



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



WP7– Large Scale Pilots and End User Experience Assessment
Deliverable D7.3 “All Four Pilots Initial Setup & Progressing”

Editor(s): Vangelis Bagiatis

Author(s): Vangelis Bagiatis, Kostas Flokos, Vasilis Markopoulos (UPCOM), Annamaria Recupero (CNIT), Angus Stewart (VERI), Dimitris Katsaros (EXUS), George Gugulea (CSGN)

Dissemination Level: Public

Nature: Other

Version: 0.9

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 1 st , 2015
Duration	36 Months

Partners

	University of Piraeus research center	Greece
	Telefonica Investigacion Y Desarrollo Sa	Spain
	Verizon Nederland B.V.	The Netherlands
	Certsign SA	Romania
	Wedia Limited	Greece
	EXUS Software Ltd	U.K.
	Upcom Bvba (sme)	Belgium
	De Productizers B.V.	The Netherlands
	Cyprus University of Technology	Cyprus



Universidad Carlos III de Madrid

Spain



Consorzio Nazionale
Interuniversitario per le
Telecomunicazioni

Italy



Studio Professionale Associato
a Baker & McKenzie

Italy

Document History

Version	Date	Author	Remarks
0.1	01/03/2017	Vangelis Bagiatis (UPCOM)	Initial Table of Contents
0.2	31/03/2017	Vangelis Bagiatis (UPCOM), Kostas Flokos (UPCOM), Vasilis Markopoulos (UPCOM), Annamaria Recupero (CNIT)	Added sections 4 and 6
0.3	07/04/2017	Angus Stewart (VERI)	Added section 3
0.4	11/04/2017	Dimitris Katsaros (EXUS)	Added section 5
0.5	24/04/2017	George Gugulea (CSGN)	Added section 2
0.6	25/04/2017	Vangelis Bagiatis (UPCOM), Vasilis Markopoulos (UPCOM)	Editor review. Also, added sections 1, 7 and Executive Summary
0.7	27/04/2017	George Gugulea (CSGN), Angus Stewart (VERI), Dimitris Katsaros (EXUS), Annamaria Recupero (CNIT)	Final adjustments, according to editor's review
0.8	30/04/2017	Konstantinos Papadamou (CUT)	Final review by CUT
0.9	25/08/2017	Vangelis Bagiatis (UPCOM)	Removed IPR, anonymized some data, and other minor corrections

Executive Summary

In deliverable D7.2, we described the initial setup of the campus-wide Wi-Fi and web services access control pilot, which started very early in the project (M05), in order to demonstrate device-centric-authentication (DCA) and attribute-based device-centric access control solution in university premises. In this deliverable, we describe the extended version of this pilot, including the addition of new modules, changes to the pilot flows, UX changes, as well as the setup of the pilot environment in UC3M premises.

In this deliverable, we also describe the initial setup of the three remaining pilots:

- Student Authentication & Offers Pilot
- Age Verification Online Gateway
- Microloan Origination

For each pilot, we describe the main scenarios and flows, and we provide an overview of their hardware and software architecture while describing their main components and its role. We also highlight the privacy and security considerations for each pilot, in an attempt to also address the operational objectives of the PIA and Maturity Assessment during the four pilots.

Finally, we identify and describe the process and the methods that will be used for the UX assessment of the four pilots. The actual UX assessment will take place during the last year of the project and its results will be reported in D7.4.

Table of Contents

Executive Summary	4
List of Figures	7
1 Introduction	9
2 Campus Wi-Fi and Web Services Access Control	10
2.1 Description of the Pilot	10
2.2 Updates of the User Device Android Application	10
2.2.1 User Registration.....	10
2.2.2 Attributes Retrieval	12
2.2.3 Resource Access:	13
2.3 Hardware Architecture	16
2.4 Software Architecture	17
2.5 QR Authentication Extension	19
2.6 Privacy & Security Considerations	23
2.6.1 Physical Protection and Network Security	23
2.6.2 Configuration and Security Settings.....	23
2.6.3 Access Control.....	23
2.6.4 Monitoring	23
2.6.5 Malware Protection	24
2.6.6 Patch Management.....	24
2.6.7 Change Management.....	24
2.6.8 Incident Management.....	24
2.6.9 Protection of Logs and Data.....	24
2.6.10 Cryptography and Protection of Electronic Communication	24
2.7 Risk Assessment	25
2.7.1 Initial Risk Score	25
2.7.2 Risk Actions	25
3 Student Authentication & Offers	27
3.1 Description of the Pilot	27
3.1.1 Merchant Registration	27
3.1.2 Campaign Management.....	28
3.1.3 Purchase of Offers.....	30
3.2 Components Overview.....	32
3.3 Hardware Architecture	35

3.4	Software Architecture	36
3.5	Privacy & Security Considerations	37
3.6	Risk Assessment	38
3.6.1	Initial Risk Score	39
3.6.2	Risk Actions	39
4	Age Verification Online Gateway	40
4.1	Description of the Pilot	40
4.1.1	End-user Registration.....	40
4.1.2	Website Registration.....	41
4.1.3	Age Verification.....	41
4.2	Components Overview.....	42
4.2.1	Age Gate Mobile App	42
4.2.2	Age Gate Server	44
4.2.3	Identity Consolidator (as Identity Provider).....	46
4.2.4	Service Provider(s)	47
4.3	Hardware Architecture	48
4.3.1	Database Server - Application Server	48
4.3.2	User Device	49
4.4	Software Architecture	49
4.4.1	Infrastructure Software.....	50
4.4.2	Required Modules.....	50
4.4.3	Environment and Deployment.....	52
4.5	Privacy & Security Considerations	53
4.5.1	Physical Protection and Network Security.....	53
4.5.2	Configuration and Security Settings.....	54
4.5.3	Access Control.....	54
4.5.4	Monitoring	55
4.5.5	Malware Protection	55
4.5.6	Patch Management.....	56
4.5.7	Change Management.....	56
4.5.8	Incident Management.....	57
4.5.9	Protection of Logs and Data.....	57
4.5.10	Cryptography and Protection of Electronic Communication.....	57
4.6	Risk Assessment	57

4.6.1	Initial Risk Score	57
4.6.2	Risk Actions	58
5	Microloan Origination	59
5.1	Description of the Pilot	59
5.1.1	End User Registration to ReCRED Platform	60
5.1.2	Bank Website / Mobile Application Initialization	60
5.1.3	Microloan Verification	60
5.2	Components Overview.....	61
5.2.1	Microloan Mobile App	61
5.2.2	Microloan Website / Service Provider	64
5.2.3	ReCRED Identity Consolidator / Provider.....	65
5.2.4	Behavioral Authentication Server	66
5.2.5	QR Authentication Server	66
5.3	Hardware Architecture	66
5.4	Software Architecture.....	67
5.4.1	Required ReCRED Components.....	67
5.5	Privacy & Security Considerations	70
5.6	Risk Assessment	71
5.6.1	Initial Risk Score	71
5.6.2	Risk Actions	71
6	UX Assessment.....	72
7	Conclusions / Future Activities.....	73

List of Figures

Figure 1: Campus Wi-Fi pilot - Registration Flow.....	11
Figure 2: Campus Wi-Fi pilot - User switch between CUT and IMDEA premises.....	12
Figure 3: Campus Wi-Fi pilot - Obtaining User Attributes	13
Figure 4: Campus Wi-Fi pilot - Access to Resources	14
Figure 5: Campus Wi-Fi pilot (IMDEA) - Network Infrastructure	16
Figure 6: Campus Wi-Fi pilot (IMDEA) - Software components and REST Interfaces.....	18
Figure 7: Campus Wi-Fi pilot (IMDEA) - Network interfaces	19
Figure 8: Campus Wi-Fi pilot - Architecture after QR integration	21
Figure 9: Campus Wi-Fi pilot - Authorization server after QR integration	21
Figure 10: Campus Wi-Fi pilot - Flow after QR integration.....	22
Figure 11: Student pilot - Overview flow diagram.....	27

Figure 12: Student pilot - Merchant registration.....	28
Figure 13: Student pilot - Management of campaigns	29
Figure 14: Student pilot - Part of the campaign creation form.....	30
Figure 15: Student pilot - Offers and purchases	32
Figure 16: Student pilot - Consent management.....	32
Figure 17: Student pilot - Component diagram	33
Figure 18: Student pilot - QR Code OpenAM flow	34
Figure 19: Student pilot - Hardware architecture.....	36
Figure 20: Age verification pilot - Scan QR code using the Age Gate mobile app	43
Figure 21: Age verification pilot - View access history and revoke access	44
Figure 22: Age verification pilot - Register new website to Age Gate	45
Figure 23: Age verification pilot - Review and accept / reject requests (operator)	45
Figure 24: Age verification pilot - Reports generation.....	46
Figure 25: Age verification pilot - Selection of age verification method	47
Figure 26: Age verification pilot - QR code creation.....	47
Figure 27: Age verification pilot - Entrance to the Service Provider’s website	48
Figure 28: Age verification pilot - Hardware architecture	48
Figure 29: Age verification pilot - Environment and deployment	52
Figure 30: Microloan pilot - Welcome screen.....	62
Figure 31: Microloan pilot - Show microloans	63
Figure 32: Microloan pilot - Show microloan details.....	64
Figure 33: Microloan pilot - Loan selection	65
Figure 34: Microloan pilot - Loans history	65
Figure 35: Microloan pilot - Hardware architecture.....	67
Figure 36: Microloan pilot - Software components.....	70

1 Introduction

In the end of the first year of the project, a first prototype of the campus-wide Wi-Fi and web services access control pilot was deployed at CUT premises, acting as a somewhat controlled setting with the goal to demonstrate the functionalities of the ReCRED systems “at large”. This pilot has been further extended during the second year with additional flows and functionality as well as with several improvements to the user interface (UI) in order to improve users’ experience. These improvements were according to a preliminary UX assessment that was performed by CNIT. Later on, in the end of the second year the Wi-Fi and web services access control pilot has also been deployed at IMDEA premises. All the functional, operational and technical details of this new prototype of the Wi-Fi pilot are described in Section 2 of this deliverable.

At the same time, three additional pilots have been initialized in the end of the second year of the project (M24) and will be executed until the end of the project. Each of these pilots is focused on a different real-life scenario, aiming at demonstrating the TRL7 readiness of the ReCRED’s software modules, and at proving the viability of our proposed new commercial services that make use of electronic identification and authentication.

1. In the **Student Authentication and Offers** pilot, ISIC students will be able to earn discounts and access offers seamlessly through their DCA-enabled mobile devices. Affiliated merchants will be able to register and use a back-end system (Campaign Manager), in order to create their offers and define certain policies on them.
2. In the **Age Verification Online Gateway** pilot, end-users that want to visit an age-restricted website will be able to anonymously prove that they are above a certain age, with the use of device centric authentication and Quick Response (QR) code based credential transfer to their desktop. The website owners will be able to register their age-restricted websites and set age-related access policies (e.g. visitors must be above 21 years old).
3. In the **Microloan Origination** pilot, bank customers will be able to apply for microloans and have them granted (or rejected), without revealing or disclosing any of their personal and/or sensitive data. The microloan providers will be able to review these microloan applications, based on whether the applicant’s financial information is above a certain limit or not

In sections 3-5 of this deliverable, we present in detail the following:

- i. the flows of these three pilots
- ii. the required components and the role of each component in each pilot
- iii. the hardware architecture of each pilot
- iv. the software architectures, including the required infrastructure software and the ReCRED modules that are used in each pilot (and their role)

- v. the privacy and security considerations that need to be addressed during the execution of the pilots
- vi. the initial risk assessment for each pilot, including foreseen mitigation actions

Furthermore, during the last year of the project an expanded assessment of the users’ experience will be performed for all the pilots. The users’ feedback will be collected and analyzed, according to which any improvements to the applications UI will be implemented. The methodology and the research methods that will be used for the assessment of the users’ experience are described in Section 6 of this deliverable.

2 Campus Wi-Fi and Web Services Access Control

2.1 Description of the Pilot

The goal of the campus Wi-Fi Pilot is to control user access to various campus resources, such as Wi-Fi and web services. These resources can be accessed by the various users (students/professors/visitors), by revealing the values of their identity attributes. Resource authorization rules are defined by network administrators, in the form of policies that define which attribute values can unlock certain resources.

In the previous deliverable (D7.2), we described the authentication and authorization of the user with the ReCRED software stack, in order to allow access to the CUT network premises. In this deliverable, we mainly focus on the deployment of the pilot on the IMDEA premises, which has a different architecture but retains the same functionality: user access to the network resources. We will also present the modifications made to the pilot software components, both to the mobile app and the web services.

2.2 Updates of the User Device Android Application

For this deliverable, a new version of the pilot has been developed, that includes UI changes, usage of new open source libs, such as Volley for HTTPS communication and Realm for ORM. The FIDO UAF client logic has been moved inside an Android Library (AAR), an AAR that provides an SSLContext class that permits Volley and other HTTPS libs to recognize the demo certificate configured inside the gateSAFE container available at IMDEA premises.

All the users can use the same application on the Android device, which is currently distributed through the Google Console. There are two lists of users, one for CUT and one for IMDEA, and both lists are associated to the same mobile application.

To form an understanding of how the new pilot works we present bellow its three main operations.

2.2.1 User Registration

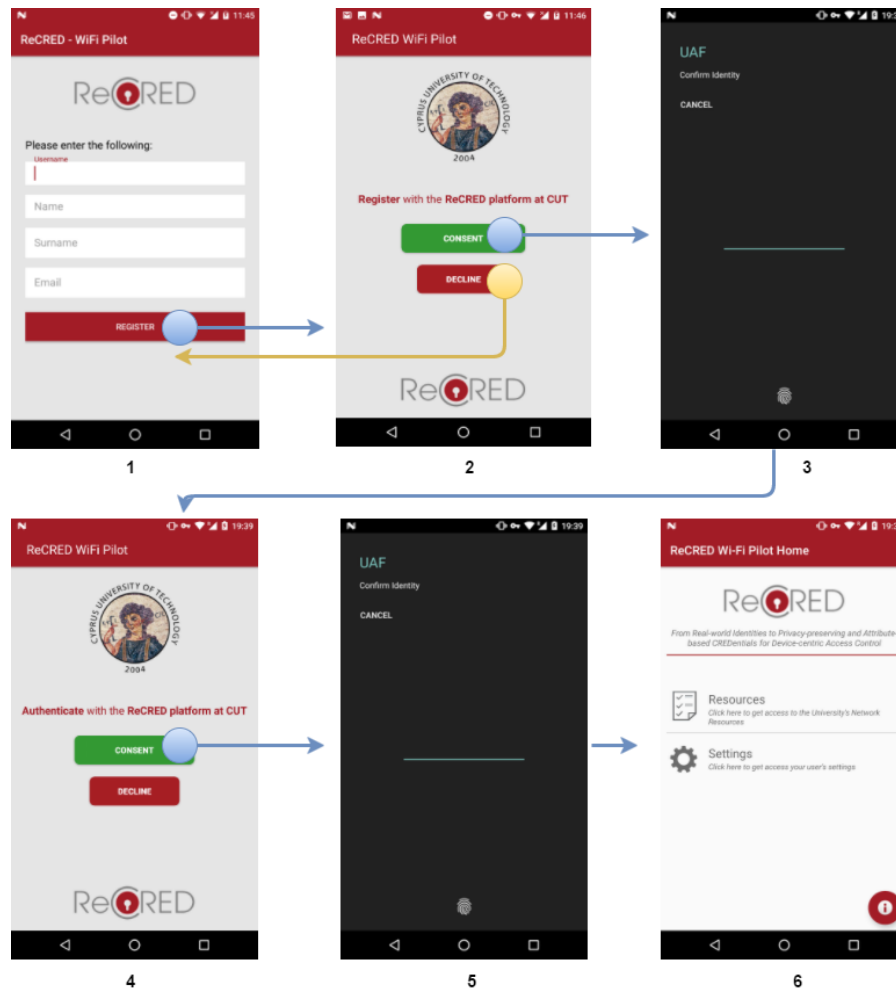


Figure 1: Campus Wi-Fi pilot - Registration Flow

In order to register, a user goes through the following steps:

1. The first time the user opens the Wi-Fi pilot application, he is presented with a registration screen. The registration process requests the user to enter the username given by the network administrator, along with other basic information, such as his name, surname and email. After the user inputs the information, he must choose his location (CUT or IMDEA). As we tried to avoid user confusion given by complicated configurations, the user has a choice on the first page between CUT and IMDEA premises. According to the user's selection, the URL end-points are updated, in order to match the selected campus.
2. The application asks for the user's consent to register with the service.
3. The user enters his fingerprint or his pin, depending on his current setup.
4. After the registration process ends, the application automatically tries to authenticate to the ReCRED platform and asks for the user's consent again.
5. The user enters his fingerprint or pin, depending on his current setup.
6. The user is then redirected to the main screen of the Wi-Fi application. After the registration process is completed, every time the user tries to open the application, he will go through the authentication process only (steps 4 – 6).

The user can select between registering at the ReCRED platforms available at CUT or IMDEA, by using the switch button highlighted in the following picture:

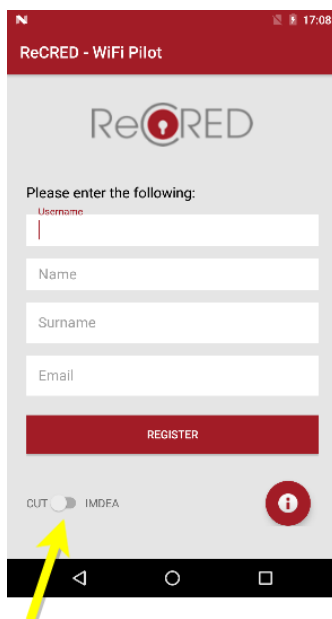


Figure 2: *Campus Wi-Fi pilot* - User switch between CUT and IMDEA premises

2.2.2 Attributes Retrieval

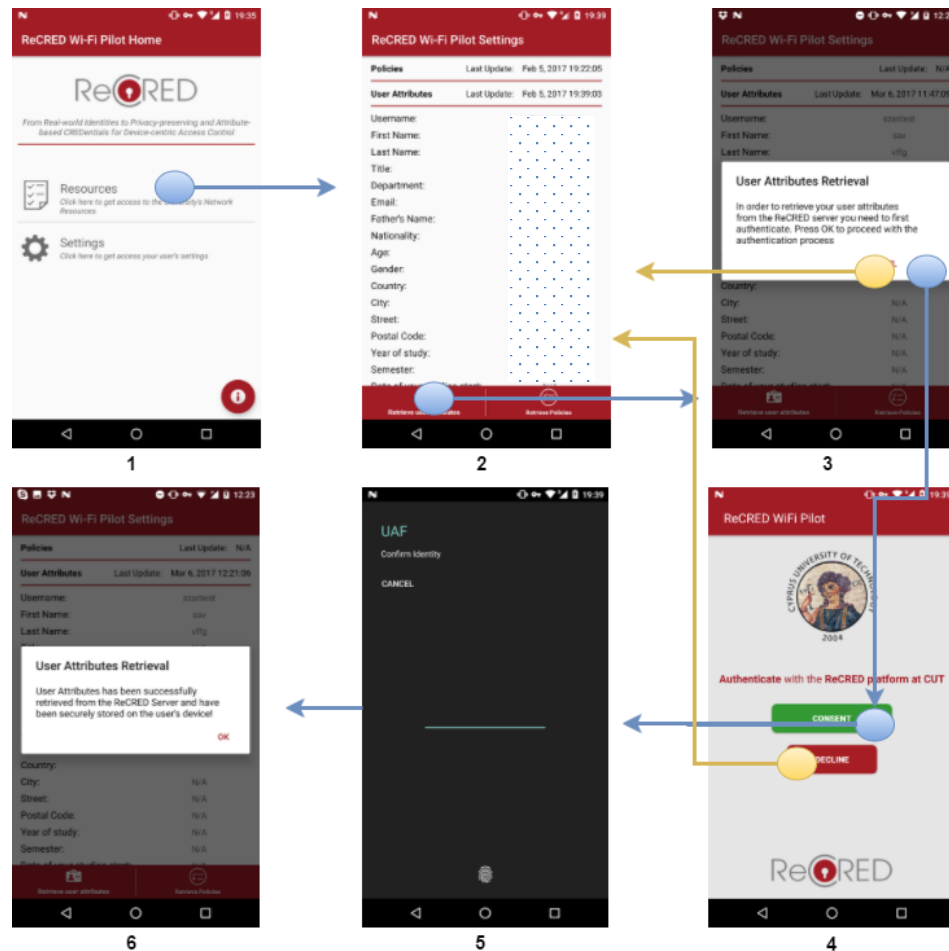


Figure 3: Campus Wi-Fi pilot - Obtaining User Attributes

In order to retrieve attributes from the Authentication server, the following steps are required:

1. The user selects the Settings section from the main screen.
2. From the Settings screen, the user can view and update his attributes, and also retrieve the newest policies defined by the network administrator.
3. After selecting to retrieve his attributes, the user is presented with a dialog, informing him how the retrieving process functions.
4. The user must consent or decline the authentication to the ReCRED platform.
5. The user enters his fingerprint or pin, depending on his current setup.
6. A dialog informing the user about the attribute retrieval success or failure is shown.

2.2.3 Resource Access:

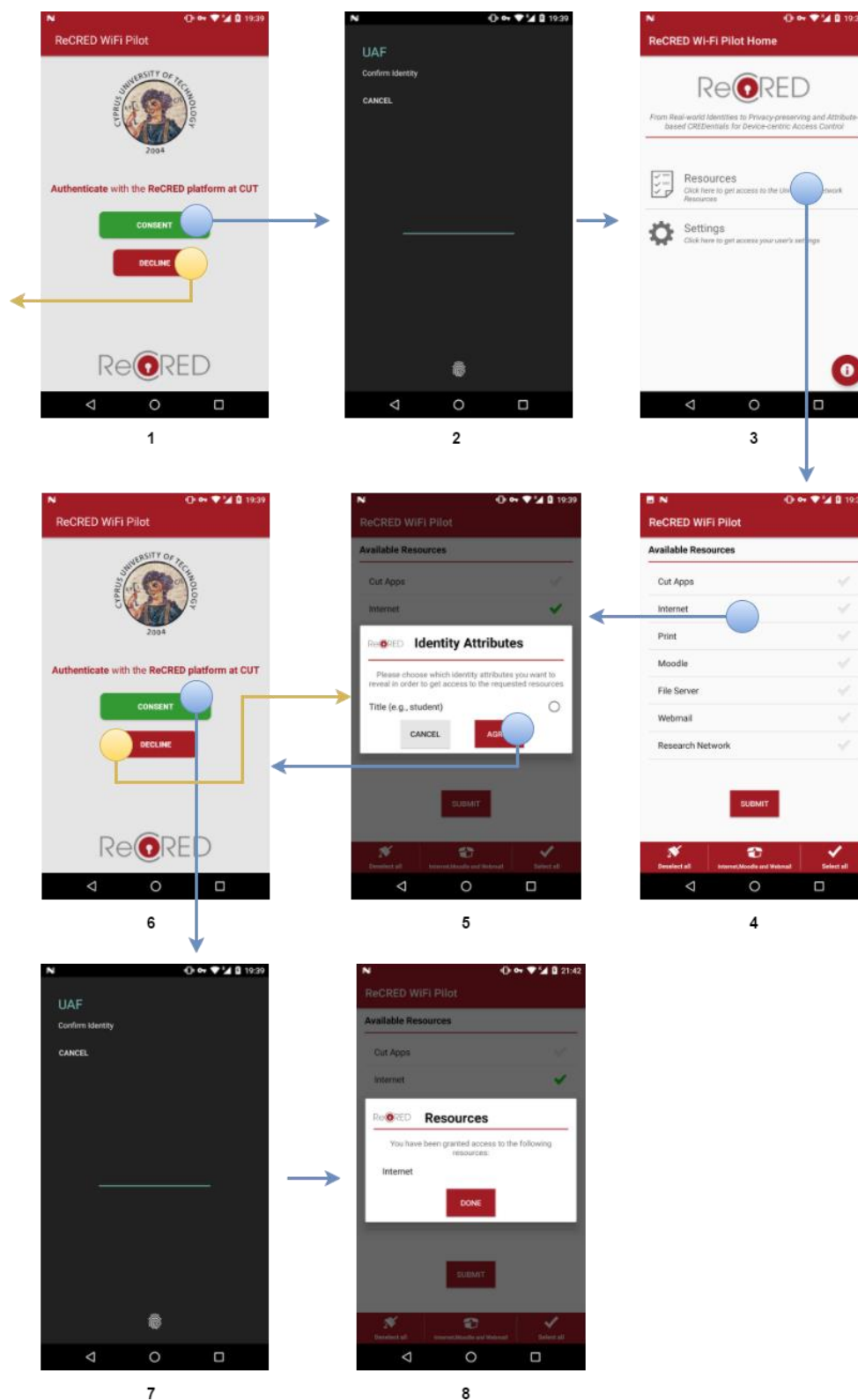


Figure 4: Campus Wi-Fi pilot - Access to Resources

In order to access each campus available resources, the user must go through the following process:

1. In steps 1 – 3 the user authenticates to the pilot and selects the resources menu from the main screen.
2. In order to access the resource, in steps 4 – 5 the user is presented with a list of attributes which he must consent to be revealed.
3. In steps 6 – 8, the user consents to reveal the required attributes and he is informed if the attribute authentication process was executed successfully or not.

ReCREDSSLContext Android Library

Considering that the gateSAFE instance at IMDEA premises is configured with a certificate issued by an authority not recognized as trusted by Android, a method to overcome this issue was developed in the form of an AAR that leverages the way Java and subsequently Android implements TLS.

Android delegates trust decisions to a TrustManager class. Each SSLSocket instance created has access to this class via the associated SSLContext. Each TrustManager has a set of trusted CA certificates (trust anchors) and makes trust decisions based on those: if the target party's certificate is issued by one of the trusted CA's, it is considered trusted itself.

One way to specify the trust anchors is to add the CA certificates to a Java key store file, referred to as a 'trust store'. The default Android TrustManager is initialized using the system trust store which is generally a single key store file, saved to a system location and pre-populated with a set of major commercial and government CA certificates. If you want to change this, you need to create an appropriately configured TrustManager instance, either via a TrustManagerFactory, or by directly implementing the X509TrustManager interface.

The ReCREDTrustManager class implements the X509TrustManager interface and uses two trust stores, the system one and another which contains the authority not recognized by default. When this trust manager checks to see if the authority is located inside the system trust store and fails to find it, continues to search in the new defined trust store.

ReCREDSSLContext class creates the trust store that contains the untrusted authority certificate and passes it to the new trust manager. Using the new trust manager instance, a new SSLSocketFactory class that generates SSLSockets which recognize the custom authority is created. This SSLSocketFactory can then be used by HTTP clients when connecting to the IMDEA services.

Following is a short example of how the new custom SSLSocketFactory can be used with the Volley HTTP client:

```

HurlStack hurlStack = new HurlStack() {
    @Override
    protected HttpURLConnection createConnection(URL url) throws IOException {
        HttpURLConnection httpsURLConnection =
            (HttpURLConnection)super.createConnection(url);
        try {
            httpsURLConnection.setSSLSocketFactory(
                ReCREDSSLContext.ReCREDSSLSocketFactory(activityContext));
        }
        catch (Exception e) {
            e.printStackTrace();
        }
        return httpsURLConnection;
    }
};
final RequestQueue requestQueue = Volley.newRequestQueue(this, hurlStack);
requestQueue.add(request);

```

2.3 Hardware Architecture

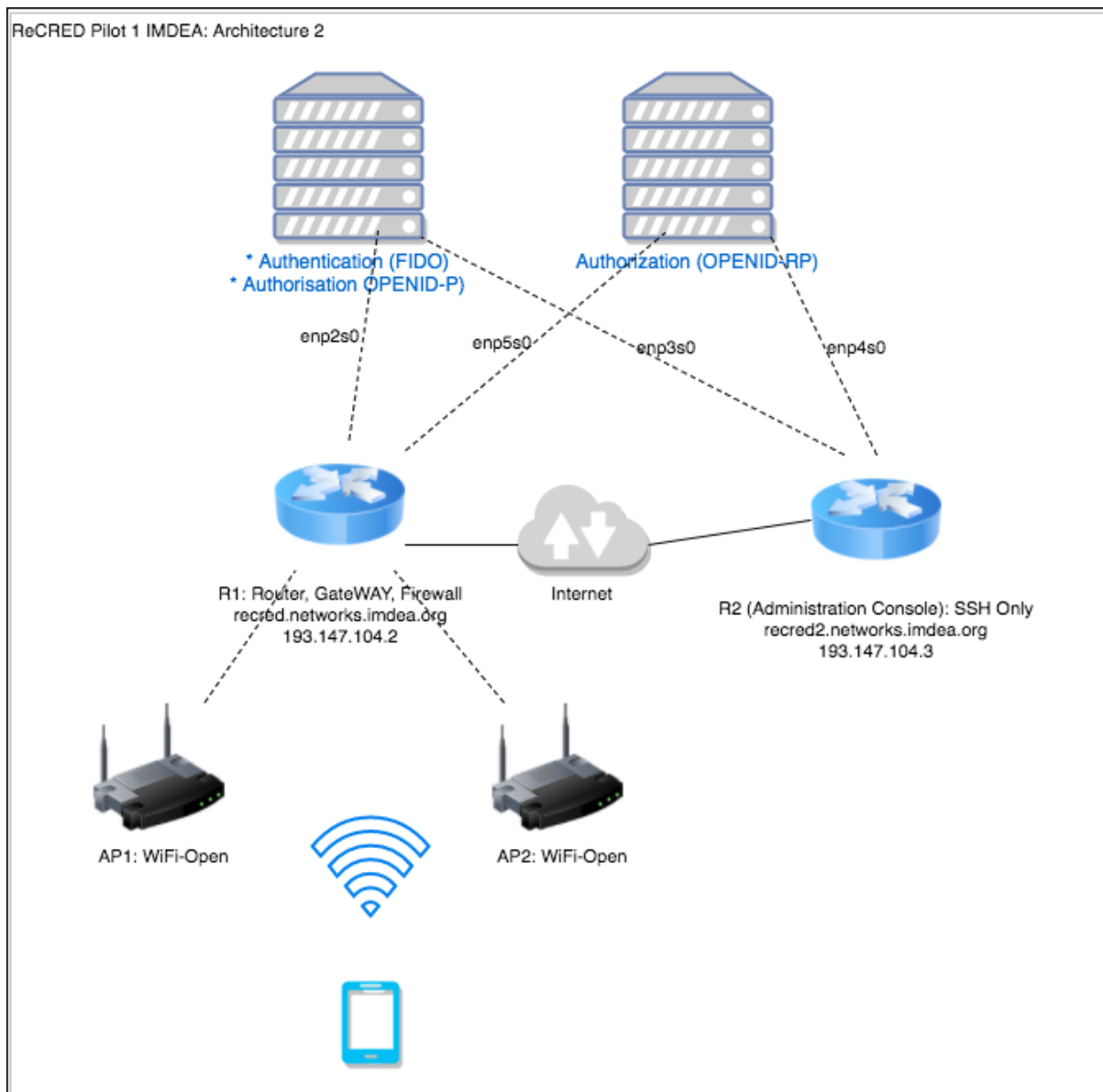


Figure 5: Campus Wi-Fi pilot (IMDEA) - Network Infrastructure

Components:

- **R1:** Has the role to route network traffic between the Wi-Fi, ReCRED infrastructure (S1, S2) and Internet connection.
- **R2:** The role of R2 is administrative only, it has access to the administration interfaces of S1 and S2.

The network access enforcement is realized by the mean of R1 firewall rules. In case of a misconfigured firewall rule in the development process, the access to the pilot servers might be denied and for this reason we need a different route for administration purposes.

This different route is realized by the mean of R2 that has the only role of exporting SSH connections to the ReCRED server S1 and S2. That is realized by IP tables rules, and both servers will have private IP addresses.

- **AP1, AP2:** Open Wi-Fi. There can be as many access points as necessary to ensure the appropriate radio coverage for all the users
- **S1:** Authentication Server: Also does the OpenID Provider part of authorization
- **S2:** Authorization Server: Also controls R1

Before the authentication, the mobile phones are able to access only S1 and S2 ReCRED services, through the R1 router. The router is able to route through all the unauthenticated traffic originating on the user device, only to the ReCRED services and not to the internet connection. The internet traffic from Wi-Fi is blocked by the firewall service running on R1.

The ReCRED application stack performs the authentication and the authorization process, and upon a successful authentication, the Authorization Service performs an update on R1 firewall rules, adding the user to the Internet access list

2.4 Software Architecture

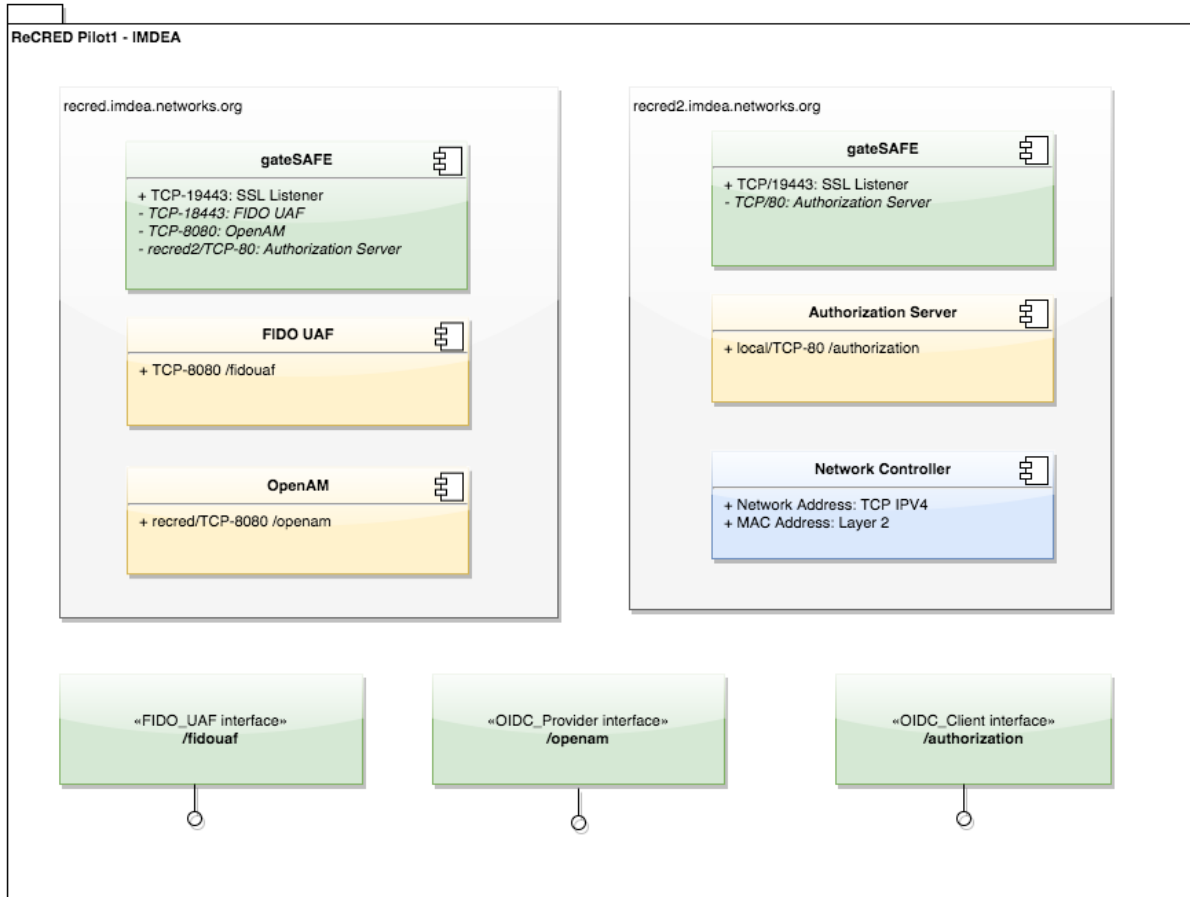


Figure 6: Campus Wi-Fi pilot (IMDEA) - Software components and REST Interfaces

The ReCRED software stack contains web services and other software components, that together ensure a good policy, authenticate and authorize the user and, in the end, enforce the configured policy on the network level. There are three web services that ReCRED exposes to authenticate and authorize the user: OpenAM, Authorization Service and FIDO UAF Service. Corresponding to these three components, are the three interfaces exposed by ReCRED, corresponding to the following URL:

- /fidouaf
- /openam
- /authorization

In front of each web service, gateSAFE is deployed, along with reverse proxy and SSL terminator. Each software component runs in its own Docker container and they communicate one with each other through the TCP/IP network stack.

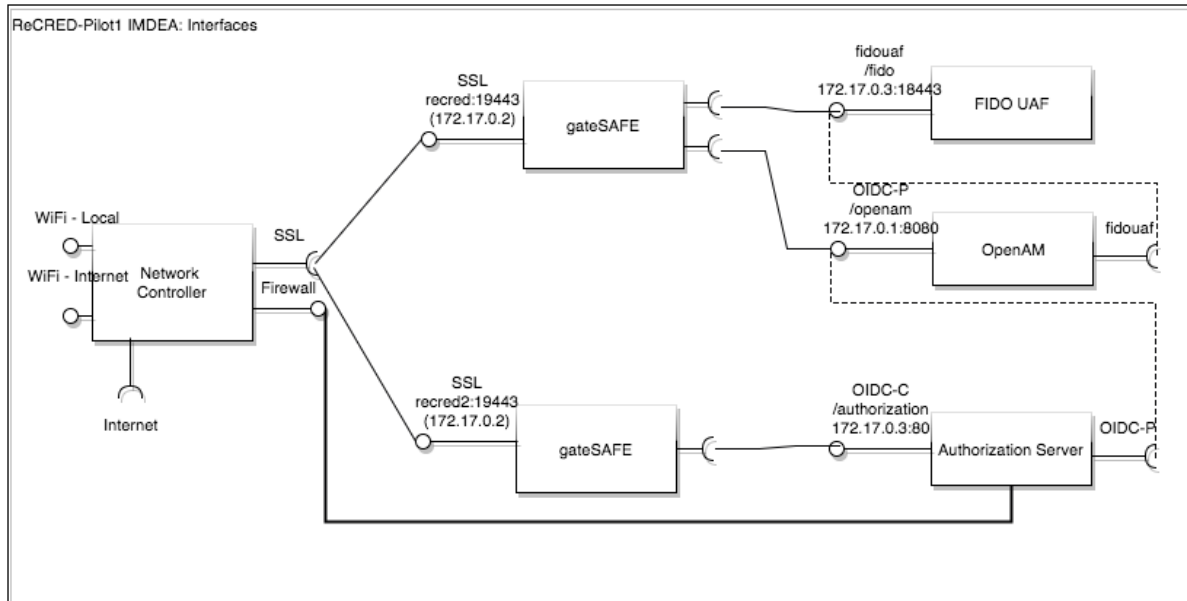


Figure 7: Campus Wi-Fi pilot (IMDEA) - Network interfaces

The diagram above depicts the network interfaces used for the pilot.

- Network Controller exposes three interfaces:
 - Unauthenticated local network access where the access is restricted to the ReCRED software stack only
 - Authenticated Internet Access that is used by the user device after the user successfully authenticates
 - Network access configuration (Firewall) that is only accessible to the Authorization Service
- gateSAFE components expose one TLS enabled server-side authentication interface, and require one HTTP interface to the service they protect
- FIDO UAF ReCRED Server is deployed to provide user authentication. It provides an interface that is accessed by the user device and the OpenAM service as well
- OpenAM component exposes one interface for the user device and requires one for the FIDO UAF protocol
- Authorization Server exposes one interface for the user device and requires two: one for the OpenID Connect protocol with OpenAM and one with the Network Controlled for the user network access enforcing. The last interface is a remote shell one and is available only to the Authorization Server

2.5 QR Authentication Extension

In ReCRED, we focus on the problem of authenticating users to resources using the user’s mobile phone and in this pilot, we demonstrate a real-life scenario, where the students will obtain access to

the university resources from their mobile phone. But sometimes this is not enough, as usually students have another mobile device, a laptop, and use their laptop in the studying process and they do need access to the university resources from their laptops as well. As the students already have a mobile device authenticated to the Wi-Fi network, they don't need to have the ReCRED client-side software stack running on the laptops as well, but they will use their already authenticated mobile phones to authenticate the second device, the laptops, in a process of “credential transfers” from the phone to the laptop. In reality, no credential will be transferred, but a new session, the laptop session will be authenticated using the student phone as a trusted device.

To integrate the Quick Response (QR) authentication module inside the Wi-Fi Pilot we introduced some changes in the Authorization Server (Relying Party) and Mobile Application. More specifically, we have added an Android Library (AAR) that aims to scan a QR code received from the QR Authentication Server and send it to the Authorization Server to authenticate the web session. The steps of the web application authentication process using QR have been described in deliverable D3.3.

The QR module includes three big sub-components:

- A client-side component that runs on the user device as Android Library (AAR) and is included in the Wi-Fi Pilot Android Application;
- A Service Provider that has been integrated into the Authorization Server. This component includes a generic view that defines the authentication process to a specific resource as well as a backend end that will be an extension of the REST interfaces within the RP;
- A QR Authentication Server which acts like a Service Provider and validates the QR received from the RP. The validation of the QR code is realized based on a previous request received from the Service Provider back-end (the service the user is trying to log in).

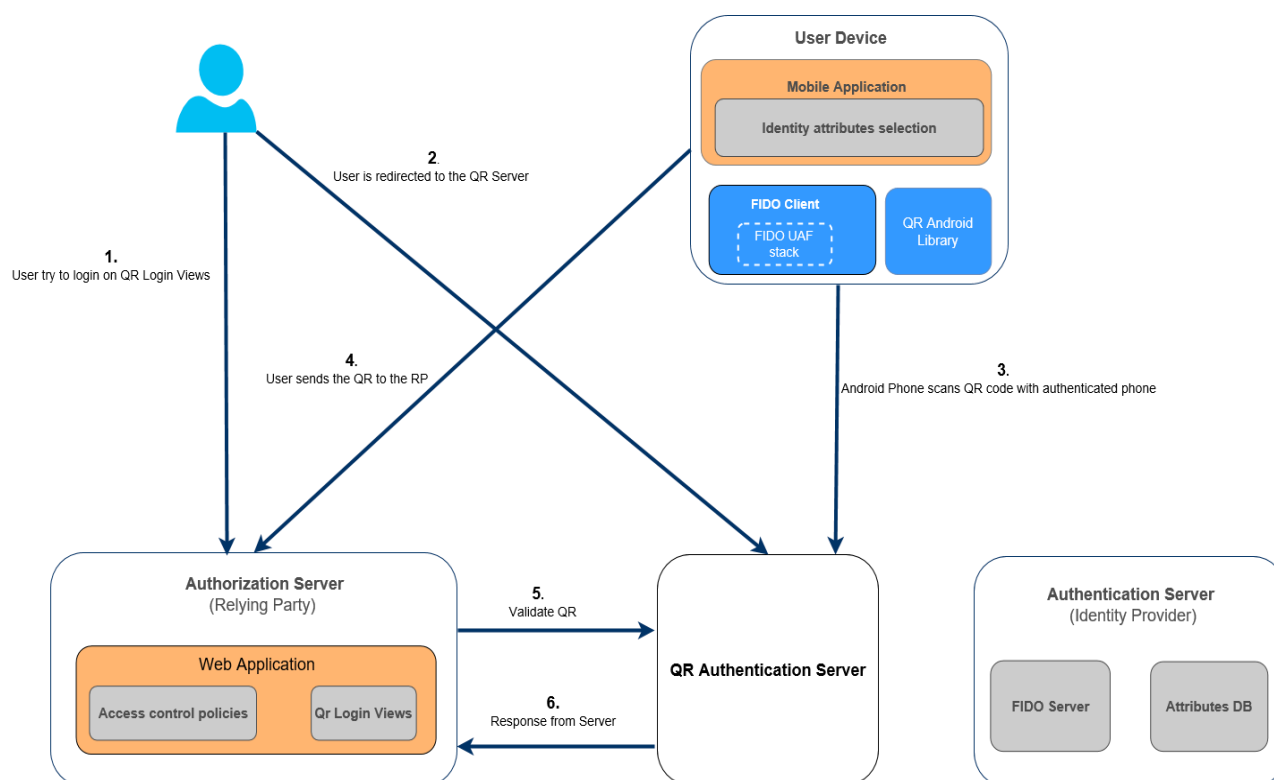


Figure 8: Campus Wi-Fi pilot - Architecture after QR integration

As mentioned earlier, several changes have been made to the Authorization Server to be able to integrate the QR component. The Relying Party within the Pilot behaves as an OpenID connect client (OIDC) for the Authentication Server. To be able to authenticate the web application to the Service Provider will use the previous authenticated connection that exists between the Android terminal and the Authorization Server. When the user sends the QR code to the Authorization Server, the RP will realize that this connection is authenticated and will make a request to the QR server to validate the received code (the QR authentication server will trust the Relying Party and behaves as a Service Provider in this case). If the validation of the code succeeded, the QR Server will notify the Service Provider by calling a callback function, as described in D3.3.

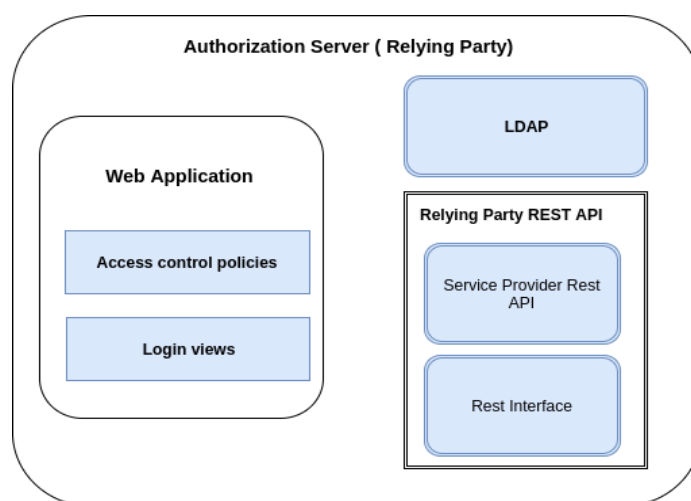


Figure 9: Campus Wi-Fi pilot - Authorization server after QR integration

Pilot Flow after QR integration:

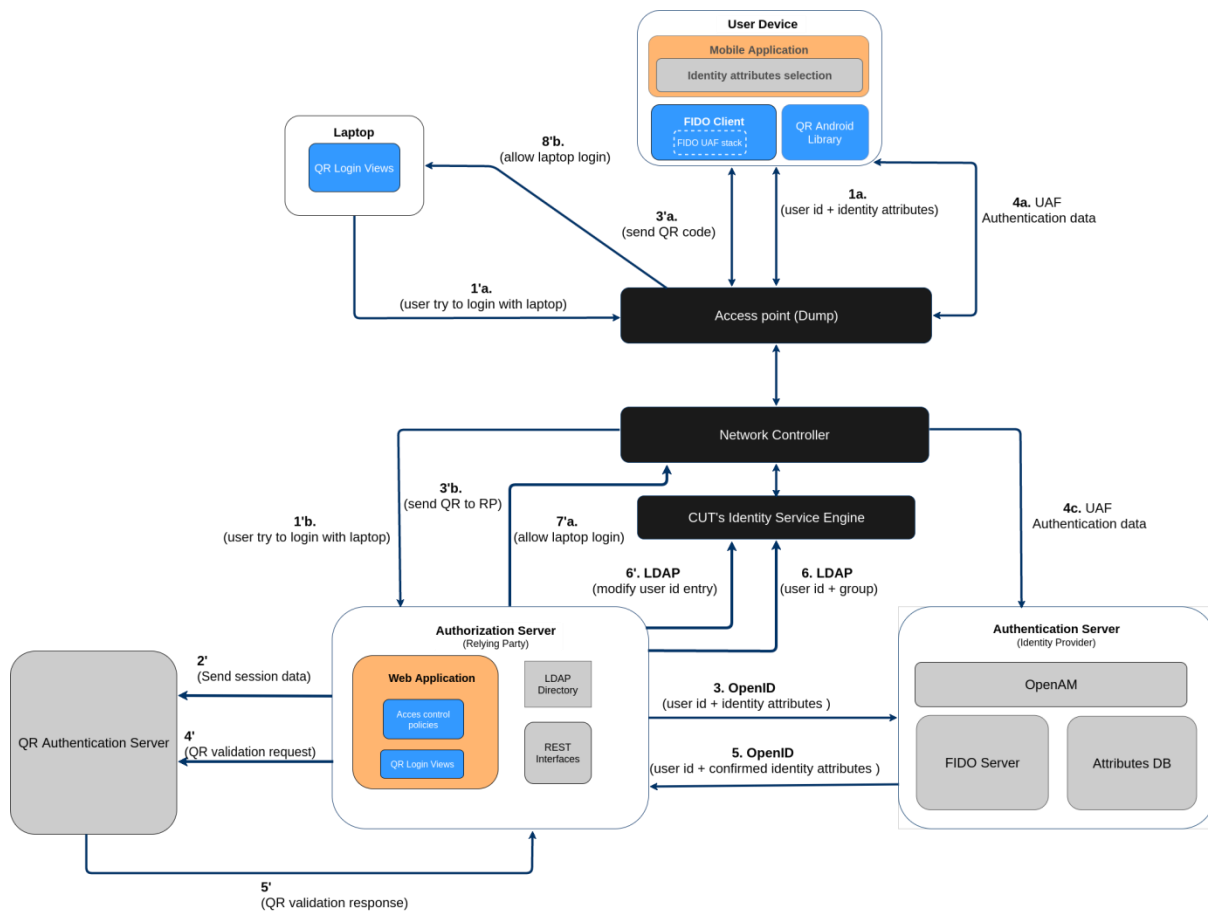


Figure 10: Campus Wi-Fi pilot - Flow after QR integration

Initially, the user must download and open the Wi-Fi pilot smartphone application. From there, she will choose a set of identity attributes that will be used for the authentication/authorization. Then, she connects to the nearest access point where he is redirected to the Authorization Server (Steps 1a-1c) through the Access Point and the Controller. The next step involves the initiation of the Authorization/Authentication procedure. The Authorization Server, which acts as the Relying party, will contact the Authentication Server, which acts as the Identity Provider, via the OpenID connect protocol, and it will transfer the user's set of identity attributes (Step 3). From there the Authentication Server will perform a FIDO UAF authentication by asking the user to provide his fingerprint (the authentication is performed as is documented in the FIDO UAF Authentication Specification) (Steps 4a-4c). After that, the Authentication Server will check the provided set of identity attributes against the already stored identity attributes in the attributes database that it maintains. When the authentication is completed, the Authentication Server will inform (again via the OpenID connect protocol) the Authorization Server regarding the outcome of the authentication (Step 5). The Authorization Server will ask the Authentication Server to provide the identity attributes for the user. From there, the Authorization Server will use the already pre-defined access control policies to decide which resources will grant to the user. Finally, the Authorization Server will update his LDAP directory with the authorization decision. The authorization decision involves the

assignment of a group to a user and the update of the LDAP directory with this decision (the Authorization Server maintains a mapping between network resources and groups. A group may consist of one or several resources).

If the user wants to authenticate another user device/desktop/laptop to a generic service provider, she accesses the Login QR View from the Authorization Server. The request is forwarded (Steps 1'a-1'b) through the Access Point and the Network Controller. The REST interface (Service Provider Back-End) sends information about the current request to the QR Authentication Server (Step 2') as well as a callback function which the QR Server will call if the authentication process succeeds.

After sending this information, the new device is redirected to the QR server where a QR code is being displayed. With the authenticated phone, the user scans the QR code using ReCRED Android application and sends the QR (again through Access Point and Network Controller) to the Authorization Server. The Relying Party verifies that the request was made via an authenticated channel and then sends the QR code to the QR Authentication Server (Step 4').

If the authentication succeeded, the server will call the callback function received previously from the Relying Party. In the callback function, the Authorization Server allows the new user device to login and also modifies the user id entry by adding a desktop identification (session ID) which allows the desktop to access the same resources as the mobile application.

2.6 Privacy & Security Considerations

2.6.1 Physical Protection and Network Security

The physical access to the servers is secured by each University provider. The access to the Universities premises where the servers are running is monitored.

2.6.2 Configuration and Security Settings

The operating systems of the servers are common Linux distributions with a large active supporting community that provide up to date security fixes. The versions of the Linux distributions used are the most stable at the moment of installation. Patch management is implemented.

User access is realized through Transport Layer Security (TLS) connections. As the central point of access gateSAFE acts as a gateway, securing the communication with the client and accessing the requested resource on client's behalf. gateSAFE has the possibility to configure the X.509 authentication mechanism to either always request a certificate from peer, optionally request the certificate, or never request, the authentication being server-side only.

2.6.3 Access Control

The servers can be accessed either from the console or through SSH connection. For security reasons, the remote authentication of users via SSH was changed to public key and the root access to SSH, restricted. Each user had generated a pair of keys (private and public).

2.6.4 Monitoring

The network is constantly monitored by each University. Firewall and server logs are periodically reviewed.

2.6.5 Malware Protection

There is no malware protection currently in place.

2.6.6 Patch Management

Every time an operating system patch, a security patch, software patch or a new release should be applied, the following process is followed:

- Restrict service port on firewall temporarily (e.g. database port)
- Take a snapshot of the machine before applying the patch(es)
- Apply one patch at a time
- Make checks on the system
- Enable the service port on firewall

In case of a failure during a patch execution the following process is followed:

- Logs are saved in another server
- The machine is restored to the latest taken snapshot
- The service port is enabled in firewall
- The System Administrators investigate the reasons of the patch application failure. If needed, they try to reproduce it at a similar environment

2.6.7 Change Management

Change management for ReCRED applications is realized by using the integration platform of the project and the continuous integration strategy, as described in Deliverable D6.2 “First integrated system”. Before being deployed to production environment the updates are tested.

After the successful test execution and approval of the changes and evaluation of possible implications, the changes are planned to be deployed on the production environment following the Patch Management process.

2.6.8 Incident Management

In case of a security incident, the System Administrators are notified and take immediate actions to stop and eliminate the threat. They investigate the incident, they keep all necessary logs to a safe place, they correct the security breach, and enable the network traffic again.

2.6.9 Protection of Logs and Data

Periodic data backup is scheduled using a cron job.

2.6.10 Cryptography and Protection of Electronic Communication

gateSAFE enables secure access, accounting and control to both modern and legacy web applications by leveraging state of the art technologies like Transport Layer Security (TLS) and Digital Certificates.

Remote access to the servers is realized through SSH console, using public keys cryptography.

2.7 Risk Assessment

The initial identified risks for the Campus Wi-Fi pilot are summarized in the following tables. These tables will be constantly updated during the execution of the pilot, and a final version will also be included in deliverable D7.4.

2.7.1 Initial Risk Score

#	Risk Events	Risk Scenarios	Risk Category	Likelihood	Impact	Risk Score	Recommended Actions
1	Pilot1_WiFi Pilot_Pentest_SQL injection	Data Integrity (Damage/Destruction)	Operations/Service Delivery	High	Medium	5 - High	Enhance existing risk mitigation controls
2	Pilot1_WiFi Pilot_Pentest_Missing tamper detection	Data Integrity (Damage/Destruction)	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
3	Pilot1_WiFi Pilot_Pentest_Missing certificate pinning	Data Integrity (Damage/Destruction)	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
4	Pilot1_WiFi Pilot_Pentest_Information disclosure through logging feature	Software Configuration Errors	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
5	Pilot1_WiFi Pilot_Pentest_Unencrypted sensitive data storage	Regulatory Compliance	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
6	Pilot1_WiFi Pilot_Pentest_LDAP injection	Data Integrity (Damage/Destruction)	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
7	Pilot1_WiFi Pilot_Pentest_Debug/stack trace error messages disclose application stage	Software Configuration Errors	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
8	Pilot1_WiFi Pilot_Pentest_Cryptographically weak SSL/TLS configuration	Software Configuration Errors	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
9	Pilot1_WiFi Pilot_Pentest_HTTP header fields disclose version information	Software Configuration Errors	Operations/Service Delivery	Low	Low	3 - Low	Defer action until future assessment
10	Pilot1_WiFi Pilot_Pentest_Missing code obfuscation	Software Configuration Errors	Operations/Service Delivery	Low	Low	3 - Low	Defer action until future assessment
11	Pilot1_WiFi Pilot_Pentest_Insufficient protection against snapshots	Data Theft	Operations/Service Delivery	Low	Low	3 - Low	Defer action until future assessment

2.7.2 Risk Actions

#	Risk Events	Recommended Actions	Risk Action to be Taken	Required Follow-up
1	Pilot1_WIFI Pilot_Pentest_SQL injection	Enhance existing risk mitigation controls	Enhance existing risk mitigation controls	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
2	Pilot1_WIFI Pilot_Pentest_Missing tamper detection	Defer action until future assessment	Enhance existing risk mitigation controls	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
3	Pilot1_WIFI Pilot_Pentest_Missing certificate pinning	Defer action until future assessment	Enhance existing risk mitigation controls	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
4	Pilot1_WIFI Pilot_Pentest_Information disclosure through logging feature	Defer action until future assessment	Enhance existing risk mitigation controls	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
5	Pilot1_WIFI Pilot_Pentest_Unencrypted sensitive data storage	Defer action until future assessment	Enhance existing risk mitigation controls	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
6	Pilot1_WIFI Pilot_Pentest_LDAP injection	Defer action until future assessment	Defer action until future assessment	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
7	Pilot1_WIFI Pilot_Pentest_Debug/stack trace error messages disclose application stage	Defer action until future assessment	Defer action until future assessment	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
8	Pilot1_WIFI Pilot_Pentest_Cryptographically weak SSL/TLS configuration	Defer action until future assessment	Defer action until future assessment	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
9	Pilot1_WIFI Pilot_Pentest_HTTP header fields disclose version information	Defer action until future assessment	Defer action until future assessment	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.
10	Pilot1_WIFI Pilot_Pentest_Missing code obfuscation	Defer action until future assessment	Defer action until future assessment	It was agreed that all risks will be addressed. Specifically, the high and medium risks will be addressed in the first version of the pilot and the low risks will be addressed in the final version of the pilot.

3. After filling-in all the required details, the merchant submits the form in order to finalize his registration.

STEP 1: PROFILE INFORMATION

USERNAME

PASSWORD

CONFIRM PASSWORD

SELECT YOUR AUTHENTICATION METHOD

☒ EMAIL

☐ SMS

Please select the method to receive the passcode to strongly authenticate in the system. You may choose an email or the SMS. As soon as the registration completes, the system will send you a passcode in the selected method and you will have to provide it in the next step. Upon successful submission of the passcode, the selected method will be used in the future to strongly authenticate you in the system.

GIVEN NAME

LAST NAME

PHONE NO. (OPTIONAL)

EMAIL ADDRESS

COMPANY NAME

COMPANY TYPE

COMPANY IMAGE

Browse...

No file selected.

DESCRIPTION

TERMS & CONDITIONS

☐ I ACCEPT THE [TERMS & CONDITIONS](#)

SUBMIT

Figure 12: Student pilot - Merchant registration

3.1.2 Campaign Management

A registered merchant can create new campaigns (offer), and manage the existing ones, through the Campaign Manager module, and by following the steps above:

1. The merchant logs in to the Campaign Manager and selects Campaigns.

2. The merchant can see and manage (edit / delete) the campaigns he has created.
3. The merchant selects “Add a new Campaign,” in order to create a new campaign.
4. The merchant fills-in the new campaign’s details, including its type, its validity period, its status, as well as a series of required attributes / policies.

PRODUCT NAME

SKU

ITEM TYPE

- Any -

PRICE TYPE

- Any -

APPLY

CAMPAIGNS











THUMBNAIL	MERCHANT	SKU	NAME	ITEM TYPE	PRICE TYPE	VALID UNTIL	UPSELL ONLY	ACTIVE	ACTIONS
	Foo Corp.	SKU-0019	T-Shirt	Online	Fixed	Sun, 12/31/2017 - 14:00	No	Yes	
	Foo Corp.	SKU-002	15% off laptop	Instore	Percentage	Sun, 10/08/2017 - 23:45	No	Yes	
	Upcom	Product-001	A nice present	Online	Percentage	Sat, 09/30/2017 - 03:15	No	Yes	
	Upcom	WEB-01	Infinity WebSite	Online	Fixed	Sat, 09/30/2017 - 01:00	No	Yes	
	Upcom	WEB-02	Alice in wonderland	Instore	Fixed	Tue, 09/26/2017 - 01:00	Yes	Yes	

Figure 13: Student pilot - Management of campaigns

Thumbnail *

Browse...

No file selected.

Upload

Files must be less than 50 MB.
Allowed file types: png gif jpg jpeg.

Product SKU *

Supply a unique identifier for this product using letters, numbers, hyphens, and underscores. Commas may not be used.

Campaign caption *

Details *

B I U

Path: p

Disable rich-text

Text format: Filtered HTML

- Web page addresses and e-mail addresses turn into links automatically.
- Allowed HTML tags: <a> <cite> <blockquote> <code> <dt> <dd>
- Lines and paragraphs break automatically.

More information about text formats

Discount type *

- Select a value -

Initial price *

EUR

Price *

EUR

VALIDITY *

FROM:

Date

Time

27/04/2017

13:45

E.g., 27/04/2017

E.g., 20:45

to: *

Date

Time

27/04/2017

13:45

E.g., 27/04/2017

E.g., 20:45

Stock *

0

Bypass stock limit *

Off

On

Is purchasable *

Yes

No

Upsell only *

No

Yes

Upsell

- None -

Locations

- None -

Branch one

Brussels

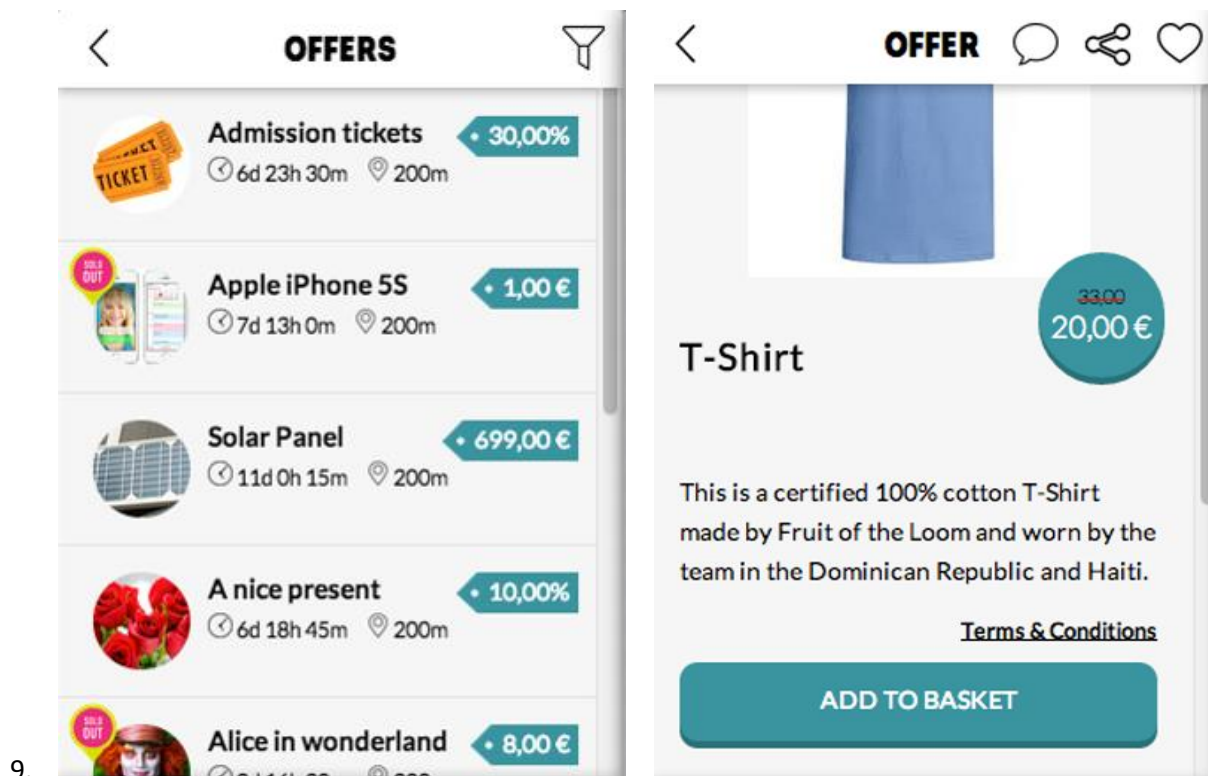
Brussels (Center)

Figure 14: Student pilot - Part of the campaign creation form

3.1.3 Purchase of Offers

A student can use the Student Offers mobile app, in order to see the available offers (according to his identity attribute) and make purchases. The purchasing of offers includes the following steps:

1. The student opens the Student Offers mobile app and sees a list of offers.
2. The student selects an offer to view its details and selects to make a purchase.
3. The Student Offers mobile app initiates FIDO UAF authentication with the FIDO UAF server sitting on the IdC, and the user is prompted to provide his fingerprint to the FIDO UAF Client.
4. Upon successful authentication, the FIDO UAF Server returns an authentication token, which is returned by the mobile app back to the Campaign Manager backend.
5. The Campaign Manager (acting as an SP/RP) passes the received authentication token to the IdC's OpenAM (acting as an IdP), and requests to receive the user's attributes that are required to evaluate the merchant's policy for the selected offer.
6. The IdC (OpenAM) returns the requested attribute values back to the Campaign Manager (acting as an SP), upon user's consent.
7. The Campaign Manager evaluates the merchant's policy defined for the requested offer against the user's actual attribute values, and either approves or rejects the purchase.
8. If the student is eligible to the offer, he can pay directly through the mobile app.



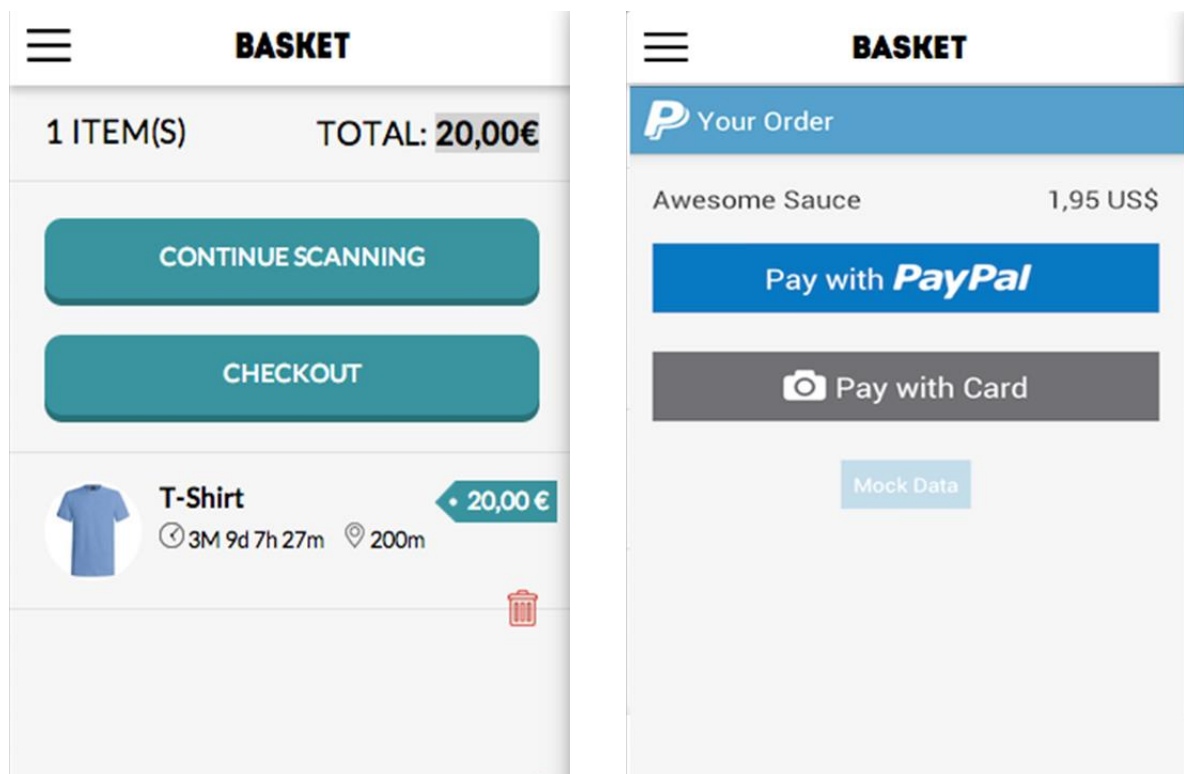


Figure 15: Student pilot - Offers and purchases

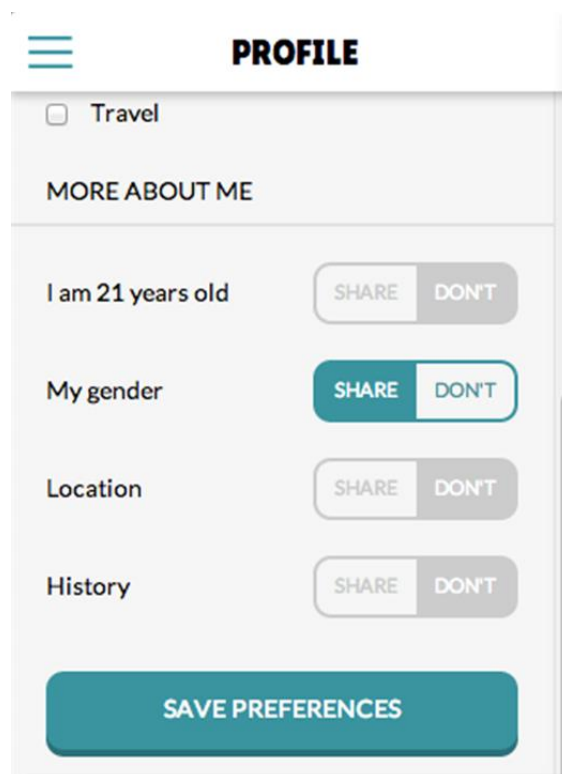


Figure 16: Student pilot - Consent management

3.2 Components Overview

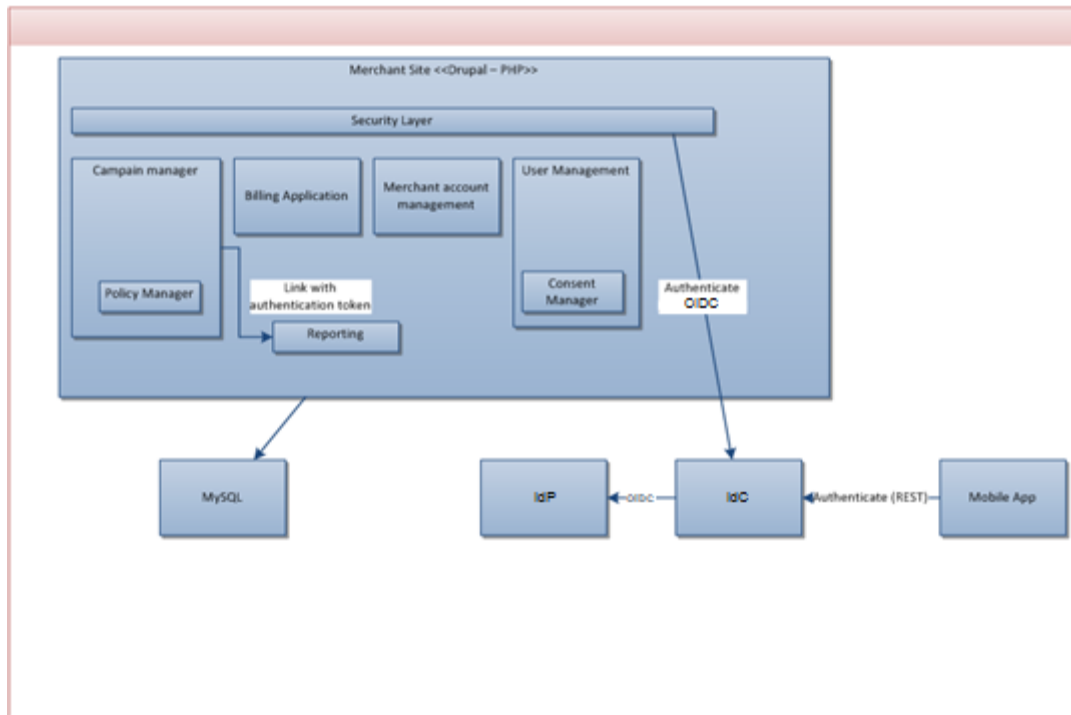


Figure 17: Student pilot - Component diagram

The Student Pilot requires the following components and sub-components in order to function:

- **Merchant Website:** The merchant website includes the following modules:
 - **Campaign Manager:** The Campaign Manager application allows discount campaigns and tickets to be created, edited, and managed through an administrative hub. It is composed of the following sub-functions:
 - Policy Manager
 - Reporting
 - MySQL
 - **Billing Application:** The billing application manages the process of billing students for items with discounts applied.
 - **Merchant Account Management:** This component allows Merchant Account holders to manage their accounts, as well as to attach campaigns and tickets.
 - **User Management:** Users are allocated an account role (Administrator, Issuer, Merchant, Student, Verizon, and Authenticated User) according to how they will be using the Campaign Manager. Each role has different permissions based on its purpose.
 - **Content Manager:** The content available to users is restricted by the permissions granted to their role, e.g. Merchants are able to create and edit billing information for customers, Administrators are able to edit other user permissions, etc.

- **Security Layer:** Authentication is handled using OpenID Connect to sign in against a central instance of OpenAM. Users are granted accounts with OpenAM through an identity consolidator.
- **Student Mobile App:** The student mobile app is an Android app that can be used by students, in order to view and purchase offers provided by the merchants (in-store and online), according to their revealed identity attributes and the policies created by the merchants for each offer. Through the mobile app, the students can also have access to all their previous purchases. Finally, the students can manage their preferences and decide which identity attributes they consent to be revealed to the Campaign Manager.
- **Merchant Mobile App:** The merchant mobile app is a simple Android app that can be used by the merchants’ cashiers (at a physical store), in order to validate the student’s attributes and redeem purchases that can be made in-store only.
- **Identity Consolidator (as Identity Provider):** For the Student Authentication & Offers pilot, the Identity Consolidator acts as a trusted Identity Provider that holds the verified identity attributes of the students. The Identity Consolidator offers various mechanisms to the end-users, in order to register and prove their attributes (e.g. the users can scan RFID-enabled official documents using NFC).
- **QR Code and OpenAM:** Creates a QR code which can be scanned by the mobile device, in order to authenticate the user and redirect him back to the Service Provider.

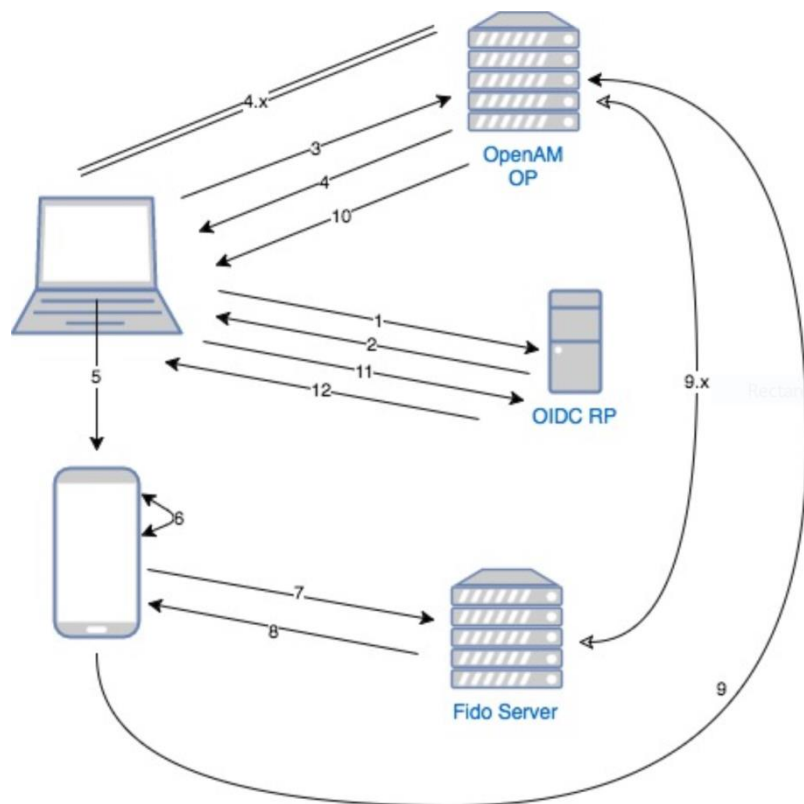


Figure 18: Student pilot - QR Code OpenAM flow

1. Client machine tries to access a resource on the OIDC Relying Party

2. The browser is redirected to the OpenAM OIDC Provider for authentication
3. The user’s browser makes a request to the OP
4. The OpenAM sees that the client is on a desktop computer and generates a QR code that contains:
 - i. A Random number
 - ii. The Fido server URL for the user to Authenticate against
 - iii. The OpenAM server callback URL where the Fido AuthID is to be returned
- x. The client keeps a connection to the OpenAM server to periodically call to see if authentication has been completed
5. The user scans the QR code with the ReCRED Authentication app
6. The App “decodes” the data in the QR code and passes it to the Fido authentication part of the mobile app
7. The app performs Fido Authentication against the Fido Server (Process simplified in this diagram)
8. The Fido Server returns an Authentication ID to the mobile device
9. The mobile app takes the AuthID and the random number initially passes and submits it back to the callback endpoint
- x. The OpenAm server validates that the Authentication ID provided is valid
10. The OpenAM server uses the 4.x channel to return a message that the user is now authenticated
11. The user’s browser is redirected back to the RP
12. The RP validates that the user is authenticated correctly and returns the user’s requests content

3.3 Hardware Architecture

The ISIC Campaign Manager is hosted in Verizon’s cloud environment on a Virtual Machine running 64-bit CentOS 7. The same VM hosts the database required to run Drupal and store users. The VM consists of a quad-core virtual CPU running at 2.8GHz, 8 GB of RAM, and two 40 GB hard disk drives. The VM is controlled and monitored through an administrative control panel, and can be brought on and offline with minimal hassle.

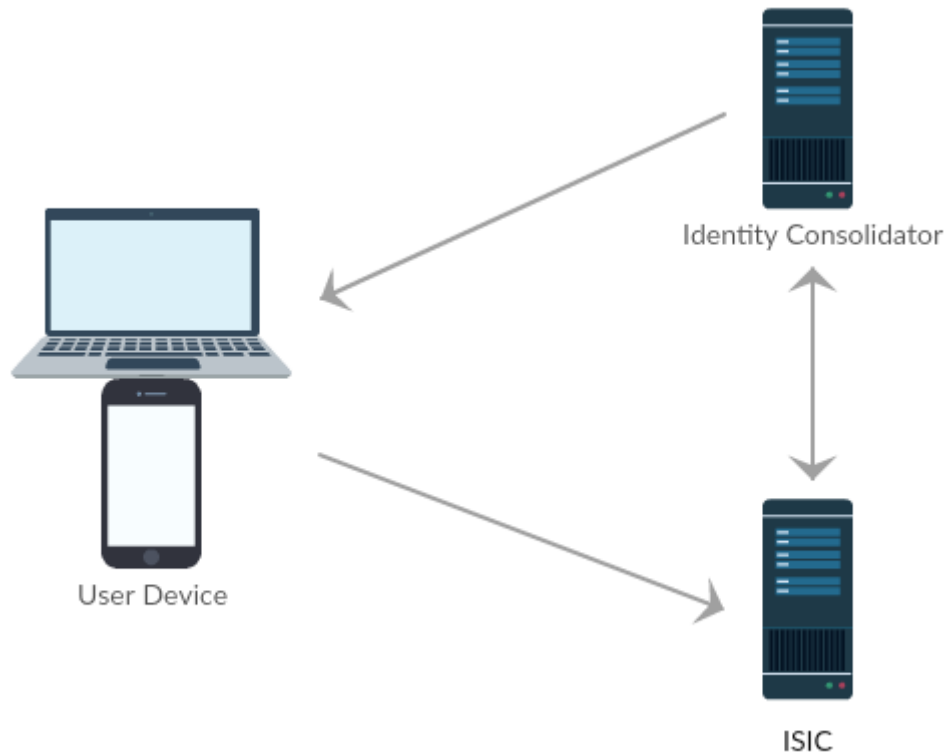


Figure 19: Student pilot - Hardware architecture

Users are provisioned into the Identity Consolidator (IdC), where their details (email address, security Q&A, etc) are stored. Using OpenID Connect, the ISIC Campaign Manager allows users to authenticate against the IdC to claim their discounts.

3.4 Software Architecture

- **CentOS 7:** The server’s operating system is CentOS v7. The CentOS Linux distribution is a stable, predictable, manageable and reproducible platform derived from the sources of Red Hat Enterprise Linux (RHEL). Since March 2004, CentOS Linux has been a community-supported distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with RHEL.
- **Android:** Both the student and the merchant mobile apps are cross-platform HTML5 apps, implemented using the Cordova framework. However, a custom Android plugin has been used, for managing the Fido registration / authentication in the native environment.
- **Apache:** The Campaign Manager Web application runs on Apache web server v2.4. Apache is the most widely used web server software. Developed and maintained by Apache Software Foundation, Apache is open source software available for free. It runs on 67% of all web servers in the world. It is fast, reliable, and secure. It can be highly customized to meet the needs of many different environments by using extensions and modules.
- **Drupal:** The content of the Campaign Manager is delivered using Drupal 7. Drupal is free, open source software that can be used by individuals or groups of users to easily create and manage many types of Web sites. The application includes a content management platform and a development framework.

- **MariaDB:** Drupal requires a database in order to function, and it contains user info, error logs, module settings and other config information. MariaDB is a community-developed fork of the MySQL relational database management system intended to remain free under the GNU GPL.
- **OpenID Connect:** Users authenticate against OpenAM using Drupal’s OpenID Connect module to sign into the Campaign Manager. OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol, which allows computing clients to verify the identity of an end-user based on the authentication performed by an authorization server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner.
- **OpenAM:** OpenAM uses accounts created through the identity consolidator to confirm users have access to the Campaign Manager. OpenAM is an open source access management, entitlements and federation server platform. It is sponsored by ForgeRock.

3.5 Privacy & Security Considerations

- **Physical Protection and Network Security:** Verizon’s cloud datacenters are protected by CCTV and access-restriction enforced by an on-site security team.
- **Configuration and Security Settings:** The Campaign Manager is running on the most stable version of CentOS 7, and is kept up to date with the most recent security patches and fixes. Access to the VM hosting the Campaign Manager is restricted to whitelisted IP addresses via SSH on port 22 and using https on port 443.
- **Access Control:** The VM can only be accessed using an encrypted SSH method from a whitelisted IP address, and only the Verizon dev team have user accounts on the machine. The default user has been removed, and the database is owned by a local user with limited permissions.
- **Monitoring:** Drupal monitors for suspicious activity and saves all logs to the Watchdog table in the database. Access and error logs are stored locally.
- **Patch Management:** The Campaign Manager runs on an older version of Drupal with a number of modules requiring updates; this is complicated by the fact that updating Drupal and the modules overwrites custom code required by the Campaign Manager’s core functionality. This issue will have to be addressed in the future whenever it is updated.
- **Change Management:** Change Management Process will provide single point of entry for all Requests for Change during the Pilot Operations. Change management ensures that changes are controlled and followed-up during their entire life-cycle
 - Changes are recorded (Phabricator and JIRA tools)
 - Changes are assessed (impact and risk analysis)
 - Changes are prioritized
 - Changes are authorized
 - Changes are planned in conjunction with the release schedule
 - Changes are communicated

- Changes are tested and validated
- Changes are moved into pilot environment
- Changes are reviewed
- Changes are documented
- **Incident Management:** Incident Management process will be put in place which will aim to manage the lifecycle of all Incidents including security incidents. The objective of the Incident Management process is to restore normal service operation as quickly as possible and minimize any adverse impact on Pilot operations. The Incident Management Process will ensure that:
 - Incidents are properly logged
 - Incidents are properly routed
 - Incident status is accurately reported
 - Incidents are properly prioritized and handled in appropriate sequence

The high-level activities are:

- Incident detection and Logging
- Categorization and Prioritization including determination if the incident is categorized as a **security incident**
- **Security incident only:** the impact on security is determined. Based on the impact a decision is made if functional escalation is required.
- Investigation and Diagnosis (if the incident has not a resolution and are the result of the recurring Problem)
- Resolution and Recovery
- Incident closure
- **Protection of Logs and Data:** Logs and data are stored locally.
- **Cryptography and Protection of Electronic Communication:** The Campaign Manager has numerous fields that accept user input, causing potential vulnerabilities to injection attacks such as SQL Injection and XSS. Drupal employs a level of abstraction between user input and the database, allowing all input to be sanitized for escape characters and JavaScript. Authentication and Session Management is handled by OpenAM; users authenticate against OpenAM using OpenID Connect to sign in to the Campaign Manager. User sessions are then identified using OpenAM's iPlanetDirectoryPro cookie. Passwords stored through Drupal are hashed and salted before being stored in the database, although most users will be authenticating through OpenAM and their log in credentials will be stored externally on a separate server.

3.6 Risk Assessment

The initial identified risks for the Student Authentication & Offers pilot are summarized in the following tables. These tables will be constantly updated during the execution of the pilot, and a final version will also be included in deliverable D7.4.

3.6.1 Initial Risk Score

#	Risk Events	Risk Scenarios	Risk Category	Likelihood	Impact	Risk Score	Recommended Actions
1	Pilot2_Student_Pilot_Outdated Drupal Modules	Software Obsolescence	Operations/Service Delivery	Low	High	5 - High	Enhance existing risk mitigation controls
2	Pilot2_Student_Pilot_Incorrect Deployment	Software Configuration Errors	Programme/Project Delivery	Low	Low	3 - Low	Defer action until future assessment
3	Pilot2_Student_Pilot_DDoS Attacks	Externally Originated Attack	Operations/Service Delivery	Very Low	Medium	2 - Very Low	Accept residual risk; no mitigation needed
4	Pilot2_Student_Pilot_Loss of Data	Data Integrity (Damage/Destruction)	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
5	Pilot2_Student_Pilot_Accidental damage and natural hazards	Acts of Nature	Operations/Service Delivery	Very Low	High	3 - Low	Defer action until future assessment
6	Pilot2_Student_Pilot_Security Breach	Externally Originated Attack	Operations/Service Delivery	Low	High	5 - High	Enhance existing risk mitigation controls
7	Pilot2_Student_Pilot_Physical Security	Externally Originated Attack	Operations/Service Delivery	Very Low	Medium	2 - Very Low	Accept residual risk; no mitigation needed

3.6.2 Risk Actions

#	Risk Events	Recommended Actions	Risk Action to be Taken	Required Follow-up
1	Pilot2_Student_Pilot_Outdated Drupal Modules	Enhance existing risk mitigation controls	Defer action until future assessment	Outdated Drupal modules will be updated before the Student Pilot is fully operational. A Pen-Test will be carried out on the Student Pilot before it is fully operational.
2	Pilot2_Student_Pilot_Incorrect Deployment	Defer action until future assessment	Defer action until future assessment	A Pen-Test will be carried out on the Student Pilot before it is fully operational.
3	Pilot2_Student_Pilot_DDoS Attacks	Accept residual risk; no mitigation needed	Accept residual risk; no mitigation needed	A Pen-Test will be carried out on the Student Pilot before it is fully operational.
4	Pilot2_Student_Pilot_Loss of Data	Defer action until future assessment	Defer action until future assessment	The database will be periodically backed up to an external repository. A Pen-Test will be carried out on the Student Pilot before it is fully operational.
5	Pilot2_Student_Pilot_Accidental damage and natural hazards	Defer action until future assessment	Accept residual risk; no mitigation needed	
6	Pilot2_Student_Pilot_Security Breach	Enhance existing risk mitigation controls	Enhance existing risk mitigation controls	An incident response plan will be drafted before the Student Pilot is operational. A Pen-Test will be carried out on the Student

				Pilot before it is fully operational.
7	Pilot2_Student_Pilot_Physical Security	Accept residual risk; no mitigation needed	Accept residual risk; no mitigation needed	Physical Security is handled by our cloud service providers, who have their own risk mitigation procedures in place.

4 Age Verification Online Gateway

4.1 Description of the Pilot

The age verification pilot is based on the new Age Gate solution, an online age verification service, with the purpose of granting or denying access to age-restricted resources, without revealing or disclosing any other personal and/or sensitive data of the user.

An age-restricted online resource could be any of the following:

- an age-restricted web site (e.g. porn or violence related),
- specific age-restricted content (e.g. an NC-17 movie),
- age-restricted online services (e.g. gambling) or purchases (e.g. alcohol or tobacco).

The providers of those resources do not need to know any personal information about their visitors. They only need to be able to guarantee that the visitors are above a certain age, which can be defined as a policy.

The age verification pilot includes three flows, which are described in more detail in the following subsections.

1. End-user registration
2. Website registration
3. Age verification

4.1.1 End-user Registration

In order to be able to prove their age to age-restricted websites, the users first need to register with an Identity Provider supported by ReCRED and verify their age. Initially, the Identity Consolidator will be used as an authorized Identity Provider, and in that case the end-user registration flow includes the following steps:

1. The user registers with ReCRED, through the Authentication Management module. During his registration, the user also registers his fingerprint to the FIDO server.
2. The user can use the NFC functionality of the ReCRED’s Physical Identity Acquisition module, in order to scan an RFID document that proves his age (e.g. an identity card or passport). In the next version of the pilot, the users will be able to also link a trusted physical Identity Provider (e.g. a government authority or a bank), through the Online Identity Acquisition module, in order to verify their age.

3. The user can use the Credential Management module, in order to issue a cryptographic credential that will prove his age, and securely store it in his mobile device. FIDO UAF authentication is initiated before the credentials are stored in the device.

4.1.2 Website Registration

A website owner needs to register with Age Gate, before being able to register his websites. Each website registration request is reviewed and approved by an Age Gate operator. More specifically, the website registration flow includes the following steps:

1. The website owner registers with the Age Gate platform, by filling in a simple web form.
2. The website owner can register one or more websites. For each website, he needs to define: the website's title, a short description, the URL, and the age policy (e.g. > 18).
3. An Age Gate operator reviews each request for website registrations, and typically approves them.
4. A notification is sent to the website owner, along with a small script (OpenID Connect Client) that needs to be embedded to their website.
5. The website owner embeds the provided script and redeploys their website. After that, the new visitors are able to use the Age Gate solution in order to access the website.

In addition, a website owner can change the details of a registered website or completely unregister a website from Age Gate. Each of these actions, also require review and approval by an Age Gate operator.

4.1.3 Age Verification

Any user registered with ReCRED can use his Age Gate mobile app in order to prove his age and gain access to an age-restricted website that uses the Age Gate solution. The proof of age can happen in two ways: (1) through an age cryptographic credential that is stored in the user device or (2) through OpenID Connect. These two flows differ in some steps and are describes as follows:

Age Verification through Anonymity-preserving Cryptographic Credentials

1. The user attempts to visit an age-restricted website using his PC / laptop.
2. The website (acting as an SP) asks from the Age Gate Server (acting as an IdP) to verify the visitor's age.
3. The Age Gate server returns a QR code, which is displayed in the age-restricted website and the user can use his Age Gate mobile app, in order to scan the QR code and prove his age. Note that this step is not required if the user attempts to visit a website using his mobile device.
4. The Age Gate mobile app searches for cryptographic credentials in the user's device, that prove the user's age.
5. The Age Gate Server (acting as a verifying IdP) runs idemix / uprove, so it can verify the user's age (or whether the user's age is above or below a threshold) using the found credential.

6. The Age Gate Server evaluates the age policy defined for the requested website (e.g. age > 18), against the user’s actual age credential, and returns a true/false value to the website.

Age Verification through OpenID Connect

1. The user attempts to visit an age-restricted website using his PC / laptop.
2. The website (acting as an SP) asks from the Age Gate Server (acting as an IdP) to verify the visitor’s age.
3. The Age Gate server returns a QR code, which is displayed in the age-restricted website and the user can use his Age Gate mobile app, in order to scan the QR code and prove his age. Note that this step is not required if the user attempts to visit a website using his mobile device.
4. The Age Gate mobile app displays all the supported Identity Providers and the user choses to prove his age through the ReCRED IdC. Please note that the ReCRED IdC will be the default IdP that will be used during the pilot. At a later phase, additional IdPs can be supported (e.g. the Belgian National Register)
5. The Age Gate mobile app initiates FIDO UAF authentication with the FIDO UAF server sitting on the IdC, and the user is prompted to provide his fingerprint to the FIDO UAF Client.
6. Upon successful authentication, the FIDO UAF Server returns an authentication token, which is returned by the mobile app back to the Age Gate Server.
7. The Age Gate Server (acting as an SP/RP) passes the received authentication token to the IdC’s OpenAM (acting as an IdP), and requests to receive the user’s age.
8. The IdC (OpenAM) returns the user’s age back to the Age Gate Server (acting as an SP), upon user’s consent.
9. The Age Gate Server evaluates the age policy defined for the requested website (e.g. age > 18), against the user’s actual age, and returns a true/false value to the website.

In both scenarios, the Age Gate Server acts both as a Service Provider (SP) and as an Identity Provider (IdP), so it runs both OpenAM and OIDC client.

- The Age Gate Server acts as an IdP, which receives requests from websites (SPs) that wish to delegate their visitors' age verification, evaluates the websites policies and return a true or false value.
- The Age Gate Server acts as an SP, which relies on other supported IdPs in order to retrieve the value of a user's age attribute (upon the user's consent).

4.2 Components Overview

4.2.1 Age Gate Mobile App

The Age Gate mobile app is an Android app that can be downloaded and be used by the end-users, in order to issue age-related cryptographic credentials, prove their age and manage their access to

age-restricted websites. More specifically, the Age Gate mobile app offers the following functionality:

- **Issue Age Cryptographic Credentials:** The user needs to login to the Identity Consolidator web-app and visit the Credential Management module. From there, he can select to issue a cryptographic credential proving his age. A QR code is created and displayed on the website, and the user can use the mobile app in order to scan this code and securely store the age-related cryptographic credential to the mobile device. For this, FIDO UAF authentication is initiated before the credentials are stored in the device.
- **Prove Age:** Every time the user wants to visit an age-restricted website supporting the Age Gate solution, a QR code is displayed on the website, and the user can use the mobile app in order to scan this code and prove his age.

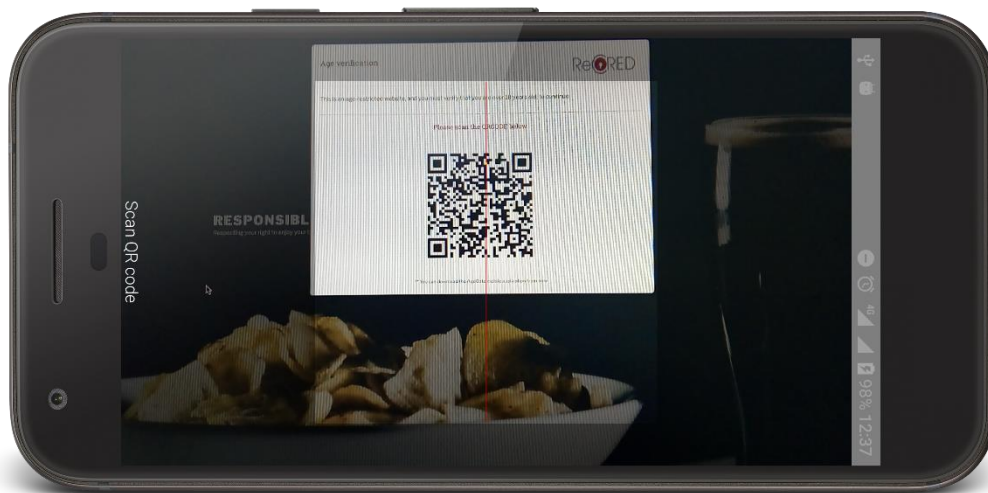


Figure 20: Age verification pilot - Scan QR code using the Age Gate mobile app

- **View Access History:** The end-user can use the mobile app in order to see a list with all the age-restricted websites to which the user has been granted access. By selecting one of these websites, the user can see a detailed report with all the logged access attempts, including specific timestamps and the attempts results (granted / rejected). In addition, the user can choose to revoke access to a certain age-restricted website.

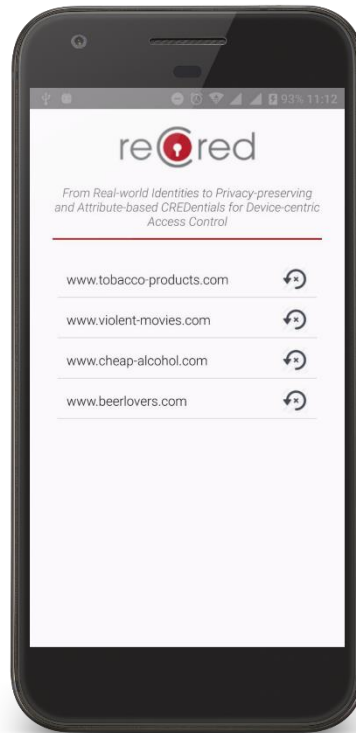
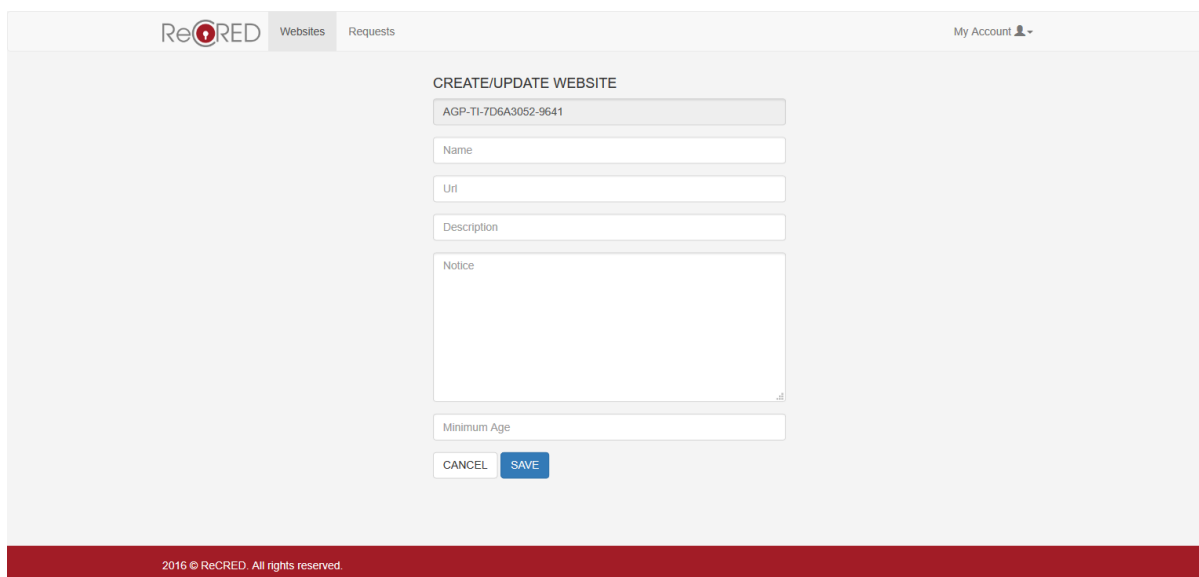


Figure 21: Age verification pilot - View access history and revoke access

4.2.2 Age Gate Server

The Age Gate Server is the backbone of the Age Gate solution, since it allows website owners to register their websites and set policies, it handles the authorization requests, and it generates ad-hoc and recurring reports. More specifically, the Age Gate server offers the following functionality:

- **Register Websites and Set Policies:** Website owners can request to register their website with Age Gate, in order to be able to prove their age and grant them access according to age policies. They can also request to modify the age policies, or even unregister their website from Age Gate. All these requests are reviewed by authorized operators, before being approved or rejected. Upon successful registration of a website, a script is automatically created, which must be included in the registered website pages.



CREATE/UPDATE WEBSITE

AGP-TI-7D6A3052-9641

Name

Url

Description

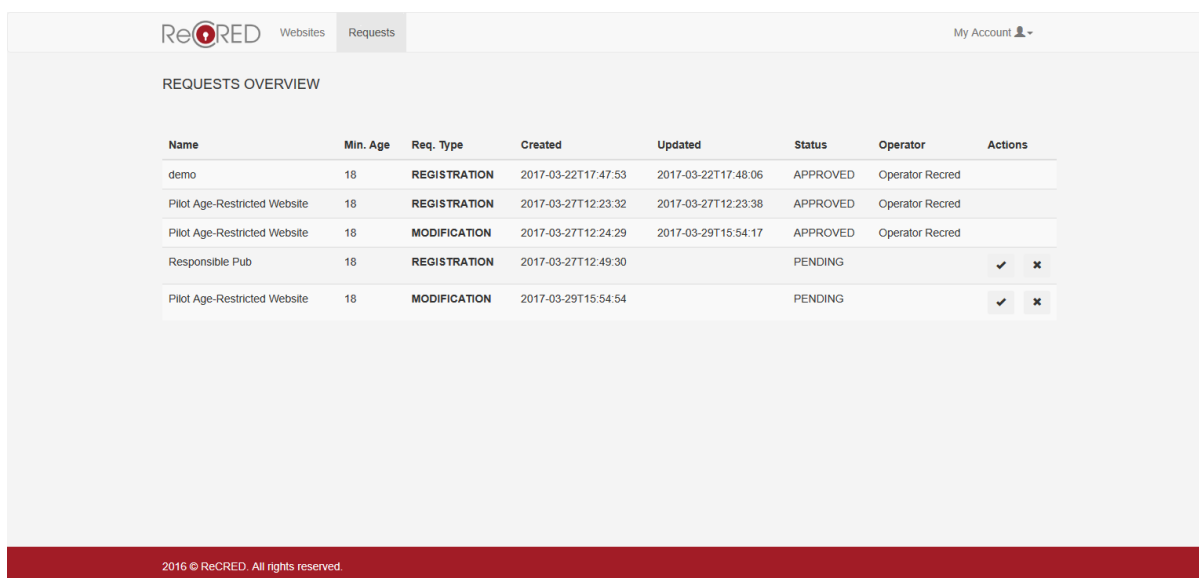
Notice

Minimum Age

CANCEL SAVE

2016 © ReCRED. All rights reserved.

Figure 22: Age verification pilot - Register new website to Age Gate



REQUESTS OVERVIEW

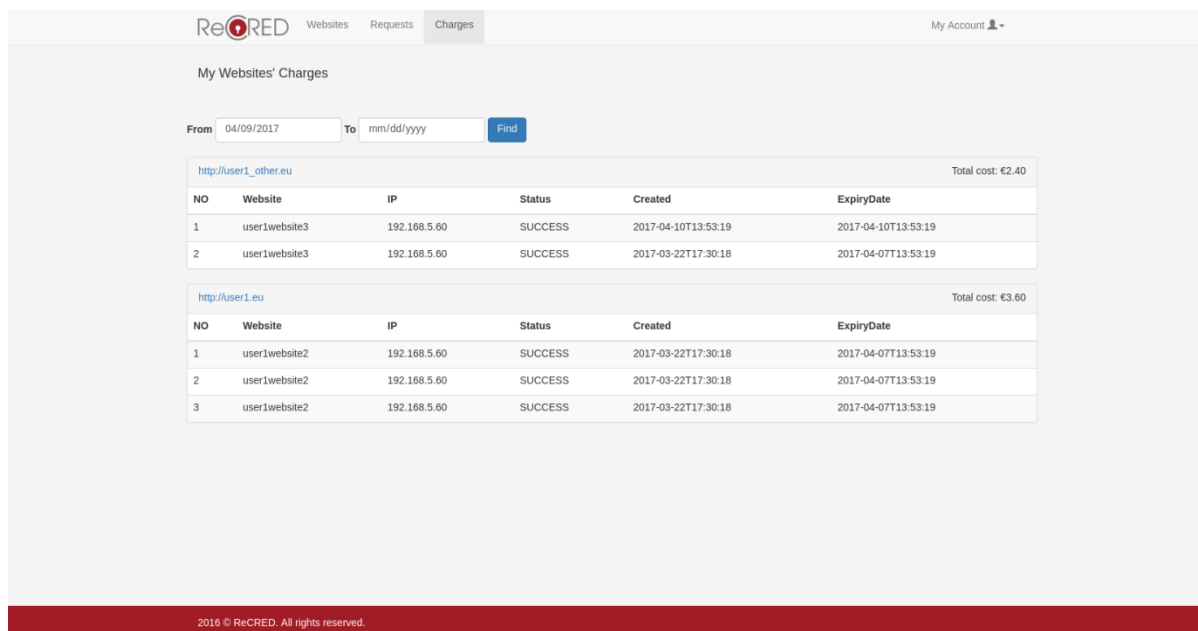
Name	Min. Age	Req. Type	Created	Updated	Status	Operator	Actions
demo	18	REGISTRATION	2017-03-22T17:47:53	2017-03-22T17:48:06	APPROVED	Operator Recred	
Pilot Age-Restricted Website	18	REGISTRATION	2017-03-27T12:23:32	2017-03-27T12:23:38	APPROVED	Operator Recred	
Pilot Age-Restricted Website	18	MODIFICATION	2017-03-27T12:24:29	2017-03-29T15:54:17	APPROVED	Operator Recred	
Responsible Pub	18	REGISTRATION	2017-03-27T12:49:30		PENDING		✓ ✕
Pilot Age-Restricted Website	18	MODIFICATION	2017-03-29T15:54:54		PENDING		✓ ✕

2016 © ReCRED. All rights reserved.

Figure 23: Age verification pilot - Review and accept / reject requests (operator)

- **Handle Authorization Requests:** The Age Gate Server receives authorization requests from registered age-restricted websites. For each request, a QR code is generated and returned to the website, in order to be displayed. After the QR code is scanned by the Age Gate mobile app, the Age Gate Server receives the proved age of the user, which is evaluated against the specific website’s age policy. According to this evaluation, a response is sent to the age-restricted website and the user is granted or denied access, respectively. In any case, the Age Gate Server logs the authorization request, along with the result (for reporting / auditing purposes).
- **Audit Sample Records:** The Age Gate Server allows personal data auditors to audit sample records of authorization requests, in order to verify that access is in line with the regulations. The auditor can search for audit records either randomly or with predefined filters in the legally defined date range. For each advised record, specific information is provided, such as: request from the website, interaction with the user, response to the web site.

- **Generate Reports:** Both ad-hoc and recurring reports can be generated by the Age Gate Server. Recurring reports are automatically generated periodically, in non-changeable PDF format, and they are emailed to website owners for invoicing purposes. Each recurring report includes aggregated age verification totals, per website. Upon request of a website owner, detailed reports can also be generated, which include detailed lists of age verifications in a predefined time period.



My Websites' Charges						
From 04/09/2017 To mm/dd/yyyy Find						
http://user1_other.eu						Total cost: €2.40
NO	Website	IP	Status	Created	ExpiryDate	
1	user1website3	192.168.5.60	SUCCESS	2017-04-10T13:53:19	2017-04-10T13:53:19	
2	user1website3	192.168.5.60	SUCCESS	2017-03-22T17:30:18	2017-04-07T13:53:19	
http://user1.eu						Total cost: €3.60
NO	Website	IP	Status	Created	ExpiryDate	
1	user1website2	192.168.5.60	SUCCESS	2017-03-22T17:30:18	2017-04-07T13:53:19	
2	user1website2	192.168.5.60	SUCCESS	2017-03-22T17:30:18	2017-04-07T13:53:19	
3	user1website2	192.168.5.60	SUCCESS	2017-03-22T17:30:18	2017-04-07T13:53:19	

Figure 24: Age verification pilot - Reports generation

4.2.3 Identity Consolidator (as Identity Provider)

For the age verification pilot, the Identity Consolidator acts as a trusted Identity Provider that holds the verified age of the end-users. The Identity Consolidator offers various mechanisms to the end-users, in order to register and prove their age. Currently, the users can scan RFID-enabled official documents (using NFC), but in a following version of the pilot, the users will be able to also link trusted physical Identity Providers. In addition, the Credential Management module of the Identity Consolidator is also used, so that the users can issue to their device cryptographic credentials with their age.

The Identity Consolidator includes a FIDO server, in order to be able to perform FIDO UAF authentication. It also includes an attributes database that maps the user's identity with confirmed identity attributes (i.e. age), so that the Identity Consolidator can verify the users' age.

In addition, the Identity Consolidator includes the gateSAFE module, for FIDO/OpenID Connect authentication. It also acts as an OpenID Connect provider and it is responsible to provide authentication to the Age Gate Server (which acts as the relying party, in that case), along with the user's age (if required). gateSAFE provides a single-sign-on implementation, such that users authenticate once; subsequent authentications, if necessary, take place without user intervention. gateSAFE has a modular architecture, allowing the parallel operation of more servers, answering to a big number of connections.

4.2.4 Service Provider(s)

The final component of the age verification pilot is the Service Providers, all those age-restricted websites that rely on the Age Gate solution in order to verify that their visitors are above a certain age. Therefore, the Service Providers act as the relying parties and they only need to register to Age Gate and embed a simple script to their websites.

Each time an end-user visits any of the website’s pages, he is redirected to Age Gate and can select to either verify his age through Age Gate or simply state that he is above the required age.

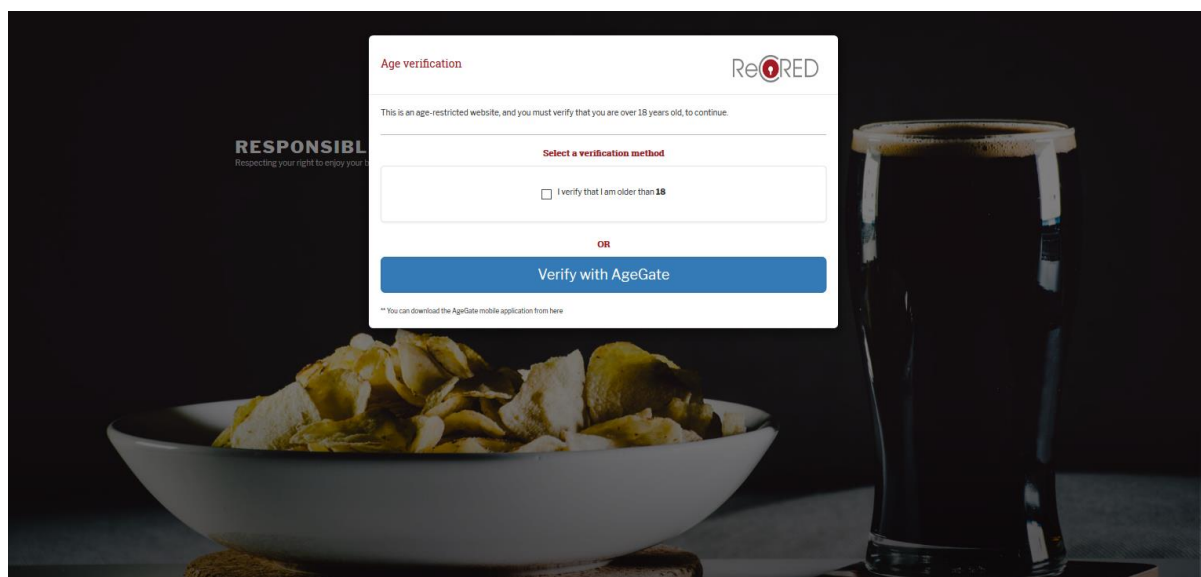


Figure 25: Age verification pilot - Selection of age verification method

If the user selects to verify his age through Age Gate, a QR code is created, which is displayed and the user must scan it with the Age Gate mobile app.

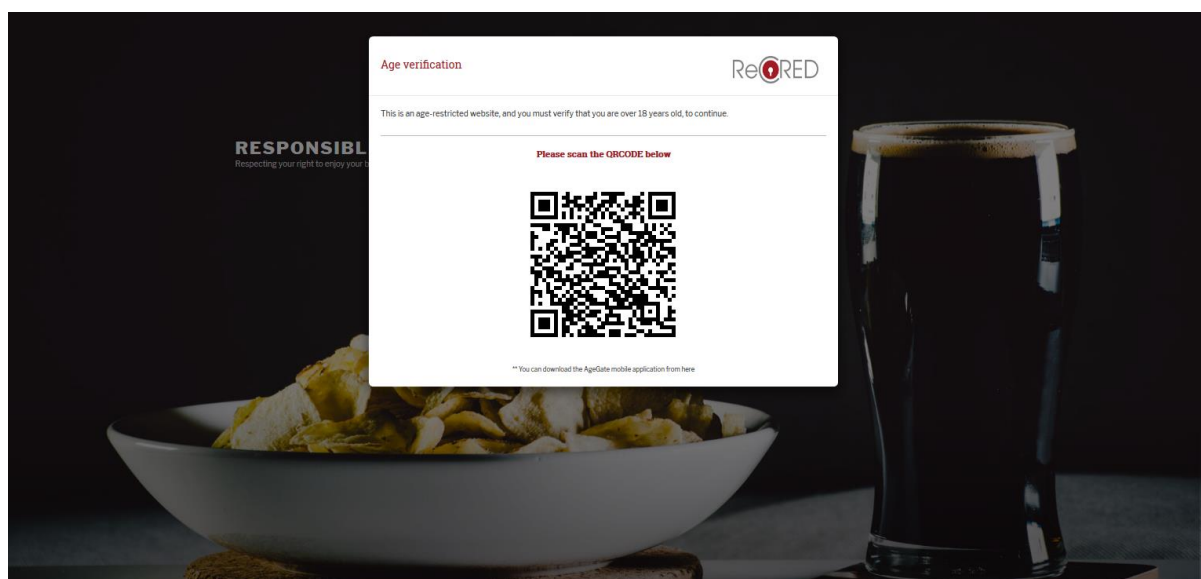


Figure 26: Age verification pilot - QR code creation

As long as the age of the user is verified and it is above the required age (as set by the Service Provider in the respective age policy), the user is granted access to the website.



Figure 27: Age verification pilot - Entrance to the Service Provider's website

4.3 Hardware Architecture

The hardware architecture describes all the hardware components that are part of the pilot and their role and their configuration. An overview of the hardware architecture is described in the following figure:

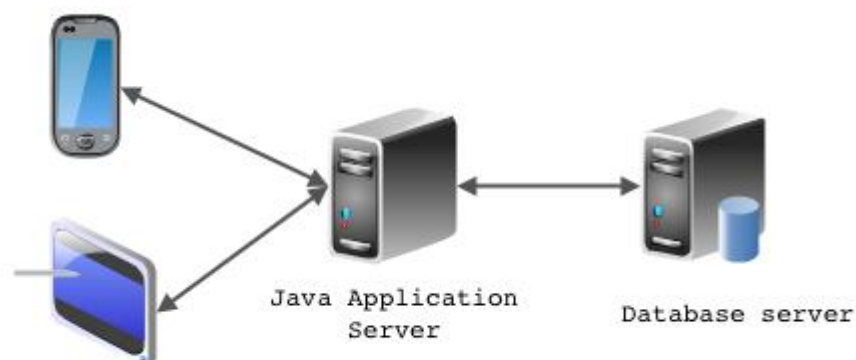


Figure 28: Age verification pilot - Hardware architecture

4.3.1 Database Server - Application Server

The database server and application server are hosted each one on a high performance Virtual Private Server (VPS) running on OVH Cloud datacentre served by OpenStack Cloud Operating System. OpenStack is a cloud operating system that controls large pools of compute, storage, and networking resources throughout a datacentre. Each Virtual Private Server is consisted of 1 virtual CPU Core running at 2.4GHz, 4 GB of RAM memory, 20 GB of storage on a Local RAID 10 SSD hard drive. The server accesses internet through a 100Mbps line.

Each VPS server is covered with a 99,95% SLA, can scale easily through a control panel, is protected by Anti-DDOS Professional services provided by the infrastructure of OVH datacentres and is continuously monitored in detail.

OVH offers a vast range of IT services for businesses and technophiles in particular. From web hosting to virtual datacentres, dedicated servers and storage solutions, all services benefit from continuous innovation and are regularly enriched with new features. OVH is the number 3 internet hosting company in the world, offering 260.000 servers, in 20 datacentres distributed in 17 countries all over the world.

4.3.2 User Device

Age verification online gateway was tested in a Samsung S5 and a OnePlus One. Both devices run an Android Marshmallow operating system, which complies with the application’s minimum SDK restrictions. Specifically:

- Samsung S5
 - Chipset: Qualcomm MSM8974AC Snapdragon 801
 - CPU: Quad-core 2.5 GHz Krait 400
 - GPU: Adreno 330
 - WLAN: Wi-Fi 802.11 a/b/g/n/ac, dual-band, Wi-Fi Direct, hotspot
 - Sensors: Fingerprint (front-mounted), accelerometer, gyro, proximity, compass, barometer, gesture, heart rate
 - Memory: 32GB internal memory, 2 GB RAM
- OnePlus One
 - Chipset: Qualcomm MSM8974AC Snapdragon 801
 - CPU: Quad-core 2.5 GHz Krait 400
 - GPU: Adreno 330
 - WLAN: Wi-Fi 802.11 a/b/g/n/ac, Wi-Fi Direct, DLNA, hotspot
 - Sensors: Accelerometer, gyro, proximity, compass
 - Memory: 64 GB internal memory, 3 GB RAM

As not both devices include a fingerprint sensor, it is important to note FIDO client’s versatility, enabling the user to authenticate himself to the FIDO-server via different ways of user to device authentication, i.e. pin, fingerprint.

4.4 Software Architecture

The Software Architecture describes all the software components of the pilot, including the OS and OS Tools. This is the software view of the pilot.

4.4.1 Infrastructure Software

4.4.1.1 Servers Operating System

The servers’ operating system is CentOS v7. The CentOS Linux distribution is a stable, predictable, manageable and reproducible platform derived from the sources of Red Hat Enterprise Linux (RHEL). Since March 2004, CentOS Linux has been a community-supported distribution derived from sources freely provided to the public by Red Hat. As such, CentOS Linux aims to be functionally compatible with RHEL.

4.4.1.2 Mobile Device Operating System

The Age Gate mobile app is a native Android app that can be installed on any mobile device running Android 6.0+ (Marshmallow). The app also makes use of external libraries, such as Zxing QR library, and Junit.

4.4.2 Required Modules

The age verification online gateway pilot takes advantage and integrates various technologies and software modules which have been implemented during the project’s technical Work Packages (WP3, WP4, WP5), along with additional pilot specific functionality. These are deployed inside the respective pilot’s components.

4.4.2.1 Age Gate Server

It acts as the Relying Party to the Identity Consolidator, in order to receive the age of its users. It includes the following modules:

- **OpenID Connect Client:** The Age Gate Server is configured as an OpenID Connect Client (Relying Party) and it interacts with the Identity Consolidator, that runs OpenAM and is configured as an OpenID Connect Provider. The Age Gate Server is configured to follow the authorization code flow of OpenID Connect.
- **Access Control Policy Module:** The Age Gate Server provides a web front-end to the website owners, through which they can register age-restricted websites and define access control policies regarding the minimum age of their visitors.
- **QR Authentication Server:** The Age Gate Server receives authorization requests by the registered websites, and generates QR codes to be scanned by the Age Gate mobile app, in order to initiate the users’ authorization flow.
- **Reporting Tool:** The Age Gate Server includes a reporting tool that allows personal data auditors to audit sample records of authorization requests, and website owners to generate recurring and ad-hoc reports.

4.4.2.2 Age Gate Mobile App

The Age Gate mobile app is a native Android app that is used to issue age cryptographic credentials to the user’s device, initiate the authorization flow and display the user’s history of access to age-restricted websites. It includes the following modules:

- **FIDO UAF Client:** The mobile app includes a FIDO UAF stack that allows the end-user to perform human-to-device authentication (mainly through biometrics / fingerprint).

- **QR Client:** Scans and decodes the QR codes that are displayed on age-restricted websites, in order to initiate the users’ authorization flow.
- **Cryptographic Credentials Storage:** Securely stores the cryptographic credentials that are received by the Identity Consolidator, and uses them to prove the age of the user.
- **Access History Module:** Shows historical data regarding the user's access to age-restricted websites. It also allows the user to revoke access to one or more websites.

4.4.2.3 Identity Consolidator

The ReCRED Identity Consolidator acts as the Identity Provider, which authenticates the users and verifies and proves their age. Of all the modules that are deployed in the Identity Consolidator, the following are used in the age verification pilot:

- **Authentication Management Module:** The Authentication Management module is responsible for registering new end-users to the Identity Consolidator. It also allows registered users to login to their ReCRED account.
- **Physical Identity Acquisition Module:** Registered ReCRED users can use the Physical Identity Acquisition module, in order to scan official documents that prove their age (ID, passports, driving licenses, etc.).
- **Credential Management Module:** Issues age-related cryptographic credentials, either directly from the Identity Consolidator or from another trusted Identity Provider. In the latter case, either the Identity Provider issues directly the credential (as long as it supports the ReCRED issuance module) or the Identity Consolidator acquires the user's age from the Identity Provider (which does not support the ReCRED issuance module) and issues the credential on behalf of that Identity Provider.
- **Open AM:** OpenAM has been configured on the Identity Consolidator as an OpenID Connect Provider. It authenticates the user and sends his age back to the Age Gate server (upon user’s consent).
- **FIDO UAF Server:** Provides FIDO UAF enrolment and authenticates the user to his FIDO-enabled device. The FIDO UAF Server interacts with OpenAM, regarding the authentication processes and username registration
- **Identity Repository:** Stores the user's age-related attribute values.

4.4.3 Environment and Deployment

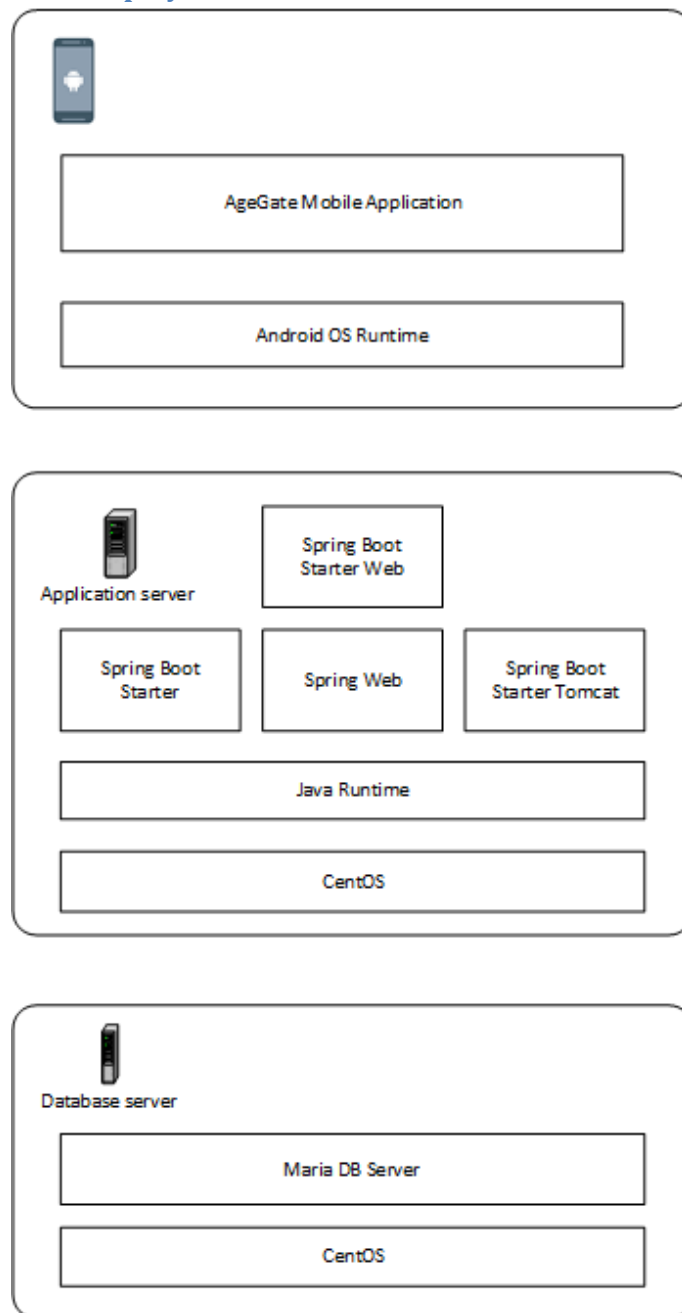


Figure 29: Age verification pilot - Environment and deployment

As a database server software, MariaDB Server v5.5 is used. It is one of the most popular database servers in the world. It is made by the original developers of MySQL and guaranteed to stay open source. Notable users include Wikipedia, WordPress.com and Google. MariaDB turns data into structured information in a wide array of applications, ranging from banking to websites. It is an enhanced, drop-in replacement for MySQL. MariaDB is used because it is fast, scalable and robust, with a rich ecosystem of storage engines, plugins and many other tools make it very versatile for a wide variety of use cases.

The Java application is built in Java SE v8, and is based on Spring Boot. It is a stand-alone Spring Platform based Application, running on the embedded Apache Tomcat v8 application server. The

Apache Tomcat® software is an open source implementation of the Java Servlet, Java Server Pages, Java Expression Language and Java WebSocket technologies. The Java Servlet, Java Server Pages, Java Expression Language and Java WebSocket specifications are developed under the Java Community Process. The Apache Tomcat software is developed in an open and participatory environment and released under the Apache License version 2. The Apache Tomcat project is intended to be a collaboration of the best-of-breed developers from around the world. Apache Tomcat software powers numerous large-scale, mission-critical web applications across a diverse range of industries and organizations. The java application is built into an executable .jar file type. It is executed with the following command:

```
nohup java -jar age-gate-0.0.1-SNAPSHOT.jar --spring.profiles.active=accept &
```

(The jar file name can be different according to the version of the application).

The application connects securely using TLS protocol to the database server.

The initial deployment has the following steps:

- Execute db creation SQL script at database server
- Copy the java application jar file into the server that will host the application.
- Start the application using the previous command.
- Install the android application into the mobile device

In order to deploy a new version:

- Execute and db update SQL script at database server (if any)
- Copy the new java application jar file into the application server.
- Stop the previous version of the application and execute the new one.
- Update the android application into the mobile device

4.5 Privacy & Security Considerations

4.5.1 Physical Protection and Network Security

The physical access to the servers is secured by OVH provider. All access to the OVH premises is strictly monitored. To prevent any intrusions or hazards, every boundary is secured using barbed-wire fencing. Video surveillance and movement detection systems are also in continuous operation. Activity within the datacentres and outside the buildings is monitored and recorded on secure servers, while the surveillance team are on site 24/7. In order to control and monitor access to the OVH premises, strict security procedures have been put in place. Every member of staff receives a RFID name badge which is also used to restrict their access. Employee access rights are reassessed regularly, according to their remit. To access the premises, employees must hand in their badges for verification, before passing through the security doors. The datacentres have an even higher level of protection, as only authorised personnel can gain entry. OVH installations are strictly for their own use.

Every datacentre room is fitted with a fire detection and extinction system, as well as fire doors. OVH complies with the APSAD R4 rule for the installation of mobile and portable extinguishers, and also has the N4 conformity certification for all our datacentres.

The OVH teams provide a human presence in the datacentres 24 hours a day and 365 days a year, to guarantee that the servers are constantly maintained. In the event of a technical incident, they will react immediately to ensure that your server is repaired as quickly as possible. Most servers are equipped with double power supplies and double network cards, so that the infrastructure is redundant from end to end.

The OVH datacentres are powered by two separate electrical power supplies and are also equipped with UPS devices. Power generators have an initial autonomy of 48hrs to counteract any failure of the electricity supply network.

All OVH dedicated hosting services include protection against all types of DDoS attacks. Three 160 Gbps anti-DDoS infrastructures have been set up in the Roubaix, Strasbourg and Beauharnois datacentres.

To guarantee high speed, high quality bandwidth and low latency time, OVH has chosen to deploy its own global fibre optic network. The network is managed using DWDM devices and is currently being migrated to 100G coherent technology, offering a total capacity of 10 Tbps to the worldwide web. To guarantee the maximum redundancy and availability of the server internet connection, all links are at least doubled at every routing point. Two Cisco routers (each with two network cards) make up the physical connection to each server. The fibre optic cables are at least doubled, and sometimes tripled.

4.5.2 Configuration and Security Settings

Upcom uses servers from the most secure Datacentres that conform with ISO security standards. The operating systems used are common Linux distributions with a large active supporting community that provide up to date security fixes. The versions of the Linux distributions used are the most stable at the moment of installation. The system administrators are monitoring daily the security notices of any of the operating system or software used, and plan to be applied as soon as possible following the Patch management process described later in this document.

A strict security and access policy is applied on all operating system and software settings. Only needed network ports and specific public IP addresses are enabled through firewall. All services run with Linux users with very restricted access to the file system. All settings are regularly reviewed by system administrators.

4.5.3 Access Control

The servers can be accessed either through a KVM console or through SSH connection. Both connections are encrypted and the only people that have access are the System Administrator of Upcom and the System Security Manager of Upcom. Root access is disabled through SSH connection. The database server software and the java application are executed using a local account that has very restricted permission and file access, and does not have access to a shell or SSH session.

4.5.4 Monitoring

The network is constantly monitored by OVH provider and is protected by an DDoS attacks as described above.

The servers are monitored by OVH provider regarding hardware malfunction and in case of technical incident, OVH's personnel react immediately.

The services, database service and java application service, are monitored by a NodePing server availability monitoring provider, which provides checks to see if that site or service is responding properly. If the services do not respond correctly, the service automatically notifies someone by email, SMS, voice, Pushover, twitter direct message, etc. Results are stored in NodePing databases so they are available for reports. The Age Gate services are checked every 5 minutes using a list of globally distributed check servers that NodePing service provides. In case of the service becomes unavailable, the System Administrators are notified by e-mail and SMS.

Performance and server availability monitoring is done using Zabbix software. A Zabbix agent is installed on both servers. Monitoring performance indicators like CPU, memory, network, disk space and processes is done easily with Zabbix agent, which is available for Linux, UNIX and Windows platforms. The agent communicates with Upcom's Zabbix Monitoring Server which receives all the information about the performance and availability of the servers. In case of problem detection e-mails containing any related information are sent to the System Administrators of Upcom. The System Administrators act immediately to solve any performance related issue, e.g. high CPU usage, low disk space etc.

Security monitoring and intrusion detection is done using ConfigServer Security & Firewall (CSF), which is a Stateful Packet Inspection (SPI) firewall, Login/Intrusion Detection and Security application for Linux servers, together with the Login Failure Daemon (lfd) process that runs all the time and periodically (every X seconds) scans the latest log file entries for login attempts against the server that continually fail within a short period of time. Such attempts are often called "Brute-force attacks" and the daemon process responds very quickly to such patterns and blocks offending IP's quickly.

The firewall has been setup with a very strict policy to allow only SSH port, Zabbix agent port, database server port and java application server port connections. All blocked accesses to other ports or from blacklisted IP addresses are logged in the system, keeping the timestamp and detailed description of the event.

The System Administrators are notified by e-mail for any root or super admin access to the server, or for any attack or continuously fail attempt for login to various services (SSH, database server, java application service etc.). The IP address of the client that fails to login for more than 5 times in less than 360 seconds is blocked permanently. A whitelist of IP addresses has been defined, containing the static IP addresses of Upcom premises network and any related server that is accessed by the Age Gate servers.

4.5.5 Malware Protection

Malware protection on both machines is done using Rkhunter (Rootkit Hunter), which is a Unix-based tool that scans for rootkits, malware, backdoors and possible local exploits. It does this by

comparing SHA-1 hashes of important files with known good ones in online databases, searching for default directories (of rootkits), wrong permissions, hidden files, suspicious strings in kernel modules, and special tests for Linux. Rkhunter runs automated once a day with the help of a Cron job and the results send by email to the System Administrators of Upcom. The System Administrators act immediately if a machine has malware infection to solve the problem.

4.5.6 Patch Management

In order to have the most efficient and affordable backup strategy we create snapshot of the virtual machine. Contrary to a full backup, there is no need to lock the data to prevent modification during the process. The snapshot allows us to keep an image of the VPS in real-time and restore to that point in case something goes wrong.

Every time an operating system patch, a security patch, software patch or a new release should be applied, the following process is followed:

- Send notification e-mail for service unavailability/maintenance
- Restrict service port on firewall temporarily (e.g. database port)
- Take a snapshot of the machine before applying the patch(es)
- Apply one patch at a time
- Make checks on the system
- Enable the service port on firewall
- Send notification for end of unavailability/maintenance

In case of a failure during a patch execution the following process is followed:

- Logs are saved in another server
- The machine is restored to the latest taken snapshot
- The service port is enabled in firewall
- A notification of end of maintenance is sent
- The System Administrators investigate the reasons of the patch application failure. If needed, they try to reproduce it at a similar environment

4.5.7 Change Management

A staging environment has been setup in order to deploy fixes, enhancements and new releases of the developed services. They are thoroughly tested, by executing automatic unit tests, developed with jUnit, functional tests developed using jUnit, SoapUI and Selenium tools. A Testing Plan containing an extensive list of manual test cases is also executed on the staging environment. After the successful test execution and approval of the changes and evaluation of possible implications, the changes are planned to be deployed on the production environment following the Patch Management process.

4.5.8 Incident Management

In case of a security incident, the System Administrators are instantly notified by the monitoring systems and takes immediate actions to stop and eliminate the threat. They are notified by either e-mail or SMS, they login to the systems through KVM console and disable all network traffic through firewall software. They investigate the incident, they keep all necessary logs to a safe place, they correct the security breach, and enable the network traffic again.

4.5.9 Protection of Logs and Data

A daily system data backup is scheduled using a cron job. Important data, database data, system setting and important logs are collected and saved as a zip file. The backup file is securely copied to a remote backup server hosted on another datacentre. In total, the last 7 daily backups, the last 3 weekly backups and the last 6 monthly backups are archived.

4.5.10 Cryptography and Protection of Electronic Communication

All communication with the servers is encrypted with SSL protocol, access to the server through SSH console, java application http access through https protocol and database access through TLS protocol. The remote copy of backups is done using secure copy command (SCP) that uses SSL encryption.

4.6 Risk Assessment

The initial identified risks for the Age Verification Online Gateway pilot are summarized in the following tables. These tables will be constantly updated during the execution of the pilot, and a final version will also be included in deliverable D7.4.

4.6.1 Initial Risk Score

#	Risk Events	Risk Scenarios	Risk Category	Likelihood	Impact	Risk Score	Recommended Actions
1	Pilot3_Age Gate_User Engagement_Not sufficient participating end-users	Capacity Planning	Programme/Project Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
2	Pilot3_Age Gate_User Engagement_No participation from a real service provider	Project Quality	Programme/Project Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
3	Pilot3_Age Gate_User Engagement_Delays to the acceptance of the mobile app from Google Play	Project Time Over-runs	Programme/Project Delivery	Very Low	High	3 - Low	Defer action until future assessment
4	Pilot3_Age Gate_Security_Unauthorized physical access	Internally Originated Attack	Operations/Service Delivery	Very Low	High	3 - Low	Defer action until future assessment
5	Pilot3_Age Gate_Security_Accidental damage and natural hazards	Acts of Nature	Operations/Service Delivery	Very Low	High	3 - Low	Defer action until future assessment
6	Pilot3_Age	Externally Originated	Operations/Service Delivery	Very Low	Medium	2 - Very Low	Accept residual risk;

	Gate_Security_DDoS attacks	Attack		Service Delivery				no mitigation needed
7	Pilot3_Age Gate_Security_Malware, backdoors, local exploits	Malware		Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
8	Pilot3_Age Gate_Security_Security incident	Externally Originated Attack		Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
9	Pilot3_Age Gate_Security_Loss of data	Data Integrity (Damage/Destruction)		Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment

4.6.2 Risk Actions

#	Risk Events	Recommended Actions	Risk Action to be Taken	Required Follow-up
1	Pilot3_Age Gate_User Engagement_Not sufficient participating end-users	Defer action until future assessment	Enhance existing risk mitigation controls	Additional users can be recruited by services such as www.cint.com, so that we have a large base of end-users.
2	Pilot3_Age Gate_User Engagement_No participation from a real service provider	Defer action until future assessment	Defer action until future assessment	For the duration of the pilot, Age Gate will be an alternative age verification method. Visitors will have the option to verify their age using either the Age Gate mobile app or any other existing method (e.g. check a disclaimer).
3	Pilot3_Age Gate_User Engagement_Delays to the acceptance of the mobile app from Google Play	Defer action until future assessment	Defer action until future assessment	Upcom is very experienced on submitting mobile apps to Google Play, and will take all the necessary actions to ensure that the app will be available on time.
4	Pilot3_Age Gate_Security_Unauthorized physical access	Defer action until future assessment	Defer action until future assessment	All the pilots' servers will be hosted to OVH. All access to the OVH premises is strictly monitored. To prevent any intrusions or hazards, every boundary is secured using barbed-wire fencing. Video surveillance and movement detection systems are also in continuous operation. Activity within the datacentres and outside the buildings is monitored and recorded on secure servers, while the surveillance team are on site 24/7.
5	Pilot3_Age Gate_Security_Accidental damage and natural hazards	Defer action until future assessment	Defer action until future assessment	All the pilots' servers will be hosted to OVH. Every OVH datacentre room is fitted with a fire detection and extinction system, as well as fire doors. OVH complies with the APSAD R4 rule for the installation of mobile and portable extinguishers, and also has the N4 conformity certification for all our datacentres.
6	Pilot3_Age Gate_Security_DDoS attacks	Accept residual risk; no mitigation needed	Defer action until future assessment	All the pilots' servers will be hosted to OVH. All OVH dedicated hosting services include protection against all types of DDoS attacks. Three 160 Gbps anti-DDoS infrastructures have been set up in the Roubaix, Strasbourg and Beauharnois datacentres.

7	Pilot3_Age Gate_Security_Malware, backdoors, local exploits	Defer action until future assessment	Defer action until future assessment	Malware protection on both pilot servers will be done using Rkhunter (Rootkit Hunter), which is a Unix-based tool that scans for rootkits, malware, backdoors and possible local exploits. Rkhunter runs automated once a day with the help of a Cron job and the results send by email to the System Administrators of Upcom. The System Administrators act immediately if a machine has malware infection to solve the problem.
8	Pilot3_Age Gate_Security_Security incident	Defer action until future assessment	Defer action until future assessment	In case of a security incident, the System Administrators will be instantly notified by the monitoring systems and will take immediate actions to stop and eliminate the threat. They are notified by either e-mail or SMS, they login to the systems through KVM console and disable all network traffic through firewall software. They investigate the incident, they keep all necessary logs to a safe place, they correct the security breach, and enable the network traffic again.
9	Pilot3_Age Gate_Security_Loss of data	Defer action until future assessment	Defer action until future assessment	A daily system data backup is scheduled using a cron job. Important data, database data, system setting and important logs are collected and saved as a zip file. The backup file is securely copied to a remote backup server hosted on another datacentre. In total, the last 7 daily backups, the last 3 weekly backups and the last 6 monthly backups are archived.

5 Microloan Origination

5.1 Description of the Pilot

The microloan origination pilot is aiming to provide small loans via an entirely online process. This pilot will be based on a Bank web site and a mobile application with the purpose of granting or denying microloans, without revealing or disclosing any personal and/or sensitive data of the user, other than the absolutely necessary.

The microloan provider only needs to know whether the applicant’s financial information is above a certain limit or not. This information has been already acquired by the Banking sector. In addition, EXUS is intending to contact an administrator from the banking sector in order to assess the flow and the results of the pilot. More details are going to be given in the deliverable D7.4.

The microloan origination pilot includes the below flows, which are described in more detail in the following subsections.

1. End-user registration to ReCRED platform
2. Bank Website, mobile application initialization with regards to ReCRED platform
3. Microloan verification

4. Loan granted or denied

5.1.1 End User Registration to ReCRED Platform

Microloan stakeholders need first to be ReCRED users to be able to exploit the functionalities offered by the microloan pilot web application. This process will verify their ability to fulfil the bank's policy for giving or not the loan.

The following steps are needed to be taken:

1. The user registers to the ReCRED via the Account Management module of the ReCRED identity consolidator. The user will at first need to register his fingerprint via the microloan ReCRED based mobile application to the FIDO server of the Identity Consolidator.
2. The user is requesting to issue cryptographic credentials for his financial info regarding income etc. through the Credential Management module of the Identity consolidator
3. FIDO authentication occurs and the credentials are stored in the Mobile application for future usage.

5.1.2 Bank Website / Mobile Application Initialization

1. The Microloan website needs to register to the QR Authentication server to be able to issue QRs that the mobile app will scan in order to connect to the current session and send the required credentials to the bank.
2. The Microloan pilot mobile application will need to register to the FIDO Server so as to be able to function properly.
3. Definition of policies for granting loans is needed to the Access Control Policy Reasoning Tool in the Service provider itself (the Bank website).

5.1.3 Microloan Verification

According to the financial information of the microloan users which is included in the cryptographic credentials the Microloan website will verify them and apply the policy defined for granting loans.

5.1.3.1 Microloan Verification through Cryptographic Credentials

1. A user wants to ask for a potential micro-loan grant.
2. The microloan website generates a QR code which is displayed to the user.
3. The user scans with his ReCRED-microloan mobile app the QR code which then searches for a cryptographic credential in the mobile device with the appropriate financial info to validate his fulfilment of the policy for the loan.
4. The mobile app sends the credentials to the Microloan website policy tool for checking.
5. The policy is applied and the user is granted or denied the microloan.

EXUS has gathered alongside with bank experts a pool of policies that are applied to possible end-users that will be granted a micro-loan. It has been formulated and clearly defined so that it can be imported as simple rules that will define according to the incoming ReCRED credentials data the grant or not of a loan. Namely this financial information includes amongst other the following attributes:

- Debt to state
- Employed or not
- Income
- Monthly loan payments
- Overloan payments
- Age
- Address history
- Location

The financial information that resides in the ReCRED Identity Management module has been designed to be aligned with this data taken into account. Therefore, all the cryptographic credentials that will be issued are covering every possible information that a bank will need for granting loans.

5.2 Components Overview

The components described below are all the components that will be used and needed for the successful implementation of the Microloan pilot. Initially not all of them will be involved since the vast majority is under development at the moment. However, for the design and initial implementation we have to take into account all the aspects and parameters of the ReCRED platform functionality.

Initially functionalities regarding a small end to end scenario will be tried to be covered involving all the ready to use components.

5.2.1 Microloan Mobile App

The microloan mobile app is an Android application that will be downloaded by end-users so as to issue financial information based cryptographic credentials. This would enable them to justify their financial status and have access or not to microloans.

The microloan mobile app involves the following functionalities:

1. The mobile application has a FIDO client that will talk to the FIDO server of the Web app so as to create a public private key for the device.
2. Also, Mobile connect should be included for the mobile app since we need maximum LOA.
3. An Idemix client will be needed for asking for credentials.
4. UProve client for allowing access to financial products.
5. A behavioral extraction daemon is needed to be running in the mobile so that for example typing way, walking habits and antennas connecting to the device can be captured and sent to the behavioral authentication server.

6. QR client for scanning the QRs generated in the website.
7. Mobile browsing of bank products and submission of credentials for core microloan functionality.
8. Securely stores the cryptographic credentials received from the Identity consolidators/Identity providers.

A first version of the mobile application will be demonstrated in the following screenshots. Currently we have set up the mobile application part which directly interacts with the mobile application backend without interfering with the website. The final initial version will include the QR reader to scan the QR from the microloan website.

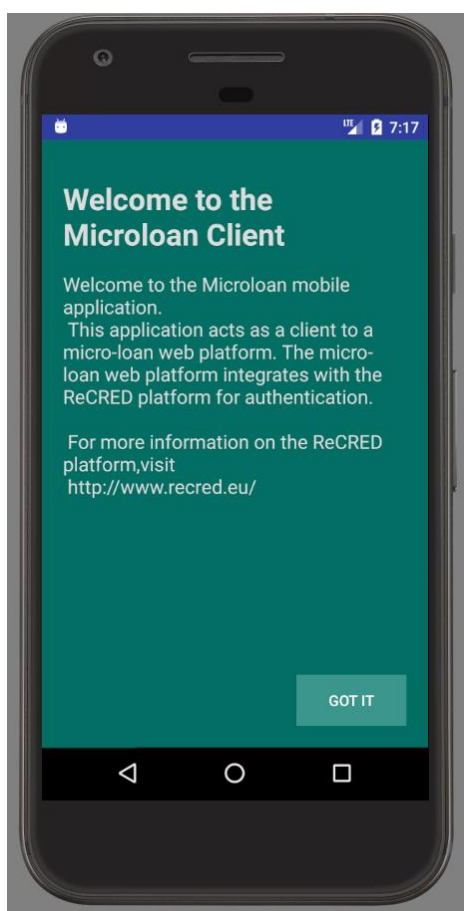


Figure 30: Microloan pilot - Welcome screen

Initial screen informs the mobile user about the application and its goal.

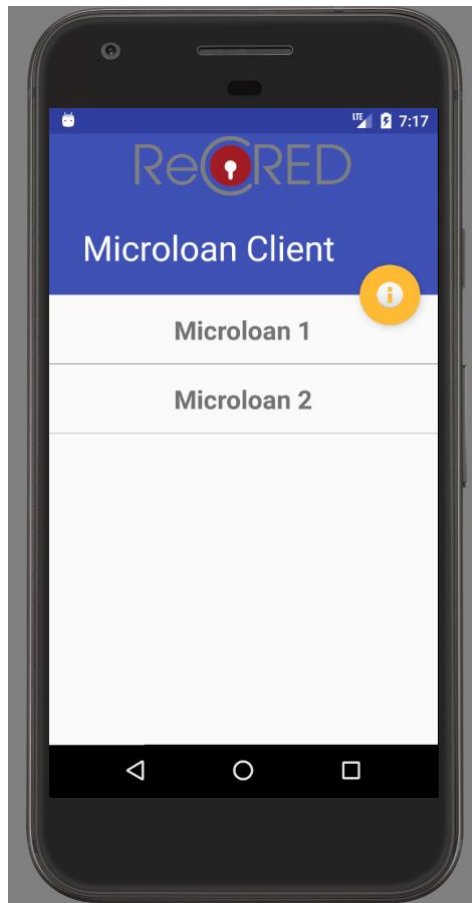


Figure 31: Microloan pilot - Show microloans

The user is prompted to see all the available microloans for buying. This can also be done through the website but initially direct access to the backend is shown.

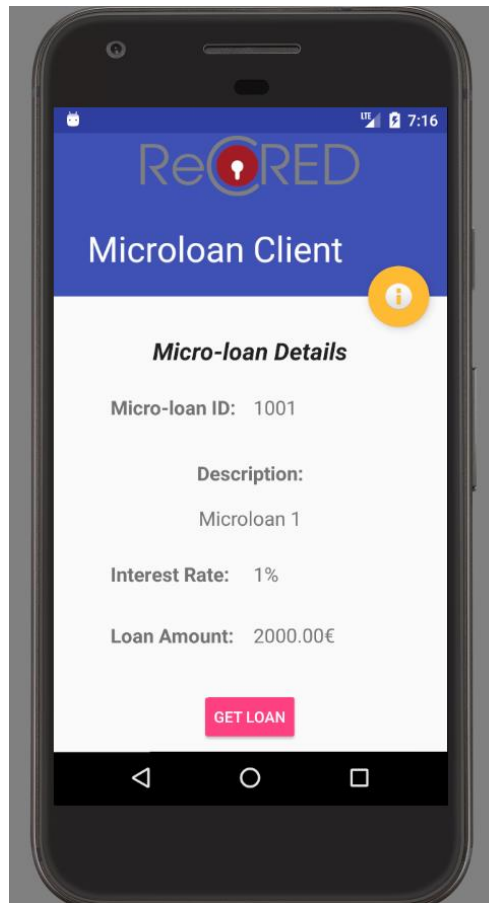


Figure 32: Microloan pilot - Show microloan details

The details screen shows the details of the loan so as the user will proceed to the get loan mechanism and have the loan granted through ReCRED mechanisms.

5.2.2 Microloan Website / Service Provider

The Microloan website is offering the core functionality needed by this pilot which is to grant or deny loans.

Thus, it offers the following:

1. It involves an Access Control Policy Reasoning Tool which is needed for setting rules for end-users' financial verification and verifying the users' credentials.
2. A behavioral client is needed that will ask the Behavioral server for validating the user.
3. Finally, financial services regarding microloans will be available.

Some initial concept screens for the website are the following:

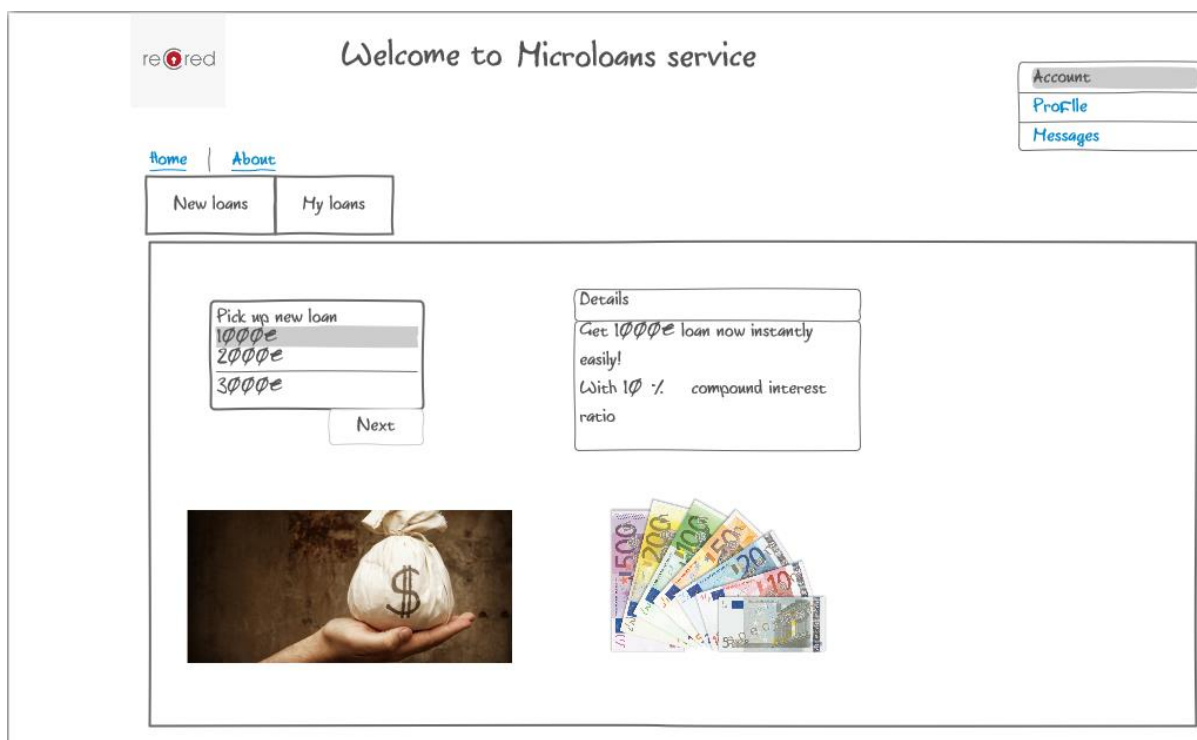


Figure 33: Microloan pilot - Loan selection

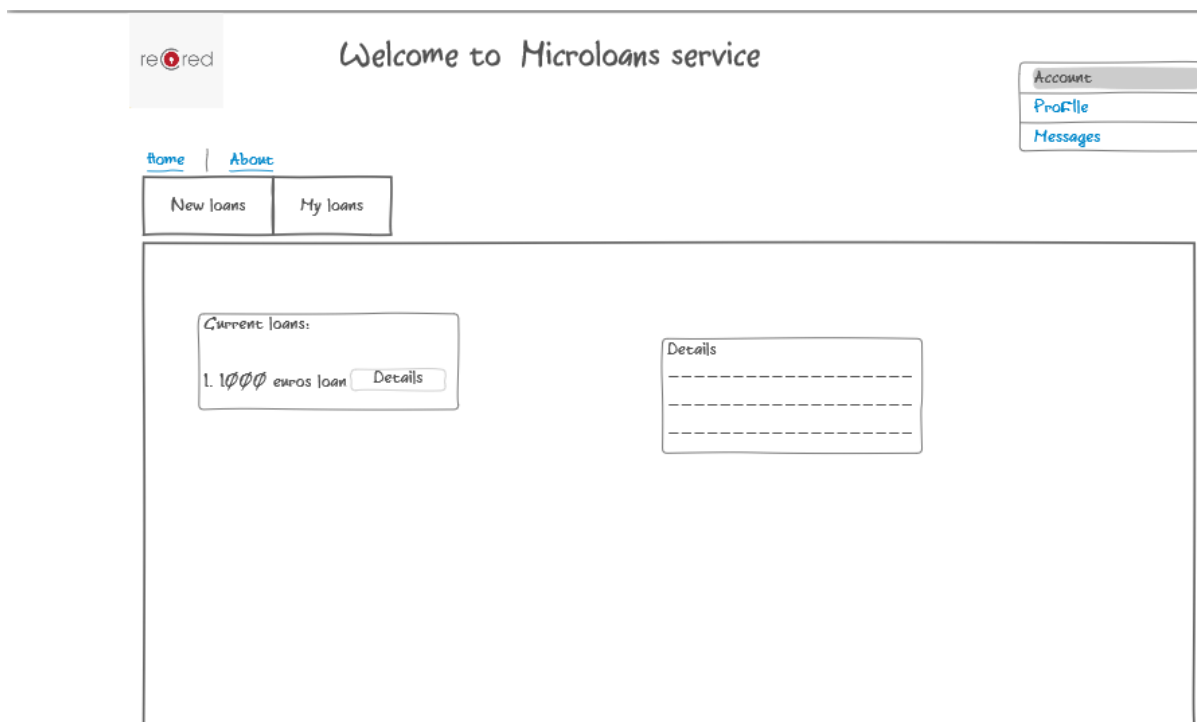


Figure 34: Microloan pilot - Loans history

5.2.3 ReCRED Identity Consolidator / Provider

ReCRED Identity Consolidator will play the role of the trusted and certified Identity Provider which is holding all the relevant information of the end-users either financial or not. Currently there is no

trusted Identity Provider that can certify the users’ financial information so it would be assumed that the ReCRED Identity Provider offers trusted and approved financial information.

5.2.3.1 ReCRED Identity Consolidator Financial Data

EXUS after an extensive workshop with bank experts has identified end users’ financial information distribution and such emulated financial data will be imported into the Identity Consolidator for the end users.

5.2.3.2 ReCRED Identity Consolidator Operations Description

The following functionalities are mostly describing the goal of the usage of the ReCRED Identity consolidator for the microloan pilot:

1. The inclusion of a FIDO server is needed as well to provide FIDO UAF authentication mechanisms and registering the mobile application using the end-user fingerprint.
2. The issuance of credentials will be done by the ReCRED identity consolidator using IDemix or UProve credentials issuers.
3. The Identity management module will be needed for asking the credentials issuer for credentials.
4. The Account Management module is needed for registering the user and having access to his details.

5.2.4 Behavioral Authentication Server

The mobile application will need to run behavioral extraction daemon that will send behavioral information such as walking style, typing letters style and antennas condition to a Behavioral Authentication Server. Then the microloan website upon receiving the request from the mobile application for validating the user will also ask the Behavioral Authentication Server for validation as well according to the data gathered so far.

5.2.5 QR Authentication Server

Generates QR codes that the bank customer will scan using the mobile app of the microloan pilot in order to connect to the current session and send the required credentials to the microloan service provider.

5.3 Hardware Architecture

The required hardware components and their role

EXUS will provide 1 dedicated Server allowing for the quick and reliable testing of the prototypes developed in the context of ReCRED pilot. The server configuration is as follows:

Intel Xeon E5-2407 2, 20GHz, 10M Cache, 6,4GT/s QPI

- 16 GB Memory Module - 2Rx4 RDIMM 1600MHz SV NEW
- Additional info: 1U RACK Chassis, for Up to 4x 3, 5" HDDs, Dual, Hot-plug, Redundant Power Supply (1+1), 550W
- 1TB NL SAS 6Gbps 7,2k 3, 5" HD Hot Plug Fully Assembled – Kit
- Heat Sink for Additional Processor
- PCIe Riser for 2CPUs R420 – Kit

- Fan 12V 40x40 – Kit

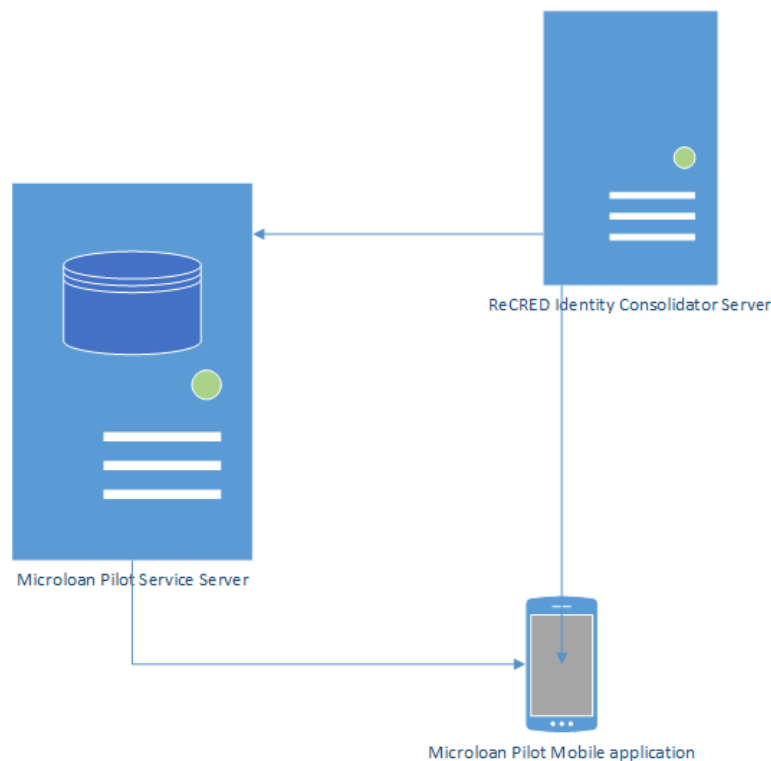


Figure 35: Microloan pilot - Hardware architecture

5.4 Software Architecture

Software will be deployed @ EXUS server. Operating system is Ubuntu server 16.04 which is stable and LTS. Core technologies for implementing the microloan pilot specific functionality are:

- Java
- Spring boot
- Docker
- PostgreSQL
- AngularJS or ReactJS
- Android for the mobile application

And are open to change due to the integration of core ReCRED functionalities to happen both in the android mobile application and the backend service.

5.4.1 Required ReCRED Components

5.4.1.1 Microloan Mobile App

The Microloan mobile app will be downloaded as a native Android app in the end-users' devices for being able to search for available microloan plans and offerings based on their financial information existing in the Identity Consolidator. It will mainly issue cryptographic credentials, initiate authentication based on biometrics and browse the bank products.

More specifically:

1. **Pilot Specific User Device Functionality:** The bank customers will browse the bank products, and submit the appropriate credentials in order to be able to purchase them.
2. **FIDO UAF Client:** Allows the end-user to perform human-to-device authentication (mainly through biometrics)
3. **QR Client:** Scans QR codes corresponding to the Banks financial products in order to initiate the submission of the appropriate credentials.
4. **Gait Capturing Module, Typing Capturing Module:** The EXUS pilot must include the usage of the BAA components for additional authentication.
5. **Idemix Client:** Submits Idemix credentials required by the Bank in order to allow access to financial products.
6. **U-Prove Client:** Submits U-Prove credentials required by the Bank in order to allow access to financial products.
7. **Cryptographic Credentials Storage:** Securely stores the cryptographic credentials received from the IdC / IdPs

5.4.1.2 *Microloan Website / Service Provider*

The Microloan Bank website will be the main service provider which will offer the core functionality for the loans grant.

The following components will be available:

1. **Access Control Policy Reasoning Tool:** Allows the Bank to define the policy that is applied to accept/reject customer applications for financial products. It will have an interface with ReCRED Access Control Policy reasoning tool.
2. **Specific Microloan Backend service:** Offering the core functionality for loans

5.4.1.3 *ReCRED Identity Consolidator*

ReCRED Identity Consolidator will be our trusted Identity Provider that will handle the users' data and user's authentication for income and financial info verification. The following components from ReCRED are needed:

1. **Physical Identity Acquisition Module:** The Microloan Origination pilot will use the Physical ID document as credential.
2. **Online Identity Acquisition Module:** Currently none of the required ID Providers e.g. IRS, supports OAuth2 access to user profiles. At least one ID Provider e.g. the IRS must be emulated somehow in a next release.
3. **Account Management Module:** Allows the end-user to manage / delete his ReCRED account and recover his accounts. It also acts as a BAA discovery service.

4. **Credential Management Module:** Customer applications for financial products will be rejected/approved based on credentials issued by the ID Consolidator.
5. **Authentication Management Module:** Allows ReCRED users to login to the ID Consolidator and manage their profile.
6. **Identity Management Module:** Allows the user to manage attributes in the user's Identity Profile. The attributes are important because they will be used in the credentials used for the pilot.
7. **FIDO UAF Server:** Enrolls user and authenticates to mobile device
8. **QR Authentication Server:** Generates QR codes that the bank customer will scan in order to connect to the current session and send the required credentials to the bank.
9. **Account Locking (aka Latch):** Will lock all user accounts in the case of account abuse by malicious users.
10. **Identity Repository:** Stores user attributes. Necessary for the issuing of credentials.

5.4.1.4 *Behavioral Authentication Server*

1. **Behavioral Profile Extraction:** Captures behavioral aspects of the user to be used for authentication.
2. **Behavioral Profile Verification:** Verifies a user's profile based on captured behavioral aspects of the user.
3. **Behavioral Profiles Database:** Stores captured behavioral information associated with a user's profile.

5.4.1.5 *QR Authentication Server*

A QR Authentication server where the Microloan service will be registered for issuing new QRs.

A diagram with a synopsis is following:

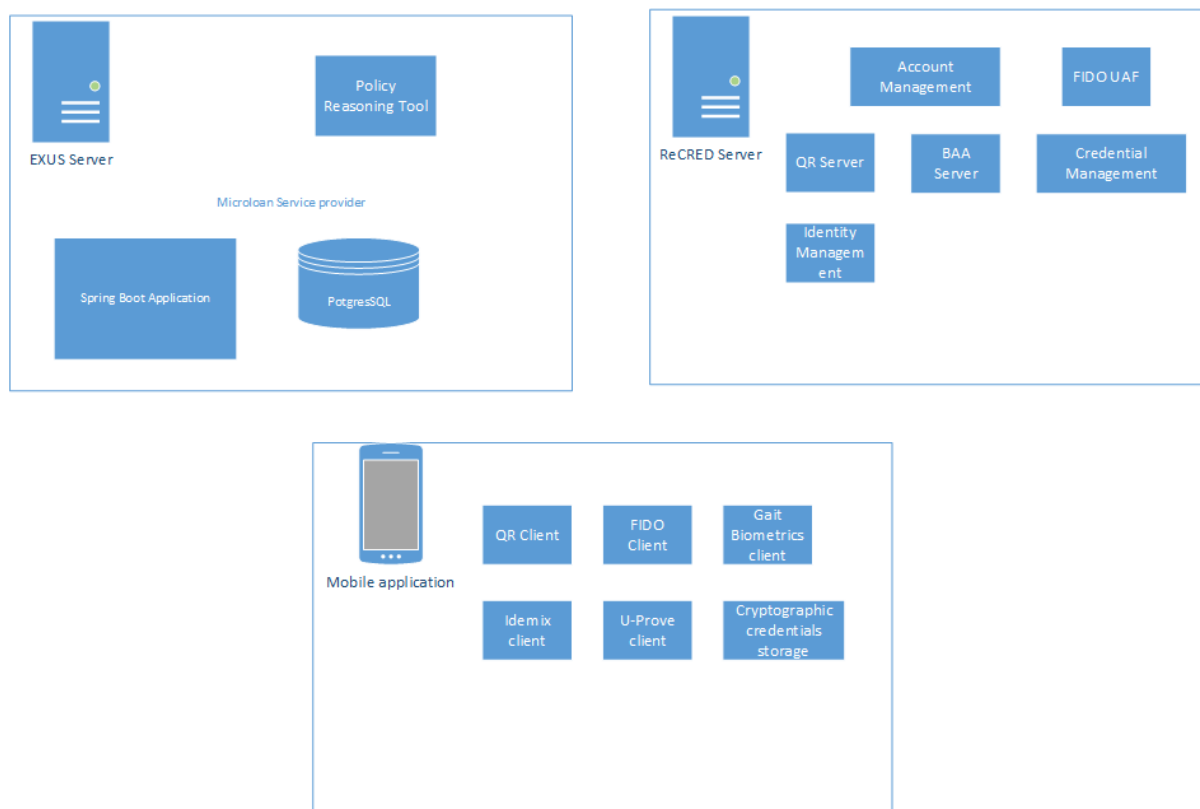


Figure 36: Microloan pilot - Software components

5.5 Privacy & Security Considerations

EXUS servers are coming with the latest OS versions (Ubuntu server LTS, Centos OS 7) to avoid any security issue or malfunction through package patches and fixes. The system administrator is keeping the server up to date on a periodic basis.

A firewall consisting of strict rules is allowing access only to the services defined by the application to avoid any breach. There is also a logging of activity which enables the system administrator to monitor any potential threat.

Access is granted to the server using SSH through credentials or certificates. Connection provided by SSH is encrypted and does not allow root access. For security reasons, also there is a logging of this activity.

With regards to monitoring of the system the infrastructure, microloan origination service, the remote connection and the database are monitored using various tools so that their status is under control.

Finally, a data backup is scheduled to occur on periodic basis so that application data, the database and system settings are backed up to a remote server for maintaining the latest snapshot of the current system in case of emergency incidents regarding security, environmental threats or any other external problems.

5.6 Risk Assessment

The initial identified risks for the Age Verification Online Gateway pilot are summarized in the following tables. These tables will be constantly updated during the execution of the pilot, and a final version will also be included in deliverable D7.4.

5.6.1 Initial Risk Score

#	Risk Events	Risk Scenarios	Risk Category	Likelihood	Impact	Risk Score	Recommended Actions
1	Pilot4_Microloan origination__User Engagement_Delays to the acceptance of the mobile app from Google Play	Project Time Over-runs	Programme/Project Delivery	Very Low	Medium	2 - Very Low	Accept residual risk; no mitigation needed
2	Pilot4_Microloan origination_Security__Security incident	Externally Originated Attack	Operations/Service Delivery	Very Low	Medium	2 - Very Low	Accept residual risk; no mitigation needed
3	Pilot4_Microloan origination_Security__DDoS attacks	Externally Originated Attack	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
4	Pilot4_Microloan origination_Security_Malware, backdoors, local exploits	Malware	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment
5	Pilot4_Microloan origination_Security_Loss of data	Data Integrity (Damage/Destruction)	Operations/Service Delivery	Low	Medium	4 - Moderate	Defer action until future assessment

5.6.2 Risk Actions

#	Risk Events	Recommended Actions	Risk Action to be Taken	Required Follow-up
1	Pilot4_Microloan origination__User Engagement_Delays to the acceptance of the mobile app from Google Play	Accept residual risk; no mitigation needed	Defer action until future assessment	EXUS web and mobile team is very experienced and can handle in due course any such potential issue
2	Pilot4_Microloan origination_Security__Security incident	Accept residual risk; no mitigation needed	Defer action until future assessment	In case of a security incident, the System Administrator will take immediate actions to stop and eliminate the threat.
3	Pilot4_Microloan origination_Security__DDoS attacks	Defer action until future assessment	Defer action until future assessment	In case of a security incident, the System Administrator will take immediate actions to stop and eliminate the threat.
4	Pilot4_Microloan origination_Security_Malware, backdoors, local exploits	Defer action until future assessment	Defer action until future assessment	In case of a security incident, the System Administrator will take immediate actions to stop and eliminate the threat.
5	Pilot4_Microloan origination_Security_Loss of data	Defer action until future assessment	Defer action until future assessment	In case of a security incident, the System Administrator will take immediate actions to

data

stop and eliminate the threat.

6 UX Assessment

Considering the Human-Computer Interaction, usability is a fundamental issue that determines the success or the failure of a design solution. In general terms, what makes something usable is the absence of frustration in using it, because when a service is truly usable, “the user can do what he or she wants to do the way he or she expects to be able to do it, without hindrance, hesitation, or questions.”¹

As part of the design process, the ReCRED solution will be tested both by usability experts and by a group of target end-users. The aim is to analyze the different dimensions which determine the usability (i.e. effectiveness and efficiency, learnability, the information architecture, the aesthetic design etc.), and improve the Graphic User Interface (GUI) before releasing the final version of ReCRED.

This objective will be achieved using as mix method, within a circular process where the collected feedbacks provide recommendations to modify the GUI, that will be further tested.

Such iterative process includes the following phases.

1. Some usability experts will investigate the GUI according to the usability heuristics and provide a list of issues to fix.
2. A group of target end-users, who are experts in the field of ICT as well as non-expert, will be involved in individual test sessions within natural context (i.e. in the University campus), following the think aloud procedure: they are invited to describe their thoughts, expectations and doubts while using the system. This direct observation method is helpful for determining users' expectations and identifying what aspects of a system are confusing. It also reveals important clues about how they are thinking about the system, and whether the way it works matches up with the way it was designed².
3. The improved version of the ReCRED solution will be spread among stakeholders who are invited to use it and to provide their opinion completing a brief ad-hoc questionnaire. Such questionnaire was created by integrating some items of the System Usability Scale³ with specific items related to the usability heuristics⁴. Data collected through the questionnaire aim to evaluate the degree to which the ReCRED solution meets specific usability criteria.

At the same time, the UX of the backend modules that will be used by the Service Providers will also be assessed. These include the user interfaces for Service Providers registration, policy creation,

¹ Rubin, J., & Chisnell, D. (2008). *Handbook of usability testing: how to plan, design and conduct effective tests*. John Wiley & Sons, p.4.

² Rubin, J., & Chisnell, D. (2008). *Handbook of usability testing: how to plan, design and conduct effective tests*. John Wiley & Sons, p.4.

³ <https://www.usability.gov/how-to-and-tools/methods/system-usability-scale.html>

⁴ <https://www.nngroup.com/articles/ten-usability-heuristics/>

reporting etc. Feedback from the Service Providers point of view will be gathered through questionnaires, including both closed-ended and open-ended questions.

7 Conclusions / Future Activities

In the end of the second year of the project, all four pilots have been initially setup. The required ReCRED modules have been integrated and further customized in order to meet the requirements of the pilots’ scenarios. Also, the required software and hardware architecture has been implemented and all the modules have been deployed.

During the final year of the project, these pilots will remain in operation, and will be further enhanced and fine-tuned according to the feedback from the users’ assessment that we will perform. More specifically, during the following year, the following activities will take place:

- We will recruit additional users, through multiple means, in order to create a strong user-base for analysis and UX assessment.
- We will promote and demonstrate the value of the ReCRED modules, in order to engage more Service Providers for the pilots.
- We will collect empirical data from the end-users participating in each pilot, in order to evaluate them and conclude the UX assessment.
- We will further enhance the existing ReCRED modules, and will improve their UIs according to the users’ feedback, so that these modules become more user friendly.
- We will perform penetration tests for all the pilots and will try to enhance the security of both the individual modules and the overall pilot environments.
- We will be monitoring the systems and the networks for the duration of the pilots, consistently applying system and software patches, and using incident management and logs protection.

The outcomes of these activities will be included in the deliverable D7.4: All Pilots in Operation and End-user Assessment Report, which is due for the end of the project (M36).