

# ReCRED project takes device-centric access control into the future

January 15 2016

---

With e-commerce now exceeding 1 trillion USD per annum, the sharing economy on the rise, and the emergence of the Internet of Things, the need for reliable and user-friendly authentication and authorization mechanisms is more pressing than ever. Researchers from IMDEA Networks are collaborating in the newly launched ReCRED (ReCRED: Real-world Identities to Privacy-preserving and Attribute-based CREDentials)– a research project that aims to improve end-user internet security using the mobile as an authorization proxy.

The ultimate goal of ReCRED 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: (i) local user-to-device and remote device-to-service secure authentication mechanisms; (ii) multi-factor authentication mechanisms based on behavioral and physiological user signatures not bound to the device; (iii) 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.

## **A research project with an end user focus**

Being an innovation project, ReCRED does not nearly limits to develop and prototype technologies or systems, but comprises a broad set of activities devised to assess the impact of such technologies over real world end users, identify business strategies to exploit the ReCRED system and its individual technology components, and promote ReCRED's technologies to the perspective users and the research and innovation community.

**More information:** [www.recred.eu/](http://www.recred.eu/)

Provided by IMDEA Networks Institute

Citation: ReCRED project takes device-centric access control into the future (2016, January 15)  
retrieved 20 June 2024 from <https://phys.org/news/2016-01-recred-device-centric-access-future.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.