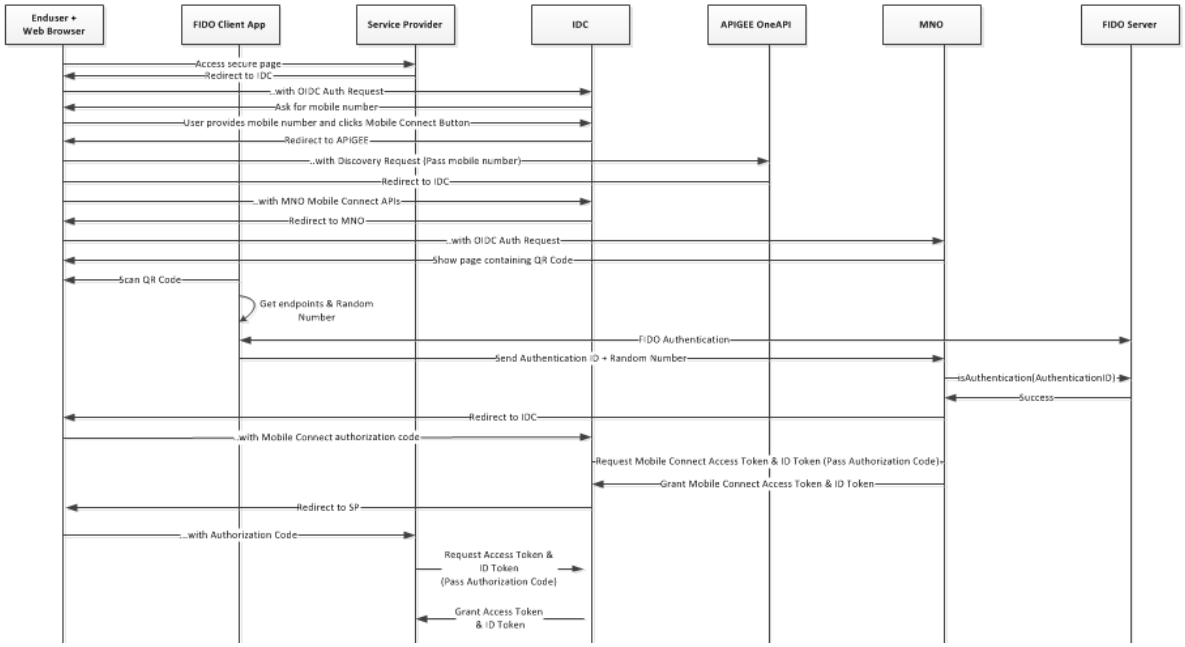


Figure 3: Mobile Connect Proxy Service

Code Number	**D4.2.6.12 - T381**
Business Value	**High**
Title	**Implementation of Service Provider that is not Mobile Connect-enabled**
Description	**As a** user **I want to** be able to retrieve attributes validate by Telco providers **So that** I can obtain LoA 4 identity attributes without having to register as a Service Provider with the Mobile Connect API exchange.
Acceptance Criteria	1. The Service Provider will only trust the ID Consolidator as the contact point to the Mobile Connect Telco providers federation that determines the Telco Provider for a given identifier. 2. The Service Provider is unaware of the Mobile Connect infrastructure. But it knows that there are LoA 4 attributes that can be retrieved from Mobile Connect providers or less than LoA 4 attributes that are only reliably known to MC providers, e.g., phone number, whether last bill was paid and how much it cost, etc. These attributes should be described in the OIDC

scope in such a way that the IDC knows that it needs to invoke MC to retrieve them, e.g., first- name-loa4-mc.

3. The Identity Consolidator acts as an OpenID Connect ID Provider that stores attributes retrieved via Mobile Connect sessions. If the IDC does not have a fresh cached version of the attribute, the user opens two simultaneous sessions: one OIDC session with the Service Provider that is not Mobile Connect-enabled and one Mobile Connect session with the IDC as service provider.

4. The user inputs as OIDC username to the SP the username it uses at the IDC. It inputs as username for the MC session the identifier used by MC, e.g., phone, MSISDN, IP, etc.

5. The Identity Consolidator invokes the GSMA APIGEE API Exchange-enabled discovery service on a trusted Mobile Connect Telco provider. The API Exchange is used as the federation mechanism for Mobile Connect. It ensures that Service Providers (in this case the IDC) only need to connect to one operator of a federation to get access to customers of all connected operators.

6. The IDC (Service Provider) uses the GSMA APIGEE API Exchange Discovery Service of the trusted Mobile Connect provider to ask for the Telco Provider for a given phone number, IP, MSISDN, etc.

7. The IDC (Service Provider) calls the APIGEE API of the discovered Telco provider to initiate a Mobile Connect session between the user and the Telco Provider.

8. The user authorizes the transfer of attributes between (see user story T627) the Mobile Connect Provider and the IDC.

9. The IDC stores those Mobile Connect-retrieved attributes for a predetermined period that depends on the staleness of the attributes.

10. The IDC then continues to act as the ID Provider for the OpenID Connect session with the non-Mobile Connect enabled Service Provider

Credential Management Module

The Credential Management Module provides the required functionality for the issuance and management of cryptographic credentials (CC). When a user requests the issuance of a CC, this module is responsible to retrieve the appropriate identity attribute from the identity repository, issues the credential and sends it to the user’s device. Additionally, it allows the user to maintain different degrees of privacy against the Identity Consolidator by giving him the option to back up the issued

credentials to the consolidator. In such a case, the authentication level should also increase. Below we list a non-exhaustive list of the functional requirements for the Credential Management Module.

End user operations with the Credential Management Module

Code Number	**D4.2.7.1.1 - T196**
Business Value	**High**
Title	**Implementation of Credential Issuance**
Description	**As** a user **I want** to be able to issue cryptographic credential directly to my mobile device from the ID consolidator. **so that** I can use it to access service provider that request you to prove a particular attribute (e.g., that the user is a student)
Acceptance Criteria	1. Verify that the cryptographic credential has been issued and sent to the mobile device of the user. 2. Verify that the credentials have been stored securely to the mobile device of the user (utilize device's TEE for secure storage). 3. Verify that the issued credential has been deleted from the ID consolidator (if the user does not desire to back it up on the Identity Consolidator). 4. All connections for transferring data should be tunneled through gateSAFE

Code Number	**D4.2.7.1.2 - T197**
Business Value	**High**
Title	**Implementation of operation for listing supported attributes per Identity Provider**
Description	**As** a user **I want to** be able to see a list of the Identity Providers alongside with a set of supported attributes **so that** I can have a global view of the Identity Providers

Acceptance Criteria	1. The user should be able to view the list of Identity Providers and the list of supported attributes for each Identity Provider. To do, the module should make use of the IDC’s Storage API in order to get information from the Identity Repository.

Code Number	**D4.2.7.1.3 - T198**
Business Value	**Low**
Title	**Implementation of operation for listing issued credentials**
Description	**As** a user **I want to** be able to see a list of the issued credentials to my device **so that** I can check my credentials
Acceptance Criteria	1. Successfully display though an intuitive interface the details of the issued credentials

Code Number	**D4.2.7.1.4 - T199**
Business Value	**Low**
Title	**Implementation of operation for viewing issued credential details**
Description	**As** a user **I want to** be able to select an issued credential **so that** I can see the details of the credential
Acceptance Criteria	1. The user should be able to view for a specific credential the issued date, the expiration date, the issuer, whether it has been backed up to the IDC, a history of the credential's uses, etc.

Code Number	**D4.2.7.1.5 - T200**

Business Value	**High**
Title	**Implementation of operations for reissuing an expired credential**
Description	**As a** user **I want to** be able to reissue an expired credential **so that** I can still use the expired credential
Acceptance Criteria	1. A new credential must be issued, by the same authority and with a new expiration date 2. The IDC and the user's device should synchronize with the change of the expired credential 3. A user should be able to activate an option (through the user settings) to authorize the IDC to automatically attempt to reissue expired credentials

Code Number	**D4.2.7.1.8 - T203**
Business Value	**High**
Title	**Implementation of operation for backing up credentials**
Description	**As** a user **I want to** be able to back-up my credentials to the IDC **so that** I am more robust to device failure
Acceptance Criteria	1. The credentials should be transferred to the IDC through a secure channel. To achieve this all connections should be tunneled through gateSAFE. 2. The process should allow the user to set settings in order to automatically back-up credentials to the IDC. 3. The credentials should be stored to the Identity Repository by utilizing the consolidator Storage API.

Code Number	**D4.2.7.1.9 - T204**
Business Value	**High**
Title	**Implementation of operation for restoring credentials**
Description	**As** a user **I want** to be able to restore credentials from the IDC to my device **so that** I have the credentials directly to my device (useful when a device is reset or a new device is purchased)
Acceptance Criteria	1. The credentials must be transferred through a secure channel. This will be achieved by tunneling all connections through gateSAFE. 2. The credentials should be securely stored on the user's device by utilizing the device's TEE. 3. This operation should be accessible by the consolidator 3rd Party API

Code Number	**D4.2.7.1.10 - T205**
Business Value	**High**
Title	**Implementation of operation for erasing credentials**
Description	**As** a user **I want** to be able to erase specific credentials **so that** I can update my current credentials or remove credentials that do not apply anymore
Acceptance Criteria	1. The user should be able to delete credentials from the IDC, from her device or both.

Identity provider administrator operations with the Credential Management Module

Code Number	**D4.2.7.3.1 - T212**
Business Value	**High**
Title	**Implementation of operations for managing supported attributes**
Description	**As an** Identity Provider Administrator **I want to** be able to manage the supported by the IDP attributes **so that** I can select which of those attributes are supported by the IDP
Acceptance Criteria	1. An IDP can issue cryptographic credentials only for templates for which all the required attributes are supported.

Code Number	**D4.2.7.3.2 - T213**
Business Value	**High**
Title	**Implementation of operations for issuing credentials**
Description	**As an** Identity Provider Administrator **I want to** be able to issue cryptographic credential directly to a user's mobile device **so that** the user can use it to access service provider
Acceptance Criteria	1. Verify that the cryptographic credential has been issued and sent to the mobile device of the user. 2. Verify that the credentials have been stored securely to the mobile device of the user. 3. The user should have the option to select if the issued credential should be backed-up at the Identity Consolidator or not.

Code Number	**D4.2.7.3.3 - T214**
Business Value	**High**

Title	**Implementation of operations for listing issued credentials**
Description	**As an** Identity Provider Administrator **I want to** be able to list all the issued cryptographic credentials **so that** I can check the issued credentials
Acceptance Criteria	1. This process should be able to list all the credentials that were issued by a specific Identity Provider. 2. The user interface for viewing the credentials should specify which credentials are backed-up on the Identity Consolidator 3. The user interface should include all the necessary statistics of the credentials (e.g., issued date, expiration date, etc.)

Code Number	**D4.2.7.3.4 - T215**
Business Value	**High**
Title	**Implementation of operations for revoking credentials**
Description	**As an Identity Provider Administrator** **I want to be able to revoke user credentials** **so that they cannot use their issued credentials**
Acceptance Criteria	**1. After the completion of this operation, the user should not be able to use the revoked credentials** **2. All the revoked credentials will be securely removed from the user's device** **3. If the credential is backed up at the IDC, the back-up of the revoked credential should be removed from the IDC or marked as "revoked"**
Code Number	**D4.2.7.3.5 - T216**
Business Value	**High**

Title	**Implementation of operations for viewing statistics**
Description	**As an** Identity Provider Administrator **I want to** be able to see statistics regarding issued credentials by IdP **so that** I have a clear view of the issued credentials
Acceptance Criteria	1. The administrator can check all the statistics regarding the credentials 2. The consolidator should offer a highly intuitive user interface for the identity provider administrator so that he can view the statistics for the credentials. Some examples of credentials are creation date, expiration date (if set), type of credentials, etc.

Operation for creating rules

Code Number	**D4.2.7.2.1 - T208**
Business Value	**High**
Title	**Implementation of operation for creating rules**
Description	**As a** Service Provider Administrator **I want** to be able to create rules **so that** I can grant access to a specific resource (e.g. access to the liquor department of an online store is allowed only for UK citizens that can provide a valid credential proving they are above a certain age)
Acceptance Criteria	1. A rule can include conditions on specific attributes (age>21 AND country="UK") 2. Each rule should contain a list of "trusted" IDP's for each attribute that is used on the rule

Operations for listing and applying rules

Code Number	**D4.2.7.2.2 - T209**

Business Value	**High**
Title	**Implementation of operations for listing and applying rules**
Description	**As a** Service Provider Administrator **I want to** be able to see a list of the created rules **so that** he can interact and make modifications to the rules
Acceptance Criteria	1. The list should include all the necessary details regarding the attributes and conditions 2. The administrator should be able to update a rule 3. The administrator should be able to deactivate a rule

Service provider administrator operations with the Credential Management Module

Code Number	**D4.2.7.2.3 - T210**
Business Value	**High**
Title	**Implementation of operations for viewing statistics**
Description	**As a** Service Provider Administrator **I want to** be able to see statistics regarding user accesses through credentials issued by ReCRED **so that** I have a clear view of usage of the issued credentials
Acceptance Criteria	1. The administrator can check all the statistics regarding the accesses to the service via the ReCRED issued cryptographic credentials.

Identity Management Module

The Identity Management module is the common framework that serves as a standard for the definition and representation of user identity attributes within a given online service. Identity

Management module is subdivided into two sub-modules, the identity profile management and the consent management.

In general, the Identity Management module provides an identity matrix containing the different type and range of identifiers, and unique identity attributes a user can have. Additionally, this module offers a protocol to transfer identity attributes between ID providers and at the same time guarantees the security in the transfer of such sensitive information. Furthermore, it gives users the option to create partial verifiable profiles, which consist of selected identity attributes of a user, to be presented to verifiers depending upon the context and the access control requirements. Furthermore, it allows users to define their consent for the management of their various identity attributes.

Identity Profile Management Module

This sub-module provides the user’s interface that allows the user to know and manage what each identity provider and Service Providers knows about them. It enables the user to transfer attributes between ID providers and between ID providers and the IDC using OpenID Connect sessions in which the destination ID provider acts as the Service Provider. When transferring attributes, the system abides to the policies defined within the identity consent management module. The transfer of attributes from ID providers to the IDC is performed by invoking functionalities of the online ID acquisition module. Furthermore, the user has the ability to delete an identity attribute from an IDP.

The user can only view, delete and insert new validated attributes that are accompanied with a certain LoA (see Authentication Management Module). The LoA of an attribute depends upon the identity proofing mechanism that was used to verify it. The LoA of a user session depends upon the authentication mechanism. The LoA of the transferred attributes is decided by the consolidator by taking into account the minimum LoA of the attribute and the user session. For example, a LoA 4 attribute transferred during a LoA 3 user session, is stored as a LoA 3 attribute at the destination ID provider.

It also enables the user to determine the risk of identity providers and Service Providers inferring information about them that they did not explicitly reveal to them. The value of identity attributes that were not explicitly revealed to an ID or Service provider can leak by statistically analyzing correlations between identity attributes, thus the risk will be calculated by using similar techniques.

Lastly, this module provides the required functionality to the user to create and manage partial verifiable profiles as described below.

De-anonymization Risk Management

Privacy awareness browser app and mobile application that inform the user about his risks of de-anonymization and identity data leakage due to authenticating with specific attributes to specific verifiers and to store specific ID attributes at ID providers. It enables the user to determine the risk of identity providers and Service Providers inferring information about him that he has not explicitly revealed. This information can leak by statistically analyzing correlations between identity attributes, thus the risk will be calculated by using similar techniques.

Implementation of Partial Verifiable Profiles

Users can group some of their attributes in profiles so that Service Providers may be offered only a selection of verified attributes instead of the entire collection of the user’s stored identity. For example, a user may choose to only prove that he/she is a citizen of the European Union, or that a User is a registered professional with the corresponding national Professional Association. The process should create a shareable URL that will be presented to the user. The link can be accessed directly by other users without the need of credentials.

Code Number	**D4.3.1.1.4 - T115**
Business Value	**High**
Title	**Implementation of Partially Verifiable Profiles**
Description	**As a** user **I want to** be able to create/modify/delete partially verifiable profiles **so that** I can prove to others my profile (e.g., 3rd parties)
Acceptance Criteria	1. The process should create a URL that will be presented to the user so he would be able to share it with other users 2. The URL should display a public web page where the user's profile will be displayed. 3. The process should easily allow the user to share the URL 4. The user should be able to select the type of URL (permanent, one-time, with expire date) 5. The process should allow the user to choose which identity attributes will be included to the partial verifiable profile. For example, a user might want to choose to create a profile for revealing his age and his nationality only. 6. After the creation of a verifiable profile the user should be able to modify it or delete.

Code Number	**D4.3.1.1.4.4 - T114**
Business Value	**High**

Title	**Implementation of public View Profile Web Page**
Description	**As a** user **I want** to be able to view the Partially verifiable profile that a user has created **so that** I can review the attributes and their values that the creator of the partially verifiable profile has published
Acceptance Criteria	1. The identity management application will display a web-page that will contain all the attributes (and their values) included in the partially verifiable profile exposed by the corresponding url. 2. The profile will be shown only if the partial verifiable profile has not expired.

Implementation of Identity Profile Back-end

Code Number	**D4.3.1.1.5.3 - T187**
Business Value	**High**
Title	**Implementation of De-anonymization Risk Management back-end.**
Description	**As a** user **I want to** get privacy risk indicators from both the ReCRED’s identity management web and mobile applications **so that** I can get the appropriate measures to protect my privacy
Acceptance Criteria	1. The identity management back-end should provide API methods to retrieve privacy risk indicators that define the risk of involuntary de-anonymization. 2. The identity management provides API methods to retrieve privacy risk indicators that define the identity attribute inference by verifiers that the user has not explicitly shown a specific attribute. 3. These methods will make use of statistical analysis techniques in order to calculate the risks for De-anonymization of specific attributes without the user's explicit consent.

Code Number	**D4.3.1.1.3.3 - T121**
Business Value	**Medium**
Title	**Search ID Providers per attribute**
Description	**As a** user **I want to** be able to search for ID Providers that maintain information regarding specific attributes of my identity **so that** I am aware of which ID Providers maintain data regarding the specified attributes of my identity
Acceptance Criteria	1. The identity profile management module should provide a REST API method to retrieve a list of available attributes from which the user selects the ones to be investigated 2. The identity profile management module should provide a REST API method to retrieve a list of ID Providers that maintain data regarding the specified attributes

Code Number	**D4.3.1.1.3.4 - T122**
Business Value	**Medium**
Title	**Search attributes per ID Provider**
Description	**As a** user **I want to** be able to search for identity attributes per ID Provider **so that** I can review the attributes that the selected ID Provider(s) maintain regarding my Identity
Acceptance Criteria	1. The identity profile management module should provide a REST API method to retrieve a list of available ID Providers from which the user selects the ones to be queried 2. The identity profile management module should provide a REST API method to retrieve a list of attributes (with the attribute values) grouped by (specified) ID Provider

Code Number	**D4.3.1.1.3.5 - T123**
Business Value	**High**
Title	**Delete attribute from ID Provider or the Identity Consolidator**
Description	**As a** user **I want to** be able to delete an attribute from an ID Provider or the Identity Consolidator **so that** I can remove this attribute from the collection of attributes that the selected ID Provider(s) or the IDC maintain regarding my Identity
Acceptance Criteria	1. The identity profile management module should provide a 3rd Party REST API method to retrieve a list of available attributes from which the user selects the ones to be deleted 2. The identity profile management module should provide a 3rd Party REST API method to remove the specified attributes from the specified ID Providers or the IDC (Identity Repository). 3. The Identity providers should expose a REST API to the identity profile management module for deleting attributes. 4. The profile management module should call the corresponding Storage API call to delete the identity attribute from the Identity Repository.

Implementation of Identity Profile Mobile Application Front-end

Code Number	**D4.3.1.1.2.1 - T284**
Business Value	**High**
Title	**Manage Identity Data**
Description	**As a** user **I want to** be able to view and manage my identity attributes on the IDC

	so that I can centrally update my identity data and keep them synchronized across different IDPs
Acceptance Criteria	1. The user can see a list of all the identity attributes supported by the IDC and the current value for each attribute (in the case that he trusts the consolidator and the consolidator maintains the values), along with its verification status. 2. The identity attributes are grouped in homogeneous tabs (e.g. personal details, contact details, job details). 3. The user can update (or fill-in or erase) one or more identity attributes and update requests are sent to all the IDPs that maintain the updated identity attributes. 4. The application validates any updated attribute values (not empty mandatory attributes, values comply with the attribute types, etc.) and displays comprehensible messages guiding the user to resolve the errors. 5. Upon successful completion, the application displays a success message to the user. 6. In case of any system errors, the application aborts the update and displays comprehensible error messages to the user. 7. All operations for retrieving data from the Identity repository should use the IDC’s Storage API.

Code Number	**D4.3.1.1.2.2 - T285**
Business Value	**Medium**
Title	**View Identity Attributes Shared with Service Providers**
Description	**As a** user **I want to** be able to see which identity attributes are shared with which service provider **so that** I am aware of what the various service providers know about me
Acceptance Criteria	1. The user can select an identity attribute and see a list of all the service providers that have access to the selected attribute. Alternatively, the user can select a

	service provider and see a list of all the identity attributes that are shared with the selected service. 2. This operation should make use of the IDC’s Storage API.

Code Number	**D4.3.1.1.2.3 - T286**
Business Value	**Medium**
Title	**View Identity Attributes Maintained by Identity Providers**
Description	**As a** user **I want** to be able to see which identity attributes are maintained by which IDP **so that** I can then transfer values among different IDPs or between an IDP and the IDC
Acceptance Criteria	1. The user can select an identity attribute and see a list of all the IDPs that maintain the selected attribute. Alternatively, the user can select an IDP and see a list of all the identity attributes that are maintained by the selected IDP. 2. This operation should make use of the IDC’s Storage API.

Code Number	**D4.3.1.1.2.4 - T287**
Business Value	**High**
Title	**Transfer Identity Attribute Values from an IDP to the IDC**
Description	**As a** user **I want to** be able to transfer the values of identity attributes from an IDP to the IDC **so that** I can enhance my IDC account with my identity attributes
Acceptance Criteria	1. The user can select one or more attribute values maintained by an IDP and transfer them to the IDC. This will be achieved by using OpenID Connect. In this

	case, the IDC will act as the Service Provider (Relying Party) for the Identity Provider. 2. The application asks the user to authenticate to the selected IDP and authorize the transfer of data to the IDC. It displays error messages in case of authentication or authorization failure. 3. Upon successful completion, the application displays a success message to the user. 4. The application doesn’t transfer any attribute values if the user doesn’t trust the IDC (highest degree of privacy) 5. In case of any other error, the application displays a comprehensible error message to the user.

Code Number	**D4.3.1.1.2.5 - T288**
Business Value	**High**
Title	**Transfer Identity Attribute Values among the IDPs**
Description	**As** a user **I want to** be able to transfer the values of identity attributes among IDPs **so that** I don’t have to verify the same identity attribute to all my IDPs separately
Acceptance Criteria	1. The user can select one or more attribute values maintained by an IDP and transfer them to one or more selected IDPs. 2. The application asks the user to authenticate to the selected IDP and authorize the transfer of data to other IDPs. It does so by invoking OpenID Connect where the destination IDP acts as Service Provider. It displays error messages in case of authentication or authorization failure. 3. The application verifies that the attribute values are transferred / obtained successfully. 4. Upon successful completion, the application displays a success message to the user.

	5. Before the transfer of any attribute values, the application checks if the transfer abides by the policies defined by the user and the IDP (through the Consent Management Module). If it does not abide, the transfer is not allowed. 6. In case of any other error, the application displays a comprehensible error message to the user.

Code Number	**D4.3.1.1.2.6 - T289**
Business Value	**High**
Title	**Delete Identity Attribute Values from an IDP**
Description	**As a** user **I want to** be able to issue requests for identity attributes deletion from one or more IDPs **so that** I can determine which IDPs I trust to hold my sensitive personal information
Acceptance Criteria	1. The user can select one or more identity attributes and request the deletion of those attributes from a set of IDPs and/or the IDC. 2. The application verifies that the issued requests are obeyed by the IDC and the IDPs. 3. Upon successful completion, the application displays a success message to the user. 4. In case of any error, the application displays a comprehensible error message to the user.

Code Number	**D4.3.1.1.2.7 - T189**
Business Value	**Medium**
Title	**View de-anonymization risk indicators**

Description	**As a** user **I want** to get privacy risk indicators from the ReCRED’s identity management application **so that** I can take the appropriate measures to protect my privacy
Acceptance Criteria	1. The identity management application should be able to present the user with privacy risk indicators that define the risk of involuntary de-anonymization. 2. The identity management application should be able to present the user with privacy risk indicators that define the identity attribute inference by Service Providers that the user has not explicitly shown a specific attribute. 3. The user can select an attribute and see the risk indicators per unassociated ID Provider. 4. The user can select an ID Provider and see the risk indicators per unassociated attribute. 5. The user should have the option to enable or disable this functionality.

Implementation of Identity Profile Web Application Front-end

Code Number	**D4.3.1.1.5.2 - T188**
Business Value	**Medium**
Title	**Implementation of Risk Management web front-end**
Description	**As a** user **I want to** get privacy risk indicators from the ReCRED’s identity management application **so that** I can get the appropriate measures to protect my privacy
Acceptance Criteria	1. The identity management application should be able to present the user with privacy risk indicators that define the risk of involuntary de-anonymization.

	2. The identity management application should be able to present the user with privacy risk indicators that define the identity attribute inference by Service Providers that the user has not explicitly shown a specific attribute. 3. The user should have the option to enable or disable this functionality.

Implementation of Identity Consolidator and Identity Provider Account deletion

Code Number	**D4.3.1.1.6 - T296**
Business Value	**High**
Title	**Implementation of IDC and ID Provider Account deletion**
Description	**As a** user **I want to** be able to issue requests for account deletion from ID providers **so that I** maintain the privacy of my personal identity information when I will stop using the Identity Provider’s services
Acceptance Criteria	1. The ID consolidator must verify that the user who requests the deletion is the holder of the account 2. If the user chooses to delete ID Provider accounts, the service must verify that all identity attributes of the user have been successfully deleted from the selected Identity Providers

Consent Management Module

The Consent Management module allows users and IDPs to define their consent for their various identity attributes. Furthermore, the consent management module is subdivided into the following:

The Consent Management module will provide the user and the Identity provider with the ability to involve the LoA in the policy decision process.

- User-defined policy for attribute transfer and proof: Such functionality is used when the user wants to define policies about to which IDPs and verifiers, their attributes should be revealed. The Consent Management module will provide the user with the ability to involve the LoA in the policy decision process. For example the user may define that it does not wish to reveal their address to online social network services or any service provider under certain LoA.
- Identity Provider-defined policy for attribute transfer and proof: It is responsible for obtaining policies (with respect to what identity attributes can each verifier see) for individual attributes from identity providers ensuring that the Identity Consolidator reveals attributes to verifiers according to these policies. The Consent Management module will provide the identity provider with the ability to involve the LoA in the policy decision process. This is used, especially from ID Providers who do not wish certain attributes, or attributes with specific LoA, to be revealed to certain unauthorized parties or other identity providers. For example, the Social Security Administration (ID provider) provides the social security number that should be revealed only to reputable verifiers, such as banks. Or an IDP may decide that it does not want the attributes of its users to be proven using idemix/u-prove and that they should be proven through the IDP via OAuth instead (so that the IDP always knows where these credentials have been shown).

The credential management module is responsible for abiding by these set policies (for example not issue Idemix credentials to the device if the IDP specified so). The ReCRED authentication app running on the device also has to abide by this policy. The profile management module also has to respect the IDP's and the user's policies regarding attribute transfer between IDPs. Furthermore, the Identity Management module has access to the Identity Repository via the Storage API. It implements a REST API that allows users to manipulate their identity attributes maintained by the ID Consolidator. This API will be utilized both by a Web Application as well as a Mobile Application in order to accommodate a variety of User Interfaces and Devices (i.e. Desktop, Tablet, Smartphone).

Implementation of Mobile Application for Consent Management Module

Code Number	**D4.3.1.2.3.1 - T430**
Business Value	**High**
Title	**Create new Consent Policy**
Description	**As a** user **I want** to be able to create new policies regarding the attributes that are revealed to IDPs and Service Providers **so that** I have total control on the protection of my personal data

Acceptance Criteria	1. The user can select an identity attribute and then select one or more IDPs and Service Providers that he wants to block - not reveal his identity attributes to them (among a list of already connected IDPs and Identity Providers). 2. The user cannot create more than one policy per identity attribute. 3. The user can save his selection as a new policy.

Code Number	**D4.3.1.2.3.2 - T431**
Business Value	**High**
Title	**View List of Consent Policies**
Description	**As a** user **I want to** be able to view a list with all the policies that I have created **so that** I can further edit them or delete them
Acceptance Criteria	1. The user can see a list with all the policies he has created. 2. For each policy, the respective identity attribute is displayed, along with the date it was created.

Code Number	**D4.3.1.2.3.3 - T432**
Business Value	**High**
Title	**Edit an Existing Consent Policy**
Description	**As a** user **I want** to be able to edit a policy I have created **so that** my policies are always up to date
Acceptance Criteria	1. The user can select a policy (identity attribute) from the policies list, in order to edit it.

	2. The user sees the current IDPs / Service Providers that are blocked for the selected attribute. 3. The user can block additional IDPs / Service Providers. 4. The user can unblock any of the blocked IDPs / Service Providers. 5. The user can save the updated policy. 6. If no IDPs / Service Providers were blocked, the policy is practically deleted (it won’t show in the list of active policies).

Code Number	**D4.3.1.2.3.4 - T433**
Business Value	**High**
Title	**Delete an Existing Consent Policy**
Description	**As a** user **I want to** be able to delete a policy I have created **so that** my policies are always up to date
Acceptance Criteria	1. The user can swipe left a policy (identity attribute) from the policies list, in order to delete it. 2. The deleted policy won’t show in the list of active policies.

Implementation of Web Front-End for Consent Management Module

Code Number	**D4.3.1.2.4 - T294**
Business Value	**High**
Title	**Implementation of Web Front-End for Consent Management Module**
Description	**As a** user

	I want to be able to access the consent for identity attributes **so** that I can define my consent for the various identity attributes through a simple user interface
Acceptance Criteria	1. Successfully access consent for identity attributes using a web interface. 2. Successfully edit any consent for identity attributes 3. Successfully save any changes to consents for identity attributes

Implementation of Back-End for Consent Management Module

Code Number	**D4.3.1.2.5 - T295**
Business Value	**High**
Title	**Implementation of Back-End for Consent Management Module**
Description	**As a** user **I want to** be able to access the consent for identity attributes **so that** I can define my consent for the various identity attributes through a simple user interface
Acceptance Criteria	1. Define policies about to which IDPs and Service Providers, the users attributes should be revealed 2. Obtain policies for individual attributes from identity providers ensuring that the Identity Consolidator reveals attributes to Service Providers according to these policies.

Implementation of User-defined-policy for identity attribute transfer and proof

Code Number	**D4.3.1.2.1 - T108**
Business Value	**High**

Title	**Implementation of User-defined Policy for Identity Attribute Transfer and Proof**
Description	**As a** user **I want** to have my consent policies enforced **so that** my identity attribute values are not revealed to IDPs / Service Providers that I have blocked
Acceptance Criteria	1. Whenever the user tries to transfer an attribute value among different IDPs, this value is not transferred to IDPs in case that the user has defined policies that prohibit this. 2. The user cannot reveal an attribute value, and thus prove an identity attribute to a Service Provider, if he has blocked the Service Provider for this attribute. 3. The consent policies should allow the user to explicitly involve the LoAs of online services. For example, a user might not want to reveal attributes to a service that is below a specific LoA. 4. The user should be able to involve attributes LoAs (or confidence scores) in the consent policies. For example, a user might not want to reveal attributes that are below a certain Confidence Score.

Implementation of Identity-provider-defined policy for attribute transfer and proof

Code Number	**D4.3.1.2.2 - T106**
Business Value	**High**
Title	**Implementation of Identity-provider-defined Policy for Attribute Transfer and Proof**
Description	**As an** IDP **I want to** have my consent policies enforced **so that** certain attributes values are not revealed to unauthorized parties or other identity providers

Acceptance Criteria	1. Whenever a user tries to transfer an attribute value from IDP A to IDP B, this value is not transferred if IDP A has blocked IDP B for this attribute. 2. The IDC cannot reveal an attribute value to a verifier if the IDP that holds the attribute value has blocked the Service Provider for this attribute. 3. A user cannot issue credentials for an identity attribute using a specific protocol (e.g. u-prove) if the IDP that holds the attribute has blocked the specific protocol. 4. The IdP should be able to involve LoA of other IdPs in the policies. For example, an IdP might not want to reveal attributes to other entities that are below a certain LoA

Code Number	**D4.3.1.2.6 – T647**
Business Value	**High**
Title	**Implementation of Access Control Reasoning Tool for Consent Management Module**
Description	**As an** IDP **I want to** have my consent policies enforced **so that** certain attributes values are not revealed to unauthorized parties or other identity providers
Acceptance Criteria	1. The policies should be XACML compliant. The implementation should be based on the Reasoning tool that was demonstrated during the Wi-Fi pilot 2. The policies should be able to take into consideration the different IdPs and Service Providers of the ReCRED ecosystem. For example, the tool should allow the block of attributes reveal to a particular IdP or SP. 3. The policies should be able to take into consideration the different LoAs of IdPs and Service Providers of the ReCRED ecosystem. For example, the tool should allow the block of attributes reveal to a particular IdP or SP that is below a specific LoA. 4. The policies should be able to take into consideration the different LoAs or confidence scores for each identity attribute. For example, the tool

should allow the block of attributes, which are below a particular LoA, reveal to a particular IdP or SP

Authentication Management Module

The ID Consolidator offers a versatile Authentication Management Module (AMM), which supports multiple authentication methods, with each method offering a different Level of Assurance (LOA) and allowing access to different categories of the user’s data and different actions. The supported authentication methods comply with the following Levels of Assurance defined by the National Institute of Standards and Technology (NIST), in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. Of course, the token methods allowed for each given level are also allowed for all of its lower levels.

Using the Authentication Management Module mobile application, the user has to register with the Identity Consolidator (IDC), up to a given authentication LoA which depends on the proofs of his identity he has provided and whether his device and Identity Providers support the appropriate soft or hard cryptographic tokens. This can be achieved by using the Physical Identity Acquisition Module to provide proofs of real-life identity, combined with proofs from the Online Identity Acquisition Module. Upon registration, the Identity Consolidator issues' FIDO credentials on his device.

Alternatively, a user may register at a given LoA if he provides via OpenID Connect proof that he owns an account with a certain Idenity Provider (IdP) for the given LoA and the IDC trusts that IdP at this level. For example, the IDC may trust a Telco to provide LoA 4, so a user will be considered LoA 4 if he uses Mobile Connect to connect his Telco account with the IDC and uses OAuth2 to transfer his real-life identity information from the Telco to the IDC.

The user authenticates to the IDC primarily by using his IDC-issued FIDO credential. Depending on the authentication method, the user is authenticated up to a certain LOA, which is decided by the IDP following the NIST guidelines[7]. For example, if the user authenticates to the IDC solely by using his IDC-issued FIDO credential, he is considered authenticated at LoA 2. If he also uses FIDO+OIDC with another ID provider, he is considered authenticated at LoA 3. If he uses Mobile Connect that uses OIDC and two different SIMs from the same or different Telco's (multiple hard tokens), he is considered LoA 4. Therefore, the chosen IdPs and the method via which authenticates to it determines the LoA. As soon as the user is authenticated and the LOA has been determined, then he can view, transfer or delete attributes depending on his session’s LoA. In particular, the Identity provider may optionally set policies to restrict the access to attributes by the user, depending on his session LoA.

[7] Burr, William E., et al. "Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology-Special Publication 800-63-1." (2012).

For example, if the user chooses to authenticate to the ID Consolidator by signing in to his Facebook account (through a username / password challenge), the user is authenticated with LOA 1. In this case he can only perform actions or view identity attributes for which the ID providers have specified that they allow access with LOA 1. If the user wants to be granted access to additional functions and/or data, then he has to authenticate by choosing a method that offers a higher LOA. For example, he can choose to authenticate using his IDC FIDO credential and a Mobile Connect Provider which can provide a LoA between 3 and 4. If a user is authenticated at LoA 3, then he can access all attributes that the ID providers have specified that can be accessed when the user session is LoA 3. Nevertheless, the ID Consolidator and the IDPs may employ additional policies to regulate access to the identity attributes according to the authentication type) and data sensitivity.

Please note that as soon as the user is authenticated to the IDC and a certain IDP, the user, through the Identity Profile Management Module, can initiate the transfer of identity attributes from the IDP to the ID Consolidator. Importantly, those attributes are labeled with the minimum LoA of the LoA they had at the origin IDP and the LoA of the user session (See Identity Management Module).

The AMM provides some recovery mechanisms for cases where users are unable to login to theirs ID Consolidator accounts (e.g., forgot their master password). Such mechanisms consist of a set of security questions that were defined during the registration with the ID Consolidator, SMS verification and prove of possession of online accounts (such as Facebook, Google, etc.,) via well-known protocols (such as FacebookConnect, OpenID Connect, etc.).

The AMM implementation will be based upon the OpenAM identity solution. All the aforementioned features will be checked against the current implementation of OpenAM and we will provide extensions to cover all the scenarios that are required by ReCRED.

The LoA can be achieved as follows:

- Password tokens can satisfy the LoA 1 and LoA 2.
- Soft cryptographic tokens may be used for LoA 1 to 2,
- If Soft cryptographic tokens are combined with a password or biometric then LoA 3 can be achieved (e.g., FIDO UAF authentication).
- Hard tokens that are activated by a password or biometric can satisfy assurance requirements for LoA 4 (FIDO UAF enhanced with TEE capabilities for storing keys).

Code Number	**D4.2.1.10 – T73**
Business Value	**High**
Title	**Access attributes based on User Session LoA**
Description	**As a** user

	I want elevate my LoA to LoA 4 **So that I can** access attributes in the Identity Consolidator with LoA 4
Acceptance Criteria	1. LoA 4 attributes can only be access using an enhanced with TEE capabilities FIDO UAF authentication. 2. The user will access the Identity Consolidator using single authentication factor for LoA 2 or multifactor authentication for LoA 3. 2. Initialize authentication with the Telco providers using Mobile Connect. The Identity Consolidator will contact the GSMA gateway to discover the Telco providers for the given phone numbers. 3. The Telco provider(s) will authenticate the user using SMS authentication and respond to the Identity Consolidator 4. The Identity Consolidator based on the responses of the Telco providers will elevate the User session to LoA 4.

User registration with the Identity Consolidator

Code Number	**D4.2.1.1 - T193**
Business Value	**High**
Title	**Implementation of user's registration with the ID Consolidator**
Description	**As a** user **I want** to be able to easily create an account to the ReCRED’s ID consolidation service **So that** I can make use of all the features that ReCRED offers (such as Physical Identity Acquisition, binding of multiple online accounts, etc.)
Acceptance Criteria	1. The ID consolidator must check that the user that wants to register is unique and there is no registered user with the same personal information. In particular the user will need to provide and proof his real life name, surname and Identity document number. 2. The service must verify that an email confirmation has been sent to the email address that the user declared.

	3. The service must verify that all the declared identity information of the included passport and user’s photos are valid. In order to do that it will utilize the acquisition and verification features of the Physical Identity Acquisition module. 4. The user should be able to set up some basic configuration for his consolidator account (e.g., account locking policies, the degree of privacy of the consolidator, etc.) 5. The registration will make use of OpenAM's backend infrastructure because the Authentication Management Module is based on OpenAM. The IDC acts as the IdP with which the user explicitly registers via this functionality. 6. The user's registration will involves the registration with the FIDO server component that will run on the Identity Consolidator.

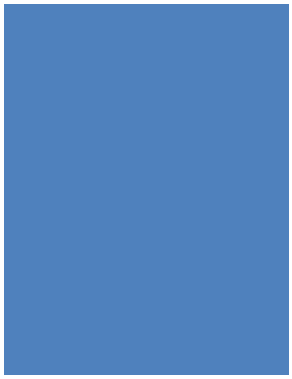
User registration with the Identity Consolidator using Mobile Connect

Code Number	**D4.2.1.9 - T629**
Business Value	**High**
Title	**Implementation of user's registration with the Identity Consolidator using Mobile Connect**
Description	**As a** user **I want** to able to easily create an account to the ReCRED’s ID consolidation service using Mobile Connect **So that** I can make use of all the features that ReCRED offers
Acceptance Criteria	1. The Identity Consolidator must check that the user that wants to register is unique and there is no registered user with the same personal information. 2. The service must verify that an email confirmation has been sent to the email address that the user declared. 3. The user's registration will involve the registration with the FIDO server component that will run on the Identity Consolidator.

	4. The User will provide at least one valid phone number. The Identity Consolidator will contact the GSMA gateway to identify the Telco provider for that specific phone number 5. The Identity Consolidator will contact the Telco provider(s) to verify the credentials of the user. 6. The Telco provider(s) will verify the user using an SMS verification code, and respond to the Identity Consolidator. 7. After a successful verification from the Telco provider(s), if the user is verified with one SIM he will be considered authenticated at LoA 3. If the user is verified by at-least two SIMs he will be considered LoA 4. 8. The user should be able to set up some basic configuration for his consolidator account (e.g., account locking policies, degree of privacy, etc.) 9. The registration will make use of OpenAM's backend infrastructure because the Authentication Management Module is based on OpenAM. The Identity Consolidator acts as the Identity Provider with which the user explicitly registers via this functionality. 10. The user's registration will involve the registration with the FIDO server component that will run on the Identity Consolidator.

User authentication using Mobile Connect

Code Number	**D4.2.1.7 - T627**
Business Value	**High**
Title	**User Authentication using Mobile Connect**
Description	**As a** user **I want** to authenticate to the IDC through a Telco Mobile Connect ID provider using a specific phone number, IP, MSISDN, etc. **So that** I access the Identity Consolidator
Acceptance Criteria	1. The IDC acts a Mobile Connect Service Provider. If it does not know the contact point of the Mobile Connect ID provider, it invokes Mobile Connect discovery using the Open Exchange apigee API invoked on a known Federated Mobile Connect Provider.



2. The Authentication can be performed using FIDO.

3. Authenticating using FIDO user session as authenticated at LoA 3.

4. Authenticating using FIDO that is powered with the TEE capabilities and the hardware processor security guarantees, labels the user session as authenticated LoA 4

Failover Authentication Mechanisms

This module will describe the Implementation of fail-over authentication mechanisms in a cases where the user loses access to the device and wants to restore his credentials on a new device, using:

- Mobile Connect
- Behavioral Authentication Authorities (BAA)

Normally a user can access the IDC just by proving the possession of the FIDO cryptographic key, which is bound to his device. This task concerns the case when the user has lost his device. In the case of loss or theft, which we treat similarly because loss may actually be theft, the following steps are performed:

If the user has no other device, he logs in to the IDC with his secure master password or security questions, and selects whether his device is lost/stolen or damaged, and whether he still has possession of his old SIM card. In doing so, he is granted only temporary and tentative access, which provides limited functionality. Tentative access is the Level of Assurance (LOA) LOA-1. In addition, the IDC invokes Latch to lock all the IDP accounts managed by the IDC. In particular, he cannot view or restore credentials, and he cannot view the attributes. He can only see who his IDPs and BAAs are. Importantly, he also has the ability to lock the account so that the thief cannot access the IDP via the stolen device.

Subsequently, the IDC acts as Service Provider authenticating the user through a Telco Identity Provider via Mobile Connect. Because the user no longer has his device, he cannot use FIDO to authenticate to Mobile Connect IDP, he has to authenticate to the IDP via SMS using his SIM card. In the case of a stolen or lost device, to ensure, the access attempt is performed by the legitimate user the IDC needs to confirm with the Mobile Connect IDP that the given Phone and his phone was reported lost and a new SIM was issued, via OpenID connect. In the case where the user declares the mobile damaged and still has possession of his old SIM card the IDC does not need to communicate with the Mobile Connect IDP.

By providing the IDC Master password and proving his identity to the Mobile Connect IDP, the user gains full access to the IDC to restore his credentials on a new device and reset the credentials to the compromised accounts.

Code Number	**D4.2.1.6.2.3 - T499**
Business Value	**High**
Title	**Implementation of Access Promoting from Tentative to Full IDC based on the BAA responses**
Description	**As the** Identity Consolidator **I want to** verify that the user in tentative mode is the real user **so that** I can provide him with full access to his account
Acceptance Criteria	1. Collect the responses from all BAAs through OpenID Connect. This will be achieved by utilizing the Consolidator's 3rd Party API. 2. Based on the responses calculate the probability that the user is the legitimate one 3. According to the defined Identity Consolidator Policies for account management (see Account Management Module), if the IDC is highly confident that the user is the legitimate one then it will be able to provide full access to the user

Code Number	**D4.2.1.6.2.1.2 - T501**
Business Value	**High**
Title	**Implementation of Tentative Access to Identity Consolidator without Backup Credentials**
Description	**As a** User **I want to** login to the system without using my master password **so that** I can regain access to the IDC's features in case that I don't have my master password
Acceptance Criteria	1. Been able to identify myself to the system using a new device 2. The user should be able to select that he is unable to login to the system using his master password

	3. The user should be prompted with a series of security questions so that the user can prove to the IDC his identity 4. The IDC might decide to require additional BAA verification means.

Code Number	**D4.2.1.6.2.1.1 - T500**
Business Value	**High**
Title	**Implementation of Tentative Access to Identity Consolidator with Backup Credentials**
Description	**As a** user **I want to** login to the Identity Consolidator system using my master password **so that** I can regain access to the Consolidator's features
Acceptance Criteria	1. The user should be able to login to the Identity Consolidator by providing the correct master password

Failover Authentication Mechanisms using Behavioral Authentication Authorities (BAA)

The user is now granted only temporary and tentative access, which provides limited functionality. The system will contact all the BAA authorities via OIDC to verify the identity of the user. The IDC running on the tentative mode will contact all the BAA available for the user through OIDC. After a BAA is contacted using a tentative mode, the BAA will also run in tentative mode and will request the backup credentials (i.e., a secure BAA recovery password), in order to provide full access. If the user is incapable to provide the backup credentials for the BAA, the BAA will initialize the authentication procedure based on the behavioral signatures of the specific user, for a required period of time. If the behavioral signatures match the user, the BAA will authenticate the user to IDC. A notification will also be sent to the user.

After the IDC collects the responses from the BAA of the user, it will decide if the user in tentative mode is the real user and provide full access or an imposter and lock the account.

Code Number	**D4.2.1.6.2.2 - T498**

Business Value	**Medium**
Title	Implementation of User Authentication on Tentative Access to BAA
Description	**As a** User **I want to** prove my identity on a BAA **so that** the BAA can enable my behavioral profiles (disabled because of tentative mode) so that I can use them for BAA verification
Acceptance Criteria	1. The user should be able to select between providing the backup credentials for the BAA or compare its behavioral profiles with his current behavior 2. The user should receive a notification regarding the outcome/decision of the BAA

Failover Authentication Mechanisms using Mobile Connect

In the case of damaged phone, where the user still has access to his SIM card, the IDC acts as Service Provider authenticating the user through a Telco Identity Provider via Mobile Connect. Because the user no longer has his device, he cannot use FIDO to authenticate to the Mobile Connect IDP, thus he has to authenticate to the IDP via SMS.

1. If the user is unable to access the IDC due to the loss or theft of his device, the system will provide him with an option to login using his master password. If the user is incapable to provide the master password, the user can initialize an alternative login procedure based on a series of security questions.
2. The IDC will ask the user if one of the devices is stolen or damaged. If the user selects a specific device then the IDC will invalidate the credentials for that particular device.
3. The user is granted only temporary and tentative access (LoA 1), which provides limited functionality. In particular, he cannot view or restore credentials, and he cannot view the attributes. Importantly, he also has the ability to lock the account so that the thief cannot access the IDP via the stolen device. The system will contact the Telco provider via OIDC to verify the identity of the user.
4. The Telco Mobile Connect provider will send an SMS verification code to the user. The device will use the SMS verification code to authenticate to the Telco provider using the SMS Custom Authentication Module. The Mobile Connect provider will respond to the IDC if is the real user or an impostor.
5. After the IDC received the responses from the Telco provider, it will decide if the user in tentative mode is the real user and will provide full access (in the case of Mobile Connect - LoA 4) or lock the account if it is an impostor.

In the case of loss or theft, which we treat similarly, because loss may actually be theft, and the user does not have his SIM card the following steps are performed:

1. The user needs to contact the Telco provider to invalidate his old SIM card and the FIDO credentials.
2. The user will need to physically visit the Telco provider to issue a new SIM card and the FIDO credential can be loaded to the new device.
3. The user will use these credentials to be verified to the IDC and gain full access (LoA 4).

Code Number	**D4.2.1.6.1 - T495**
Business Value	**High**
Title	Implementation of Failover Authentication Mechanisms using Mobile Connect
Description	**As a** User **I want to** use my SIM card (Mobile Connect) **so that** I can regain access to the IDC
Acceptance Criteria	1. The IDC should make use of the Mobile Connect protocol in order to verify that the user in the legitimate one. 2. The IDC should act as a Service Provider and the Telcos should act as Identity Providers 3. The user should be able to be notified for the outcome with a notification. 4. The Telcos will make use of the user's SIM card in order to verify the user's identity.

Storage API and Repository schema

The Storage API is the module that provides access to the Identity Repository to other components of the Identity Consolidator. Additionally, the Identity Repository is a central database where all the necessary information is stored. The Storage API interacts with the Identity Repository in order to perform CRUD operations on the repository. The Storage API will be exposed via a REST Interface and all the calls should be authenticated either by username/password or oAuth2.0 tokens.

The database schema should store at least the following:

1. User accounts information
2. Physical Identity information
3. Identity Providers information
4. User acquired locations information (for the purpose of verification)
5. Verification information for all the data
6. Audits information (for the purpose of verification)

7. Financial information (for the purpose of loan origination pilot)
8. Behavioral Authorities references
9. User to BAA and user to IdP mappings

Code Number	**D4.2.5.1 - T83, T86**
Business Value	**High**
Title	**Implementation of Storage API**
Description	**As the** Identity Consolidator **I want** to be able to store information that I acquire from the ReCRED ecosystem in an identity repository **So that** I can provide to users all the interesting features of ReCRED
Acceptance Criteria	1. The Storage API should support CRUD operations for all the tables that are in the Identity Repository 2. All the operations should be exposed using REST calls. Specifically, Create operations should use HTTP POST, Read operations should use HTTP GET, Update operations should use HTTP PUT and Delete operations should use HTTP DELETE. 3. Calls to the Storage API should be authenticated using a username/password combination or oAuth2.0 tokens 4. The Storage API should be only accessible by the Identity Consolidator's internal components only

3rd Party API

The 3rd party API is used for communication purposes between the Identity Consolidator component of ReCRED architecture and other 3rd parties. Such parties include other ReCRED’s components (e.g., Behavioral Authentication Authorities), Identity Providers and Service Providers that want to interact with the Identity Consolidator.

The 3rd party API offers, but is not limited to, the following operations:

- Service Providers should be able to interact with the Identity Consolidator component for the purpose of transferring trust between the services.
- Service Providers should be able to communicate with the Identity Consolidator component for the purpose of Two-Factor Authentication (2FA), if they desire. Specifically, the consolidator should be able to provide a reference to which Behavioral Authentication Authority (BAA) so that they can perform the additional authentication step.

- The BAA should be able to inform the Identity Consolidator component what behavioral aspects of each user they store. As a result, the consolidator always has a synchronized reference to the behavioral attributes that are stored in BAAs databases.
- The BAA should be able to inform the Identity Consolidator regarding the outcome (accept/reject) of an authentication attempt of a user to an online service. During this operation, the ID consolidator will check the defined securities policies and if are violated then it may lock some or all of user’s account.
- A Service Provider should be able to request the status of a user’s account. Specifically, a Service Provider should be able to query the Identity Consolidator which will reply with the account status (locked or unlocked).
- The ID consolidator should be able to issue cryptographic credentials directly to user’s devices. Additionally, if the user desire so, the consolidator should be able to back up those issued credentials.

Operations between User devices and ID consolidator

Code Number	**D4.2.11.3.1 - T415**
Business Value	**Medium**
Title	**Implementation of 3rd Party API call for issuing a cryptographic credential to a user's device**
Description	**As** a user **I want to** be able to call the Identity Consolidator **so that I** can issue a cryptographic credential to my device
Acceptance Criteria	1. The 3rd Party API should call the Credentials Management's module internal API in order to issue a new cryptographic credential 2. The process should allow to backup the credential to the IDC too if the user wants. Alternatively, the credential will be issued and stored only to the user's device. The IDC will not keep state of the credential. 3. The user's device should make sure that upon reception of the cryptographic credential that is will be stored in the device's cryptographic credentials secure storage. 4. The REST call should be tunneled through gateSAFE in order to provide adequate SSL protection. 5. The REST call should require authentication either by username/password or OAuth.

Implementation of operations between Service Providers and ID consolidator

Code Number	**D4.2.11.2.1 - T412**
Business Value	**Medium**
Title	**Implementation of 3rd Party API call to transfer trust between services**
Description	**As a** user **I want to** be able to inform the Identity Consolidator about my desire to transfer attributes between service providers **so that** trust between service providers can be transferred
Acceptance Criteria	1. The process should make sure that the source and destination service providers allow the exchange of identity attributes and that they are on the appropriate format 2. The process should inform the user whether the request was successful or not. For instance, the request might not be successful if one of the 2 involved service providers does not allow exchange of identity attributes. 3. The process should make sure that the accounts on both involved service providers are not locked. To verify this, the 3rd Party API will call the Account Management module's internal API 4. The REST call should be tunneled through gateSAFE in order to provide adequate SSL protection. 5. The REST call should require authentication either by username/password or OAuth.

Code Number	**D4.2.11.2.2 - T413**
Business Value	**Medium**
Title	**Implementation of 3rd Party API call for providing BAA's that have behavioral profiles for a user**

Description	**As a** Service Provider **I want to** be able to query the Identity Consolidator **so that I** can obtain a list of BAA's that maintain behavioral profiles for a particular user
Acceptance Criteria	1. The 3rd Party API should query the Identity Consolidator's repository through the storage API in order to obtain the list of BAA's that maintain behavioral profiles for the user 2. The result should be a JSON object which should contain the following: which user we getting information for, the list of BAA's and the appropriate behavioral profile type that they maintain other metadata about the BAAs. 3. The REST call should be tunneled through gateSAFE in order to provide adequate SSL protection. 4. The REST call should require authentication either by username/password or OAuth.

Code Number	**D4.2.11.2.3 - T414**
Business Value	**Medium**
Title	**Implementation of 3rd Party API call for checking the status of an account to a particular Service Provider**
Description	**As a** Service Provider **I want to** be able to check the status of a particular account **So that** I can verify if I should proceed with an authentication attempt or not.
Acceptance Criteria	1. The 3rd Party API should call the account's management module internal API in order to get the account status of a particular account to the specified Service Provider 2. The call should return a JSON object that contains the account's details and its status. If the account is locked then it should provide the timestamp of the lock

	(when the locked occurred) and if the lock was performed from the user or from the Identity Consolidator. 3. The REST call should be tunneled through gateSAFE in order to provide adequate SSL protection. 4. The REST call should require authentication either by username/password or OAuth.

Implementation of operations between BAA and ID consolidator

Code Number	**D4.2.11.1.1 - T410**
Business Value	**Medium**
Title	**Implementation of 3rd Party API call for informing IDC regarding behavioral profiles**
Description	**As** a BAA **I want to** be able to inform IDC regarding behavioral profiles that I have **so that** the IDC can have a holistic view of the behavioral profiles that are stored by the BAAs
Acceptance Criteria	1. The IDC should store such information to its repository (using Storage API) 2. The 3rd Party API should make use of the IDC’s core components internal APIs in order to provide this functionality 3. The REST call should be tunneled through gateSAFE in order to provide adequate SSL protection. 4. The REST call should require authentication either by username/password or OAuth.

Code Number	**D4.2.11.1.2 - T411**
Business Value	**Medium**

Title	**Implementation of 3rd Party API call for informing IDC regarding authentication attempts**
Description	**As a** BAA **I want** to be able to inform the Identity Consolidator about outcomes of authentication attempts **so that t**he Identity Consolidator can trigger account locks
Acceptance Criteria	1. The authentication attempts should be stored to the Identity Consolidator 2. The Identity Consolidator should check if the authentication attempt should trigger an account lock. If yes, then the 3rd Party API should call the Account Management Module's internal API in order to perform an account lock according to the details of the authentication attempt. 3. The (least) information that should be contained to the outcome of the authentication attempts is: service provider that the user tried to authenticate, which user is, a timestamp and the outcome of the authentication (reject/accept). 4. The REST call should be tunneled through gateSAFE in order to provide adequate SSL protection. 5. The REST call should require authentication either by username/password or OAuth.

Code Number	**D4.2.11.1.3 - T502**
Business Value	**Medium**
Title	**Implementation of 3rd Party API calls for informing ID consolidator for signs of unusual behaviour**
Description	**As a BAA** **I want to** be able to inform IDC about signs of unusual behaviour **so that** the IDC can continuously authenticate users from the received data from BAAs
Acceptance Criteria	1. The IDC should log all the signs of unusual behavior

	2. The 3rd Party API should make use of the IDC's Account management module in order to decide if an account should be locked (according to the defined policies) and to enforce the actual lock (using Latch) 3. The REST call should be tunneled through gateSAFE in order to provide adequate SSL protection. 4. The REST call should require authentication either by username/password or OAuth.

Deployment of gateSAFE on the Identity Consolidator

Code Number	**D4.2.12 – T592**
Business Value	**Medium**
Title	**Integration of gateSAFE on the Identity Consolidator**
Description	**As** the Identity Consolidator **I want to** be able to inform IDC regarding behavioral profiles that I have **so that** the IDC can have a holistic view of the behavioral profiles that are stored by the BAAs
Acceptance Criteria	1. The gateSAFE product of CSGN should be deployed to the Identity Consolidato 2.gateSAFE should be configured so that all connections to the back-end components that run on the Identity Consolidator are tunneled through gateSAFE. Also, the calls to the 3rd Party API should be configured so that are tunneled through gateSAFE 3. gateSAFE should be deployed in a docker container

10.2.2. Security & Privacy Requirements

#	Security & Privacy Requirements	Rational / Comments	Mandatory or Not
S&P2.1	The Identity Consolidator service should be security-hardened so that it is very difficult to compromise and so that no unauthorized entity is able to access or modify the complete (or partial components of the) identity of the user.	The Identity Consolidator service must ensure that the complete identity of the user can be constructed by unauthorized entities only if the user wishes to.	Yes

S&P2.2	The Identity Consolidator service should use secure protocols in the interaction with end users and verifying online service.	The Identity Consolidator service must rely on secure protocols to communicate with end-users and verifying online service.	Yes
S&P2.3	The Identity Acquisition service should be security-hardened so that it is very difficult to compromise and so that no unauthorized entity is able to construct the complete identity of the user.	The Identity Acquisition service must ensure that the complete identity of the user can be constructed by unauthorized entities only if the user wishes to.	Yes
S&P2.4	The Identity Acquisition service should use trusted software and hardware paths on the devices in order to securely and verifiably capture images of a user, images of documentation and locations.	The Identity Acquisition service must ensure that the captured identity information of the users (e.g., passport photo, user photo, location) are captured securely from their device and are not altered by malicious users.	Yes
S&P2.5	The Identity Acquisition service must ensure that the peer-to-peer verification of the personal identity information of the users is secure and the privacy of the users is preserved.	-	Yes
S&P2.6	Cryptographic credentials should be stored remotely for recovery such that only the user can recover and decrypt them	-	No
S&P2.7	Information about the user must be encrypted and difficult to decrypt, even by a system administrator	-	Yes
S&P2.8	The system must obtain explicit consent from the end user to collect and process its personal data according to the legislation.	-	Yes
S&P2.9	The system must obtain explicit consent from the end user to transfer its personal data between ReCRED consortium members according to the legislation.	-	Yes
S&P2.10	All communication must occur over a secure channel	-	Yes
S&P2.11	Personal de-anonymization risk must be revealed only to the owner of the account and not to other ReCRED users.		Yes
S&P2.12	All communication must occur over a secure channel	-	Yes
S&P2.13	User data must not be revealed to other users.		Yes
S&P2.14	Users must not be allowed to manipulate data other than their own.		Yes
S&P2.15	All communication must occur over a secure channel	-	Yes
S&P2.16	Personal information of a user must be storage in a secure server	-	Yes
S&P2.17	All communication have to be secure if the	-	Yes

	authenticated option have been chosen		
S&P2.18	At LoA 1, assertions and assertion references require protection from manufacture/modification and reuse attacks. Also at LoA 1 the system is required to be at least weakly resistant to man-in-the middle attacks.	-	Yes
S&P2.19	In LoA 2, in addition to LoA 1 requirements, assertions are resistant to disclosure, redirection, capture and substitution attacks.	-	Yes
S&P2.20	In LoA 3 and LoA 4 the system should also be strongly resistant to man-in-the-middle attacks.	-	Yes
S&P2.21	The system should strongly resists online guessing attacks - An attack where the attacker performs repeated logon trials by guessing possible values of the token authenticator.	-	Yes
S&P2.22	The system should strongly resists passive attacks - An attack against an authentication protocol where the attacker intercepts data traveling along the network between the user and the system, but does not alter the data.	-	Yes
S&P2.23	The system should strongly resists active attacks - An attack on the authentication protocol where the attacker transmits data to the user, the identity providers or the service provider.	-	Yes
S&P2.24	The system should be resistant to Man-in-the-middle Attacks - An attack on the authentication protocol run in which the Attacker positions himself in between the user and system so that he can intercept and alter data exchange between them.	-	Yes
S&P2.25	The system should be resistant to Pharming Attach – The attacker corrupts an infrastructure service such as Domain Name Service (DNS) causing the user to be misdirected to a forged identity provider, which could cause the user to reveal sensitive information, download harmful software or contribute to a fraudulent act.	-	Yes
S&P2.26	The system should be resistant to Replay Attacks - The attacker is able to replay previously captured messages, which are legitimate, and to masquerade as the user to the service provider.	-	Yes
S&P2.27	The system should be resistant to session Hijack Attacks - The attacker is able to insert himself between a user and the system, and	-	Yes

	hijack a successful authentication exchange between the two parties. The Attacker is then able to pose as the legitimate user to the system or vice versa.		
S&P2.28	Verifier Impersonation Attack - The attacker impersonates the system in an authentication protocol, usually to capture information that can be used to masquerade as a user to the system.	-	Yes

10.2.3. Operational Requirements

#	Operational Requirements	Rational / Comments	Mandatory or Not
O2.1	The web interface and/or mobile application for users to interact with the Identity Consolidation service must be simple and friendly	-	Yes
O2.2	The communication protocol between the validating service provider and the Identity Consolidator must be lightweight and simple	-	Yes
O2.3	The communication protocol between the end-users devices and the Identity Consolidator must be lightweight and simple	-	Yes
O2.4	The Identity Acquisition service should allow the users to prove any attributes of their identity in a usable way.	The user can easy declare and prove any attribute of his identity using intuitive workflows.	Yes
O2.5	The Identity Acquisition service should allow the users to prove any attributes of their identity in an efficient way.	The service should allow the users to quickly declare and prove attributes of their identities.	Yes
O2.6	The user must be registered to the mobile device in order to access the Credentials Backup & Restore application.	-	Yes
O2.7	The user must have a valid ReCRED account in the ID Consolidator.	-	Yes
O2.8	All requests to the server must be authenticated and authorized.	-	Yes
O2.9	The server will check and accept requests to manipulate only the requesting user's data. Requests to manipulate other users' data will be rejected.	-	Yes
O2.10	The user must first authenticate in order to access the web application.	-	Yes
O2.11	The web application will display appropriate messages in case of faults or errors.	-	Yes
O2.12	The web application will validate all user input and display appropriate error messages in case of invalid entry values.	-	Yes

O2.13	The internal users of the Identity Consolidator Module must have an account for the identity repository in order to have the required permissions to handle the data they need.	-	Yes
O2.14	The internal users of the Identity Consolidator Module have to be able to use all the features of the Identity Repository	-	Yes

10.3. Service Providers

The Service Provider component refers to online services that provide a service to end-users. Our aim in ReCRED is to minimize the number of required modifications on this component. The Service Providers will only have an access control module for regulating their users’ access to their service, and also it will have the OpenID Connect’s Relying Party code so that they can connect to Identity Providers and retrieve identity attributes.

10.3.1. Functional Requirements

Integration of OpenID Connect Relying Party code on Service Providers

Code Number	**D3.2.8.1 – T575**
Business Value	**High**
Title	**Integration of OpenID Connect Relying Party code on Service Providers**
Description	**As a** Service Provider **I want** to be able to delegate authentication and acquire identity attributes from an Identity Provider **so that** i can grant access to my service for my users
Acceptance Criteria	1. The Service Provider should have the OpenID Connect Relying Party code within its daemon so that he can query an Identity Provider for user attributes 2. The Service Provider should maintain, for each Identity Provider, the following information: i) a list of the IdP's OpenID Connect endpoints; ii) registered with the IdP client id and iii) registered with the IdP client secret. In case that the Service Provider does not have this information for a particular IdP, then it should perform a dynamic registration with the IdP in order to acquire and store this information for future use.

Access Control Policy Reasoning Tool on Service Providers

Service Providers need to define the attribute-based policies for user access to services. The Access Control Policy Reasoning Tool aids them in the definition of these policies. Furthermore, the access

control policy reasoning tool offers a machine learning-based recommendation system that aims to provide recommendations for modifying the access control policies.

Code Number	**D5.3.1.2.13 – T576**
Business Value	**Medium**
Title	**Implementation of ABAC policies creation**
Description	**As a** Service Provider Administrator **I want to** be able to define ABAC policies **so that** i can clearly define how and when my users can get access
Acceptance Criteria	1. The administrator should be presented with a highly intuitive interface for declaring ABAC policies. 2. The ABAC policies should follow the XACML specification. 3. Upon the successful creation the policy database should be updated.

Code Number	**D5.3.1.2.1 - T391**
Business Value	**Medium**
Title	**Implementation of ABAC policies and special permissions view**
Description	**As a** Service Provider administrator **I want to** be able to view the active ABAC policies and special permissions **so that** I can evaluate the active ABAC policies and the special permissions

Acceptance Criteria	1. The ABAC policies and the special permissions should be presented in a user-friendly interface 2. The user should be able to export the ABAC policies to an XACML-compliant file.

Code Number	**D5.3.1.2.6 - T396**
Business Value	**Medium**
Title	**Implementation of ABAC policy recommendation request**
Description	**As a** Service Provider administrator **I want** to be able to request policy recommendation from the Machine Learning recommendation system **so that** I can improve the ABAC policies of the system
Acceptance Criteria	1. The request should return a set of recommended policies. 2. The policies should only be stored on the active ABAC policies database upon the confirmation of the Service Provider administrator.

Code Number	**D5.3.1.2.3 - T393**
Business Value	**Medium**
Title	**Implementation of denied requests search**
Description	**As a** Service Provider administrator **I want** to be able to search the denied requests **so that** I can add a special permission on a specific user for a specific resource

Acceptance Criteria	1. The search should be able to be executed with a variety of attributes (e.g., time of request or type of resource) 2. The search results should be presented in an easy to read format 3. The search operation should be executed in the log files that contain the authorization requests.

Code Number	**D5.3.1.2.4 - T394**
Business Value	**Medium**
Title	**Implementation of special permissions creation**
Description	**As a** Service Provider administrator **I want to** be able to add permission to a user for a resource **so that** I can offer identity-based access control
Acceptance Criteria	1. The permissions should be added into the policies database 2. The special permission policy should be active after the addition 3. The special permission policy should be able to be added from denied requests view (see Task 393)

Code Number	**D5.3.1.2.10 - T400**
Business Value	**Medium**
Title	**Implementation of special permissions reduction request**
Description	**As a** Service Provider administrator **I want to** be able to request special permissions reduction

	so that any special permissions that are already covered by the ABAC policies be removed
Acceptance Criteria	1. The request should return the special policy that should be removed and the ABAC policy that replaced it. 2. The special policies should not be deleted without the Service Provider administrator's acceptance.

Code Number	**D5.3.1.3.1 – T224**
Business Value	**Medium**
Title	**Implementation of logging for authorization requests**
Description	**As a** Service Provider administrator **I want** to have the logs of the XACML requests **so that I** can evaluate the decisions of the ABAC policies
Acceptance Criteria	1. The logs should include the request in the XACML format. 2. The logs should include environment attributes e.g. time of the request 3. The logs should include the decision of the request 4. The logs should include the state of the ABAC policies and the state of special permissions. The state should reflect the active policies at the time of the request

Code Number	**D5.3.1.2.8 - T398**
Business Value	**Medium**
Title	**Implementation of ABAC policies refinement request**

Description	**As a** Service Provider administrator **I want to** be able to request policy refinement **so that** the ABAC policies do not include overlaps
Acceptance Criteria	1. The request should return the policies that overlap and their recommended refinement. 2. The policies should not be refined without the service provider administrator's acceptance. After the acceptance, the changes should be applied to the ABAC policies database. 3. The refinements can include modifications (merge) or deletions of ABAC policies

Code Number	**D5.3.1.1 – T125**
Businness Value	**High**
Title	**Implementation of the Machine Learning Recommendation System**
Description	**As a** Service Provider Access control module **I want to** be able to get recommendation about my policies **so that** I can offer a better access control solution to my users.
Acceptance Criteria	1. The recommendation system should be a ML-based system (ABAC policy mining). 2. The system should take as an input the active ABAC policies, the special permissions and the data from the authorization requests log files. The system should output new ABAC policies. 3. The system should be able to expose these recommendation to the Service Administrator front-end.

	4. The machine learning solution should take into consideration the criticality of each resource (e.g., if a resource is too critical then it should not make recommendations). 5. The recommendation system should aim to minimize the overall number of special permissions that are active on the ABAC reasoning tool.

Code Number	**D5.3.1.4.1 – T382**
Business Value	**High**
Title	**Implementation policy decision point module for XACML policies**
Description	**As an** Access Control Reasoning tool **I want to** be able to evaluate XACML requests **so that** I can provide access to users according to the active XACML policies
Acceptance Criteria	1. The policy decision point module evaluates the requests with the active ABAC policies. In case that, the user does not get access, then the request is evaluated with the active special permissions. If the user does not have a special permission then it gets denied. 2. The request alongside with the decision should be logged to the logs files 3. The policy decision point module should be compliant with the XACML specification.

10.3.2. Security & Privacy Requirements

#	Security & Privacy Requirements	Rational / Comments	Mandatory or Not

S&P3.1	The exchange of information between the device and the remote service must always be encrypted, with protocols such as SSL	In ReCRED, we will make use of the gateSAFE solution that provides adequate SSL protection	Yes
S&P3.2	All interactions between the device and the remote services should be audited	Auditing is essential in a data privacy enabling environment	Yes
S&P 3.3	The same Security & Privacy Requirements apply from section 1.1.2.2, S&P2.18 to S&P2.28	-	Yes

10.3.3. Operational Requirements

#	Operational Requirements	Rational / Comments	Mandatory or Not
O3.1	All interactions between the device and remote services should be logged for billing purposes	Billing is an essential part of a commercial offering. The logging should normally happen by the device, after successfully contacting a remote service, and sent to the ReCRED Billing service	Yes
O3.2	All interactions between the device and the remote service must be supported in all widely available devices, namely iOS, android and Windows Phone without significant changes to their configuration (e.g. rooting the device)	All users must be able to use their device for interacting with remote services; additionally, most users do NOT accept to root their device or perform changes that may break their guarantee	Yes
O3.3	All information sharing for a user to a third party, either in a centralized manner or from device to third party, must be monitored and audited	The platform may invoice third parties per interaction, therefore storing this information is vital	Yes
O3.4	Time to resolve user information, before it is transmitted to a third party, must be quick (less than 3 seconds per interaction)	-	Yes

10.4. Identity Providers

Within the ReCRED architecture, the Identity Providers play a major role alongside with the Identity Consolidator. They offer a variety of features to other entities such as credentials' issuance to users,

provision of identity attributes to Service Providers and much more. Below we describe the requirements that we identified for the Identity Providers component.

10.4.1. Functional Requirements

FIDO Universal Authentication Framework (UAF) Server

The FIDO UAF Server should expose the registration/authentication/deregistration process through a REST API and verify the authenticity of messages received according to the FIDO UAF protocol specification.

Code Number	**D3.3.1.4.1 - T601**
Business Value	**High**
Title	**Implementation of FacetID registration function**
Description	**As a** FIDO UAF Server **I want** be able to register FacetID that correspond to a FIDO UAF client **so that** the FIDO UAF Server can accept requests from the FIDO UAF clients
Acceptance Criteria	1. This operation should be implemented as a REST API call. 2. After the successful call of this operation, the new FacetID should be registered with the FIDO UAF Server and the FIDO UAF client should be able to execute operations on the FIDO UAF Server

Code Number	**D3.3.1.4.3 - T603**
Business Value	High
Title	**Implementation of persistence for the registration functionality on the FIDO UAF Server**
Description	**As a** FIDO UAF server **I want** be able to persist registration information from a FIDO UAF client

	So that the client can remain registered to a FIDO UAF Server on an Identity Provider .
Acceptance Criteria	1. The FIDO server will create audit logs for every registration process. 2. The FIDO server will store in an SQL database the registration data for the users. In that way, the data will persists even in the case that the FIDO UAF Server fails and needs restart or re-deployment.

Code Number	**D3.3.1.4.4 - T604**
Business Value	**High**
Title	**Implementation of message processing required for the registration functionality on the FIDO UAF server**
Description	**As a** FIDO UAF Server **I want** to be able to process registration messages from a FIDO client **So that** I can register new users.
Acceptance Criteria	1. The FIDO UAF server will send a registration request to the client, when a user is not registered (according to FIDO UAF protocol section 3.4). 2. The challenge sent in the registration request by the FIDO UAF server will be generated using cryptographic methods. 3. The FIDO server must check the validity and the integrity of the registration response sent by the FIDO UAF client. If an inconsistency is found the message is rejected (as specified in the steps described in the FIDO UAF protocol section 3.4.6.5) 4. All the functionalities for the registration functionality should be exposed using a REST interface.

Code Number	**D3.3.1.4.5 - T605**

Business Value	**High**
Title	**Implementation of the data persistence for the authentication function on FIDO UAF server**
Description	**As a** FIDO UAF server **I want to** be able to persist the authentication data **so that** I can authenticate users and not lose important authentication data
Acceptance Criteria	1. The FIDO UAF server should be able to store successful and unsuccessful authentication attempts in an SQL database. In that way, the authentication data will persist even if the FIDO UAF Server crashes.

Code Number	**D3.3.1.4.2 - T602**
Business Value	**High**
Title	**Implementation of the cryptographic operations needed for the authentication functions on the FIDO UAF server**
Description	**As a** FIDO UAF Server **I want to** rely on the cryptographic operations **so that** I can offer increased security when performing authentication functions
Acceptance Criteria	1. The FIDO UAF Server should make use of strong crypto randomness for generating server challenge. Furthermore, it should make use of multiple random sources for this task. 2. The FIDO UAF Server should support Authentication Processing Rules 3. The FIDO UAF Server should support TLS Channel binding

Code Number	**D3.3.1.4.6 - T606**
Business Value	**High**
Title	**Implementation of operations for accessing authentication data**
Description	**As a** FIDO UAF Server **I want to** be able to provide authentication-related data **so that** other entities can make use of these data
Acceptance Criteria	1. The FIDO UAF Server should be able to provide data regarding authentication such as last authentication timestamp and authentication ids. These data can be useful for other components such as OpenAM on identity providers and for the FIDO UAF client on the user’s device 2. These operations should be exposed as a REST interface.

Code Number	**D3.3.1.4.7 - T607**
Business Value	**High**
Title	**Implementation of the deregistration function on the FIDO UAF Server**
Description	**As a** FIDO UAF Server **I want** to be able to delete the registration data for a user **So that** I can deregister users from the FIDO UAF Server and therefore they will not be able to login.
Acceptance Criteria	1. The FIDO UAF server will create a deregistration request to be sent to the FIDO UAF client when it wants to delete an account.

	2. The deregistration request sent by the FIDO UAF server to the FIDO UAF client will follow the specifications from the FIDO UAF protocol section 3.6.1 3. The FIDO UAF server will delete the account information from the database. 4. This functionality should be available via a REST API on the FIDO UAF Server on the Identity Providers

ReCRED daemon on Identity providers

The Identity providers have a ReCRED daemon that gives them the ability to store identity attributes of their users and issue cryptographic credentials directly to the user’s device from the attributes using the cryptographic credentials issuance module. The user’s device or the Identity consolidator communicates with the identity providers using federated login protocols (e.g., as OpenID, OpenAuth). The credentials issued from the identity providers are also transferred to the identity consolidation service to store them so that they are backed up and accessible if the identity provider fails.

Implementation of Identity attributes storage in ReCRED daemon on ID providers

Code Number	**D4.3.8.1 - T137**
Business Value	**High**
Title	**Implementation of Identity attributes storage in ReCRED daemon on ID providers**
Description	**As an** Identity Provider **I want to** be able to securely store identity attributes **so that** i can use them for future use (such as, issue cryptographic credentials or provide identity attributes to Service Providers, etc.)
Acceptance Criteria	1. The storage should be secure to avoid tampering from attackers 2. The secure storage should be able to communicate with OpenAM in order to be able to provide identity attributes via the OpenID Connect protocol. 3. The definition of the schema for this storage will depend on the role of the Identity Provider. For instance, the university's library should have student-related

	attributes whereas government-related identity provider should have identity-related attributes.

Integration of OpenID Connect in ReCRED daemon on ID providers

Code Number	**D4.3.8.2 - T139**
Business Value	**High**
Title	**Integration of OpenID Connect in ReCRED daemon on ID providers**
Description	**As an** Identity Provider **I want to** be able to provide user attributes via the OpenID Connect protocol **so that** Service Providers can acquire user attributes
Acceptance Criteria	1. The OpenID Connect Provider will be based on the OpenAM implementation. 2. The OpenAM OpenID Connect Provider should allow the dynamic registration of clients. 3. The OpenAM OpenID Connect flow should be able to be exposed via OpenAM's REST APIs. 4. OpenAM's internal datastore should be configured according to the role of the Identity Provider. For instance, the university's library should have student-related attributes whereas government-related identity provider should have identity-related attributes.

Custom Authentication module within OpenAM

Code Number	**D4.2.1.5 - T250**
Business Value	**High**
Title	**Implementation of FIDO UAF custom authentication module within OpenAM**
Description	**As an** OpenAM instance running on Identity Providers

	I want to be able to contact the FIDO UAF server **so that** I can verify that the user authenticated
Acceptance Criteria	1. The custom Authentication module should allow the dynamic change of the FIDO endpoint. (the Identity Provider administrator should be able to easily change it through OpenAM's web interface) 2. The FIDO UAF custom authentication module within OpenAM will identify a user using a username and an authentication id. Subsequently, it will send this data to the FIDO server in order to verify that the user is authenticated. 3. The OpenAM's FIDO UAF custom authentication module will utilize the FIDO server's REST API. 4. This custom authentication module should be configured as the primary authentication mechanism within OpenAM so that all users are authenticated using the FIDO UAF protocol.

QR Authentication Server

The QR Authentication Server generates the QR patterns that are presented by the QR Web client and authenticates the QR Device Client.

Code Number	**D3.2.17.2.1 - T610**
Business Value	**High**
Title	**QR code generation**
Description	**As a** QR Web Client **I want to** present distinct QR codes to the QR Device Client **so that** the Device QR Client doesn`t generate duplicate authentication data
Acceptance Criteria	1. The QR code should be a random nonce generated according to the documentation

	2. The QR code generation operation will employ a size limit so that the codes are not too big. In that way, the client can process it fast without causing QR code expiration. 3. The operation should be exposed as a REST API call

Code Number	**D3.2.17.2.2 - T611**
Business Value	**High**
Title	**QR code transmission**
Description	**As a** QR Web Client **I want the** source of the QR codes to be trusted **so that** I can allow the QR Device Client to parse valid information and send authentication data to the same trusted server
Acceptance Criteria	1. There should be a TLS channel between QR Server and QR Web Client 2. The operation should be exposed as a REST API call

Code Number	**D3.2.17.2.3 - T612**
Business Value	**High**
Title	**Verification of QR code attestation**
Description	**As a** QR Web Client **I want the** QR Authentication Server to verify QR code attestation with the FIDO UAF Server **so that** only authorized devices can log in
Acceptance Criteria	1. Both servers behind should reside behind gateSAFE so that adequate SSL protection is provided.

	2. The operation should identify the person that scanned the QR code in order to decide which credentials needs to be send. 3. The verification process should take into consideration the QR code expiration time. If the QR code is expired, then access should not be granted 4. The operation should be exposed as a REST API call

Code Number	**D3.2.16 – T577**
Business Value	**High**
Title	**Integration of gateSAFE on Identity Providers**
Description	**As an** Identity Provider **I want to** be able to provide adequate SSL protection to connections to all the back-end components **so that t**he connections are secured and use a trusted ssl certificate
Acceptance Criteria	1. The gateSAFE product of CSGN should be deployed to the Identity Providers 2. gateSAFE should be configured so that all connections to the back-end components that run on the Identity Providers are tunneled through gateSAFE. 3. gateSAFE should be deployed in a docker container

10.4.2. Security & Privacy Requirements

#	Security & Privacy Requirements	Rational / Comments	Mandatory or Not
S&P4.1	The credentials must be protected while being transferred.	The credentials transmitted to the user must be protected (i.e., encrypted communication or using cryptographic credentials of the user) in order to avoid eavesdropping.	Yes

S&P4.2	Information about a user should be stored in the authentic source it comes from and retrieved only at request time	By keeping information in the authentic sources, it is better protected and dispersed, making it difficult for intruders to reconstruct the complete user profile	Yes
S&P4.3	Use strong crypto randomness for server challenge	-	Yes
S&P4.4	Use multiple random sources	-	Yes
S&P4.5	Implement TLS Channel binding	-	Yes
S&P4.6	The challenge sent in the registration request by the FIDO server will be generated using cryptographic methods.		Yes
S&P4.7	The FIDO server must check the validity and the integrity of the registration response sent by the FIDO client. If an inconsistency is found the message is rejected (as specified in the steps described in the FIDO UAF protocol section 3.4.6.5)	-	Yes
S&P4.8	Cryptographic keys of the IDP must be at least 2048 bits long.	-	Yes
S&P4.9	In case of a key compromise, the ReCRED operators must be notified within 24 hours by the IDP.	-	Yes
S&P4.10	The same Security & Privacy Requirements apply from section 1.1.2.2, S&P2.18 to S&P2.28	-	Yes

10.4.3. Operational Requirements

#	Operational Requirements	Rational / Comments	Mandatory or Not
O4.1	All system transactions must be logged.	-	Yes
O4.2	Log files should be kept for at least 30 days.	-	Yes
O4.3	The log files should be treated in accordance with the data protection laws.	-	Yes
O4.5	The system should ensure that all private keys are protected	-	Yes
O4.7	All IPD that use of self-signed certificates should have a long expiration time.	-	Yes
O4.8	The IPD comply with the Interoperable SAML 2.0 Web Browser SSO Deployment Profile	-	Yes

O4.9	The IPD support SAML2 Web Browser SSO Profile over HTTP Artifact Binding.	-	Yes
O4.10	The IPD support SAML2 Single Logout Profile over HTTP Redirect and SOAP Bindings.	-	Yes
O4.11	The IPD SAML endpoints should be protected by HTTPS.	-	Yes
O4.12	The IPD SAML endpoints should be under a DNS domain which is possessed by the operating organisation.	-	Yes
O4.13	The IPD be under a DNS domain which is possessed by the operating organisation.	-	Yes

10.5. Behavioral Authentication Authorities

Behavioral authentication authorities (BAA) are responsible for capturing and maintaining the behavior of the users on their devices (local behavior) or on their network or online service (remote behavior). Additionally, they are responsible to perform behavioral second-factor authentication. Those authorities (e.g., Telcos or online services) can capture and store, on their behavioral profile database, the behavior of the user (such as location patterns, gait, movement dynamics, typing patterns, etc.). In addition, BAAs receive the locally captured from the user’s device behavioral profiles and store them for future verification. Using the behavioral information, a BAA can determine whether a device currently behaves as it usually does. Depending on the result, it can certify to Service Providers, whether it believes the device is held by its legitimate user.

The behavioral authentication authorities have a ReCRED daemon which allows them to verify the behavior of the user when this is requested from the service provider as a second-factor authentication for users. In case that the behavioral authentication failed many times, the authorities can inform the IDC to activate Latch if the user opts to assign them such capability.

The device captures gait and typing signatures. It authenticates once using FIDO with the BAA and establishes a secure session with cookies or JSON tokens. It uses this secure channel to send captured behavior. Then it securely erases it from the device. For network behavior or location, the BAA does not need to receive captured behavior from the device. It captures it by itself.

If the relying party asks for a behavioral BAA factor, it asks the consolidator for legitimate BAAs and asks the device which is the corresponding BAA. It then initiates OAuth2 with the BAA. If needed, the BAA asks for FIDO authentication with the device and response with whether the user behaves the same as in the past, or it does party. The BAA's consists of four main components:

1. ReCRED daemon
2. OpenID Connect Provider component (OpenAM)
3. FIDO Server
4. Behavioral Profiles Database

10.5.1. Functional Requirements

Code Number	**D3.2.1.4 - T34**
Business Value	**High**
Title	**Implementation of a skeleton front-end application for BAA administration**
Description	**As a** BAA administrator **I want to** be able to manage the BAA data and preferences through a simple user interface **so that** I can configure parameters, manage data and actions related to the BAA profiles
Acceptance Criteria	1. The BAA administrator should have a valid user name and password to access the BAA console front-end. 2. The BAA administrator should be provided with a list of actions to access all the related to the BAA functionality.

Integration of FIDO Server on BAA

The BAA's should have a FIDO Server deployed within the ReCRED daemon so it can authenticate the user.

Code Number	**D3.2.1.5 - T308**
Business Value	**High**
Title	**Integration of FIDO Server on BAA**
Description	**As a** behavioral authentication authority **I want to** be able to authenticate the user **so that** I can setup a secure channel to transfer data
Acceptance Criteria	1. The authentication should be based on the FIDO UAF specification

	2. After the authentication is done the user's device should be able to interact with the BAA (e.g. setup secure channel and transfer data via the ReCRED daemon). 3. All the FIDO server connections should be tunnelled through gateSAFE to ensure adequate SSL protection

Code Number	**D3.2.1.3.3 - T313**
Business Value	**High**
Title	**Implementation of BAA behavioral DB**
Description	**As a** BAA **I want to** access in both read and write mode the behavioral profile database **so that** I can store/fetch user profiles
Acceptance Criteria	1. The BAA ReCRED daemon should be able to make CRUD operations on the Behavioral Profiles database. 2. The BAA should make sure that the access to this database will be prohibited for un-authorized parties. 3. The BAA should be able to expose some information from this database to other entities of the ReCRED ecosystem (e.g., Identity Consolidator). For example, the consolidator should have a reference of the stored behavioral profiles that are maintained by each BAA.

Code Number	**D3.2.1.3.4 - T309**
Business Value	**High**

Title	**Implementation of operations for establishing a secure channel between BAA and user device**
Description	**As a** behavioral authentication authority **I want to** be able to setup a secure channel to the user device **so that** I can receive data from the user's device
Acceptance Criteria	1. This channel should be persistent 2. The device sends the device-captured behavioral data to the BAA and then immediately erases them 3. The BAA stores the received data and it can determine whether those data have changed or if they match with the stored behavioral profile

Code Number	**D3.2.1.3.2.4 - T493**
Business Value	**High**
Title	**Implementation of Device-to-Service behavioral authentication using typing pattern**
Description	**As a** User **I want to** be able to provide my typing pattern to the Behavioral Authentication Authority (BAA) typing pattern capturing module **so that** it can be used from the BAA to verify my behavior in the future
Acceptance Criteria	1. The application (b-verifier) can collect my typing pattern from every application I use through a custom keyboard application 2. The app can send my typing pattern to the BAA at (almost) real time. 3. The app will keep my typing pattern to my device's RAM (under the app's ram space) securely for a limited time and then, after sending it to the BAA this information will be erased. This is guaranteed through the android memory management security.

	4. The app should be able to distinguish sessions of the (custom) keyboard usage and count/collect the typing pattern features without losing information in case of idle typing times. 5. The app will send the typing pattern information only in online (network connection) mode.

Code Number	**D3.2.1.3.2.3 - T154**
Business Value	**High**
Title	**Implementation of Device-to-Service behavioral authentication using gait**
Description	**As a** Behavioral Authentication Authority **I want to** be able to receive gait dynamics of a user **so that** I can use the behavioral profile in order to verify whether the user is behaving "as usual"
Acceptance Criteria	1. The app should upload data captured from accelerometer sensors to the BAA server 2. Given a gait model and a recent sample provided by purported user X, the server should provide a confidence score that the sample is indeed from user X

Code Number	D3.2.1.3.2.2 - T241
Business Value	**High**
Title	**Implementation of behavioral profile capture module for browsing behavior**
Description	**As a** Behavioral Authentication Authority **I want to** be able to capture http user requests

	so that I can build per-user browsing profiles
Acceptance Criteria	1. The server logs http requests from users, creates the appropriate behavioral profiles and stores them in the behavioral profile database 2. These behavioral profiles should be able to be accessed for verification means.

Code Number	**D3.2.1.3.2.1 - T153**
Business Value	**High**
Title	**Implement behavioral profile capture for typing pattern**
Description	**As a** Behavioral Authentication Authority **I want to** be able to capture the values of the typing behavioral profile from the user's device **so that** I can store and process it
Acceptance Criteria	1. The BAA should have a secure connection with the user's device 2. The BAA should receive from the mobile device all the necessary values that will allow it to extract the typing profile. 3. The BAA should store the received typing info in order to be available to the verification module.

Code Number	**D3.2.1.3.1 - T141**
Business Value	**High**
Title	**Implementation of Behavioral profile verification module in ReCRED daemon on BAA**
Description	**As a** behavioral authentication authority

	I want to be able to provide a second-factor authentication for the user when requested from a service provider **so that** I can increase the security and prevent malicious attacks
Acceptance Criteria	1. The service provider contacts through the OpenIDConnect /OAuth protocol the behavioral authentication authority and requests a behavioral authentication for a specific user. 2. The authentication authority must verify that the user currently has the same behavior as usual or not. 3. After the verification has been completed the authentication authority has to report to the service provider the result of the authentication. 4. The verification module should support all the behavioral authentication modalities (e.g., gait, typing pattern and browsing behavior)

Code Number	**D3.2.1.3.1.2 - T247**
Business Value	**High**
Title	**Implementation of Behavioral profile verification module for typing pattern**
Description	**As a** Behavioral Authentication Authority **I want to** be able to verify if a user's current behavior is the same as usual or not **so that** I can provide a second factor authentication of the user to the Service provider
Acceptance Criteria	1. The BAA should have enough data to construct a typing profile signature of the user's behavior. These data are gathered from user's device through the Behavioral profile capture module for typing pattern. 2. The BAA should have implemented classification algorithms that are able to compare the current values of the user's profile with the already extracted typing profile signature

	1. The BAA should be able to provide a score/ a result about the verification process that is to be sent to the service provider that requests the second factor authentication 2. The BAA should log the outcome of the verification to a log file for future use

Code Number	**D3.2.1.3.1.1 - T246**
Business Value	**High**
Title	**Implementation of Behavioral profile verification module for browsing behavior**
Description	**As a** Behavioral Authentication Authority **I want to** be able to verify if a user's current browsing behavior is the same as usual or not **so that** I can provide a second factor authentication of the user to the Service provider
Acceptance Criteria	1. The BAA should detect whether the current user browsing behaviour is consistent with his browsing profile 2. The BAA should be able to inform the Service Provider regarding the outcome of the second factor authentication with the browsing behavior. 3. The BAA should log the outcome of the verification to a log file for future use

Integration of OpenAM and Behavioral Authentication Authority (BAA) daemon

The OpenAM instance running on BAA should be able to inform the ReCRED BAA daemon whether a user authenticated. Within OpenAM we have implemented a custom authentication module for the authentication of the user using the FIDO Server. The FIDO server is part of the BAA trust domain and it integrates with OpenAM as specified in other tasks.
In turn, OpenAM will connect to the Relying Party BAA daemon via OpenID Connect. Thus, the BAA daemon will act as a Service Provider to OpenAM's ID provider. After the authentication, the BAA daemon and the user device obtain an authenticated channel for transferring user behavior data to the BAA.

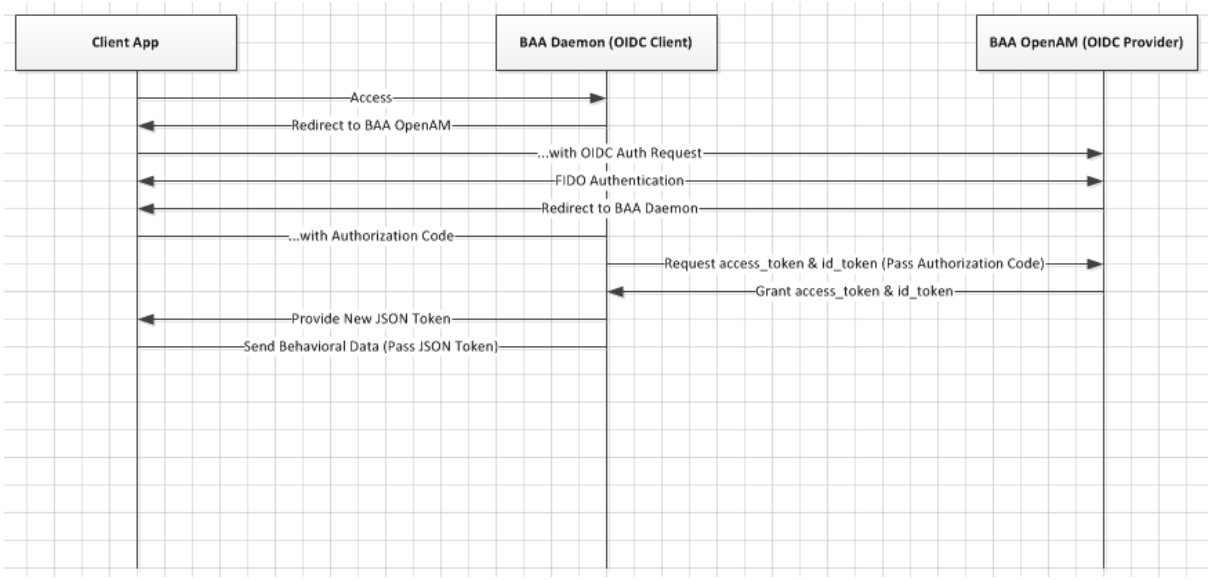


Figure 4: Integration of OpenAM and Behavioral Authentication Authority daemon

Code Number	**D3.2.1.6 - T310**
Business Value	**High**
Title	**Integration of OpenID Connect Provider (OpenAM) and BAA daemon**
Description	**As a BAA daemon** **I want to** be configured as an OpenID Connect Service Provider **so that** I can access the necessary OIDC Tokens to authenticate a username that has been authenticated to OpenAM
Acceptance Criteria	1. The BAA daemon needs to be configured as an OIDC Service Provider 2. Create necessary custom OIDC scopes 3. The BAA daemon should be able to update the attributes stored on OpenAM directly (not via OpenID connect).

	4. OpenAM should be able act as an ID provider to external Service Providers that need to determine if the given user behaves as usual.

Behavioral profiles database on BAA

This database will be responsible to store all of the user's behavioral profiles. These profiles will be created and stored by the input that will be provided by the behavioral capturing modules on BAAs and on user's devices. The database will provide input to the Behavioral profile verification module for the purposes of making sure that the captured profile matches the stored profile.

Code Number	D3.2.10.4 - T467
Business Value	**High**
Title	Delete a Stored Behavioral Profile
Description	**As a** BAA **I want to** I want to be able to delete a behavioral profile stored in the BPDB **so that** I can comply with users’ requests to erase their data
Acceptance Criteria	1. The BAA can call a REST method (DELETE) in order to delete a behavioral profile stored in the BPDB, including the identifier of the resource to be deleted. 2. Upon successful delete of the resource, the REST API returns the HTTP status 200 OK. 3. The REST API authenticates the BAA and checks that it is authorized to delete the specific behavioral profile. Appropriate HTTP statuses are returned in case of authentication (e.g. 401 Unauthorized) or authorization failures (e.g. 403 Forbidden). 4. The REST API returns appropriate HTTP statuses in other error cases (e.g. 404 Not Found).

Code Number	D3.2.10.3 - T172
Business Value	**High**
Title	Update a Stored Behavioral Profile
Description	**As a** BAA **I want to** be able to update a behavioral profile stored in the BPDB **so that** I can always maintain valid behavioral profiles, increasing the reliability of the behavioral authentication mechanism
Acceptance Criteria	1. The BAA can call a REST method (PUT) in order to update a behavioral profile stored in the BPDB, including the identifier of the resource to be updated. 2. Upon successful update of the resource, the REST API returns the HTTP status 200 OK. 3. The REST API authenticates the BAA and checks that it is authorized to update the specific behavioral profile. Appropriate HTTP statuses are returned in case of authentication (e.g. 401 Unauthorized) or authorization failures (e.g. 403 Forbidden). 4. The REST API returns appropriate HTTP statuses in other error cases (e.g. 404 Not Found).

Code Number	D3.2.10.2 - T171
Business Value	**High**
Title	Retrieve a Stored Behavioral Profile
Description	**As a** BAA **I want to** be able to retrieve from the BPDB a behavioral profile for a specific user and of a specific type

	so that I can match it with a captured behavioral profile of the same user and type (in the context of behavioral authentication)
Acceptance Criteria	1. The BAA can call a REST method (GET) in order to read a behavioral profile stored in the BPDB, including the identifier of the profile’s owner and the type of behavioral profile (gait, keystroke, mobility, browsing). 2. Upon successful retrieval of the resource, it is returned in an appropriate representation (XML or JSON), along with the HTTP status 200 OK. 3. The REST API authenticates the BAA and checks that it is authorized to read the specific behavioral profile from the BPDB. Appropriate HTTP statuses are returned in case of authentication (e.g. 401 Unauthorized) or authorization failures (e.g. 403 Forbidden). 4. The REST API returns appropriate HTTP statuses in other error cases (e.g. 400 Bad Request or 404 Not Found).

Code Number	**D3.2.10.1 - T170**
Business Value	**High**
Title	Store a new Behavioral Profile
Description	**As a** BAA **I want to** be able to store new behavioral profiles to the BPDB **so that** they can later be matched with captured behavioral profiles
Acceptance Criteria	1. The BAA can call a REST method (POST) in order to create and store a new behavioral profile resource in the BPDB. 2. The BAA can store the following types of behavioral profiles: gait templates, keystroke templates, mobility signatures, browsing signatures.

	3. Upon successful creation of the behavioral profile, the REST API returns a location header with a link to the newly-created profile, along with the HTTP status 201 Created. 4. The REST API authenticates the BAA and checks that it is authorized to store the specific behavioral profile to the BPDB. Appropriate HTTP statuses are returned in case of authentication (e.g. 401 Unauthorized) or authorization failures (e.g. 403 Forbidden). 5. The REST API checks if the resource already exists and returns the HTTP status 409 Conflict if it does.

Code Number	**D3.2.1.7 – T545**
Business Value	**High**
Title	Integration of gateSAFE on BAAs
Description	**As a** BAA **I want to** be able to provide adequate SSL protection to connections to all the back-end components **so that** the connections are secured and use a trusted ssl certificate
Acceptance Criteria	1. The gateSAFE product of CSGN should be deployed to the servers of the BAA 2. gateSAFE should be configured so that all connections to the ReCRED daemon, to OpenAM and to the FIDO server that will run on the BAAs are tunneled through gateSAFE. 3. gateSAFE should be deployed in a docker container

10.5.2. Security & Privacy Requirements

#	Security & Privacy Requirements	Rational / Comments	Mandatory or Not
S&P5.1	The behavioral authentication mechanisms shall comply with typical security	-	Yes

	properties (Confidentiality, Integrity, & Availability).		
S&P5.2	The ReCRED software that will handle the process of 2nd behavioral factor authentication shall be attack-resilient.	-	Yes
S&P5.3	The behavioral profiles shall be privacy-aware.	Behavioral profiles could be anonymized in order to protect user’s privacy. For example, in case of user mobility being used as a 2nd factor for authentication, the pattern shall be formed without giving away user’s location.	No
S&P5.4	The behavioral profiles shall be collected, created and signed in a TEE (Trusted Execution Environment).	A malicious user with physical access to the user device shall not be able to interfere with any of the processes regarding behavioral profiles.	Yes
S&P5.5	The behavioral profiles shall have high entropy so they can be used as secure unique identifiers.	The captured user behaviors shall be hard to guess and should act as unique identifiers of a user.	Yes
S&P5.6	The behavioral profiles will only be accessible by the BAAs	-	Yes
S&P5.7	The behavioral authentication authorities shall securely store the behavioral profiles.	Behavioral profiles shall be encrypted using strong encryption algorithms with high complexity.	Yes
S&P5.8	The ReCRED platform shall enforce mutual authentication between the communicating components/entities.	ReCRED platform shall employ robust security mechanisms against man-in-the-middle attacks.	Yes
S&P5.9	The behavioral authentication authorities shall successfully authenticate users only if their behavior matches with their behavioral profile patterns stored, above a certain percentage/threshold.	An ideal threshold will securely identify users with small changes in their exhibited behavior.	Yes
S&P5.10	The behavioral authentication authorities log files shall be detailed enough to support forensic analysis.	Containing timestamp, actions, involved parties etc.	No
S&P5.11	The REST API authenticates the BAA and checks that it is authorized to perform CRUD operations to the behavioral profiles. Appropriate HTTP statuses are returned in case of authentication (e.g. 401 Unauthorized) or authorization failures (e.g. 403 Forbidden).	The REST calls should be accessible by authorized authorities only (BAAs).	No

10.5.3. Operational Requirements

#	Operational Requirements	Rational / Comments	Mandatory or Not
O5.1	The behavioral authentication process and configuration shall be user-friendly.	Navigating through the interface should be easy for end users.	Yes
O5.2	The behavioral signatures shall provide gradient results.	Behavioral authentication authorities shall inform the Identity Consolidator and relying service provider about the match percentage between user's behavior and his stored profile.	No
O5.3	The behavioral multifactor authentication process must be fast and efficient.	Response time shall be within a reasonable time window.	Yes
O5.4	The behavioral profiles shall be periodically updated stored for a specific period of time.	Behavioral profiles shall be updated regularly. Previous versions of them will be deleted.	Yes
O5.4	The behavioral authentication authorities shall be able to manage high network traffic load.	-	Yes
O5.5	The behavioral Authentication Authority databases shall support process accounting log files.	Log files can give a detailed image regarding the operation of the behavioral authentication process.	Yes

10.6. Privacy Preserving Access Control

In this section, we describe the requirements for the privacy-preserving access control within the ReCRED platform. Please note that these requirements span across multiple aforementioned components, but we decided to dedicate a new section because this is a horizontal concept.

In the context of privacy-preserving access control, we describe how we will utilize anonymous credentials protocols such Idemix and U-Prove in the context of ReCRED and how we will integrate them with other various protocols such as the OpenID Connect and FIDO UAF. Below you can find the identified requirements with regard to the privacy-preserving access control.

10.6.1. Functional Requirements

PABAC and FIDO integration

The aim of the Privacy-Preserving Attribute-Based Access Control and FIDO integration in WP5 is to enable the user to employ the attributes enclosed in the Privacy-Preserving Attribute-Based Access Control credentials in the FIDO protocol exchanges.

Code Number	**D5.2.9.2.1 - T472**
Business Value	**Medium**
Title	**Implementation of the PABAC and FIDO integration**
Description	**As a** user **I want to** use ABAC in FIDO **so that** I can use privacy-preserving ABAC credentials to get authorized when accessing FIDO enabled service provider
Acceptance Criteria	1. ABAC attributes (coming from Idemix and U-Prove credentials) can be used in FIDO

Idemix and U-Prove Verifier as an OpenAM Custom Authentication Module

This module involves implementing a Custom Authentication Module on OpenAM that will act as an idemix/U-Prove verifier. Upon establishing a session with OpenAM, the user will provide a randomly generated pseudonym instead of an identifiable username. The user will prove his attribute to OpenAM via idemix/U-Prove. The Service Provider can then obtain a verified attribute from the OpenAM ID provider via OpenID Connect/OAuth2. In the common use case, the privacy-preserving-ABAC-supporting OpenAM ID provider and the Service Provider will be in the same trust domain, e.g., the same server.

Idemix and U-prove Verifier (through FiWARE) as an OpenAM Custom Authentication Module

Code Number	**D5.2.8 - T469**
Business Value	**Medium**
Title	**Implementation of Idemix and U-Prove Verifier (through FiWARE) as an OpenAM Custom Authentication**
Description	**As an** Identity Provider **I want to** be able to verify Idemix and U-Prove credentials

	so that I can provide user attributes verified from Idemix and U-prove credentials to Service Providers that do not support PABAC protocols
Acceptance Criteria	1. The user will generate a pseudonym for each request to the Identity provider. 2. The user will provide a randomly generated pseudonym instead of an identifiable username 3. The identity provider will provide the attributes to the Service Provider via the OpenID Connect protocol. 4. The untraceability guarantee is preserved 5. The multi-show unlinkability in case that the idemix stack is used is preserved 6. The custom module should make use of the FiWARE interface that enables the seamless use of the Idemix and U-Prove cryptographic stacks

ReCRED User Device PABAC Daemon

The User Device ReCRED Privacy-Preserving Attribute-Based Access Control Daemon aims at enabling the user device to use Privacy-Preserving Attribute-Based Access Control credentials. The credentials are obtained by the user from the Identity Providers or from the Identity Consolidator. These can be used to be authenticated by Service Providers (by delegating the credential verification to an IdP or to the IDC) and can be securely backed up by the user to the Identity Consolidator.

U-Prove client on the user device

Code Number	**D5.2.7.1.2.1 - T450**
Business Value	**Medium**
Title	**Implementation of U-Prove issuance (credential reception) on the User Device**
Description	**As a** user **I want to** be issued U-Prove credentials from identity providers

	so that I can use these credentials to get authorized when accessing service provider
Acceptance Criteria	1. The values of the attributes in the U-Prove credential are verified by the Identity Provider or the Identity Consolidator 2. The credential structure is presented to the user at the beginning of the exchange

Credential backup

Code Number	**D5.2.7.1.3.2 - T486**
Business Value	**Medium**
Title	**Implementation of credential restore from the IDC to the user device**
Description	**As a** user **I want** to be able to restore my ABAC credentials from the Identity Consolidator to my device **so that** if I lose my device and I get a new one, I am able to get my ABAC credentials
Acceptance Criteria	1. The credentials are stored securely. In order to achieve this, the device should utilize its TEE capabilities to securely store the issued credentials. 2. The credentials are transferred securely. The connection will be tunneled through gateSAFE, thus ensuring the security of the SSL connection. 3. In the case that the user didn't trust the Identity Consolidator with backing up his credentials, he should be able to re-issue them and transfer them to his device.

Code Number	**D5.2.7.1.3.3 - T548**

Business Value	**Medium**
Title	**Implementation of operations for encrypting/decrypting credentials**
Description	**As a** user **I want** to be able to backup credentials to the IDC or restore credentials to my device **so that i** can make use of my credentials or don't lose my credentials due to device lost/failure
Acceptance Criteria	1. When backing credentials to the IDC, the credentials are decrypted using the TEE-stored keys 2. When backing credentials to the IDC, the credentials are encrypted at the user device with a user-provided secret/passphrase 3. When restoring credentials from the IDC, the credentials are decrypted employing the secret/passphrase provided by the user 4. Only the user should know the secret/passphrase

Code Number	**D5.2.7.1.3.1 - T485**
Business Value	**Medium**
Title	**Implementation of credential backup from the user device to the IDC**
Description	**As a** user **I want** be able to backup my ABAC credentials, encrypted with a passphrase decided by me, to the ID consolidator **so that** if I I lose my device, I don't lose my ABAC credentials
Acceptance Criteria	1. The credentials are stored securely on the IDC.

	2. The credentials are transferred securely. The connection will be tunneled through gateSAFE, thus ensuring the security of the SSL connection. 3. The user should give his consent that he trusts the consolidator to store his credentials 4. The user device will call the 3rd Party API in order to perform this task. 5. Only the encrypted credentials are transferred

Identity Consolidator Cryptographic Credentials Issuance and revocation module

The Identity Consolidator Cryptographic Credentials Issuance and revocation modules do not require access to the Identity Consolidator database from the Credential Management module. The Credential Management module has its own separate database in which credentials are stored. However, the user IDs employed in the Credential Management module database are the same as the ones in the Identity Consolidator database. This allows the ID Consolidator Intelligence to use the user ids as an initial handle for credential management.

Idemix stack on the ID consolidator

Code Number	**D5.2.6.1.3 – T455**
Business Value	**Medium**
Title	**Implementation of Idemix credential structure definition on the Identity Consolidator**
Description	**As the** Identity Consolidator **I want** to be able to define the structure of the idemix credentials **so that** I can define the verified user attributes that the credentials will contain
Acceptance Criteria	1. The Identity Consolidator is able to define through a management interface different idemix credentials and the attributes included in each credential

Code Number	**D5.2.6.1.2 – T453**

Business Value	**Medium**
Title	**Implementation of Idemix attribute verification on the Identity Consolidator**
Description	**As the** Identity Consolidator **I want to** be able to verify idemix credentials containing verified attributes of users attributes **so that** the user attributes can be used by Service Providers
Acceptance Criteria	1. The credentials will be verified by using the Idemix stack on the ID consolidator. The verified identity attributes can be then transferred to Service Providers via the OpenID Connect protocol.

Code Number	**D5.2.6.1.1 – T451**
Business Value	**Medium**
Title	**Implementation of Idemix credentials issuance on the Identity Consolidator**
Description	**As an** Identity Consolidator **I want to** be able to issue idemix credentials to users **so that** the user can use these cryptographic credentials for getting access to Service Providers
Acceptance Criteria	1 The values of the attributes in the idemix credential are verified by the ID consolidator 2. The credential structure is presented to the user at the beginning of the exchange

U-Prove stack on the ID consolidator

Code Number	**D5.2.6.1.1 – T452**

Business Value	High
Title	**Implementation of U-Prove credentials issuance on the ID consolidator**
Description	**As the** ID consolidator **I want to** be able to issue U-Prove credentials to users **so that I** the user can use these credentials to get access to Service Providers
Acceptance Criteria	1. The values of the attributes in the U-Prove credential are verified by the ID consolidator using the U-Prove stack 2. The credential structure is presented to the user at the beginning of the exchange

Code Number	**D5.2.6.2.2 – T454**
Business Value	High
Title	**Implementation of U-Prove attribute verification on the ID consolidator**
Description	**As the** Identity Consolidator **I want to** be able to verify U-Prove credentials containing verified attributes of users attributes **so that** the user attributes can be used by Service Providers
Acceptance Criteria	1. The credentials will be verified by using the U-Prove stack on the ID consolidator. The verified identity attributes can be then transferred to Service Providers via the OpenID Connect protocol.

Code Number	**D5.2.6.2.2 – T456**
Business Value	High
Title	Implementation of U-Prove credential structure definition on the ID consolidator

Description	**As the** ID consolidator **I want to** be able to define the structure of the U-Prove credentials **so that** I can define the verified user attributes that the credentials will contain
Acceptance Criteria	1. The ID consolidator is able to define through a management interface different U-Prove credentials and the attributes included in each credential

Privacy-Preserving Attribute-Based Access Control (PABAC) Credential Revocation

Code Number	**D5.2.1.1.1 – T329**
Business Value	**Medium**
Title	**Implementation of PABAC credential revocation**
Description	**As an** Identity Provider **I want to** be able to revoke a PABAC credential **so that** the credential is no longer valid and cannot be employed by the user to access Service Providers
Acceptance Criteria	1. The revoked credential is no longer accepted by Service Providers

Identity Provider Cryptographic Credentials Issuance module

Identity Providers are responsible for issuing Privacy-Preserving Attribute-Based Access Control credentials to users. Identity Providers are trusted by Service Providers.

Idemix credential-issuing stack on Identity Providers

Code Number	**D5.2.5.1.3**
Business Value	**Medium**
Title	**Implementation of Idemix credential structure definition on Identity Providers**

Description	**As an** Identity Provider **I want** to be able to define the structure of the idemix credentials **so that** I can define the verified user attributes that the credentials will contain
Acceptance Criteria	1. The Identity Provider is able to define through a management interface different idemix credentials and the attributes included in each credential

Code Number	**D5.2.5.1.1 – T434**
Business Value	**Medium**
Title	**Implementation of Idemix issuance on Identity Providers**
Description	**As an** Identity Provider **I want to be** able to issue idemix credentials to users **so that** the user can use these credentials to get access to Service Providers
Acceptance Criteria	1. The values of the attributes in the idemix credential are checked against available resources (e.g. a database) 2. The values of the attributes in the idemix credential are verified by the identity provider 3. The credential structure is presented to the user at the beginning of the exchange

U-Prove credential-issuing stack on Identity Providers

Code Number	**D5.2.5.2.3 – T439**
Business Value	**Medium**

Title	**Implementation of U-Prove credential structure definition on Identity Providers**
Description	**As an** Identity Provider **I want to** be able to define the structure of the U-Prove credentials **so that** I can define the verified user attributes that the credentials will contain
Acceptance Criteria	1. The Identity Provider is able to define through a management interface different U-Prove credentials and the attributes included in each credential

Code Number	**D5.2.5.2.1 - T435**
Business Value	**Medium**
Title	**Implementation of U-Prove issuance on identity providers**
Description	**As an** Identity Provider **I want to** be able to issue U-Prove credentials to users **so that** the user can use these credentials to get access to Service Providers
Acceptance Criteria	1. The values of the attributes in the U-Prove credential are verified by the identity provider 2. The credential structure is presented to the user at the beginning of the exchange

10.6.2. Security & Privacy Requirements

#	Security & Privacy Requirements	Rational / Comments	Mandatory or Not
S&P6.1	Cryptographic credentials must be used to prove the ownership of attributes such that the privacy of the user cannot be compromised (un-traceable, un-linkable credentials)	-	Yes

S&P6.2	The platform should support revocation of leaked/obsolete cryptographic credentials	-	No
S&P6.3	The platform should provide access control	Service owners can only define their own policies. Organizations have different services requiring different policies.	Yes
S&P6.4	The solution should provide a mechanism to determine whether a rule can result in different outcomes	If a rule always gives a positive or negative result; there is probably some error.	
S&P6.5	If possible, attributes should be fetched from authentic data source in real-time		
S&P6.6	Unencrypted cryptographic credentials should be stored on user device and never leave it.		Yes
S&P6.7	Cryptographic credentials on user device must be protected by eavesdropping/leakage.		Yes
S&P6.8	Encrypted credentials should be difficult to be decrypted		Yes
S&P6.9	Cryptographic credentials should leave the device only in encrypted form.		Yes
S&P6.10	Cryptographic credentials should be encrypted by using a secure key known only to the user: only the user can recover and decrypt them.		Yes
S&P6.11	Cryptographic credentials should be stored remotely for recovery purposes only in encrypted form.		Yes
S&P6.12	Cryptographic credentials must be used to prove the ownership of attributes such that the privacy of the user cannot be compromised.		Yes
S&P6.13	When proving ownership of attributes to different services the user should be un-traceable and un-linkable.		Yes
S&P6.14	The credentials must be protected while being transferred.	The credentials transmitted to the user must be protected (i.e. encrypted communication or using cryptographic credentials of the user) in order to avoid eavesdropping.	Yes
S&P6.15	Attributes definition should be validated to avoid inconsistency and security issues.		Yes
S&P6.16	The user should be able to remove all credentials owned by him from the platform.		Yes

S&P6.17	The PII acquired by the platform should have expiration. After such expiration, the platform should delete such information.	No
S&P6.18	The user should be able to select the set of attributes that he wants to disclose in a credential verification process.	Yes
S&P6.19	The user should be informed about the PII that are going to be involved in a credential issuing process.	Yes
S&P6.20	Users cannot be able to collude by sharing credentials.	Yes
S&P6.21	Users should be informed on the terms and conditions of the service.	Yes
S&P6.22	Identity Providers should be informed on the terms and conditions of the service.	Yes
S&P6.23	Service Providers should be informed on the terms and conditions of the service.	Yes
S&P6.24	The multi-show unlinkability is guaranteed for Idemix	Yes
S&P6.25	The untraceability guarantee is preserved for U-Prove	Yes
S&P6.26	The same Security & Privacy Requirements apply from section 1.1.2.2, S&P2.18 to S&P2.28	Yes

10.6.3. Operational Requirements

#	Operational Requirements	Rational / Comments	Mandatory or Not
O6.1	The reasoning module should be able to make decisions very fast.	Complex policies should not cause slow user experience.	Yes
O6.2	The solution needs to work in a distributed model where attributes / information can in some cases by cached and in some cases retrieved in real time from the respective sources	Speed should be optimized.	No
O6.3	The user device should not be rooted (the user should not have administration privileges on the device).		Yes
O6.4	The user device should be equipped with a Trusted Execution Environment (TEE).		No
O6.5	The user device should be equipped with a camera.		No

11. Conclusion

Deliverable 2.6 is based upon the use cases of deliverable 2.5 and aims at defining concrete technical requirements of the whole ReCRED platform.

For this reason, this deliverable covers a wide range of user stories, and additionally it incorporates a number of horizontal user stories that highlight the registration and access to the ReCRED platform, and the functions that user can perform. The technical requirements derived from all the described user stories along with the reference architecture that aligns with them and is described in deliverable 2.3 are the basis for the whole ReCRED implementation outlining the work to be done in each of the technical Work Packages.