ReCRED

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

Makes your digital life **safe** and definitely **easy**!

European Commission
Horizon 2020
European Union funding
for Research & Innovation

Contents

Information

http://www.recred.eu/

https://www.linkedin.com/groups/8470632

https://www.youtube.com/channel/UClVzn8b6g_vE3dxzV1sli0g

https://twitter.com/ReCRED_H2020

https://www.facebook.com/ReCREDH2020/

PROJECT REFERENCE	FUNDED UNDER	TOTAL COST	EU CONTRIBUTION
653417	H2020-EU.3.7.	6,366,310 €	4,997,242 €

Editorial

Dear reader,

We are happy to introduce you to the ReCRED newsletters, a great vehicle for our consortium to communicate our project's achievements, activities and results. Approaching its third and final year, ReCRED is very close to fulfill its original objectives, advancing the authentication paradigm by establishing a secure-by-design and privacy-preserving device-centric authentication and access control. Co-funded by the Horizon H2020 Framework Programme of the European Union under grant agreement no. 653417, ReCRED is the product of the coordinated effort of 13 partners from 8 European countries, sharing the same goal.

The application-centric authentication model, where independent services apply individual authentication methods to verify the user's identity, has long ago failed: it's neither usable, nor secure. The ubiquity of the smartphones has laid an excellent basis for the authentication scheme to shift towards the device-centric model, where the user authenticates to a local device and the device then authenticates to online services on user's behalf. Perfectly aligned with the EU General Data Protection Regulation (GDPR) principles and balancing between security and usability, ReCRED's ultimate goal is to promote the user's personal mobile device to the role of a unified authentication and authorization proxy in the digital world.

Currently in its integration phase, ReCRED fervently prepares for its upcoming large-scale pilots that will take place during this summer. For more information and latest news regarding the project, please refer to the following sections and stay in touch with ReCRED's progress through our newsletter issues.

Prof. Christos Xenakis (xenakis@unipi.gr)
ReCRED Project Coordinator
On behalf of the ReCRED Consortium

Advantages

The use of passwords is the most popular method of authentication since it is simple and straightforward. However this method is highly insecure; users have the tendency to choose weak, easy-to-remember passwords and, therefore, easy-to-guess. Additionally, the security requirements of critical services, such as e-banking, far exceed those satisfied by ordinary passwords, which can be easily stolen or bypassed.

To counter these issues, a few alternative authentication methods have been developed that either add an extra level of security by using second factor authentication or eliminate the password from the authentication process by using biometric characteristics, such as fingerprint, iris and face recognition. Recent developments in biometric authentication are also focusing on behavioral characteristics. The way we walk, how we talk or type can identify us effectively enough to be used as authentication means.

ReCRED encompasses these latest development and taking full advantage of smartphones' inherent capabilities moves the burden of authentication from the user to the device itself. ReCRED's primary aim is to build an integrated next generation access control (AC) solution that solves issues that stem from the weaknesses of the current authentication methods with the use of the Privacy-by-Design approach.

In a nutshell, ReCRED is targeting to offer the following advantages:

1. Device centric authentication, using biometrics and behavioral characteristics that overcomes the password overload problem.

Smartphones are used as authentication and authorization proxies towards the digital world. Biometrics are the primary authentication method and they are complemented by behavioral characteristics to transparently authenticate users and raise alerts when the device is stolen.

2. Account consolidation to solve the problem of dispersed identity attributes.

ReCRED provides the tools to connect all the online accounts a person manages such as social networks, bank accounts under one account and combine them with this persons' physical and civilian identity.

3. Anonymous access to address privacy issues.

Attribute-Based Access Control (ABAC) facilitates account-less access through verified identity attributes (e.g., age or location) and only specific attributes are revealed where they are required, protecting the identity of the user.

Implementation

The design and implementation of the ReCRED platform is based on detailed user-stories that cover a wide range of real-life security and access control situations. These user stories have been translated to technical and operational requirements and have been also used to the definition of the related security and privacy considerations. Along with an extensible threat model these requirements and considerations led to the design of the overall ReCRED architecture.

According to this architecture the ReCRED framework consists of the following components: the User's Device, the Identity Consolidator, the Service Providers, the Identity Providers, and the Behavioral Authentication Authorities. To connect each-other and to ensure users' security and privacy, the following state-of-the-art technologies in the fields of security, cryptography and networking are used.

FIDO UAF

FIDO (Fast IDentity Online), aims to change the nature of authentication by developing specifications that define an open, scalable, interoperable set of mechanisms and set a new standard for devices to securely authenticate users beyond the password era. By using public key cryptography, the FIDO protocol provides a passwordless authentication mechanism to an online service.

Trusted Execution Environment

The Trusted Execution Environment (TEE) is an emerging technology that comes built-in the latest mobile devices. It provides an isolated execution environment for executing Trusted Applications with elevated security mechanisms.

Mobile Connect

Mobile Connect is the GSMA (Groupe Spéciale Mobile Association) Personal Data programme focused on positioning Mobile Network Operators (MNOs) as trusted providers of identity services to third party service providers. The programme identifies a set of propositions (including authentication, validated identity, enhanced profile, attribute brokerage) that collectively are referred to as Mobile Connect.

Implementation

OpenAM

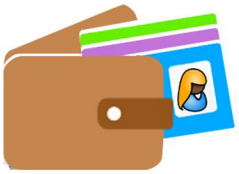
OpenAM is a web-based open-source solution that provides authentication, authorization, entitlement, and federation services. In addition to that, OpenAM's federation services allow federated members to securely share identity information with each other.

OpenID Connect

OpenID Connect (OIDC) is an enhanced version of OAuth 2.0. OpenID Connect deals with the identity of an end-user by permitting OIDC Providers to verify the identity of an end-user based on the authentication performed by an Authentication Server (Identity Provider). In addition to that, it also allows OIDC clients to request identity attributes of an end-user from OpenID Connect Provider in a REST-like fashion.

U-Prove

U-Prove is a cryptographic protocol that assures the users' privacy by minimally disclosing their certified attributes while interacting with an on-line entity.

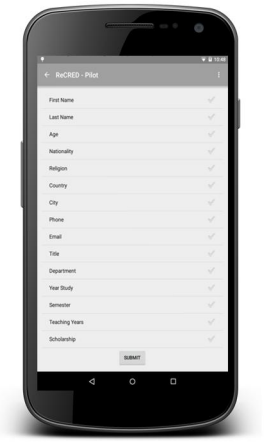


Idemix

Idemix is an identity management system based on anonymous credentials and zero-knowledge protocols.

More on the ReCRED's architecture and the technologies that are used can be found in the public deliverables available hosted at the project's website.

First ReCRED Pilot



Campus-wide Wi-Fi and web services access control

The ReCRED architecture will be deployed, demonstrated, and assessed in terms of security, performance, reliability, and end-user experience in four real-world large scale pilots. The first piloting activity, Campus-wide Wi-Fi and web services access control, has already been set up from the early stages of the project and is deployed at Cyprus University of Technology (CUT) and Universidad Carlos III de Madrid (UC3M) premises.

This pilot is deployed over the existing networking and identity management infrastructure of the Universities, which we augment in order to be able to use attribute-based authentication and FIDO. Through this pilot we address and upgrade the access to a campus-wide Wi-Fi network and corresponding campus-only web-services (e.g., Moodle) while enabling the administrators to define policies that take into account a user's identity attributes.

Specifically, students and professors are able to access the various campus resources by revealing only a set of required identity attributes, which are authenticated by the ReCRED infrastructure.

Furthermore, users are able to use their mobile device in order to access the campus Wi-Fi and other resources, through the Campus Access mobile application. The required authentication takes place using biometric solutions such as fingerprint instead of the traditional username/password scheme. This is achieved using a ReCRED-developed version of OpenID Connect that is integrated with FIDO UAF.

The pilot is being extended with Privacy-Preserving Attribute-Based Access Control mechanisms (Idemix, U-Prove and Attribute based encryption) and other features.

It will operate until the end of the project and beyond.

Latest News

The FIDO UAF Certification is a Fact! A Major Achievement for certSIGN and the ReCRED Project.

The FIDO (Fast IDentity Online) Alliance certified that gateSAFE UAF module complies with the FIDO UAF specifications. The product was developed and implemented by certSIGN as part of the ReCRED project (Real-world Identities to Privacy-preserving and Attribute-based CREDentials), making it one of the very few open source FIDO® Certified UAF Servers. The implementation successfully passed the Interoperability tests – performed with international partners form different countries, on Windows, Android and iOS clients – that took place in December 2016 and the subsequent FIDO Alliance review.

ReCRED presence in Mobile World Congress, Barcelona

Verizon was present at the Mobile World Congress in Barcelona (27 February - 2 March 2017), in order to meet major industry players, generate interest in the ReCRED project, and drive towards potential collaborations. Discussions with several technology providers such as Nok Nok labs, Safran, MePIN and ShoCard took place and reference to the ReCRED project was made in the panel session on IoT Security.

FASES Workshop 2016

The ReCRED consortium co-organized along with the TYPES (Towards Transparency and Privacy in Online Advertising Business – EU-2020) consortium the "Workshop on Future Access Control, Identity Management and Privacy Preserving Solutions in Internet Services"- FASES 2016. The workshop was held in conjunction with the 11th International Conference on Availability, Reliability and Security (ARES 2016), August 31 to September 2, in Salzburg, Austria. The goal of this symposium was to organize a set of technical sessions covering topics of interest for ReCRED and TYPES projects and create a forum of discussion around current issues identified within the context of the European Union.

The ReCRED consortium contributed 4 scientific papers to the workshop and representatives from all academic partners (University of Piraeus, Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Cyprus University of Technology, Universidad Carlos III de) were there to present their work and support the event.

Publications

Whitepaper

Read about how ReCRED is facing the password overload problem in the "Killing Passwords: Strong Authentication Beyond the Password Era" whitepaper by Prof. C.Xenakis of the University of Piraeus.

DOWNLOAD IT HERE: http://www.recred.eu/sites/default/files/paper_eng.pdf

Papers in conferences and journals

The ReCRED consortium has a strong presence in the security related conferences and journals. The academic partners' activity has resulted to more than 11 scientific papers in prestigious venues. Below are some of the latest related publications.

FIND ALL PUBLICATIONS HERE: http://www.recred.eu/publication-categories/publications

Promotional Material

Project leaflet

A leaflet and a project poster have been produced by the ReCRED consortium to support the partners' communication actions and contribute to build awareness to the ReCRED project achievements. Feel free to download and share our project's leaflet (a link to the leaflet).

DOWNLOAD IT HERE: http://www.recred.eu/sites/default/files/recred_leaflet_2017_3.pdf

Project Video

A modern informative video is available through the ReCRED project youtube channel that aims to disseminate the project's idea to the general public.

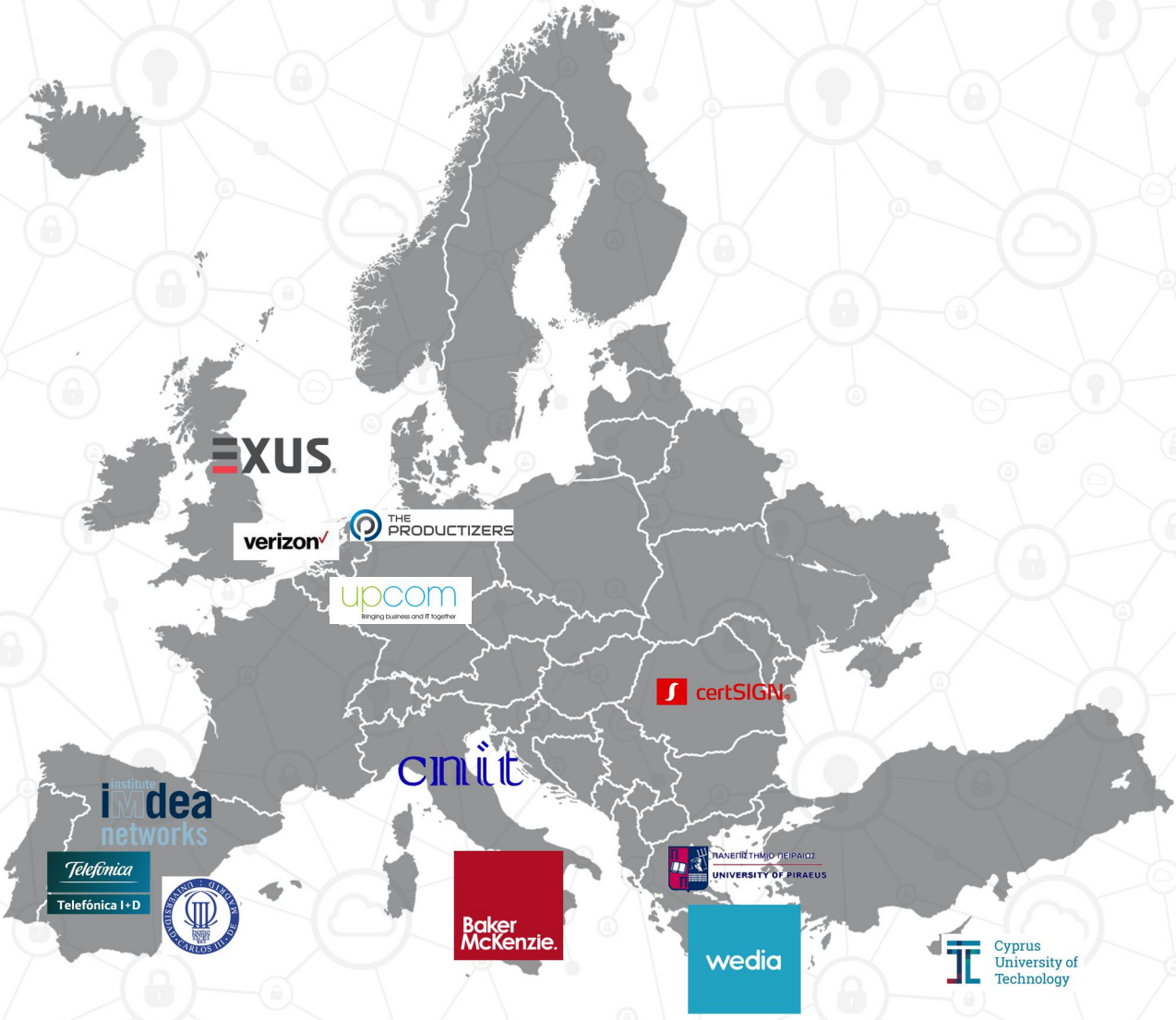
WATCH VIDEO HERE: https://www.youtube.com/watch?v=OBNU_XXyPrE

ReCRED

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

Makes your digital life **safe** and definitely **easy**!

Our Partners



European Commission
Horizon 2020
European Union funding
for Research & Innovation