

# METADATA

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

Coordinator: AIT Austrian Institute of Technology

Grant Agreement No: 653454



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

**AIT**  
AUSTRIAN INSTITUTE  
OF TECHNOLOGY

**Atos**

**Fraunhofer**  
FOKUS

**GOETHE**  
UNIVERSITÄT  
FRANKFURT AM MAIN

**TU**  
Graz

**OTE**

**InfoCert**  
TECNOINVESTIMENTI GROUP



**klughammer**

**LOMBARDIA INFORMATICA**

**sic**



@credentialH2020



CREDENTIAL Project



<https://credential.eu>



admin@credential.eu, AIT Austrian Institute of Technology GmbH

# — CREDENTIAL

Secure Cloud Identity Wallet



— You are what you keep!

---

# VISION

CREDENTIAL is an EU funded research project developing, testing, and showcasing innovative cloud-based services for storing, managing, and sharing digital identity information and other highly critical personal data with a demonstrably higher level of security than other current solutions.

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.

CREDENTIAL lets you keep

your personal information secret

control about your data and what is revealed

your data available for ubiquitous access

your identity protected from others

# OBJECTIVES



## **Adaption and improvement of cryptographic methods to securely store and share identity data in the cloud**

- protection of confidentiality, integrity, and authenticity of identity data
- mechanisms to efficiently re-encrypt and share encrypted data
- give users full control over their identity data
- protection of users' privacy beyond encryption



## **Protection of access to identity data with strong authentication mechanisms**

- use secure authentication to the cloud
- bind credentials and data to the identity
- back multi-factor authentication schemes by hardware
- support increased portability and bootstrapping methods



## **Development of a user-friendly and portable system for identity data access and management**

- new open architecture based on security by design principles
- holistic security model compatible with existing standardized approaches
- user-friendly system based on a human-centered approach
- allow for seamless integration in existing solutions



## **Creation of enabling technologies for cloud service providers and identity data consumers**

- protocol integration for interoperability and portability
- secure and efficient commercial grade software implementation
- hardware support for cloud infrastructures and clients
- high-quality development processes



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

- business models and exploitation opportunities
- European scale pilot
- demonstrate methods' capabilities and tools developed
- development of standards and guidelines for secure IAM deployment in the cloud

# EXPECTED RESULTS



## **Novel efficient cryptography to enable advanced trust models in the cloud**

- methods to treat identity data in the cloud in encrypted format only
- application of efficient proxy cryptography concepts for eID solutions
- enable cloud provider to process identity data without accessing it



## **Methods for strong authentication to the cloud**

- protocols for a merged processes of authentication and decryption to one single process of equal strength
- a boost for the use of stronger authentication mechanisms



## **Holistic privacy models for user protection and secure data sharing**

- integration of privacy features such as selective and minimal attribute disclosure into eID solutions
- application of new approach based on redactable and sanitizable signatures to realize data minimization concepts



## **Dedicated usability and HCI models for wide user adoption and maximum impact**

- novel HCI guidelines including HCI design patterns
- improve the usability of strong authentication mechanisms.



## **Secure, efficient, and portable implementations of components and protocols**

- improvement of existing standards in the field of identification and authentication protocols
- secure, efficient, and portable privacy-preserving identity management system



## **Piloting and testing on a European scale**

- an open and flexible cloud identity wallet architecture to easily connect to other identity management systems
- application of the developed tools in a European scale pilot