CREDENTIAL

Secure Cloud Identity Wallet

You are what you keep!

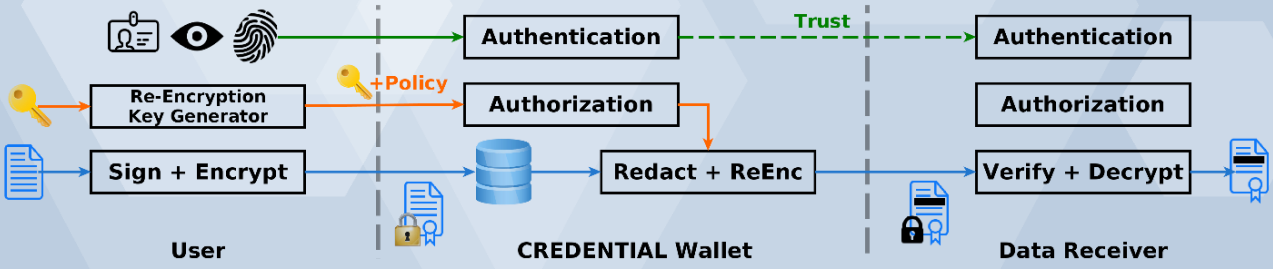
1st Newsletter – November 2016

The CREDENTIAL Newsletter series will keep you updated about the project's progress, results, and events. This issue contains a description of the overall approach taken in CREDENTIAL, an outline of its pilots, a summary of the organised events, and the scientific publications produced during the first year.

Project Vision and Architecture

The central goal of the CREDENTIAL project is to develop a data sharing platform (*wallet*) with integrated identity provider (IdP), which can be used to share authenticated data in a privacy-respecting way. CREDENTIAL's basic architecture involves three types of actors:

- ***Users*** own data to be securely stored or shared with other participants.
- The ***CREDENTIAL wallet*** is the central component of CREDENTIAL. It is a data storage and sharing service deployed in the cloud, yielding benefits such as constant availability, scalability, and cost effectiveness. A powerful identity and access management system performs multi-factor authentication and authorizes access to the stored data. The confidentiality of the stored and shared data is upheld at any point in time.
- Finally, ***data receivers*** might be service providers or users relying on data stored in, or authentication assertions issued by, the wallet. With this information, the data receiver reaches authorization decisions and performs arbitrary data processing.



To share data with others, a user first **authenticates** herself to the wallet using strong two-factor authentication. Next, the user **uploads** signed and encrypted documents to the wallet. This is done using so-called redactable signature and proxy re-encryption schemes. The former allows one to blank out predefined parts of a signed message without invalidating the digital signature, while the latter allows the CREDENTIAL wallet to forward data from the user to the data receiver without learning anything about the message and without the need for complex key-management. Now, to **share** data, the user generates and uploads the required key material based on which the wallet can translate the stored encrypted data for the receiver. Furthermore, the user defines which parts of the message should become accessible to the receiver. If the data receiver now **accesses** data, he can only read the allowed parts of the data, but still has strong authenticity and integrity guarantees for those disclosed parts.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653454.

CREDENTIAL

Secure Cloud Identity Wallet

You are what you keep!

CREDENTIAL Pilots

To evaluate and validate the capabilities of the CREDENTIAL tools and bring developed components to market-readiness, we are exploring three pilot scenarios in near-operational environments from the domains of eGovernment, eHealth, and eBusiness.

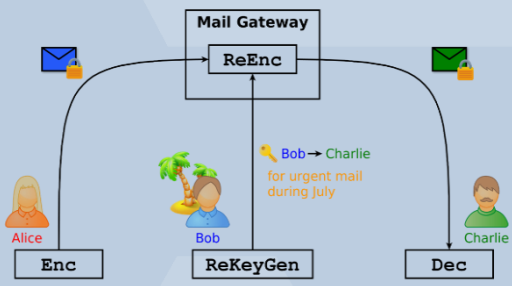
eGovernment

One aspect of the eGovernment pilot will focus on using the CREDENTIAL wallet as an identity provider for realizing a single sign-on functionality to different governmental services, e.g., for paying taxes or requesting housing support. This will relieve users from having to use their national identity cards for accessing those services. The CREDENTIAL wallet will further serve as a secure storage provider for authenticated data going beyond what is stored on an eID card. Now, if a user wants to authenticate using either CREDENTIAL or the national eID, he or she will be able to attach such data to the identity assertion issued by either identity provider and directly release it to the service provider. Special attention will be paid to the compatibility of our solutions also to existing cross-border authentication frameworks such as STORK or eIDAS.

eHealth

The eHealth pilot is developing a data sharing platform for patients, doctors, and further parties such as insurance companies, nursing personnel, or research institutions, in particular in the context of Type 2 Diabetes. Namely, the developed components will allow patients to record their health data (such as blood sugar level, weight, blood pressure, etc.) using external mobile devices. The data measured on those devices will be collected by a CREDENTIAL eHealth mobile app, which remotely stores this data into the CREDENTIAL wallet. The user can then define access rights to share specific parts of the measurements, e.g., with the family doctor, nutritionist, or personal trainer. Based on the data they see, they can then provide recommendations back to the user. Because of the confidentiality of medical data, it is of prime importance that only legitimate users are able to access the user's data. Furthermore, because of the potential consequences of wrong recommendations, the authenticity and integrity needs to be guaranteed.

eBusiness



This pilot showcases how easy the privacy offered by existing solutions can be enhanced by integrating libraries implementing CREDENTIAL's technologies. Encrypted mails are a requirement for many companies to protect their data and inventions, but they also represent a significant challenge when employees go on vacation. Currently, employees have to expose their private key material so that a substitute can still read and answer incoming mail. In contrast, with proxy re-encryption, an employee generates a re-encryption key for a substitute before leaving, with which the mail server is able to translate incoming mail during the absence.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653454.

CREDENTIAL

Secure Cloud Identity Wallet

You are what you keep!

Past Events

The CREDENTIAL consortium contributed to, and participated in, several events during the first project year. In the following we present the most relevant such events, and in particular those where CREDENTIAL contributed as a (co-)organizer.

5th Annual Cloud Security Alliance EMEA Congress

Madrid, Spain, November 15, 2016

Atos participated in the Cloudwatch2 Cloud Security Plugfest, an event organized by CloudWatch2 project (a European Cloud observatory supporting cloud policies, standard profiles & services) in cooperation with Cloud Security Alliance (CSA) and collocated with CSA EMEA Congress 2016 in Madrid. Atos represented CREDENTIAL at both events. The outcomes of both events are relevant to CREDENTIAL as they focus on gaining from the cloud research and industrial communities different perspectives, as well as on maximizing the adoption of and contribution to security standards in cloud projects and on addressing the current and coming changes in cloud security and privacy, where CREDENTIAL is enabling remarkable technological advances beyond the state of the art, with high potential for beneficial impact across Europe and beyond.

IPEN - Internet Privacy Engineering Network

Frankfurt, Germany, September 9, 2016

The 3rd IPEN Workshop took place on September 9, 2016 at the Goethe University of Frankfurt, Germany. IPEN was established in 2014 as a platform that brings together developers and data protection experts with a technical background from different areas in order to launch and support projects that build privacy into everyday tools and develop new tools which can effectively protect and enhance our privacy. The high-quality audience of this year's IPEN event was led by Achim Klabunde, head of IT Policy sector of the European Data Projection Supervisor (EDPS). Other participants included representatives from data protection authorities like ENISA and ULD, industry like Deutsche Telekom and signatu, as well as researchers. CREDENTIAL was one of two H2020 projects offering financial support to the non-profit organizers. In his presentation, Nicolás Notario presented the overall vision of CREDENTIAL as well as our approach towards privacy by design based on PRIPARE and LINDDUN methodologies, which was then followed by a brief discussion of the eHealth pilot scenario. The discussion points involved aspects like the sensitivity of different meta-data (e.g., who is allowed to access data, when is it actually accessed by whom, size and format of stored data, etc.) or the relevance of allowing multiple different accounts for the same user. Besides constructive feedback, no major objections concerning the privacy-approach of CREDENTIAL were raised from the present experts.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653454.

CREDENTIAL

Secure Cloud Identity Wallet

You are what you keep!

SECPID - International Workshop on Security, Privacy, and Identity Management in the Cloud
Salzburg, Austria, August 31, 2016

Together with our partner project PRISMACLOUD we organized at the SECPID ("International Workshop on Security, Privacy, and Identity Management in the Cloud") workshop at the 11th International Conference on Availability, Reliability and Security – ARES 2016. The workshop offered a platform to present visions and results of FP7 and H2020 projects. Besides contributions by the organizers, also presentations from SUNFISH, SAFECLOUD, and WITDOM were accepted. All papers accepted to SECPID are included in the official proceedings of ARES 2016. The audience of the workshop mainly consisted of the closer scientific community focusing on various aspects of security and privacy.

IFIP - 11th International IFIP Summer School on Privacy and Identity Management
Karlstad, Sweden, August 21–26, 2016

The event took place under the umbrella of the International Federation for Information Processing, the leading multinational, apolitical organization in ICT and related sciences. The summer school was attended by scientists at different stages of their career and with different backgrounds, e.g., cryptography and security, social sciences, usability, or law, as well as non-scientists such as the former chairperson of the European Pirate Party. In the course of the summer school, CREDENTIAL organized a workshop to present its vision and pilots, as well as to trigger a critical discussion on technical and privacy and usability related challenges, in order to identify challenges, potential obstacles, but also so far unrecognized opportunities of our approach.

1st CREDENTIAL User Advisory Board Meeting
Frankfurt, Germany, June 1, 2016

Right at the beginning of M09 we organized the first of two to three User Advisory Board meetings of CREDENTIAL. The purpose of the workshop was to discuss and get experts' feedback on use cases and technologies, to discuss about possible collaborations with other actions on the same topic, and about dissemination, exploitation, and standardization opportunities. Moreover, the consortium had the chance to exchange views with the external experts about the project's direction. While the discussions showed that many choices of the consortium are in line with the external experts' opinions, there were also vivid discussions, e.g., concerning the interoperability with existing authentication solutions (e.g., STORK), the precise trust model, business models and user-acceptance, or technical aspects like revocation or scalability.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653454.

CREDENTIAL

Secure Cloud Identity Wallet

You are what you keep!

Publications

The following list contains the findings and results of the first project year:

- David Derler, Stephan Krenn, and Daniel Slamanig. "Signer-Anonymous Designated-Verifier Redactable Signatures for Cloud-Based Data Sharing", in: CANS 2016, Milan/Italy, Springer.
- Felix Hörandner, Stephan Krenn, Andrea Migliavacca, Florian Thiemer, and Bernd Zwattendorfer. "CREDENTIAL: A Framework for Privacy-Preserving Cloud-Based Data Sharing", in: SECPID@ARES 2016, Salzburg/Austria, IEEE.
- Michael Till Beck, Stephan Krenn, Franz-Stefan Preiss, and Kai Samelin. "Practical Signing-Right Revocation", in: TRUST 2016, Vienna/Austria, Springer.
- Fatbardh Veseli and Jetzabel Serna. "Evaluation of Privacy-ABC Technologies - A Study on the Computational Efficiency", in: IFIPTM 2016, Darmstadt/Germany, Springer.
- Bernd Zwattendorfer and Daniel Slamanig. "The Austrian eID ecosystem in the public cloud: How to obtain privacy while preserving practicality", in: Journal on Information Security and Applications, Elsevier.
- Nicolás Notario, Stephan Krenn, Bernd Zwattendorfer, and Felix Hörandner. "CREDENTIAL: Secure Cloud Identity Wallet", in ERCIM News magazine nº 106, ISSN 0926-481.
- Bernd Zwattendorfer, Stephan Krenn, and Thomas Lorünser. "Secure and Privacy-Preserving Identity Management in the Cloud" in ERCIM News magazine nº 104, ISSN 0926-4981.

Future Events

- Cloud Security Expo http://www.cloudsecurityexpo.com/
  15 – 16 March 2017, Excel, London
- SECPID 2017 https://www.ares-conference.eu/conference/
  29 Aug – 2 Sep 2017, Calabria, Italy

Additional information about the CREDENTIAL project

Website: https://credential.eu
Twitter: https://twitter.com/CredentialH2020 | @CREDENTIALH2020
LinkedIn: https://www.linkedin.com/in/credential | CREDENTIAL Project
CORDIS: http://cordis.europa.eu/project/rcn/194869_en.html
Additional information can also be also requested via admin@credential.eu

Call: Digital Security: Cybersecurity, Privacy and Trust
Topic: DS-02-2014 Access Control
Type of Action: Innovation Action
Duration: 36 months
Start Date: 01.10.2015
Requested EU Contribution: ~6.0M €
Coordinator: AIT Austrian Institute of Technology GmbH

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653454.