ReCRED's Pilots

February 2018
Issue 4

Description and Use Case Scenarios

In this Issue

Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no 653417

Introduction

*by Christos Xenakis (**UPRC**), Vangelis Bagiatis (**UPCOM**) &
Spyros Evangelatos (**EXUS**)*

In the end of the first year of the project, a first prototype of the campus-wide Wi-Fi and web services access control pilot was deployed at CUT premises, acting as a somewhat controlled setting with the goal to demonstrate the functionalities of the ReCRED systems "at large". This pilot was further extended during the project's second year with additional flows and functionality as well as with several improvements to the user interface (UI) in order to improve the users' experience. These improvements were according to a preliminary UX assessment that was performed by CNIT. Later on, the Wi-Fi and web services access control pilot was deployed at IMDEA premises, and soon it will also be deployed at CNIT and CSGN's premises.

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

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

Device-centric Campus Wi-Fi and Web Services Access Control

*by Antonis Papasavva (**CUT**), Kostantinos Papadamou (**CUT**), Jose Herrera (**IMDEA**) & Claudio Pisa (**CNIT**)*

The ReCRED campus Wi-Fi Pilot is a security architecture which employs the ReCRED modules in order to control the user access to the campus Wi-Fi network and to the associated web services. Nowadays, accessing the Wi-Fi network in a campus is critical because many of the university services, like e-learning or Internet resources, need to be accessed by students, professors and visitors. Taking into consideration the characteristics of this context, there is an acute need for authentication and authorization functions which are both user-friendly and non-intrusive, while assuring a granular access which can be easily controlled by administrators.

The first scenario addressed by the Wi-Fi pilot consists in students and professors accessing the network services by presenting a minimal set of trustworthy attributes. The second scenario permits a trust transfer from the user smart-phone to another device (e.g. laptop), which can be used to access the campus network services. The trust transfer scenario uses QR code scanning along with the ReCRED security stack to authenticate and authorize the second device. The Wi-Fi pilot proposes an architecture where users will be granted access to the network resources by presenting a set of identity attributes which are validated by the ReCRED infrastructure.

ReCRED leverages the ubiquity of smart-phones to design a device-centric authentication and authorization scheme, where a Campus Access mobile application is used to gain access to the campus network resources. The user launches the mobile application to select the desired university resources and after being informed about the revealed attributes it will start the authentication process. The ReCRED campus-wide Wi-Fi and web services access pilot aims to move the burden of traditional authentication methods from the user to the device itself, taking full advantage of the smartphones' inherent capabilities. The pilot carries two main advantages: (a) the advantage of Device Centric Authentication (DCA), which enables the user to authenticate using biometrics (e.g., fingerprint) instead of having to remember a username and a complex password; and (b) enables users to prove part of their identity in order to access the universities' campus Wi-Fi and web services without the need to reveal their complete profile (Privacy-preserving Attribute-based Authentication).

In case the user wishes to use an alternate device (e.g., desktop PC) to access the campus Wi-Fi and web services, the service presents a QR code. The user should scan this QR code using the ReCRED application on her mobile device in order to authenticate her alternative device to the service. In this way, the mobile device and the alternate device are associated as belonging to the same user, and the user can use the alternate device to gain access to the Wi-Fi and the web services of the university.

The ReCRED Wi-Fi pilot permits the user to authenticate by using biometric solutions such as fingerprint, thus replacing user-name/password credentials. Among the core security technologies employed by the Wi-Fi pilot, there are protocols like FIDO UAF and a ReCRED tailored version of OpenID Connect/OAuth2. The Wi-Fi pilot has a modular structure, with separate authentication, authorization and network access structures along with the ReCRED services, thus it can be easily adapted to custom security requirements.

Student Authentication and Offers

*by Steven Winnen (**PROD**)*

The Student Discount Pilot will leverage the ReCRED platform to validate the business value of password-less device centric authentication and attribute based access control in a retail discount service model.

In other words, after the pilot we want to be able to answer the question: Does the use of the ReCRED platform result in increased conversion for retailers offering targeted discounts to their customers, without extra complexity for the customers?

To achieve this, using the ReCRED platform with a discount service must provide benefits to the customer first and the service provider second.

The main benefit for students is that they can complete all transactions on their mobile device without invasive requests or extra steps before they can purchase an offer. By using ReCRED to check for specific attributes without disclosing them to the service provider, students can prove their field of study, the university that they study and much more. Students can receive any simple or complex student discount offer.

Service providers can increase the likelihood that a customer will purchase an offer by creating more complex targeted offers without increasing the complexity of the transaction. Additionally, service providers will benefit from substitution of physical loyalty cards for mobile apps and thereby obtaining rich purchasing and conversion data for the improvement of their discount offers.

They will also see a decrease in the training requirements for staff as well as fraudulent use of discount codes.

The pilot will initially be executed in a semi-controlled environment at the Haagse Hoge School in The Netherlands, where students will perform the roles of both merchant and customer. This stage will be invaluable for collecting feedback on the end-to-end user experience from both perspectives without the need to impact an actual merchant service.

At the same time, the ReCRED platform will be evaluated by business professionals from other service categories such as the pharmacy industry to provide an assessment of the transferability of the platform to other service models.

After completion of this stage and subsequent adjustments to the pilot platform based on the feedback received, we will look to expand the pilot to include a selection of service providers to validate the pilot in a live setting with real customers.

Attributed-based Age Verification Online Gateway

*by Vangelis Bagiatis (**UPCOM**)*

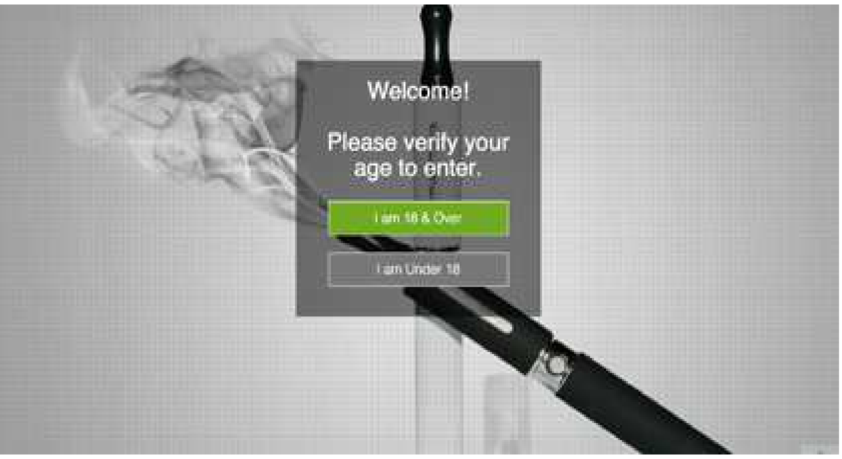
The age verification pilot is based on the new Age Gate solution, an online age verification service, with the purpose of granting or denying access to age-restricted resources, without revealing or disclosing any other personal and/or sensitive data of the user.
An age-restricted online resource could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

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

The providers of those resources do not need to know any personal information about their visitors. They only need to be able to guarantee that the visitors are above a certain age, which can be defined as a policy.
The age verification pilot includes three flows: end-user registration, website registration, age verification

End-user Registration

A new user visits your website and is presented with an option to access it using the Age Gate solution, along with a link to download the Age Gate mobile app from the respective store. After downloading and opening the mobile app for the first time, the user can choose an authentic source (government, bank, mobile operator, etc.), and permits Age Gate to obtain her date of birth from the selected source. After that, the user's date of birth is safely stored in Age Gate and associated with the unique ID of his mobile device. At the same time, the user can choose to use a fast and easy way to authenticate to the device (fingerprint, pattern, face recognition, etc.)



Website Registration

A website owner needs to register with Age Gate, before being able to register his websites, by filling in a simple web form. Then, the website owner can register one or more websites, and for each website, he needs to define: the website's title, a short description, the URL, and the age policy (e.g. > 18).
An Age Gate operator review each request for website registrations, and after he approves it, a notification is sent to the website owner, with details on how to embed Age Gate to their website. After that, the new visitors are able to use the Age Gate solution in order to access the website.

Age Verification

Each time an Age Gate user wants to visit a supported website from her mobile device, the Age Gate mobile app opens, and the user will need to authenticate using the selected method (e.g. fingerprint). If the visit is from a desktop browser, the user also needs to scan a QR code with the mobile device. In both cases, Age Gate can verify that the user is the legitimate owner of the mobile device, it evaluates her age against the age policy that you have set (e.g. age > 18) and it lets the website know whether she is above or below the required age.

You can also watch a very short introductory video on the project's YouTube channel: https://www.youtube.com/watch?v=nUHmkE4VsVw

Finally, note that our solution is completely privacy preserving. The only thing that Age Gate knows is that the owner of the mobile device with id <xxxxxx> was born in <dd/mm/yyyy>. And the only thing that the websites know is whether their visitors are above or below the required age.

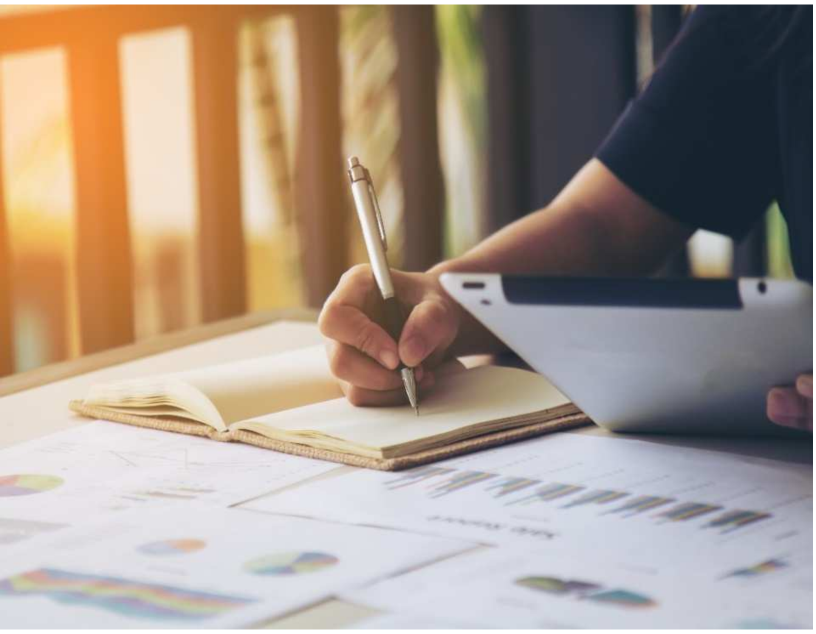
Microloan Origination

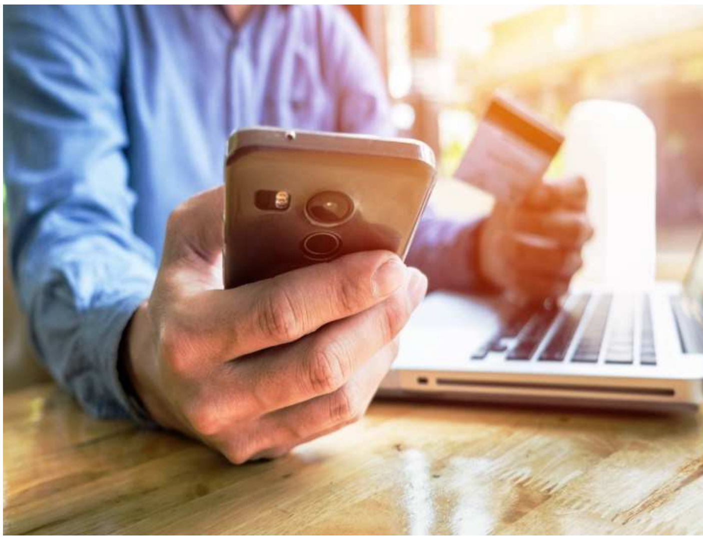
*by Spyros Evangelatos (**EXUS**) &*
*Evangelos Kotsifakos (**WEDIA**)*

Microfinance has a beguiling simplicity and a record of success mostly in promoting financial resilience. At its lowest level, microfinance is considered as a form of insurance, where repayment is high. At the next level, which many participants never aspire to, it might involve borrowing to start up a small enterprise, or to expand an existing one.

The microloan origination pilot will be based on an online origination platform that leverages on independently verifiable identity attributes to approve microloan applications. It provides the necessary tools for supporting all the steps of the microloan origination, debt collection and recovery process for financial institutions.

In addition, it can be used by financial institutes and banks in order to provide low-interest loans via an entirely online process. The benefits from the deployment of the microloan origination platform will be apparent not only to the service providers (i.e. banks, financial institutes, etc.) but also to its customers. Time and money savings are common for both parties involved in the process. Convenience, easy access, round-the-clock service and speed are some of the advantages that our microloan origination platform provides in comparison with the traditional process followed nowadays by the people visiting the banks.





Process for Online Application

Customers applying for microcredit will use the b-Verifier product, which is a tool developed by WEDIA, as a multifactor authentication system that provides increased security for banking environments.

Once users establish access to a financial institution's origination platform through their device, they will upload their financial, and professional credentials which will be certified by reliable authorities (i.e., governmental institutes) or are obtained through trusted identity acquisition.

These credentials are loaded to the user device, and can be used to prove the relevant identity attributes to the EXUS Suite running at the microloan company/institute.

The financial institution will use an access control policy creation tool, developed by CUT, to specify complex credit approval criteria. Several scenarios are going to be tested during the pilot evaluation period, ranging from microloans for medical expenses to credit cards and installment loans.

You can also watch a very short introductory video on the project's YouTube channel: https://www.youtube.com/watch?v=x3p99F86opM or read our white paper with a more detailed technical description in our website https://www.recred.eu/publication-categories/communication

ReCRED in a nutshell

ReCRED's ultimate goal is to promote the user's personal mobile device to the role of a unified authentication and authorization proxy towards the digital world. ReCRED adopts an incrementally deployable strategy in two complementary directions: extensibility in the type and nature of supported stakeholders and services (from local access control to online service access), as well as flexibility and extensibility in the set of supported authentication and access control techniques; from widely established and traditional ones to emerging authentication and authorization protocols as well as cryptographically advanced attribute-based access control approaches. Simplicity, usability, and users privacy is accomplished by:

i. hiding inside the device all the complexity involved in the aggregation and management of multiple digital identifiers and access control attribute credentials, as well as the relevant interaction with the network infrastructure and with identity consolidation services;

ii. integrating in the device support for widespread identity management standards and their necessary extensions; and

iii. controlling the exposure of user credentials to third party service providers. ReCRED addresses key security and privacy issues such as resilience to device loss, theft and impersonation, via a combination of:

   1. local user-to-device and remote device-to-service secure authentication mechanisms;
   2. multi-factor authentication mechanisms based on behavioral and physiological user signatures not bound to the device;
   3. usable identity management and privacy awareness tools;

iv. usable tools that offer the ability for complex reasoning of authorization policies through advanced learning techniques. ReCRED's viability will be assessed via four large-scale realistic pilots in real-world operational environments. The pilots will demonstrate the integration of the developed components and their suitability for end-users, so as to show their TRL7 readiness.

ReCRED Consortium

UNIVERSITY OF PIRAEUS

Cyprus University of Technology

cnit

institute imdea networks

Telefónica
Telefónica I+D

verizon

certSIGN®

BAKER & McKENZIE

THE PRODUCTIZERS

wedia

upcom
Bringing business and IT together

EXUS®