



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 D7.4 “All Pilots in Operation & End-User Assessment Report”

Editor(s): Vangelis Bagiatis (UPCOM)

Author(s): Vangelis Bagiatis (UPCOM), Sofia Savvidou (UPCOM),
Antonis Papasavvas (CUT), Savvas Zannettou (CUT),
Charis Partaourides (CUT), Kostantinos Papadamou
(CUT), Michael Sirivianos (CUT), Arya Ghodsi
(VERIZON), Annamaria Recupero (CNIT), Alessandra
Talamo (CNIT), Sorin Teican (CSGN), Nicolae Ghibu
(CSGN), George Gugulea (CSGN), Mihai Togan (CSGN),
Valentin Necoara (CSGN) Spyros Evangelatos (EXUS),
Steven Winnen (PROD)

Dissemination Level: Public









Nature: Other


Version: 1.1

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 | 14/03/2018 | Vangelis Bagiatis (UPCOM) | Initial Table of Contents |
| 0.2 | 17/04/2018 | Vangelis Bagiatis (UPCOM) Sofia Savvidou (UPCOM) Antonis Papasavvas (CUT) Savvas Zannettou (CUT) Charis Partaourides (CUT) Kostantinos Papadamou (CUT) Michael Sirivianos (CUT) Arya Ghodsi (VERIZON) Annamaria Recupero (CNIT) Alessandra Talamo (CNIT) | Added initial input for sections 2, 3, 4 and 6 |
| 0.3 | 25/04/2018 | Sorin Teican (CSGN) Nicolae Ghibu (CSGN) George Gugulea (CSGN) Mihai Togan (CSGN) Valentin Necoara (CSGN) | Additional input from CSGN to section 2 |
| 0.4 | 27/04/2018 | Vangelis Bagiatis (UPCOM) Spyros Evangelatos (EXUS) Steven Winnen (PROD) | Added sections 1, 5 and 7. Added input from PROD to sections 3 and 6. |
| 1.0 | 30/04/2018 | Vangelis Bagiatis (UPCOM) | Final version |
| 1.1 | 31/05/2018 | Vangelis Bagiatis (UPCOM) Annamaria Recupero (CNIT) Antonis Papasavvas (CUT) | Updated version with UX assessment results and some other updates |

Executive Summary

In deliverable D7.3, we described the deployment environments for all the four pilots of the project, including their flows, their architecture and the privacy and security considerations. We also did a preliminary presentation of the methodology for the assessment of the pilots from the end-user’s perspective.

In this deliverable, the final one regarding the project’s pilots, we mainly focus on the following topics:

- Any modifications to the initial flows of the pilots, or additional features that did not exist in the initial deployment of the pilots.
- Any changes to the architecture of the four pilots / new environments.
- A presentation of the pilot dissemination activities that took place during the last year of the project (participation in events, online demos and webinars, in-house dissemination, brochures, etc.)
- Updated version of the privacy and security considerations for the four pilots.
- The process, the methods and the results of the UX assessment for the four pilots, as well as their evaluation from the Service Providers.

Table of Contents

| | |
|---|----|
| Executive Summary | 5 |
| List of Figures | 8 |
| 1 Introduction | 9 |
| 2 Campus Wi-Fi and Web Services Access Control | 10 |
| 2.1 Deployment of the Pilot..... | 10 |
| 2.1.1 Changes and Improvements | 10 |
| 2.1.2 Updated Architecture | 10 |
| 2.2 Pilot Dissemination | 14 |
| 2.2.1 In-house Dissemination | 14 |
| 2.2.2 Other Dissemination activities..... | 14 |
| 2.2.3 Webinars | 18 |
| 2.3 Privacy and Security Considerations..... | 18 |
| 2.3.1 Physical Protection and Network Security..... | 18 |
| 2.3.2 Configuration and Security Settings..... | 18 |
| 2.3.3 Access Control..... | 18 |
| 2.3.4 Monitoring | 18 |
| 2.3.5 Malware Protection | 18 |
| 2.3.6 Patch Management..... | 18 |
| 2.3.7 Change Management..... | 19 |
| 2.3.8 Incident Management..... | 19 |
| 2.3.9 Protection of Logs and Data..... | 19 |
| 2.3.10 Cryptography and Protection of Electronic Communication..... | 19 |
| 3 Student Authentication & Offers | 20 |
| 3.1 Deployment of the Pilot..... | 20 |
| 3.1.1 User Workflow | 21 |
| 3.1.2 Changes to the Pilot Partner | 23 |
| 3.2 Pilot Dissemination | 24 |
| 3.2.1 Demonstration to Commercial Partners..... | 24 |
| 3.2.2 In-house Technical Analysis of ReCRED at Brocacef | 24 |
| 3.3 Privacy and Security Considerations..... | 25 |
| 4 Age Verification Online Gateway | 27 |
| 4.1 Deployment of the Pilot..... | 27 |
| 4.1.1 Changes and Improvements | 27 |

| | | |
|--------|--|----|
| 4.2 | Pilot Dissemination | 29 |
| 4.2.1 | In-house Dissemination | 29 |
| 4.2.2 | Participation in Events | 30 |
| 4.2.3 | Online Demos / Webinars..... | 31 |
| 4.3 | Privacy and Security Considerations..... | 32 |
| 4.3.1 | Physical Protection and Network Security..... | 32 |
| 4.3.2 | Configuration and Security Settings..... | 32 |
| 4.3.3 | Access Control..... | 33 |
| 4.3.4 | Monitoring | 33 |
| 4.3.5 | Malware Protection | 34 |
| 4.3.6 | Patch Management..... | 34 |
| 4.3.7 | Change Management..... | 35 |
| 4.3.8 | Incident Management..... | 35 |
| 4.3.9 | Protection of Logs and Data..... | 35 |
| 4.3.10 | Cryptography and Protection of Electronic Communication..... | 35 |
| 5 | Microloan Origination..... | 36 |
| 5.1 | Deployment of the Pilot..... | 36 |
| 5.1.1 | Changes and Improvements | 36 |
| 5.1.2 | Updated Architecture | 42 |
| 5.2 | Pilot Dissemination | 42 |
| 5.2.1 | In-house Dissemination | 42 |
| 5.2.2 | Social Media | 43 |
| 5.2.3 | Webinars | 43 |
| 5.3 | Privacy and Security Considerations..... | 43 |
| 6 | Pilots UX Assessment | 45 |
| 6.1 | Methods..... | 45 |
| 6.2 | Results..... | 48 |
| 6.2.1 | Campus Wi-Fi and Web Services Access Control | 48 |
| 6.2.2 | Student Authentication & Offers | 50 |
| 6.2.3 | Age Verification Online Gateway..... | 55 |
| 6.2.4 | Microloan Origination..... | 57 |
| 6.3 | Service Provider | 59 |
| 7 | Conclusions | 61 |
| 8 | References | 61 |

List of Figures

| | |
|---|----|
| Figure 1: Premises selection | 10 |
| Figure 2: Require the user to select an authentication method..... | 11 |
| Figure 3: New Home page of the mobile application | 12 |
| Figure 4: CertSIGN Wi-Fi pilot architecture diagram | 13 |
| Figure 5: CUT In-house dissemination | 14 |
| Figure 6: Linopetra Lyceum at CUT premises | 15 |
| Figure 7: Wi-Fi Pilot poster for CUT premises..... | 16 |
| Figure 8: Wi-Fi Pilot Leaflet..... | 17 |
| Figure 9: Pilot deployment architecture | 20 |
| Figure 10: Student pilot flow | 21 |
| Figure 11: Student authentication pilot flow | 22 |
| Figure 12: AGify logo | 27 |
| Figure 13: Indicative AGify screens | 27 |
| Figure 14: End-user registration to AGify | 28 |
| Figure 15: Age Verification through OpenID Connect | 29 |
| Figure 16: AGify at Athens Impact HUB | 30 |
| Figure 17: AGify booth in MWC | 31 |
| Figure 18: AGify booth in 4YFN | 31 |
| Figure 19 : ReCRED app-microloan | 37 |
| Figure 20 : Microloan landing webpage..... | 38 |
| Figure 21: Microloan Options | 38 |
| Figure 22: Microloan social purpose check..... | 39 |
| Figure 23: Microloan request..... | 39 |
| Figure 24: Microloan authentication via ReCRED app | 40 |
| Figure 25: Microloan consent approval | 40 |
| Figure 26: Microloan request granted | 41 |
| Figure 27: Microloan grant confirmation email..... | 41 |
| Figure 28: Microloan origination user evaluation | 41 |
| Figure 29: Updated architecture..... | 42 |
| Figure 30: Usability dimensions for Wi-Fi pilot..... | 50 |
| Figure 31: Usability dimensions for student discount pilot | 52 |
| Figure 32 ReCRED App - Expert Review | 53 |
| Figure 33 Student Pilot – Expert Review Registration email..... | 53 |
| Figure 34 Student Pilot - Expert Review Consent | 54 |
| Figure 35 Student Pilot - Expert Review Authentication..... | 54 |
| Figure 36 Student Pilot - Expert Review Discounts..... | 55 |
| Figure 37: Usability dimensions for age verification pilot | 57 |
| Figure 38: Usability dimensions for microloan origination pilot | 59 |

1 Introduction

During the final year of the project all four pilots have been deployed, tested, evaluated and optimized, when necessary.

The **Campus Wi-Fi and Web Services Access Control** pilot, which was the very first pilot to be deployed in the CUT premises and then in the IMDEA campus, has been further extended, and by the end of the project it was up-and-running in two additional environments: the CNIT campus in Rome and the CertSIGN premises in Bucharest. The functionality of the pilot has also been enhanced, enabling support for the U-Prove P-ABAC modality.

The **Student Authentication & Offers** pilot has been successfully integrated with the ReCRED Identity Consolidator (IDC). The Campaign Manager (pilot’s backend) acts as a Service Provider, retrieving the students’ identity attributes from the IDC, through OIDC. The mobile app now allows the students to authenticate to the IDC and then consent to reveal their attributes, in order to receive personalized offers.

The **Age Verification Online Gateway** pilot has been totally redesigned and its flow has been optimized, so that the users only need to prove their age once (during registration) and not every time they attempt to visit an age-restricted website. It also supports the P-ABAC modality, allowing the users to issue cryptographic credentials with their Date of Birth, as an alternative method to prove their age.

The **Microloan Origination** pilot now relies on the ReCRED app for mostly all of the functionalities regarding the human to device and device to service access. Therefore, the Microloan Origination will enable ReCRED users in general, e.g. users of the other pilot use cases, to access it seamlessly.

In addition, there has been significant effort in the **dissemination of all the pilots**, including activities such as in-house dissemination, participation in important events (such the Mobile World Congress), online demos and webinars, newsletters, brochures, infographics, etc.

Chapters 2, 3, 4 and 5 are dedicated to each one of the four pilots, and they describe in detail all the improvements, architectural changes, along with the dissemination activities and an update to the privacy and security considerations.

Finally, an in-depth **UX assessment** of the four pilots has been performed (both from the end-users and Service Providers perspective), which is described analytically in Chapter 6. In many cases, the results of this assessment have resulted further refinements and optimizations to the four pilots.

2 Campus Wi-Fi and Web Services Access Control

2.1 Deployment of the Pilot

2.1.1 Changes and Improvements

2.1.1.1 CUT

During the last period, CUT implemented Moodle Authentication and, with the help of CSGN, deployed Uprove docker and Fiware docker in recred-authentication.cut.ac.cy server, in order to support PABAC modality as well. In addition, the user interphase was updated, and new activities were added based on user evaluation and in order to support these 2 new functionalities.

2.1.2 Updated Architecture

The architecture of the Wi-Fi pilot in CUT and IMDEA has not changed. Two new environments have been added since D7.3: CNIT and CertSIGN. The CNIT architecture is exactly the same as the architecture in IMDEA.

2.1.2.1 CUT

Now, there is one consolidated application to support all four partners (CUT, IMDEA, CNIT and CSGN) practicing the Wi-Fi Pilot. When the user starts the application for the first time, before he registers to the Pilot, he is requested to select his premises, as shown in Figure 1 below.

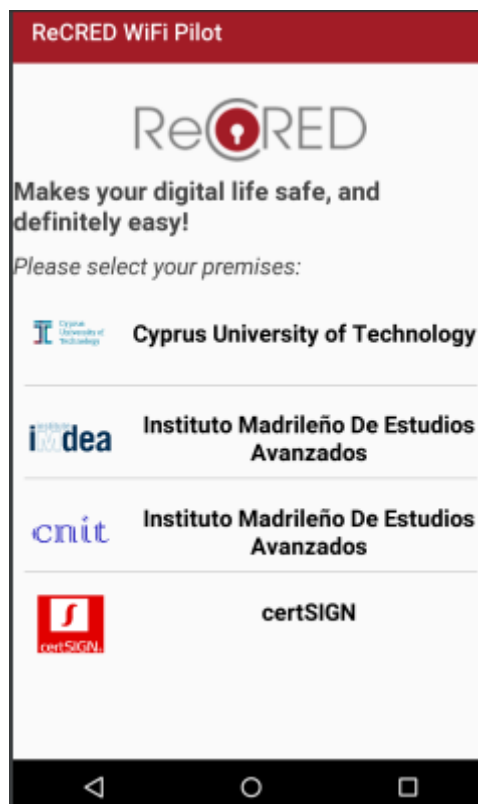


Figure 1: Premises selection

After successful registration, the user is requested to select the preferable method to access the premise’s resources. One way is by the use of biometrics (FIDO-OpenID Connect), which is the method shown in D7.3 and the other selection is PABAC, shown in Figure 2. Please note that every time the user launches the application, will be required to make this option.

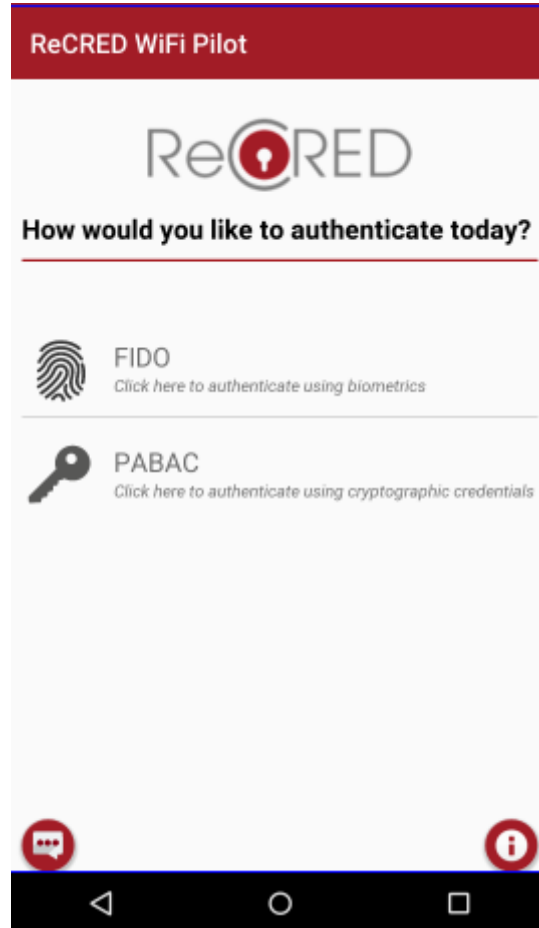


Figure 2: Require the user to select an authentication method

Last, to support Moodle authentication, the IT Department of CUT, installed OAuth and OpenID plugins in the Moodle platform of the university. The Moodle platform of the university is now configured as a Service Provide in the trusted Identity Provider of the pilot (recred-authentication.cut.ac.cy). The user has the option to authenticate to Moodle, by the use of his biometrics from the main (home) page of the pilot, as shown in Figure 3 below. Moodle authentication is only available for CUT premises.

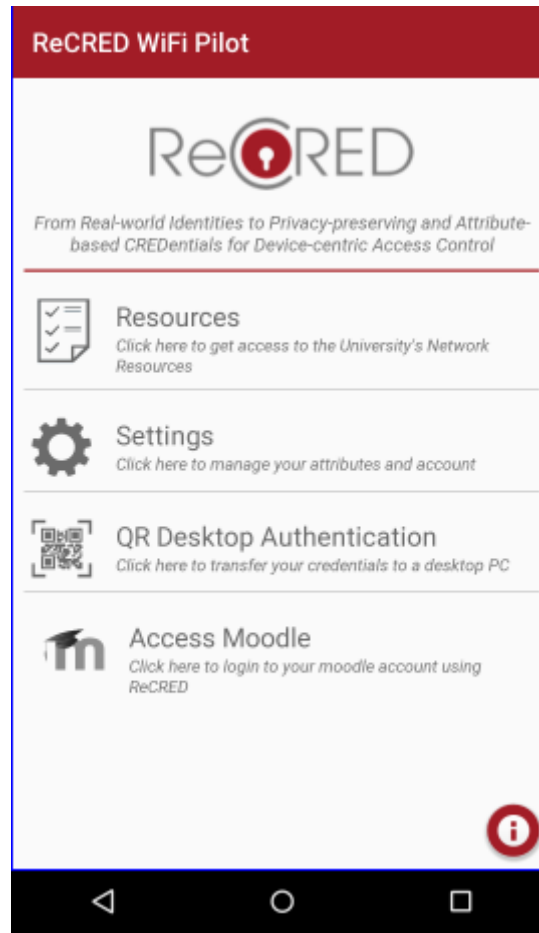


Figure 3: New Home page of the mobile application

2.1.2.2 CertSIGN

The CertSIGN Wi-Fi pilot uses an 802.1X security structure alongside the ReCRED security stack. Thus, there are two Wi-Fi access points configured as NAS which are contacting a RADIUS server in order to authenticate each connected user (or supplicant in the 802.1X terminology).

For this pilot there are two Wi-Fi networks which are open (they do not require a password or any form of authentication) and which are used in the security bootstrap phase of the pilot, where the user obtains the authorization data, necessary for the connection to a second Wi-Fi network which provides Internet access.

In the security bootstrap phase of the Wi-Fi pilot, the user is authenticated via an internal client management tool which identifies the user as being a company client. This internal client management tool pushes the client information to a Wi-Fi pilot Service Provider and the user receives an SMS with a unique code, used in authenticating to the aforementioned Service Provider.

After the user is authenticated to the Service Provider, it is given an identity in the ReCRED system and uses the ReCRED security mechanisms in order to authenticate (e.g. FIDO). If the user is successfully authenticated to the system by using the ReCRED security mechanisms, it is issued a unique token (random). This token is used as a temporary password for authenticating to the protected Wi-Fi network via 802.1X, being delivered to both the client and the 802.1X authentication server.

The Wi-Fi router (802.1X NAS) communicates with an authentication server via the RADIUS protocol. In order for this connection to be secured, a pre-shared key is used on both the NAS and the authentication server. Regarding the authentication server software, the Wi-Fi pilot employs a FreeRADIUS server with a MySQL database back-end for storing the temporary user credential.

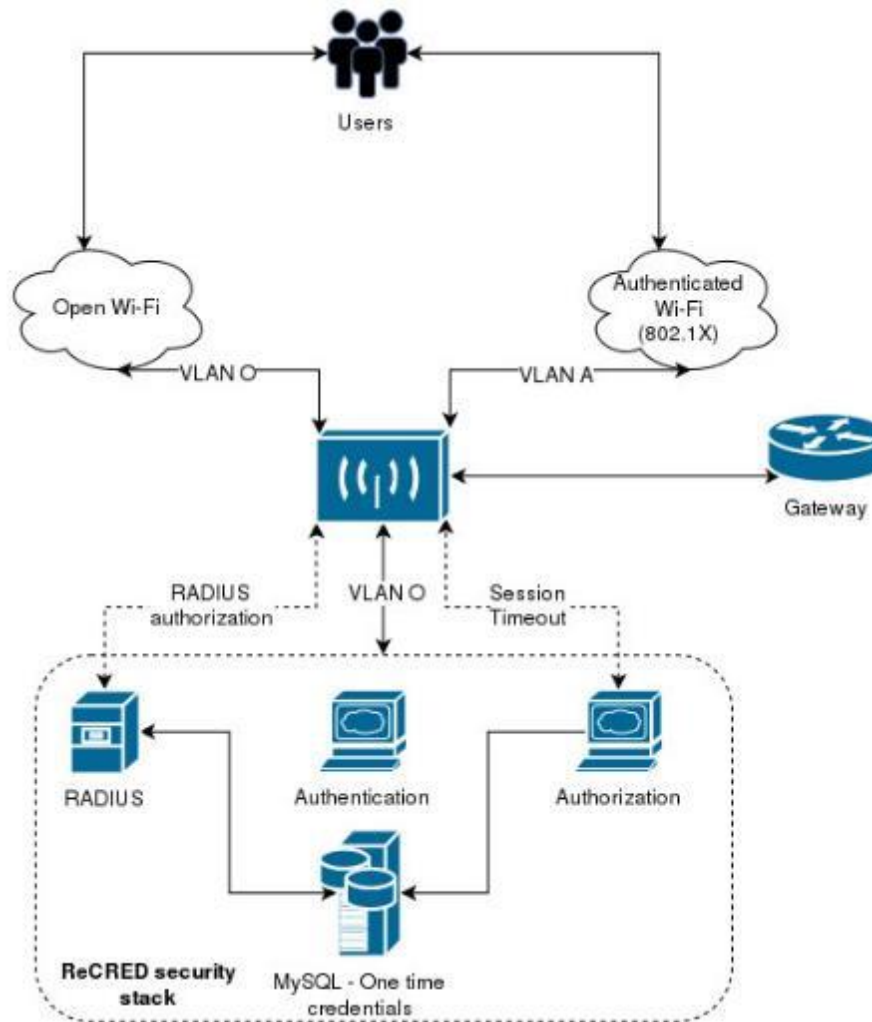


Figure 4: CertSIGN Wi-Fi pilot architecture diagram

The main flow of the 802.1X variant of the Wi-Fi pilot is the following:

1. The user obtains a random token after authenticating with the ReCRED security mechanism.
2. This token is written in a RADIUS authentication server database back-end. This token is temporary, being wiped from the database after 2 hours.
3. The ReCRED security Android application switches automatically the Wi-Fi networks, trying to connect to the protected Wi-Fi network using 802.1X with the provided random token (which plays the 802.1X password role).
4. The EAP packets reach the Wi-Fi access point NAS, which further relays the authentication packets to the RADIUS server (the Wi-Fi pilot uses the 802.1X PEAP method).

5. The RADIUS server queries the back-end database in order to validate the given password (random token).

2.2 Pilot Dissemination

2.2.1 In-house Dissemination

In house Dissemination (CUT): This event took place at the facilities of the Department of Electrical Engineering, Computer Engineering and Informatics building of the Cyprus University of Technology on the 17th of January 2018.

More than 50 people attended this event including staff, students, and faculty members. The ReCRED project was presented by Antonis Papasavva who explained the initial incentive that urged the ReCRED consortium to research and develop innovative ways for device-centric authentication. In addition, he highlighted the problems of identity fragmentation and password overload, along with the ambitions and aims of the project.

During the second part of this event, the attendees had the opportunity to be informed about the Wi-Fi Pilot that is installed and running at CUT premises. The participants learned what this Pilot aims to achieve and how it works. After this presentation, there was increased interest from the audience to take part in the Wi-Fi Pilot. The volunteers tested the ReCRED Wi-Fi Pilot android application and had the chance to authenticate on their device by the use of biometrics in order to get access to the university's Wi-Fi and web services.

Staff, students and faculty were impressed by the power of Wi-Fi pilot transferring the burden of authentication from the users to their smartphones. Attendees noted that this solution seems to be very promising approach to the problem of authentication and password overload.



Figure 5: CUT In-house dissemination

2.2.2 Other Dissemination activities

2.2.2.1 Linopetra Lyceum at CUT premises

On the 28th of February 2018, one class from Linopetra Lyceum visited CUT premises. CUT hosted 2 educators and 24 students. The presentation was consisted of two parts. One part was ReCRED goals, problem and solution, and then, for the second part, the students had the opportunity to test the Wi-Fi Pilot and evaluate it.

During this session, the following questions came up:

1. After my accounts are LATCHED, how can I retrieve them? Answer: ReCRED offers Fail-over Authentication, in case the phone is lost, or stolen and the accounts get LATCHED. In case the phone was not stolen though, then the user can simply verify his identity, by the use of his biometrics (fingerprint, etc.) and get full access to his accounts again.
2. Can two people, have access to a service by the use of a single account? Answer: Each person has an account in ReCRED Identity Consolidator as a unique person and all his online and physical identities are bounded together in one consolidated account. Users can access an SP when an IdP authenticates their identity. Two people shouldn't be bounded under one account since different people have different identities.



Figure 6: Linopetra Lyceum at CUT premises

2.2.2.2 Pilot Dissemination at CUT campus

In order to attract students and faculty to test the Wi-Fi pilot and evaluate it, CUT organized numerous presentations and demonstrations of the pilot during courses sessions from different departments, offices, library, and laboratories. More specifically, the pilot was presented to more than 1000 students, during more than 25 lecture sessions from 4 departments. During these sessions, professors and students had the opportunity to test and evaluate the Wi-Fi Pilot. To spread awareness, posters about the project and the pilot were posted around the whole campus. The posters are shown in Figure 7 below. In addition, leaflets were created and were available at the buildings of the university. Specifically, leaflets were available at the main building of the university, the library, the student's affairs building, accounting department building, deanery, etc. The leaflet is shown at Figure 8.

Τεχνολογικό Πανεπιστήμιο Κύπρου

ΓΝΩΡΙΣΤΕ ΤΟ ReCRED

Κάνει τη ψηφιακή σου ζωή ασφαλή και σίγουρα πιο εύκολη!

Το τμήμα ΗΜΜΥΠ σας δίνει την δυνατότητα να λάβετε μέρος σε ένα πρωτοποριακό πρόγραμμα πρόσβασης στο δίκτυο και τις υπηρεσίες του Πανεπιστημίου μέσω της εφαρμογής android ReCRED.

Η εφαρμογή προσφέρει πρωτοποριακές μεθόδους ασφαλείας ταυτοποίησης για την πρόσβαση σας στο δίκτυο και τις υπηρεσίες του Πανεπιστημίου.

ΔΩΝΕΤΕ ΜΕΡΟΣ ΣΤΗ ΚΛΗΡΩΣΗ!

Το ReCRED σας κερνάει καφέ και σας δίνει τη δυνατότητα να λάβετε μέρος σε κλήρωση για ένα TABLET.

Όροι και συνθήκες: Το πρώτο 100 άτομα το οποίο θα εγγραφεί και εφοκλογείν την εφαρμογή θα λάβουν δωρεάν καφέ από το HUXO café. Στη κλήρωση για το TABLET θα λάβουν μέρος όλοι όσοι εγγραφούν και εφοκλογούν την εφαρμογή.

Ανώνυμη Πρόσβαση
Δυνατότητα διατήρησης της ανωνυμίας σε διάφορες ηλεκτρονικές υπηρεσίες

Βιομετρική Επαλήθευση ταυτότητας
Χρήση δωφόνων βιομετρικών χαρακτηριστικών για επαλήθευση ταυτότητας

Ασφαλής Αποθήκευση
Χρήση διαφόρων καταστημάτων τεχνολογικών για την ασφάλεια των δεδομένων

Ταυτοποίηση με βάση τη κινητή συσκευή
Τοπική ταυτοποίηση πόρων στη κινητή συσκευή

Ενιαία Σύνδεση
Μία και μόνο σύνδεση για πολλές ηλεκτρονικές υπηρεσίες

Κύπρος Τμήματος ΗΜΜΥΠ
(Κτήριο Τσιφλή Κυριάκου),
ωθούσα ΤΕΕ, Σερφίδου 33

Επικοινωνία:
as.papadimitriou@educut.ac.cy,
c.papadimitriou@educut.ac.cy

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Ταμείο Περιφερειακής Ανάπτυξης

ΕΡΕΥΝΑ
ΕΡΕΥΝΑ

Figure 7: Wi-Fi Pilot poster for CUT premises

Κοινοπραξία

- Ερευνητικό Πανεπιστημιακό Ινστιτούτο Σαπιαντί
- Telefonica Investigacion Y Desarrollo SA
- VERIZON Nederland BV
- cutSIGN SA
- WEDIA Limited
- EXUS Software Ltd
- UPCOM BVBA
- DE PRODUCTIZERS BV
- Τεχνολογικό Πανεπιστήμιο Κίπρου
- Universidad Carlos III de Madrid - IMDEA
- Consorzio Nazionale Interuniversitario per le Telecomunicazioni, (Italy)
- Studio Professionale Associato a BAKER & MCKENZIE

Βρείτε μας

Μπορείτε να μας κάνετε like στο facebook:
<https://www.facebook.com/ReCREDH2020/>

Μπορείτε να μας ακολουθήσετε στο Twitter:
[@ReCRED_H2020](https://twitter.com/ReCRED_H2020)

Μπορείτε να μας ακολουθήσετε στο LinkedIn:
<https://www.linkedin.com/groups/8470632>

Επισκεφθείτε τη σελίδα μας:
www.recred.eu

From Research Institute to University, we are always open to you for device-centric access control

Makes your digital life safe and definitely easy!

- Βιομετρική Επαλήθευση Ταυτότητας
- Ταυτοποίηση με Βάση τη κινητή συσκευή
- Ασφαλές Αποθήκευση
- Ανώνυμη Πρόσβαση
- Ενεία Σύνδεση

Σκοπός του Έργου

Το ReCRED είναι ένα ερευνητικό πρόγραμμα το οποίο χρηματοδοτείται πλήρως από την Ευρωπαϊκή Ένωση. Ο βασικός σκοπός του ReCRED είναι να ενοποιήσει κάτω από τις προσωπικές συσκευές των χρηστών τους μηχανισμούς ταυτοποίησης και εξουσιοδότησης για ηλεκτρονικές υπηρεσίες.

Το ReCRED μεταφέρει το βάρος της ταυτοποίησης από τον χρήστη στην ίδια του τη προσωπική συσκευή, αξιοποιώντας όλα τα πλεονεκτήματα των δυνατοτήτων των κινητών συσκευών. Οι χρήστες έχουν τη δυνατότητα να ταυτοποιηθούν από τη κινητή τους συσκευή, τοπικά, χρησιμοποιώντας βιομετρικά χαρακτηριστικά και χαρακτηριστικά συμπεριφοράς όπως δακτυλικό αποτύπωμα, αναγνώριση προσώπου, βηματισμός, δακτυλογράφηση κτλ.

Παράλληλα η συσκευή σε συνεργασία με τη πλατφόρμα ReCRED παρέχει πρόσβαση σε συνδρομητικές υπηρεσίες (π.χ. λογαριασμούς e-banking, λογαριασμούς κοινωνικών μέσων, κτλ).

Επίσης, το ReCRED προσφέρει δύο επιπλέον καινοτομίες:

- Την ενοποίηση και τη διαχείριση των ηλεκτρονικών ταυτοτήτων και λογαριασμών των χρηστών.
- Την έκδοση ανώνυμων διαπιστευτηρίων (credentials) που επαληθεύουν συγκεκριμένα χαρακτηριστικά ή ιδιότητες των χρηστών.

Τεχνολογίες

- FIDO UAF
- OpenID Connect
- Trusted Execution Environment
- U-Prove
- Idemix

Το ReCRED στο Πανεπιστήμιο μας

Το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών και Πληροφορικής, σε συνεργασία με την Υπηρεσία Συστημάτων Πληροφορικής και Τεχνολογίας έχουν εγκαταστήσει στο δίκτυο του Πανεπιστημίου, συστήματα τα οποία επιτρέπουν σε φοιτητές και Ακαδημαϊκό προσωπικό την πρόσβαση στο δίκτυο και τις υπηρεσίες του Πανεπιστημίου. Αυτό είναι ειδικό χρησιμοποιώντας την πρωτοποριακή, εύχρηστη και ασφαλή μέθοδο ταυτοποίησης ReCRED.

Η μέθοδος αυτή είναι διαθέσιμη σε διάφορα κτήρια του Πανεπιστημίου και χρησιμοποιείται για σύνδεση στο ασύρματο δίκτυο με το όνομα "ReCRED".

Για να είναι δυνατή η σύνδεσή σας στο δίκτυο ReCRED πρέπει πρώτα να συμπληρώσετε τη φόρμα που θα βρείτε εδώ (<https://goo.gl/forms/5DBNw9FhnnQmvp911>) ή σαρώστε το QR:

Βρείτε μας στα γραφεία Ερευνητικών Συνεργατών τα οποία βρίσκονται στο ισόγειο του κτηρίου του Τμήματος ΗΜΜΗΥΠ (κτήριο Τροφή), ή στο email: gs.papadavva@edu.cut.ac.cy

Πλεονεκτήματα του ReCRED

Το ReCRED αποσκοπεί να παρέχει τα παρακάτω πλεονεκτήματα:

- Ταυτοποίηση με βάση τη κινητή συσκευή (Device-centric authentication)**, με τη χρήση είτε βιομετρικών χαρακτηριστικών ή χαρακτηριστικών συμπεριφοράς τα οποία υπερνικούν το πρόβλημα αυξημένου αριθμού διάφορων κωδικών πρόσβασης.
- Ενοποίηση λογαριασμών** για να λυθεί το πρόβλημα διασκορπισμένων χαρακτηριστικών ταυτότητας.
- Ανώνυμη πρόσβαση** για την αντιμετώπιση ζητημάτων ιδιωτικής ζωής.

Figure 8: Wi-Fi Pilot Leaflet

2.2.3 Webinars

The Wi-Fi and Web Services Access Control Pilot took place on the 15th March 2018, at CUT's premises over the GoToMeeting web conferencing software. Link to video: <https://drive.google.com/drive/folders/1WHa5yNgQlgOLzUM2CON6KgnLPtZSMckA>

2.3 Privacy and Security Considerations

2.3.1 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.

2.3.2 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.

2.3.3 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).

2.3.4 Monitoring

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

2.3.5 Malware Protection

There is no malware protection currently in place.

2.3.6 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

2.3.7 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.

2.3.8 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.

2.3.9 Protection of Logs and Data

Periodic data backup is scheduled using a cron job.

2.3.10 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.

3 Student Authentication & Offers

3.1 Deployment of the Pilot

The deployment of the Student pilot consists of two main parts. On the one hand the website the pilot website that is deployed on a Verizon server. On the other, the student mobile application that is developed by UPCOM.

The Pilot Website(PW) uses the ID consolidator(IDC) as an identity provider. This can be achieved either with OpenID Connect (OIDC) or FIDO. Once registered the PW acts as a relying party (RP) and gathers the profile of the user from the IDC. This is shown in **Error! Reference source not found.9**.

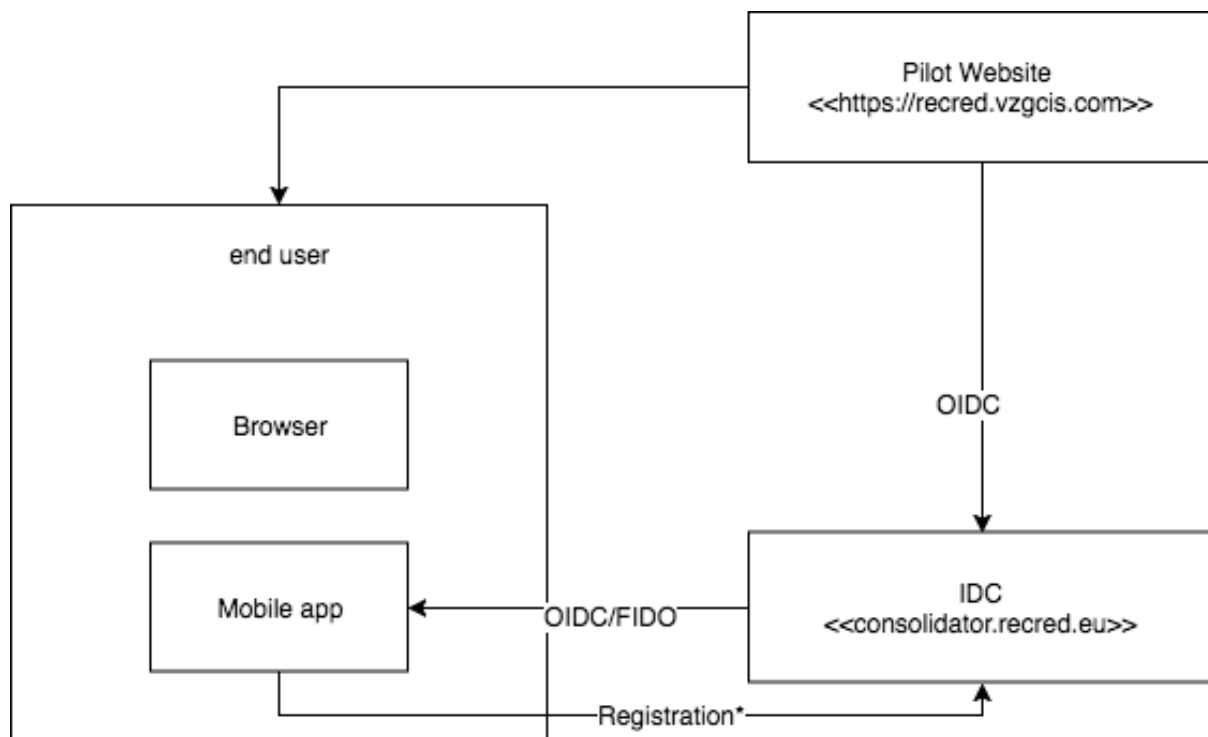


Figure 9: Pilot deployment architecture

The PW uses Drupal as the underlying CMS system. Once the user has authenticated and authorized PW to use his or her profile information a user is created in the PW Drupal system. The user gets a default “student” role. This role is allowed to make purchases. Student roles can also be upgraded to the “merchant” role, which allows them to sell items on the market place.

For the purpose of selling and buying items, student can use the mobile application made by UPCOM. In order to use the website, it is necessary to log into the website first, so that the user is created with

in Drupal. Once this has been done, the user can use the mobile app to login and start engaging in the market. This flow can be seen in **Error! Reference source not found.10**.

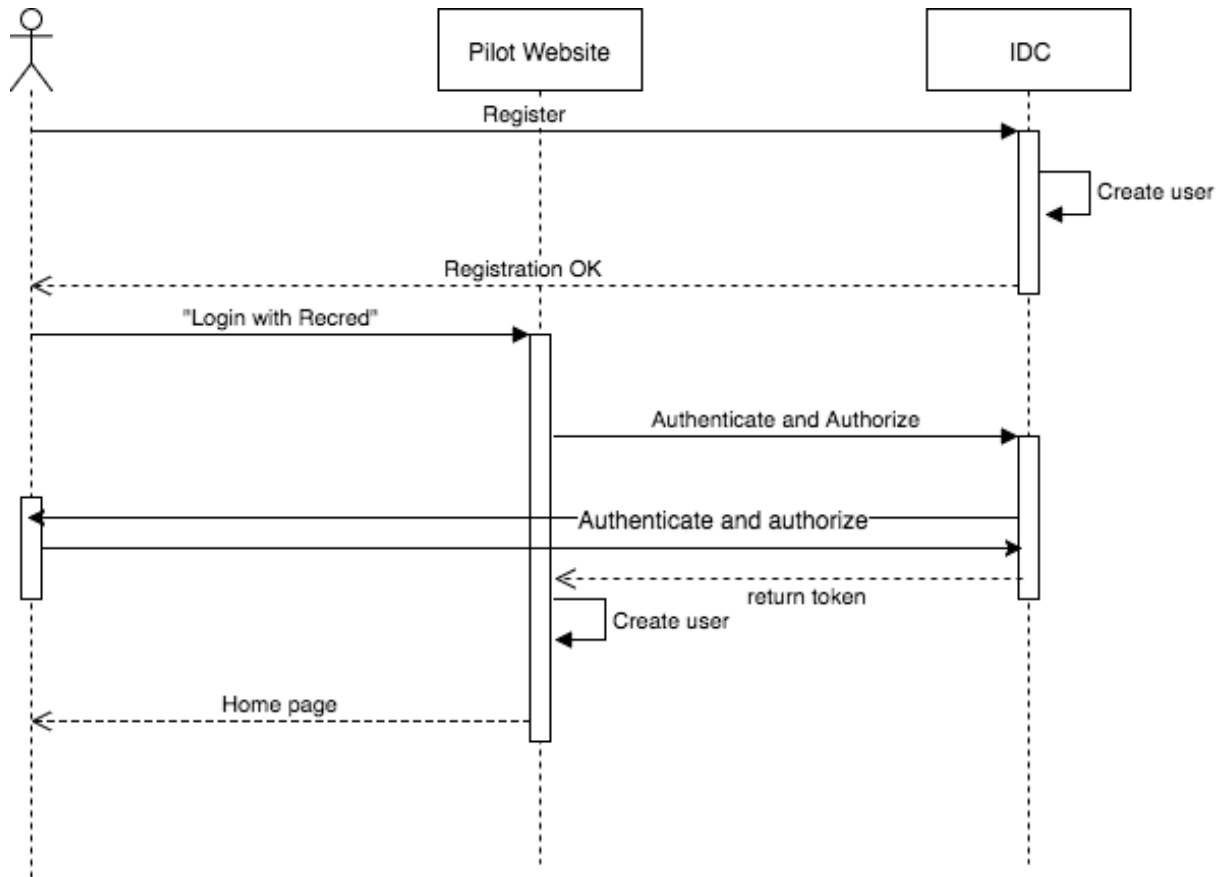


Figure 10: Student pilot flow

3.1.1 User Workflow

In this part of the workflow the user uses the ReCRED app to register to the Student Offers application – the Campaign Manager. The Campaign Manager acts as the service provider for the user and requests additional attributes from the student in order to provide the services, in this case discounts, to the user. These attributes include student status, date of birth etc. In this section the user flow as used for the student pilot and communicated to the student user group is listed below:

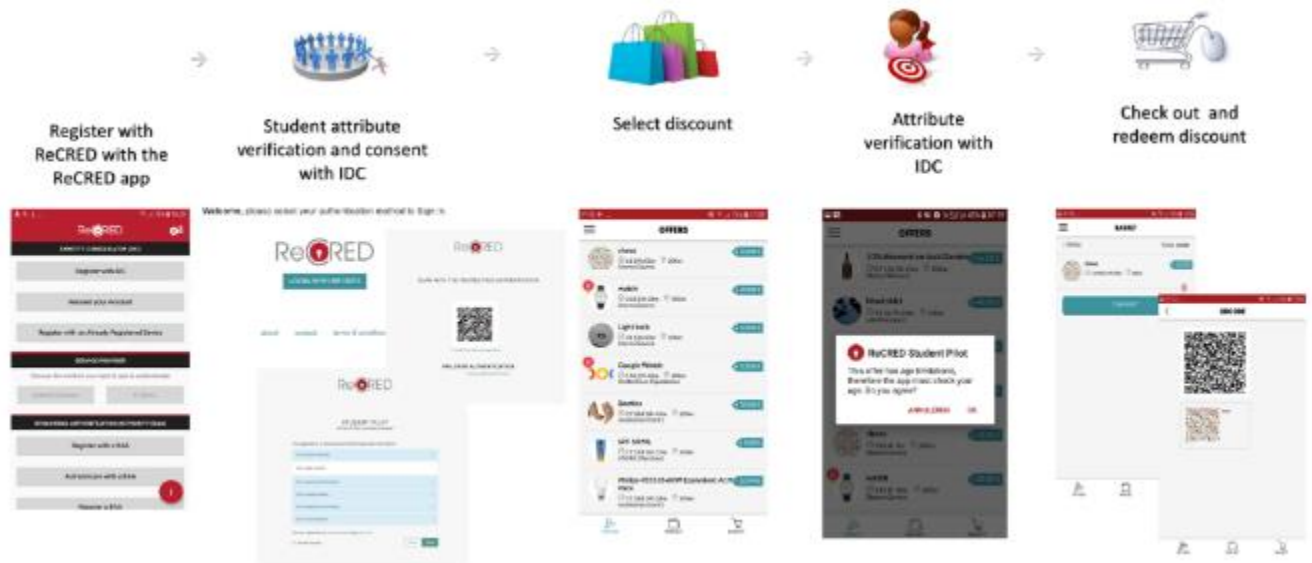


Figure 11: Student authentication pilot flow

1. Registration process

- Install (only!) ReCRED app from play store
- Open ReCRED App and Register an account with the IDC
- You get a mail, click on the link and open with ReCRED app
- Fill in the questions and a strong (20 char) password
- Go to <https://recrred.vzgcis.com/> and click "Login with ReCRED" and you will be presented with a QR code. (campaign manager)
- Open ReCRED App and click on the "Authenticate Desktop (QR Scan)" button to scan the QR code and authenticate.
- Follow the flow on your desktop to login to the campaign manager website.
- Registration process is now complete.

2. Student app (web shop application)

- Install ReCRED student app from the play store
- Open the Student Discount application and follow the flow
- Order an item and go to the merchant (different phone)

3. Merchant app (for in the virtual store)

- This app is already installed on a different phone.
- Scan the barcode of a student to register the sell.

3.1.2 Changes to the Pilot Partner

At the start of the project, Verizon (VZ) invited The Productizers (PROD) to participate in the ReCRED project in order to facilitate the Student Offers Pilot with the International Student Identity Card (ISIC). The reasoning was that The Productizers have a long history with ISIC to produce new services and products additionally, have extensive experience with the introduction of new service and products at other clients in retail, pharmaceutical, and business services industries. The context of ISIC is that it is a multinational foundation constituted of several organizations and a central support/management office. Each country is managed by a different partner in the ISIC organization and has diverse needs, business & IT maturity, and strategy – considering this, PROD was well positioned to manage this complexity for the pilot and introduce ReCRED to the individual students, introduce the concept of a student – merchant exchange and manage the definition, execution and analysis of the pilot. Success of the pilot is however also strongly dependent on receiving a fully functional platform and application as developed by the rest of the partners in the consortium.

After 2+ years, time has also not stood still for ISIC. This has regrettably resulted in the situation that ISIC has informed us (PROD) that ReCRED is no longer aligned with their short & long-term IT goals and have discontinued their participation in the pilot.

Initially, PROD had direct contact with individual ISIC country organizations and had started several initial phases for the student pilot while awaiting the maturation of the ReCRED platform and accompanying apps for use in the pilot. There was a high degree of enthusiasm and feedback for the final product and pilot – in short, our partners at ISIC were engaged and committed. The organizational, operational and managerial structure has however changed at ISIC during the past ±2 years. There is less to no autonomy for individual countries, investment budgets and decisions are now centralized, several local initiatives have been discontinued, and in spring 2017 the decision to centralize IT development and operations has been taken. The enthusiasm and commitment has not carried over from the individual countries to the global organization and despite interest in the ReCRED platform in general, ISIC will no longer participate as the pilot partner. A key factor contributing to the discontinuation of ISIC’s participation is that the platform and applications are not mature enough for commercial use and easy integration with an existing IT environment.

We have proceeded with the Student Offers Pilot with the Haagse Hogeschool - The Hague College (HHS) as the replacement for ISIC as the pilot partner. The justification for HHS is as follows:

- There is no need for changes in the original use cases. The use cases can still be applied and tested in a real-life environment with students and service providers using the existing platform, apps and websites.
- HHS provides easy access to a student population
- Additionally, achieve an extension of the pilot to not only have a student population use the applications but also receive significant feedback by aligning participation with curriculum – including multimedia design, commerce and user experience design.
- Later phases will include real life interaction with smaller local retailers i.e. Heren van Alphen

3.2 Pilot Dissemination

3.2.1 Demonstration to Commercial Partners

PROD introduced the ReCRED platform to several other organizations in retail and pharmaceuticals to evaluate and report on the interest and viability of the platform in a real business environment. In particular Brocacef, Brantano, and Beate Ushe showed initial interest in further collaboration.

- Brocacef, part of the Phoenix group, evaluated the concept/code/etc. for use in their mobile solution and we have received an extensive evaluation report and positive feedback on the possible usage / integration however, engaging Brocacef as a pilot partner would require significant changes in the use cases for ReCRED cause a conflict with the ReCRED project schedule which is not aligned with the development schedule of the Brocacef mobile app
- Brantano and Beate Uhse, large retailers in shoes and erotic goods, provided positive feedback and interest in the solution but require significant changes in the ReCRED use cases for the pilot, have internal challenges for the participation in the pilot at this time, and are looking more for a finished product versus an intermediate solution.

3.2.2 In-house Technical Analysis of ReCRED at Brocacef

Our commercial partner Brocacef performed an extended technical analysis of the ReCRED platform with regards to its feasibility as an underlying solution for their upcoming mobile solution amongst other services. For this analysis, PROD worked closely with the engineers from Brocacef for more than a month to elaborate on any technical or functional questions. The conclusion of the analysis was that even though ReCRED provides an innovative and interesting new platform, there are certain specific limitation which conflict with the needs of Brocacef and their business. Some key highlights from the report are listed below:

- **P-ABAC:** *“Uprove is the second external standard adopted here, it is similar to PKI-certificates. And it acts like a digital identification card where you can only disclose the attributes you want to. However, the Dutch government has so called “PKI-Overheids Certificaten” and they are mandatory to use when providing access to medical data.”*
- **Identity Consolidator:** *“When the current app project has furthered a bit more this might become a useful tool for updating someone’s personal information gotten from the app, or it could link information gotten via DigiD, but further design.”*
- **Behavioral Authentication Authority:** *“Extremely interesting, the problem is that legislation regarding the method is non-existent, and it would therefore be a risk to identify users based on their movement patterns, I would love to implement this, especially as it closely ties with my education in technical computer science. But the potential reputational damage for Brocacef, should they implement this, and medical data be exposed is too high of a risk in my perspective. In short: Perfect for Wi-Fi access, a no-go for sensitive information.”*
- **User device:** *“The lack of IOS versions is also problematic, as successful integration into any business will require full client coverage.”*

The final conclusion of the analyst was as follows: *“Having spent the past month or so researching the ReCred project I’m impressed by the level of international cooperation that happened, and it is surely an example what the European union can facilitate for the scientific world. I’d love to work on it, but it is simply not a project that fills the needs of Brocacef.”*

3.3 Privacy and 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.

4 Age Verification Online Gateway

4.1 Deployment of the Pilot

During the last year of the project, and after its initial deployment, there were some major changes to the age verification pilot. The flow has been altered, according to the results of the UX assessment, the solution has been rebranded and the mobile app has been redesigned for improved usability.

4.1.1 Changes and Improvements

4.1.1.1 Rebranding / Redesign

The age verification solution has been rebranded and it is now called AGify, instead of Age Gate. This is because the ‘age gate’ term is often used to describe simple controls that allow the visitors of websites to arbitrarily input their Date of Birth. A new AGify logo has also been designed.



Figure 12: AGify logo

The design of the AGify mobile app has also been redesigned accordingly. Following are some indicative screenshots of the new app.



Figure 13: Indicative AGify screens

4.1.1.2 Changes to flows

The ‘end-user registration’ and the ‘age verification’ flows have been changed since the initial deployment of the age verification pilot.

More specifically, the user had to authenticate to some Identity Provider to prove his age, each time he requested access to an age-restricted website. During an early assessment of the pilot’s usability, it was understood that this approach was not optimal in terms of UX. In addition, it created unnecessary traffic between the AGify server and the Identity Providers that know the users’ Date of Birth (DoB).

For these reasons, we implemented a new approach which allows the end-users to only prove their age once, during user registration. After the user consents to transfer his DoB from an Identity Provider, it is stored in the AGify server, and it is evaluated each time the user wants to access a website, without having to retrieve it repeatedly.

Therefore, the flows for registration and age verification have been modified as follows:

End-user registration

1. The user launches the AGify mobile app and registers to AGify by filling in some basic information.
2. The user enrolls her fingerprint and a new FIDO key is created and stored in the AGify FIDO server.
3. The user authenticates to the ReCRED Identity Consolidator (assuming he already has a ReCRED account). For this, the main ReCRED app is required.
4. The user consents to transfer his DoB from ReCRED to AGify (which is stored in the AGify OpenAM).

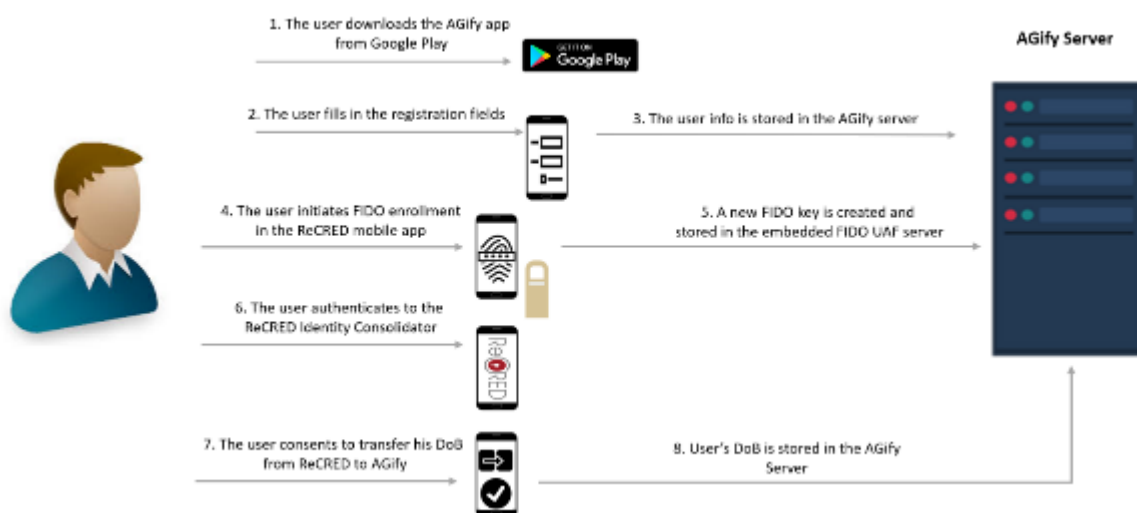


Figure 14: End-user registration to AGify

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 AGify 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 AGify 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 AGify mobile app launches the ReCRED app to initiate FIDO UAF authentication with the FIDO UAF server sitting on the AGify backend, and the user is prompted to provide his fingerprint to the FIDO UAF Client.
5. Upon successful authentication, the AGify 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.

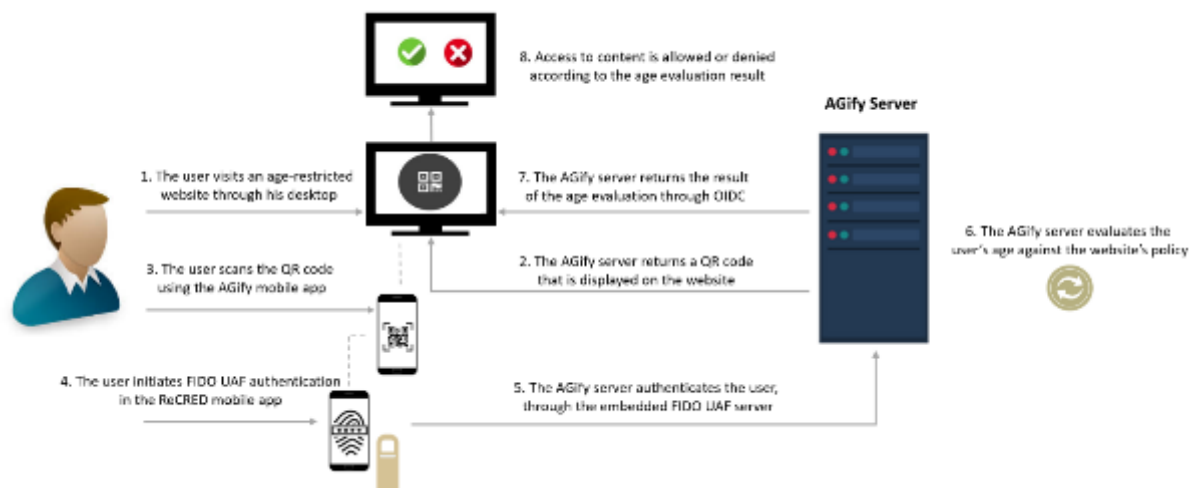


Figure 15: Age Verification through OpenID Connect

AGify has a dual role, acting both as an Identity Provider towards the websites that need to verify the age of their users, and as a Service Provider against the ReCRED IDC (which acts as the Identity Provider in that case). More specifically, an end-user can register to the ReCRED IDC, and then she can use the NFC functionality of the Physical Acquisition module, in order to retrieve her identity attributes from her RFID passport. She can then consent to reveal / transfer her DoB from ReCRED to AGify.

4.2 Pilot Dissemination

During the last year of the project, we organized multiple activities for the dissemination of the age verification pilot. These include in-house dissemination, participation in events, a new dedicated website and social media pages, along with webinars for the demonstration of the AGify solution.

4.2.1 In-house Dissemination

Upcom demonstrated the AGify solution during an event it organized within the Customer Service Week. The event took place at the Athens Impact HUB, on Oct 5, 2017, and among the attendants

were Upcom’s employees, partners and customers. Exus and Wedia, which are also among the ReCRED partners, also participated in the event.

During the event, we explained the problem that AGify attempts to solve, how it works, and what are the different alternative flows. It was explained that AGify is based on a pilot of the ReCRED project, and the main objectives of ReCRED were also presented during the event.

After the presentation, there was increased interest from the audience, who asked questions and concluded that AGify seems like a very promising approach to the problem of online age verification.



Figure 16: AGify at Athens Impact HUB

4.2.2 Participation in Events

Upcom and CUT participated in the Mobile World Congress (MWC), which took place in Barcelona from 26/2 to 1/3. MWC is one of the biggest events worldwide, in technology and telecommunications, and the purpose of our participation was the dissemination of the AGify solution. At the same time, AGify had a dedicated booth in 4YFN, which is the startup and innovation platform of MWC.

During the two events, we were able to demonstrate AGify live to the visitors who were interested in our solution and answer their questions. More specifically:

- We talked with Service Providers, who start to realize the importance of age verification and that they will soon be legally obliged to somehow verify the age of their customers.
- We had meetings with potential Identity Providers and we set the basis for future collaborations.
- We met and exchanged opinions with organizations and end-users that are concerned about the safety of minors on the Internet and online privacy in general.
- We discussed with other application developers who would be interested in integrating our solutions with their apps.

On the last day of the event, we also had a very fruitful meeting with the FIDO Alliance, who were also exhibitors in MWC. FIDO is one of the core technologies used in ReCRED, so it was a great opportunity to demonstrate our FIDO-based solutions to them, and also to present them the FIDO / OIDC extension, which has been one of the main outcomes of the project.



Figure 17: AGify booth in MWC



Figure 18: AGify booth in 4YFN

In addition, the AGify solution was presented and demonstrated during the two workshops which were organized by ReCRED, on January 31st and on April 20th, 2018.

4.2.3 Online Demos / Webinars

After the deployment of the first stable version of AGify, we created a list of potential interested Service Providers, such as alcohol retailers, tobacco retailers, online gambling services, etc. An email was sent to all these companies, describing the AGify approach to the problem of age verification and its advantages over other solutions. All these contacts were also offered the option to request a live demonstration session.

As the result of this communication, we managed to attract the attention of a few Service Providers, with whom we organized online sessions. During these sessions, we demonstrated AGify live to them, answered their questions and received their feedback.

| Date | Industry | Country |
|------------|---------------------------|---------|
| 27/10/2017 | Alcohol | UK |
| 09/11/2017 | Whine & champagne | Germany |
| 21/11/2017 | Alcohol | UK |
| 23/11/2017 | Beer | Ireland |
| 27/11/2017 | Alcohol | Ireland |
| 05/12/2017 | Alcohol brand development | UK |

More than that, a webinar was organized by Upcom towards the end of the project (13 April 2018), during which the AGify solution was demonstrated step-by-step and questions were answered.

4.3 Privacy and Security Considerations

4.3.1 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.

4.3.2 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.

4.3.3 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.

4.3.4 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 are 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.

4.3.5 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.

4.3.6 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

4.3.7 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 was 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.

4.3.8 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.

4.3.9 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.

4.3.10 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.

5 Microloan Origination

5.1 Deployment of the Pilot

Since the latest description of the Microloan Origination in D7.3 there have been several changes in the design of the Microloan website alongside with changes regarding its deployment and the software components it is comprised of. The flows and functionalities supported by the Microloan Origination remain mostly the same however in the following sections deviations from the initial implementation are going to be pinpointed.

5.1.1 Changes and Improvements

5.1.1.1 Changes in the mobile application

One of the most important changes so far is that the Microloan Origination will rely regarding its mobile part on the unified ReCRED application for mostly all of the functionalities regarding the human to device and device to service access. Therefore, the Microloan Origination will enable ReCRED users in general, e.g. users of the other pilot use cases, to access it seamlessly.

Thus, the user can register to ReCRED and access the Microloan Origination web using the ReCRED app. After registering to the ReCRED consolidator the user will be able to use e.g. the option authenticate desktop (QR Scanner) to initiate the FIDO-OpenAM process. For P-ABAC etc. the user can use the respective ReCRED app buttons.

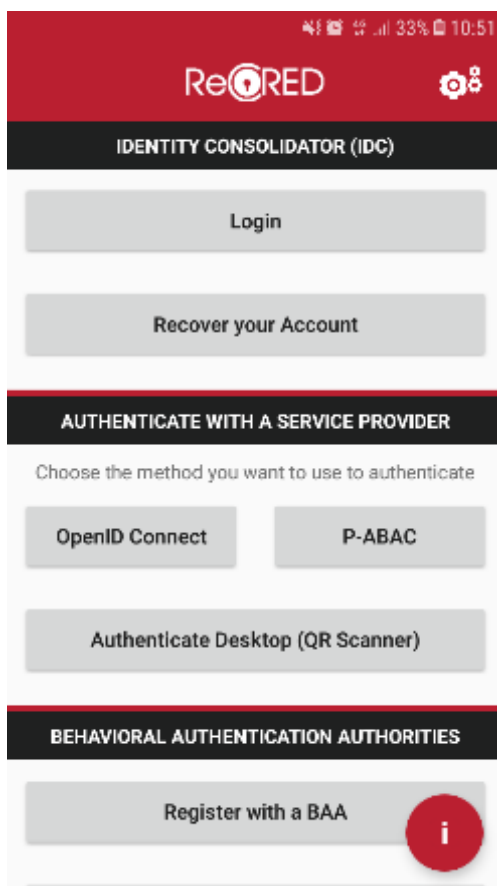


Figure 19 : ReCRED app-microloan

5.1.1.2 Changes in the web application

The Microloan website is offering the core functionality needed by this pilot namely to grant or deny loans. Below the main flow of the process is going to be presented through screenshots.

The initial screen with all the available microloans is depicted in Figure 20. The user can navigate through the menu bar at the top of the webpage and find valuable information for the functionalities offered in the ReCRED app. Information regarding the ReCRED project are also integrated into the menu together with a small description of EXUS Innovation department that leads this initiative.

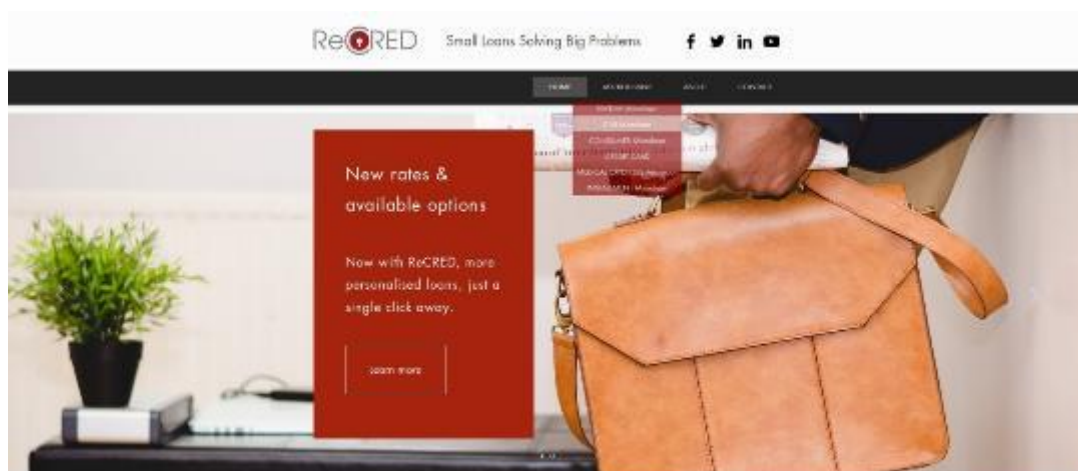


Figure 20 : Microloan landing webpage

The choice of a specific microloan plan can be found once the user scrolls down as shown in Figure 21. There is an indicative list of microloans offered such as payday, car, medical expenses and consumer microloan and credit card issuing. The user can choose the preferred microloan by simply clicking on the preferred microloan.

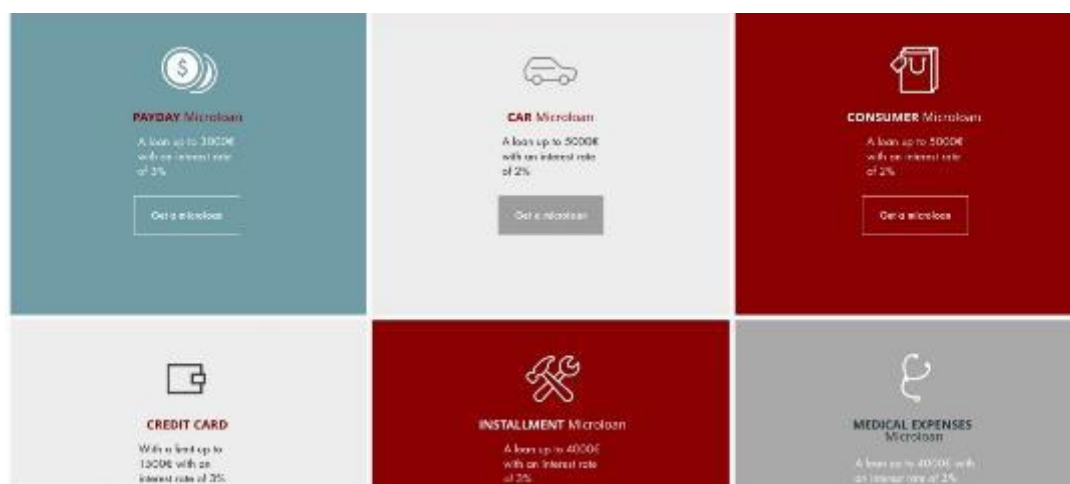


Figure 21: Microloan Options

After choosing the preferred microloan, the user is redirected to the internal microloan service. Initially he/she logs in with the platforms specific credentials and then makes a choice from a drop-down menu explaining the reason that he/she requests a microloan as shown in Figure 22. The specific step in the whole process of requesting a microloan is made in order to keep the social aspect of microloans. In that sense, a microloan can be requested by a person in need to continue working in a daily basis.

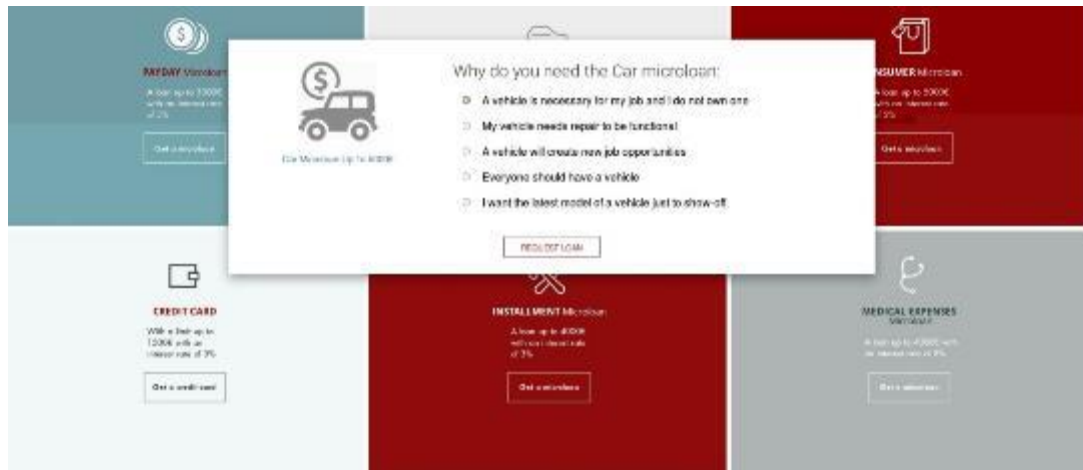


Figure 22: Microloan social purpose check

Once the user has answered, the system checks whether the user is great need of the microloan or not. From the tentative answers shown in Figure 22, one can easily understand that if the user makes a choice of any of the first three answers then the system will allow him to proceed in the next step. The next step reveals the microloan characteristics which are shown to the user for confirmation purposes. In order to proceed with the microloan, he simply clicks on the button “Next.” At the moment the basic information for the microloan are limited to the interest rate, the total amount of money requested and the currency.

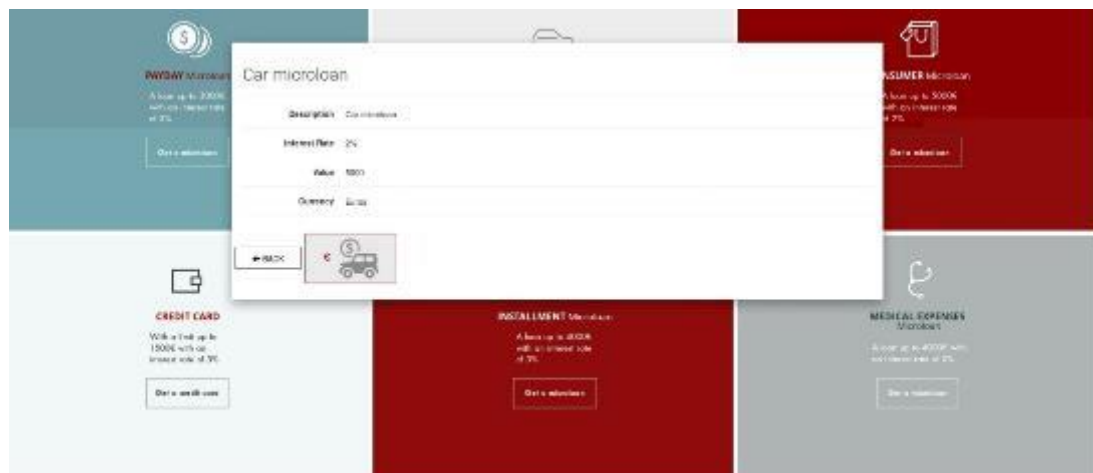


Figure 23: Microloan request

The user is prompted to authenticate with ReCRED by scanning the QR code as it can be readily seen in Figure 24 or use his backup password. The FIDO-OpenAM procedures are initiated leading to the next screen where the user gives his consent for having his personal and financial information transferred to the bank/financial institute. This information is accessible through the ReCRED IDC to the service provider which evaluates it with the ease of asking the Access control and policy reasoning tool.



Figure 24: Microloan authentication via ReCRED app

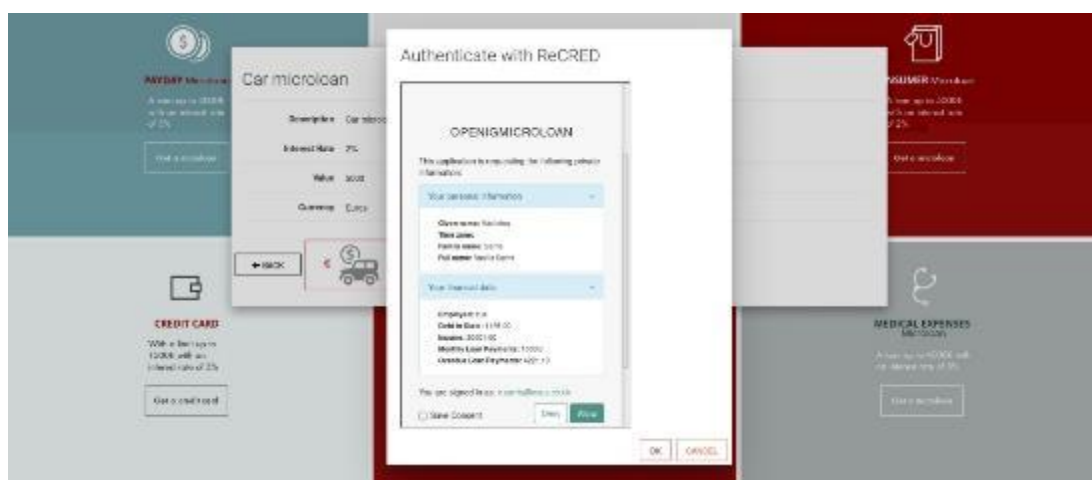


Figure 25: Microloan consent approval

After having successfully been authenticated by the service provider (bank or financial institute) the system checks the data sent and according to a policy tool implemented within ReCRED, decides whether the requested microloan should be granted or not. If the user is granted with the microloan an email is sent to him confirming that the specific amount of money has been transferred to his personal bank account. A similar procedure is followed if the user's microloan request has been rejected but this time the email contains a suggestion for another attempt for requesting a microloan.



Figure 26: Microloan request granted



Figure 27: Microloan grant confirmation email

As a final step, once the user has granted the requested microloan, he/she is redirected to the evaluation questionnaire in order to assess the pilot experience.



Figure 28: Microloan origination user evaluation

Conclusively the flow followed is:

- The user visits the microloan page where he can explore available loans.
- The user is redirected to the internal microloan service. Initially logs in with the platforms specific credentials and then answers a questionnaire explaining the rationale behind his application.
- The user is shown the characteristics of the loan for confirmation.
- The user is prompted to authenticate through the ReCRED IDC.
- The user is authenticated with BAA OpenAM.

- The user opens his mobile ReCRED app and chooses QR scanning.
- The user succeeds in logging in and then he gives his consent for providing his financial information and personal information.
- The evaluation of the user financial profile, loan characteristics is taking place in the policy tool and the user is granted or not the loan.
- An email is sent to the user with all the appropriate information regarding the application.
- The user is able to answer a questionnaire and assess the pilot experience.

5.1.2 Updated Architecture

No major updates on the architecture have occurred with the only notable exception of the OpenIG proxy addition in the microloan software components for securing the access to loans as shown in the Figure below.

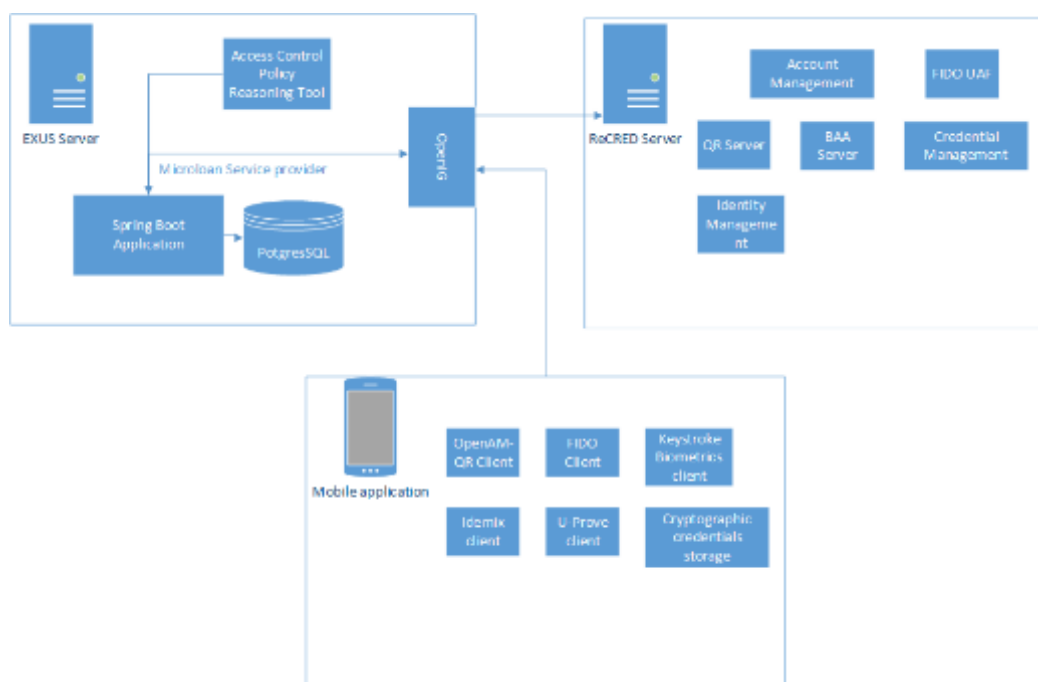


Figure 29: Updated architecture

5.2 Pilot Dissemination

During the ReCRED project lifespan, several dissemination activities have been performed in order to promote the Microloan Origination pilot and its functionalities.

5.2.1 In-house Dissemination

The microloan origination platform has been presented to all EXUS' employees. Since the majority of them are working on the prestigious EXUS Financial Suite (EFS) regarding debt collection, their feedback was invaluable. All major updates on the platform were discussed among the consortium partners leading to an enhanced version that best suits the needs of a user requesting a microloan.

5.2.2 Social Media

As with all the other ReCRED pilots and in close cooperation with the WP8, the microloan origination pilot has been promoted through our social media earning active engagement and impressions from several other EU funded projects. It is worth noticing that during the H2020PCW event, the microloan origination pilot was demonstrated to a UNHCR representative who was extremely interested since they are facing the great challenge of issuing microloan to refugees.



5.2.3 Webinars

The microloan origination pilot was showcased at a webinar where more than 25 people outside the consortium, participated. The comments received were really encouraging and promising for us. The webinar has been recorded, processed (addition of subtitles) and uploaded on our ReCRED YouTube channel so as to be visible and reachable from anyone interested in the implemented technologies and the demonstrated functionalities.

5.3 Privacy and 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.

6 Pilots UX Assessment

The goal of ReCRED is to develop a user-friendly solution so to foster its adoption by the users. To this end, the focus of the Task 7.4 is on usability, since it helps to ensure that the system is easy to learn, effective to use and satisfying from the user’s perspective.

Usability is defined as «the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use» (ISO 13407:1999).

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» (Rubin& Chisnell, 2008, p.4).

The objective of the assessment is to collect data from the end-users, in order to evaluate the degree to which ReCRED meets specific usability criteria.

The end-user assessment is driven by the following questions:

- Does the user understand the different steps needed to accomplish the task?
- Does the user easily identify the features and commands?
- How does the user interpret the meanings of icons and labels?
- Does the user easily learn how to use the system?
- Which are the problems the user meets trying to accomplish the tasks?
- Which are the critical steps when the user needs instructions to proceed?
- How does the user evaluate the usefulness of ReCRED according to his/her needs and expectations?

In addition to the end-user assessment, the Task includes the collection of service providers’ feedback in order to evaluate the impact of ReCRED on the current authentication and authorization mechanisms from business perspective. To this end, a form has been created with a set of open-ended questions, that was filled by some representatives of the target organizations.

6.1 Methods

An iterative assessment process is carried out, in order to progress towards further improvements until the final versions of the Pilot applications.

First of all, the Pilot applications are analyzed by usability experts in order to evaluate the compliance with usability heuristics and identify issues to fix.

Then, the improved versions of the applications are disseminated among the users who are asked to complete an online questionnaire providing their evaluation.

Meanwhile test sessions are performed with a sample of end-users through the think aloud method, so to observe their interaction and collect qualitative data.

- **Expert evaluation**

Two experts (one member of the ReCRED consortium, and one independent expert) analyzed in detail the interface and the navigation flow, according to the following heuristics¹.

| Heuristic | Description |
|--|--|
| Visibility of the system status | The system should always keep users informed about what is going on, through appropriate feedback within reasonable time. |
| Match between the system and the real world | The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making information appear in a natural and logical order. |
| User control and freedom | Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. |
| Consistency and standards | Users should not have to wonder whether different words, situations, or actions mean the same thing. |
| Recognition rather than recall | Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate. |
| Flexibility and efficiency of use | Accelerators may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions. |
| Aesthetic and minimalist design | Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility. |
| Error prevention | Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action. |
| Help users recognize, diagnose, and recover from errors | Error messages should be expressed in plain language, precisely indicate the problem, and constructively suggest a solution. |
| Help and documentation | Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, |

¹ <https://www.nngroup.com/articles/ten-usability-heuristics/>

| | |
|--|--|
| | focused on the user's task, list concrete steps to be carried out, and not be too large. |
|--|--|

- **Questionnaire**

The questionnaire is used as method to collect users' evaluation and assess the degree to which the ReCRED solution meets specific usability criteria, according to users' point of view.

The questionnaire was created using Google Form. For each pilot application, it includes 15 general items and 2 pilot-specific items, with a 5-points Likert scale (see Appendix).

The items are created based on the main usability heuristics, and they aim for evaluating the following aspects:

- Efficiency and effectiveness
- Easiness and learnability
- Feedback and visibility of the system status
- Control and error prevention
- Organization of the information and language
- Aesthetics
- Emotions (frustration and confidence)
- Usefulness
- Reliability

- **User test**

Regarding the user test, 15 participants are involved.

During the test, they are invited to perform some tasks thinking out loud, so to explain what they are doing, thinking and feeling in each moment.

The test sessions are moderated by a facilitator who guide the users and ask for their comments.

Through this assessment, we can evaluate both the interaction process and the elements of interface (i.e. icons, labels, organization of the information etc.).

Indeed, 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 designed.

The results collected are used to further enhance the user experience.

6.2 Results

According to the results of the User Test, ReCRED applications are considered intuitive and easy to use. Only minor issues arose, mainly related to icons and labels. They have been already fixed.

In the following paragraphs, the results of the online survey are reported. Note that 5 respondents have been excluded from the analysis due to the response set, meaning the tendency to respond systematically to items regardless of their contents.

PROD performed an additional internal assessment of the student discount pilot, with the results being described in the corresponding subsection.

6.2.1 Campus Wi-Fi and Web Services Access Control

The following table reports the number of responses for each item (number of respondents: 85).

| ITEMS | Strongly Disagree | Disagree | Uncertain Don't Know | Agree | Strongly Agree |
|---|-------------------|----------|-------------------------|-------|----------------|
| The system responds too slowly to input | 34 | 30 | 10 | 10 | 1 |
| There are too many steps required to get something to work | 20 | 36 | 11 | 15 | 3 |
| It is easy to perform the tasks required to accomplish a goal | 4 | 4 | 14 | 42 | 21 |
| The system hasn't always done what I was expecting | 21 | 32 | 16 | 14 | 2 |
| The system gives me appropriate feedback for every action I perform | 3 | 4 | 21 | 40 | 17 |
| The system keeps me informed about where I am and what to do next | 2 | 4 | 9 | 46 | 24 |
| The system allows me to easily diagnose and correct errors | 1 | 6 | 25 | 35 | 18 |
| It is easy to learn how to use the system | 3 | 4 | 10 | 40 | 28 |
| I need the support of a technical person to learn how to use the system | 20 | 38 | 13 | 9 | 4 |
| I need specific instructions to understand how the system works | 20 | 30 | 11 | 20 | 5 |

| | | | | | |
|---|----|----|----|----|----|
| The organization of the information is clear | 1 | 5 | 11 | 41 | 27 |
| The terms referred to commands and icons are clear and understandable | 2 | 5 | 1 | 48 | 29 |
| The aesthetic appearance and the graphic elements of the interface are pleasant | 0 | 3 | 12 | 39 | 31 |
| Using the system is frustrating | 30 | 29 | 14 | 8 | 4 |
| I felt very confident using this system | 4 | 4 | 21 | 38 | 18 |
| This solution makes the access to campus WiFi and web services easy and quick | 3 | 5 | 5 | 37 | 35 |
| This solution provides a reliable and secure authentication mechanism | 4 | 2 | 7 | 36 | 36 |

The following graph shows the usability dimensions with their scores (maximum score = 425).

In this way, you can easily identify the strong and weak points of the application, as perceived by the respondent users.

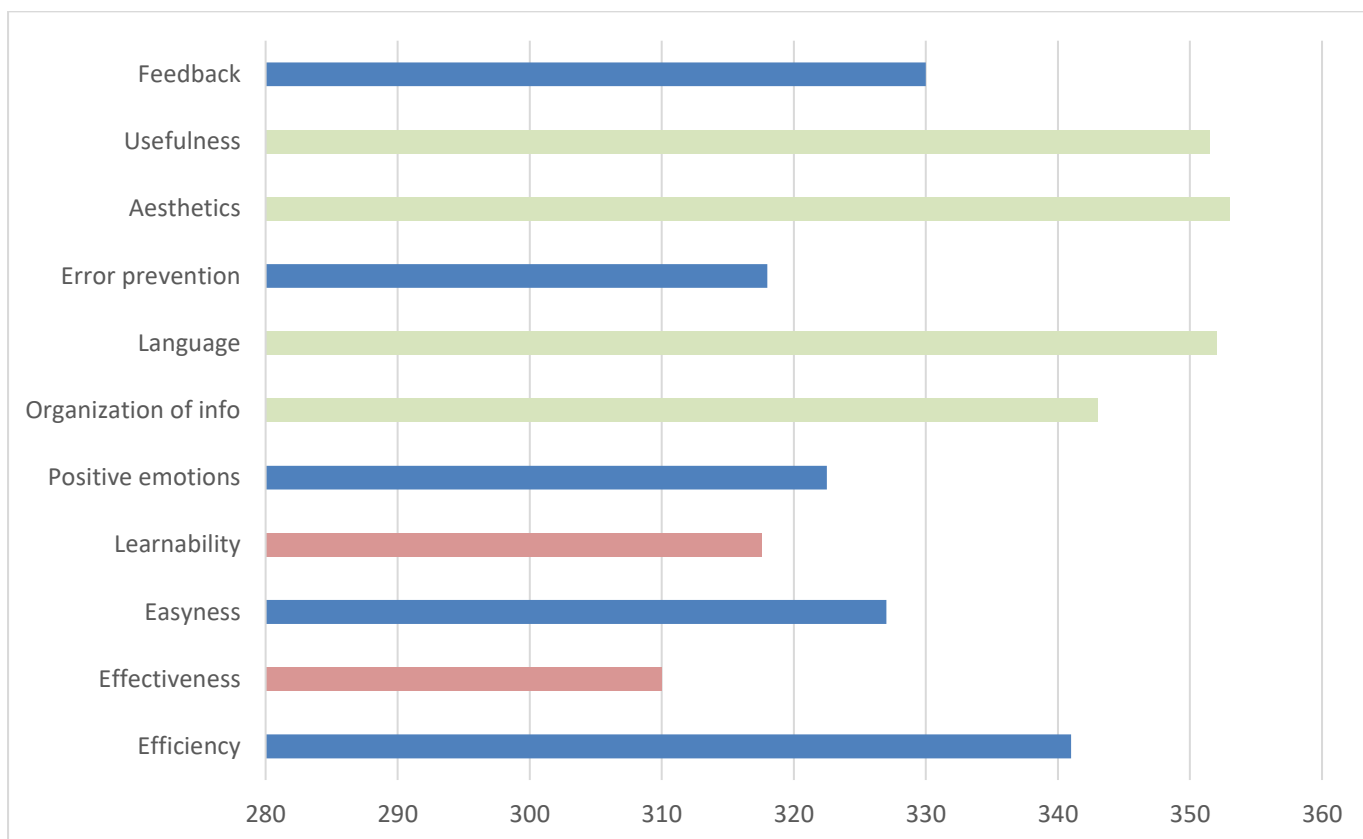


Figure 30: Usability dimensions for Wi-Fi pilot

6.2.2 Student Authentication & Offers

The following table reports the number of responses for each item (number of respondents: 9)

| ITEMS | Strongly Disagree | Disagree | Uncertain Don't Know | Agree | Strongly Agree |
|---|-------------------|----------|-------------------------|-------|----------------|
| The system responds too slowly to input | 4 | 4 | 0 | 1 | 0 |
| There are too many steps required to get something to work | 0 | 1 | 3 | 3 | 2 |
| It is easy to perform the tasks required to accomplish a goal | 0 | 3 | 4 | 2 | 0 |
| The system hasn't always done what I was expecting | 1 | 1 | 2 | 3 | 2 |
| It is easy to learn how to use the system | 1 | 1 | 4 | 3 | 0 |
| The system gives me appropriate feedback for every action I perform | 0 | 5 | 1 | 3 | 0 |

| | | | | | |
|--|---|---|---|---|---|
| The system keeps me informed about where I am and what to do next | 1 | 4 | 3 | 0 | 1 |
| I need the support of a technical person to learn how to use the system | 2 | 3 | 0 | 3 | 1 |
| I need specific instructions to understand how the system works | 0 | 2 | 2 | 4 | 1 |
| Using the system is frustrating | 1 | 2 | 4 | 0 | 2 |
| I felt very confident using this system | 1 | 2 | 4 | 2 | 0 |
| The organization of the information is clear | 0 | 1 | 2 | 6 | 0 |
| The terms referred to commands and icons are clear and understandable | 0 | 1 | 3 | 4 | 1 |
| The system allows me to easily diagnose and correct errors | 2 | 1 | 4 | 2 | 0 |
| The aesthetic appearance and the graphic elements of the interface are pleasant | 3 | 1 | 1 | 3 | 1 |
| This solution makes the authentication secure and easy | 0 | 1 | 4 | 4 | 0 |
| This solution is useful because it allows me to be authenticated as a student without revealing sensitive data | 0 | 1 | 3 | 5 | 0 |

The following graph shows the usability dimensions with their scores (maximum score =45).

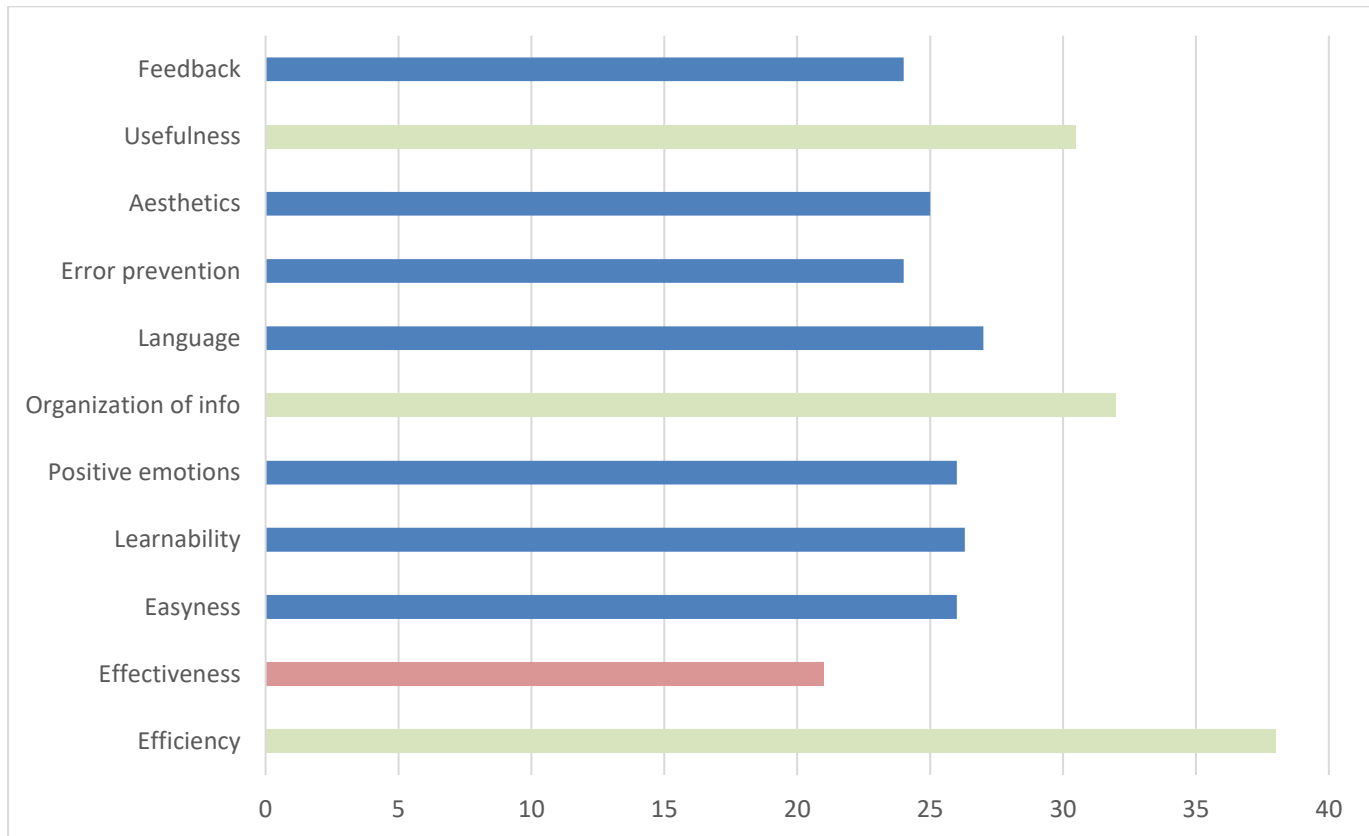


Figure 31: Usability dimensions for student discount pilot

In addition, during the pilot PROD interviewed end users with regards to their experience with the pilot applications including the registration process with the ReCRED app and performed an expert review of the apps to evaluate the user experience based on best practices in collaboration with our own UX designers and experts. As can be expected from applications that are not yet ready for full commercial exploitation and that are still in a pilot phase, there are still several user experience issues to resolve.

In general, the applications were well received. Several of the issues identified during the expert review, demonstrations to partners, and during the pilot itself have been resolved. Some key highlights from the in-house expert review are shown in the figures below:

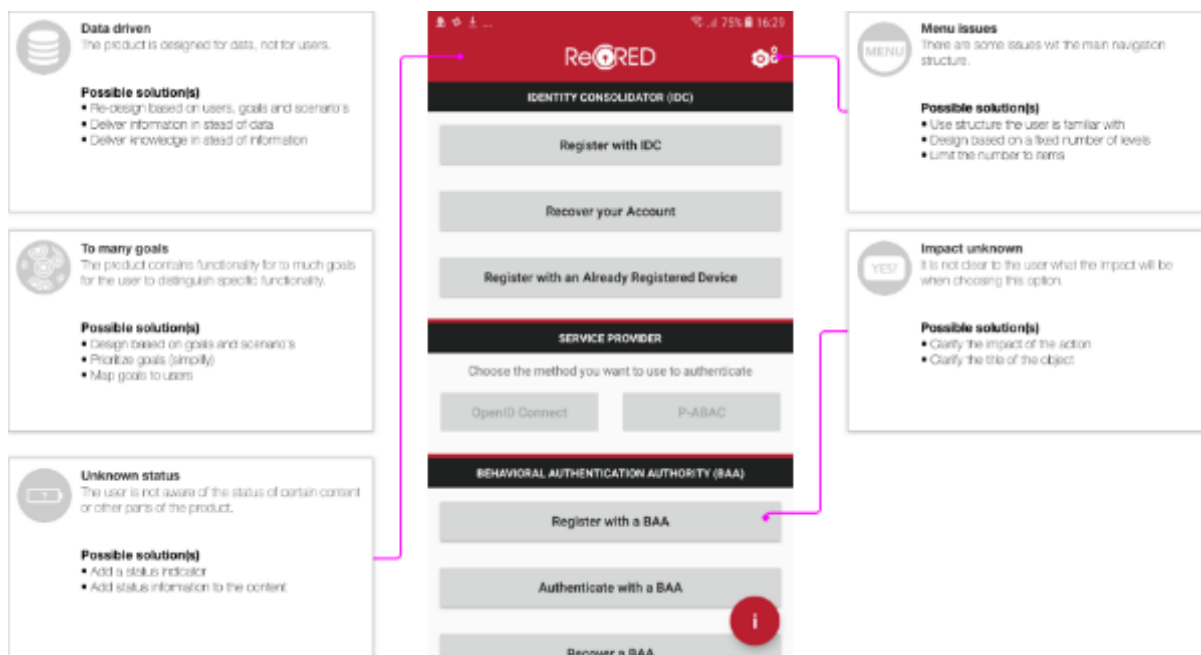


Figure 32 ReCRED App - Expert Review

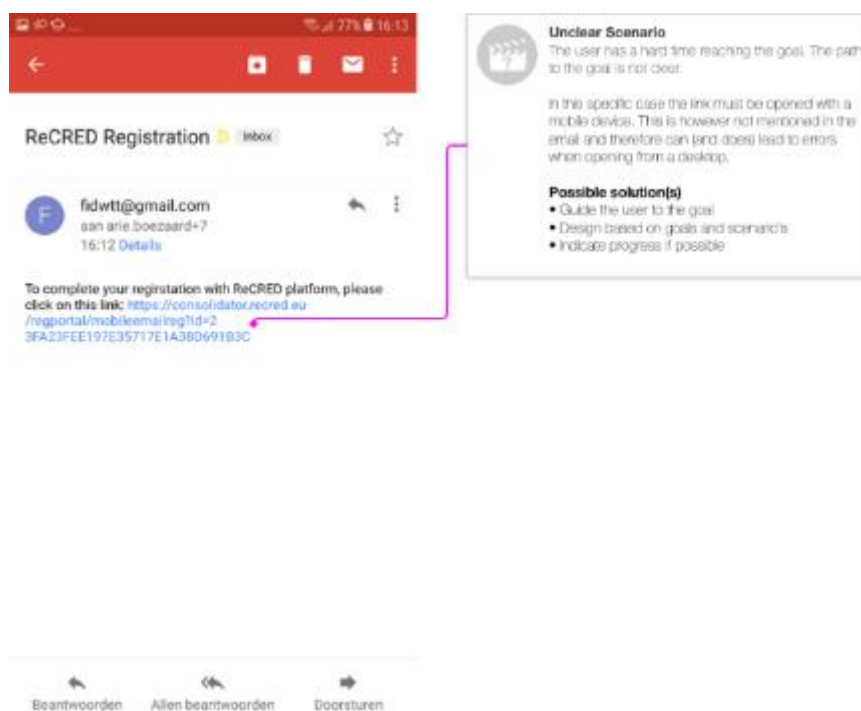


Figure 33 Student Pilot – Expert Review | Registration email

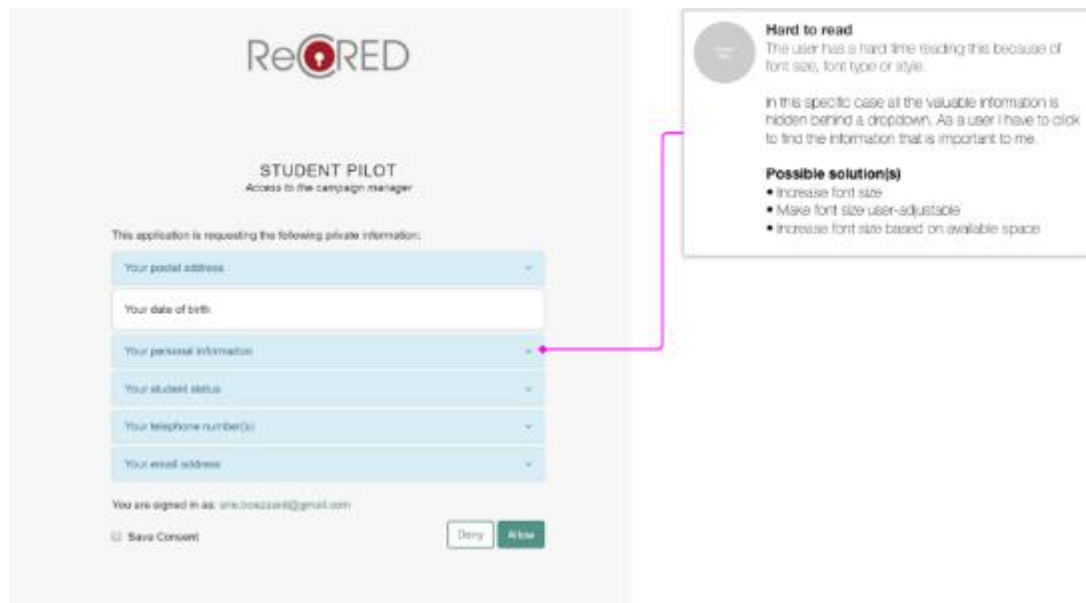


Figure 34 Student Pilot - Expert Review | Consent

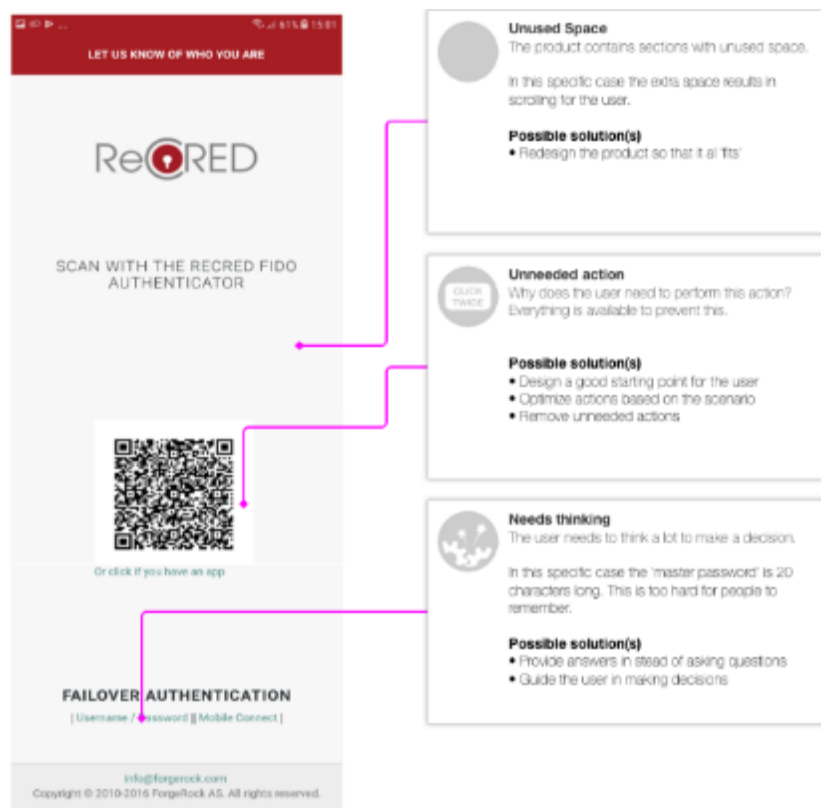


Figure 35 Student Pilot - Expert Review | Authentication



Figure 36 Student Pilot - Expert Review | Discounts

6.2.3 Age Verification Online Gateway

The following table reports the number of responses for each item (number of respondents: 19)

| ITEMS | Strongly Disagree | Disagree | Uncertain Don't Know | Agree | Strongly Agree |
|---|-------------------|----------|-------------------------|-------|----------------|
| The system responds too slowly to input | 11 | 6 | 2 | 0 | 0 |
| There are too many steps required to get something to work | 9 | 10 | 0 | 0 | 0 |
| It is easy to perform the tasks required to accomplish a goal | 0 | 0 | 0 | 8 | 11 |
| The system hasn't always done what I was expecting | 9 | 9 | 1 | 0 | 0 |
| The system gives me appropriate feedback for every action I perform | 0 | 1 | 4 | 8 | 6 |
| The system keeps me informed about where I am and what to do next | 0 | 0 | 0 | 12 | 7 |
| The system allows me to easily diagnose and correct errors | 0 | 0 | 5 | 8 | 6 |
| It is easy to learn how to use the system | 0 | 0 | 0 | 8 | 11 |

| | | | | | |
|---|----|----|---|----|----|
| I need the support of a technical person to learn how to use the system | 14 | 4 | 0 | 1 | 0 |
| I need specific instructions to understand how the system works | 7 | 11 | 0 | 0 | 1 |
| The organization of the information is clear | 0 | 0 | 0 | 6 | 13 |
| The terms referred to commands and icons are clear and understandable | 0 | 0 | 0 | 8 | 11 |
| The aesthetic appearance and the graphic elements of the interface are pleasant | 0 | 0 | 1 | 3 | 15 |
| Using the system is frustrating | 11 | 8 | 0 | 0 | 0 |
| I felt very confident using this system | 0 | 0 | 0 | 12 | 7 |
| This solution makes the access to age restricted services more secure | 0 | 0 | 1 | 0 | 18 |
| This solution is useful because it allows anonymous authentication | 0 | 0 | 1 | 2 | 16 |

The following graph shows the usability dimensions with their scores (maximum score =95).

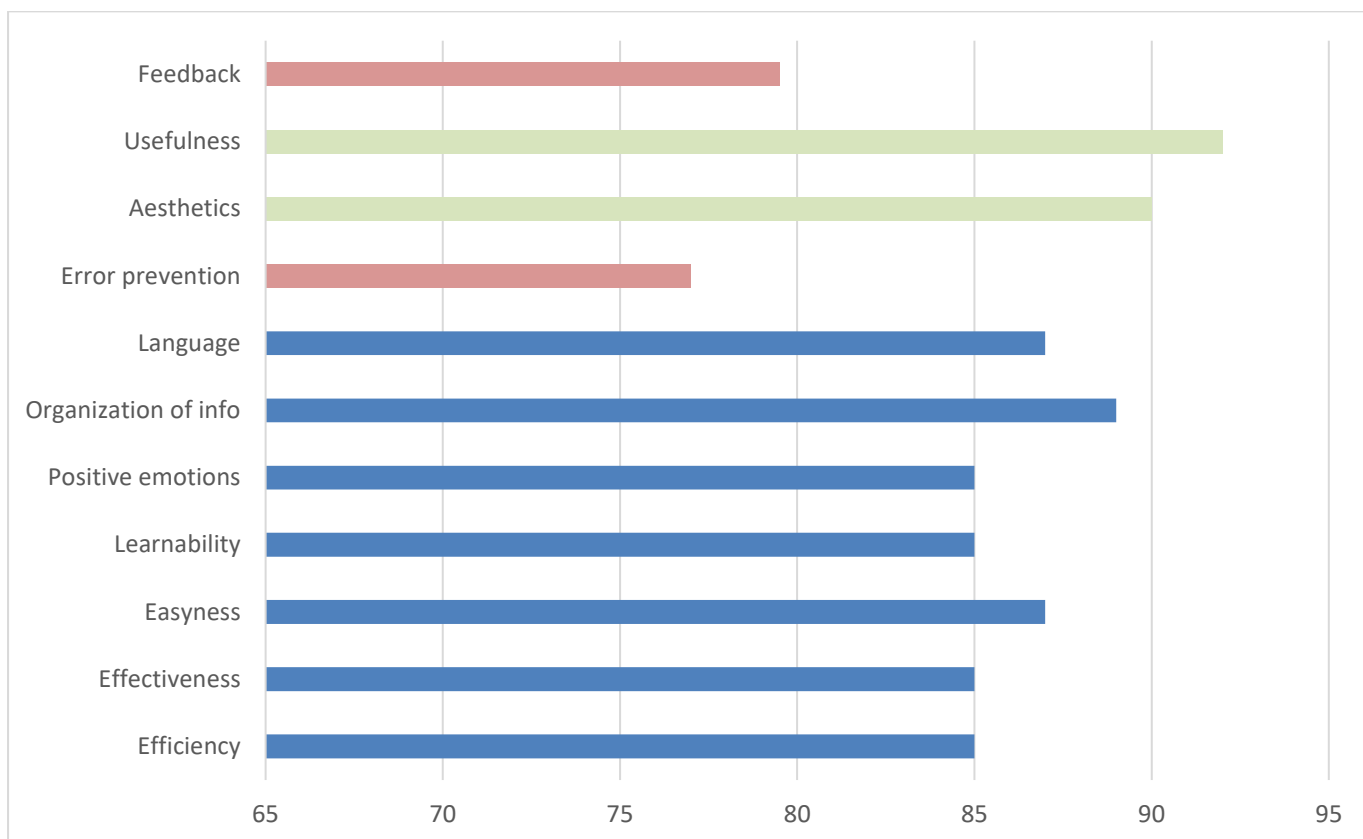


Figure 37: Usability dimensions for age verification pilot

6.2.4 Microloan Origination

The following table reports the number of responses for each item (number of respondents: 4)

| ITEMS | Strongly Disagree | Disagree | Uncertain Don't Know | Agree | Strongly Agree |
|---|-------------------|----------|-------------------------|-------|----------------|
| The system responds too slowly to input | 0 | 3 | 1 | 0 | 0 |
| There are too many steps required to get something to work | 1 | 3 | 0 | 0 | 0 |
| The path to accomplish a task is clear and intuitive | 0 | 0 | 0 | 2 | 2 |
| It is easy to perform the tasks required to accomplish a goal | 0 | 0 | 0 | 4 | 0 |
| The system hasn't always done what I was expecting | 1 | 2 | 1 | 0 | 0 |
| It is easy to learn how to use the system | 0 | 0 | 0 | 3 | 1 |

| | | | | | |
|---|---|---|---|---|---|
| I need the support of a technical person to learn how to use the system | 1 | 3 | 0 | 1 | 0 |
| I need specific instructions to understand how the system works | 1 | 1 | 1 | 1 | 0 |
| Using the system is frustrating | 1 | 3 | 0 | 0 | 0 |
| I felt very confident using this system | 0 | 0 | 1 | 3 | 0 |
| The organization of the information is clear | 0 | 0 | 1 | 2 | 1 |
| The terms referred to commands and icons are clear and understandable | 0 | 0 | 0 | 3 | 1 |
| The system allows me to easily diagnose and correct errors | 0 | 0 | 1 | 3 | 0 |
| The aesthetic appearance and the graphic elements of the interface are pleasant | 0 | 1 | 0 | 2 | 1 |
| This solution makes the process of the microloan request easy and quick | 0 | 0 | 0 | 4 | 0 |
| This solution allows me to send my financial information to the bank in a secure and reliable way | 0 | 1 | 2 | 1 | 0 |

The following graph shows the usability dimensions with their scores (maximum score =20).

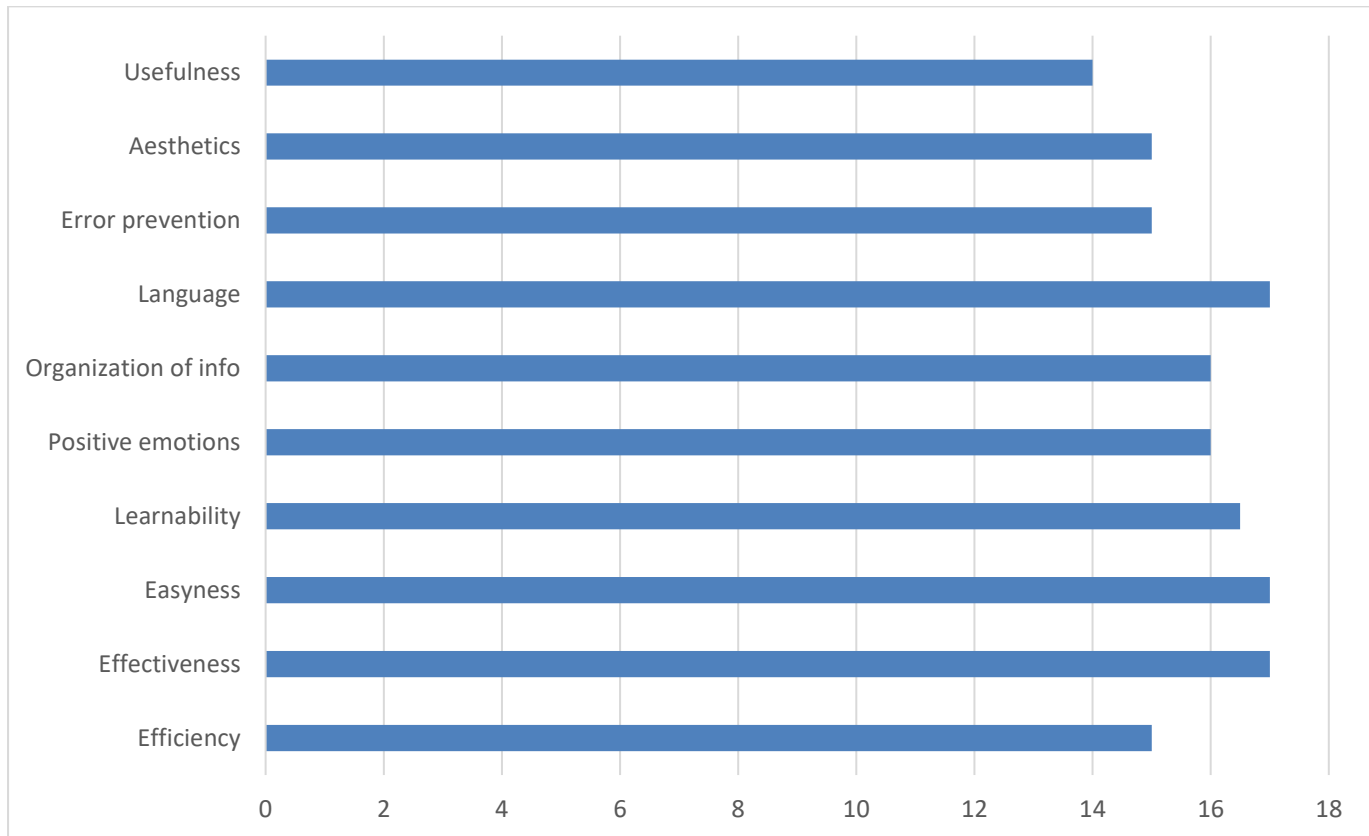


Figure 38: Usability dimensions for microloan origination pilot

6.3 Service Provider

In addition to the end-user assessment, T7.4 includes also the feedback from the Service Providers (SPs). The objective is to collect the opinions of the SPs about ReCRED, and the way it can enhance the web services by providing reliable authentication and authorization mechanisms.

The following table show the results collected.

| | |
|--|--|
| Pilot | Campus WiFi and web services |
| Service Provider | Kika Christou, IT Officer from Cyprus University of Technology |
| Materials | Demo video, Live demo |
| What are the main concerns and needs related to security in your business? | |
| <ul style="list-style-type: none"> - We need the users to authenticate in order to use our services - We need Visibility of all the devices in our network - We only permit access according to the user's role in organization | |
| How can ReCRED support your business objectives? | |
| ReCRED provides easy authentication method using biometrics. It is better than the username-password that we are currently using at CUT. To support our objectives, ReCRED already sends logs to other security devices that can apply access policies based on the user's role. | |
| What are the changes needed to implement ReCRED into your service? How much effort do they require? | |
| We needed a new SSID named ReCRED and also, we had to establish a communication between ReCRED's authentication server and the University's security assignment server. | |

| |
|---|
| <p>How can ReCRED improve the service you provide to the users?</p> <p>It provides easier authentication method.</p> |
| <p>How can ReCRED be enhanced so to better meet your needs and requirements?</p> <p><i>Not applicable</i></p> |
| <p>Additional comments</p> <p>It was easy to make all the systems work together (existing CUT services like the Wireless Controller, security assignment server and the ReCRED two servers).</p> |

7 Conclusions

During the last year of the project, all four pilots have been fully deployed and optimized, according to the findings from the end-users’ assessment and the Service Providers evaluation. Not only that, but all the pilots have been enhanced, either with additional features and modalities and/or with additional environments.

Regarding the dissemination of the pilots, we have tried to reach potentially interested parties through multiple means. We organized in-house dissemination activities, but we also participated in major events, where we were able to present our business cases and technologies to hundreds of people and gather invaluable feedback. We also organized online sessions to demonstrate our pilots and provide answers and clarifications. And, of course, we also disseminated the pilots using various digital marketing tools (newsletters, infographics, social media, etc.)

In order to further increase protection of participants’ personal data, we have identified Verizon as the Data Protection Officer (DPO) of the project. Therefore, an email address (recred2020+dpo@gmail.com) has been created for receiving participants’ requests, addressing their doubts, allowing them to exercise their privacy rights and, generally, providing them with information requested. Another email address (recred2020+support@gmail.com) has instead been created for reporting and addressing technical issues and for providing incidents support.

Last but not least, our usability experts performed a detailed UX assessment for all the pilot. This assessment, in combination with the feedback that we received from the end-users and Service Providers that we managed to reach, allowed us to discover flows and further optimize our solutions.

The end of the project does not mean the end of the pilots. All the apps and the backend infrastructure will remain up and running for at least one year after the end of the project. During this period, we will continue gathering data regarding the use of our solutions, which will provide us with useful insight and could help us in the evaluation of our initial business plans.

8 References

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