



CREDENTIAL

Secure Cloud Identity Wallet







CREDENTIAL Research Project



Call: H2020-DS-2014-1 Acronym: CREDENTIAL Type of Action: IA Number: 653454 Partners: 12 Duration: 36 months Start Date: 10/2015 Estimated Project Cost: approx. Requested EU Contribution: ap



Estimated Project Cost: approx. 6.5M Euro Requested EU Contribution: approx. 6M Euro Coordinator: Austrian Institute of Technology GmbH Technical Coordinator: Graz University of Technology



Agenda

IAIK

- Challenges for Cloud Identity Management
- (Security) Objectives
- Approach / Methodology
- Innovation
- Demonstration (Pilots)





R

- **Challenges for Cloud Identity Management**
 - Identity and access management (IAM) towards cloud steadily growing
 - For private sector already a big market
 - Facebook, Google, Microsoft, Salesforce, ...
 - Public sector more reserved
 - Legal regulations, e-Government data protection standards
 - Identity data is a critical information asset
 - Data accessible by cloud service provider
 - Owner not in full control of data
 - E2E encryption for cloud identity data needed



Security objectives / goals

- Guarantee that **identity data** in the cloud **maintains confidentiality**, integrity and authenticity;
- **Data** can be **re-encrypted but not be accessed** by the cloud identity provider hosting the data;
- Users shall have **fine-grained control** over the release and transfer of their identity data;
- Reveal minimum information about users (data minimisation);
- Protected identity data may only be accessed through strong authentication mechanisms;
- **User-friendliness** shall be ensured without lowering security requirements.



IIAIK

5



Approach

ΙΑΙΚ

6

Develop an architecture for secure and user-friendly cloud identity data access management

- Confidentiality / Authenticity
 - Securely store and process identity data in the cloud
 - Proxy Re-Encryption, Signature schemes (authenticity)
 - *"Honest but curious"* cloud service provider
 - Selective disclosure
- Strong authentication
 - Strong authentication towards the cloud
 - Bind authentication to identity data decryption
 - Federation / FIDO (UAF, U2F), HW-based authentication



Approach (2)

ΠΑΙΚ

Make it available, usable and push it to market-readiness

- Security by design / Holistic security model
 - Enhance existing protocols
 - Verification of identity data processing
- Human centered design approach
 - Consistent user experience
- Seamless integration

Pilot, test, evaluate and make it economically relevant

- Evaluate the technology in three pilot areas
- Standardization
- New business models for cloud identity management



Innovation



ΠΑΙΚ

8

The main idea and ambition of CREDENTIAL is to enable end-to-end security and improved privacy in cloud identity management services for managing secure access control. This is achieved by advancing novel cryptographic technologies and improving strong authentication mechanisms.

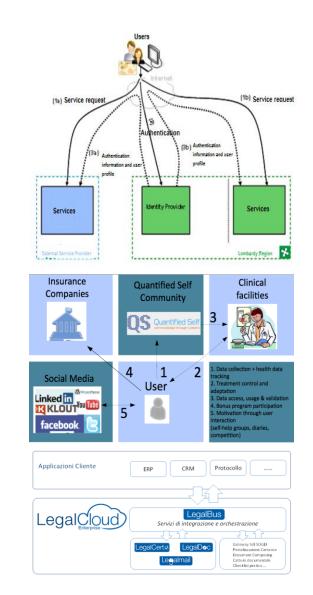
- Advance novel cryptography to enable advanced trust models
- Strong authentication to the cloud
- Holistic privacy models and methods for user protection and secure data sharing
- Dedicated usability and HCI models for wide user adoption and maximum impact
- Secure, efficient and portable implementation of components and protocols
- Piloting and testing on a European scale



Demonstration

e-Government pilot

- Italy Lombardy Region SP for public administration
- Wallet for employees and citizens
- e-Health pilot
- German partners
- Quantified self / Medical patient data store
- e-Business pilot
- InfoCert LegalCloud trust services
- Cloud identity provider for public and private sector







www.iaik.tugraz.at



Contact



ΙΑΙΚ

11

Technical coordinator:

Dr. Arne Tauber

Arne.Tauber@iaik.tugraz.at

Project coordinator: Thomas Lorünser <u>Thomas.loruenser@ait.ac.at</u>

LinkedIn: https://at.linkedin.com/pub/credential-project/b5/a6/92



IIAIK 12

Project overall goals vs. results



O1 - Adapt and improve cryptographic methods to securely store and share iden-**Objectives** tity data in the cloud

O2 - Protect access to identity data with strong authentication mechanisms

O3 - Development of a userfriendly and portable system for identity data access and management

O4 - Creation of enabling technologies for cloud service providers and identity data consumers

O5 - Transfer of project results into market-ready identity management technologies and standards

Novel efficient cryto-R1 graphic protocols and solutions for privacy preserving cloud based IAM services

R2 - Strong authentication methods which are highly portable and can be broadly integrated into existing systems and devices

R3 - Secure by design architecture for secure IDMaaS and specs. for interoperability and integration

R4 - Market-ready, secure, efficient and portable implementation of generic components

R5 - Extensive evaluation and testing results as well as standards and deployment guides

ഗ Result REDENTIA

()

DENTIAL

CRE