CREDENTIAL

Secure Cloud Identity Wallet

You are what you keep!

Secure Identity Services within the Cloud

Alexandros Kostopoulos, Ph.D., and Mr. Evangelos Sfakianakis, M.Sc.

Research Programs Section Fixed

Research and Development Department, Fixed & Mobile

Technology Strategy & Core Network Division, Fixed & Mobile

Hellenic Telecommunications Organization (OTE S.A.)

infocom world | infocom media

Athens, Greece _ October 25, 2017

OTE GROUP OF COMPANIES

Motivation

- In traditional IDMaaS systems **an IdP has full access to the user's identity data.**
- The shift of such services into the cloud **discloses sensible user data** to the cloud provider.
- **User's privacy is compromised**, and legal issues and challenges for service providers may arise.
- Invention of *proxy-re-encryption* and *redactable signature algorithms* → **outsource an IdP into a cloud environment without disclosing the processed data to the cloud provider.**

➢ ***Novel cryptographic technologies*, but *not yet included in market-ready products.***

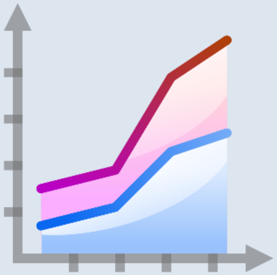
Challenges for Cloud IdM

➢ **IAM towards cloud steadily growing**

- ✓ *MarketsandMarkets:* USD 5.13 billion (*2013*) to USD 10.39 billion (*2015*)
- ✓ *Gartner:* IDMaaS on of the top 3 most sought after services (*2014*)
- ✓ *Forrester:* USD 2.6 billion (*2006*) to USD 12.3 billion (*2014*)

○ **For private sector already a big market**

- *Facebook*, *Google*, Microsoft, …



○ **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

Goal

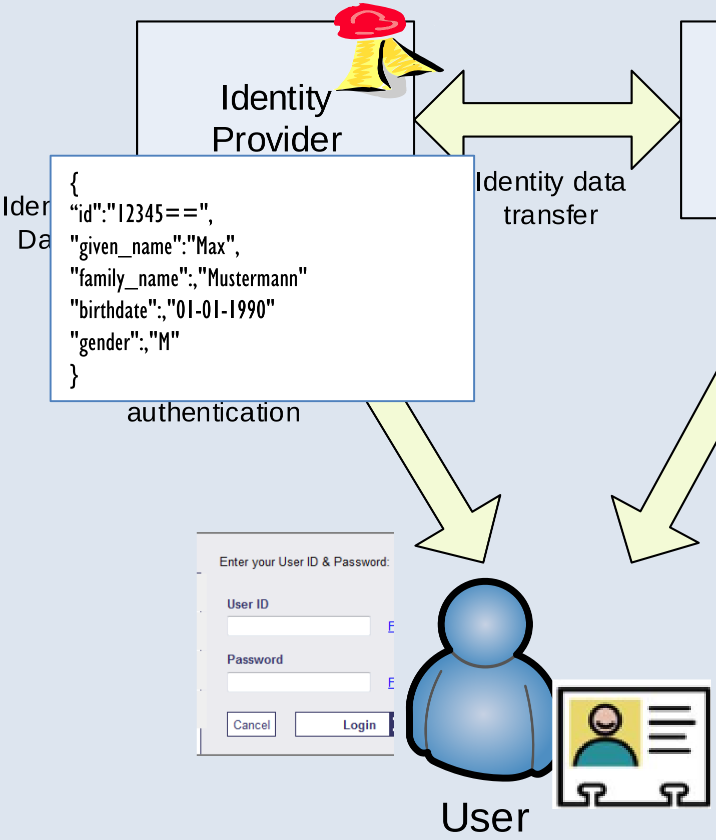
- *Create a data-sharing and IAM platform in the cloud, which increases the security and privacy level compared to already existing solutions by using cryptographic primitives*.

□ Main features & benefits offered

- **Store and view** personal data in the wallet
- **Share** personal data with other participants
- **Using** Wallet as IAM system for accessing other services
- **Hide** information in documents to other participants **while still guaranteeing** the authenticity of the revealed data
- ✓ **Increased flexibility**
- ✓ **High security & strong authenticity guarantees**

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.

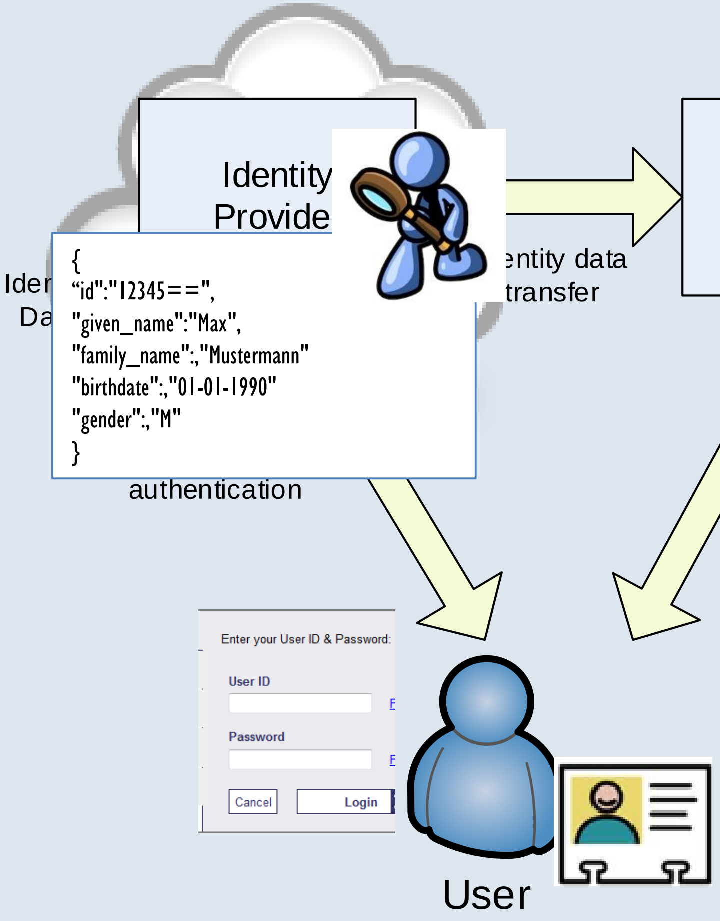
SOTA: Identity Management



```
{
“id":"12345==",
"given_name":"Max",
"family_name":,"Mustermann"
"birthdate":,"01-01-1990"
"gender":,"M"
}
```

- **Service Provider (SP)**
  - provides different online services to users
- **Identity Provider (IdP)**
  - handles identification and authentication of users for the SP
- **User**
  - wants to access protected service at SP that requires authentication

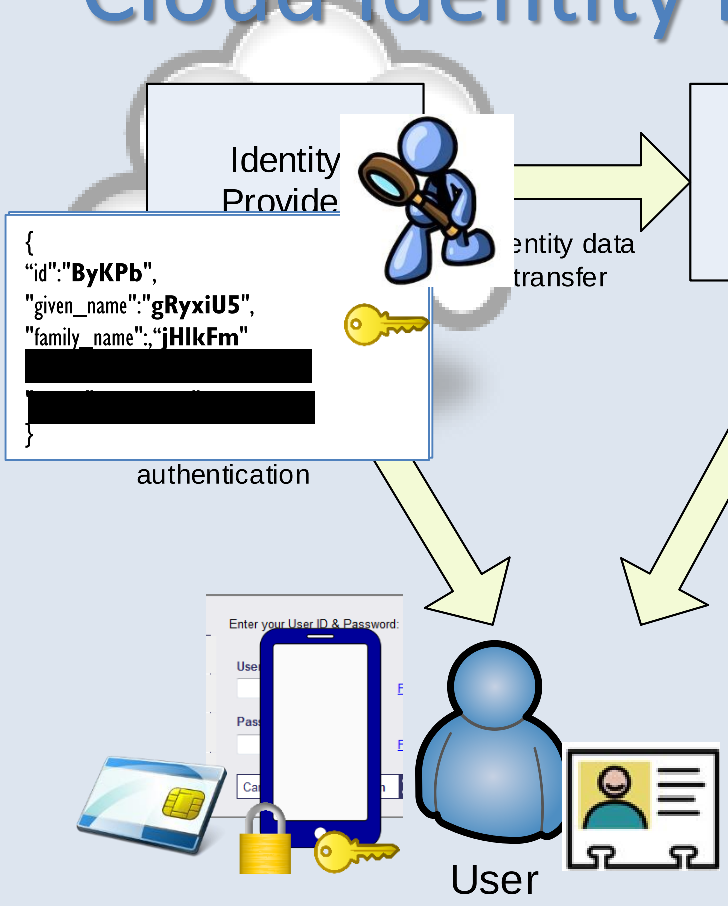
SOTA: Cloud Identity Management



```
{
"id":"12345==",
"given_name":"Max",
"family_name":,"Mustermann"
"birthdate":,"01-01-1990"
"gender":,"M"
}
```

- **Service Provider (SP)**
  - provides different online services to users
- **Identity Provider (IdP)**
  - handles identification and authentication of users for the SP
- **User**
  - wants to access protected service at SP that requires authentication
- **Advantages:**
  - Scalability, Elasticity, Cost Effectiveness…
- **Disadvantages:**
  - Privacy

CREDENTIAL: Cloud Identity Management



```
{
"id":"ByKPb",
"given_name":"gRyxiU5",
"family_name":"jHIkFm"
[redacted]
}
```

- **Service Provider (SP)**
  - provides different online services to users
- **Identity Provider (IdP)**
  - handles identification and authentication of users for the SP
- **User**
  - wants to access protected service at SP that requires authentication
- **Advantages:**
  - Scalability, Elasticity, Cost Effectiveness…
  - **Privacy**
  - **Strong Authentication**

Technological Context

- **Encrypted identity data**
  - Encrypt data in a way that we can selectively reveal parts of it to different service providers
  - Identity provider should learn none of the attributes (identity data)
  - Apply proxy re-encryption

- **Malleable signatures**
  - Identity provider should be able to verify that attributes are authentic
  - When using conventional signature schemes removing attributes invalidates the signature
  - Apply malleable signatures (e.g., redactable signatures)

- **Strong HW-*based* authentication mechanisms**
  - Two-Factor authentication instead of username/password
  - Inclusion of strong hardware-based approaches incorporated in client devices

CREDENTIAL Ecosystem

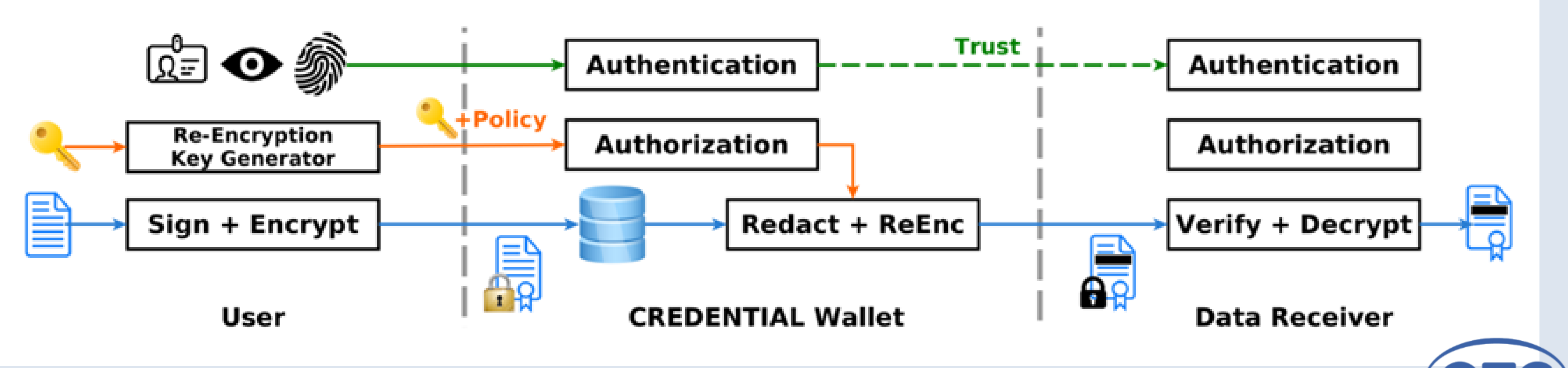
- **CREDENTIAL Wallet:**
  - **Stores** user data and identity data in a secure cloud.
  - A cloud platform **enabling** others sharing user data with other participants or service provider, in a secure way and preserving user privacy.
  - **Comprises** an IAM system, **performing** authentication and **providing** authorization to access those data.

***Main advantages*:**

- ✓ Proxy re-encryption system does not expose plain data.
  - → ***data confidentiality***
- ✓ Once a re-encryption key is available for some specific set of data as specified by the user, *these data can be shared with specified receivers even if the user or his/her client application are not available.*

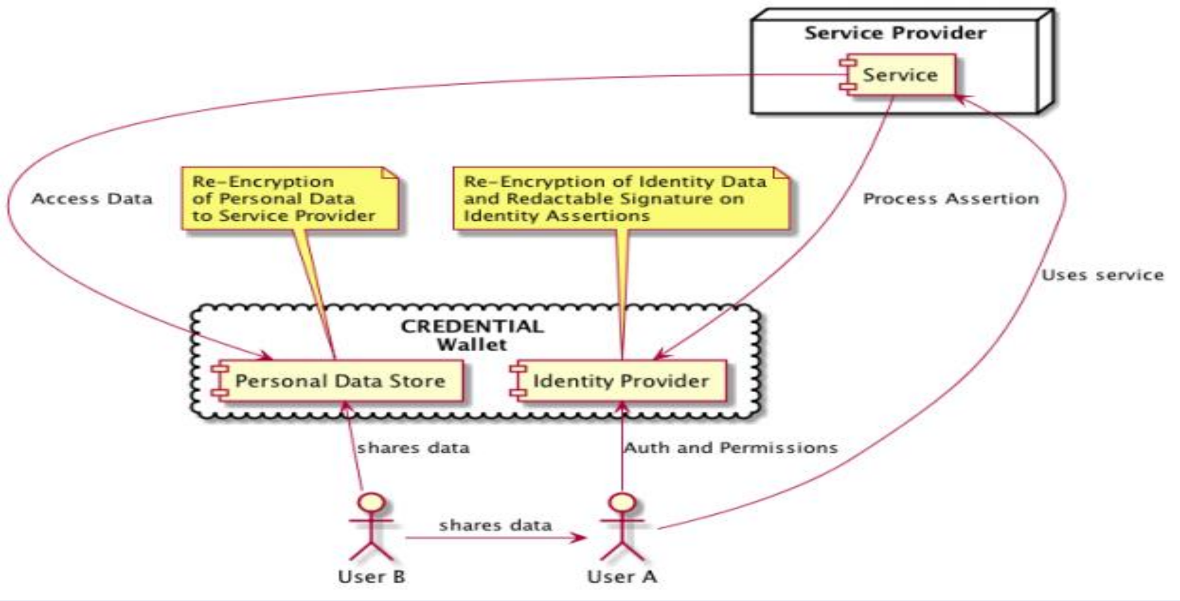
CREDENTIAL Ecosystem *(cont.)*

- An **external Identity Provider** can be embedded to offer authentication functionality for end-users.
- The **end-user**
  - **owns** data securely stored or shared with other account-holders
  - **has** the absolute control over the data flow of his/her personal and sensitive data
  - a *client application* **handles** cryptographic operations involving the user's private key
- The **data receiver** reaches data stored in or authentication assertions and can perform arbitrary data processing
  - *another CREDENTIAL user*
  - or a *service provider*



CREDENTIAL Ecosystem *(cont.)*

- A *user* can **store any personal information** safely in the cloud and **decide to share** such information with other users by providing a *forward rule* in the Wallet.
- The *other user* is able to **read the data without** any more user **interaction from data owner**, because the *wallet can process the forward rule*. Since the data is encrypted, the wallet has to **re-encrypt** the data for the other user. Thus, the **data** is **never disclosed** for the wallet provider by design.
- Users can also **share** their **data with service providers**.



Data Sharing Process

1. The user **authenticates** at the Wallet **to get read and write permission** to her Wallet account, which are used to upload signed and encrypted data.

2. To later **share** this **data**, the user **generates a re-encryption key** towards a selected data receiver in her trusted domain. Along with this key, the user **defines a policy** *defining which data may be disclosed to which entity* and **installs it at the Wallet**.

3. When an authorized receiver tries to access the user's data, **not required parts are redacted** and the **remaining parts are transformed** into cipher-text for the data receiver **by using the re-encryption key**.

4. Finally, the data receiver is able to **decrypt the data and verify the signature** on the disclosed parts.

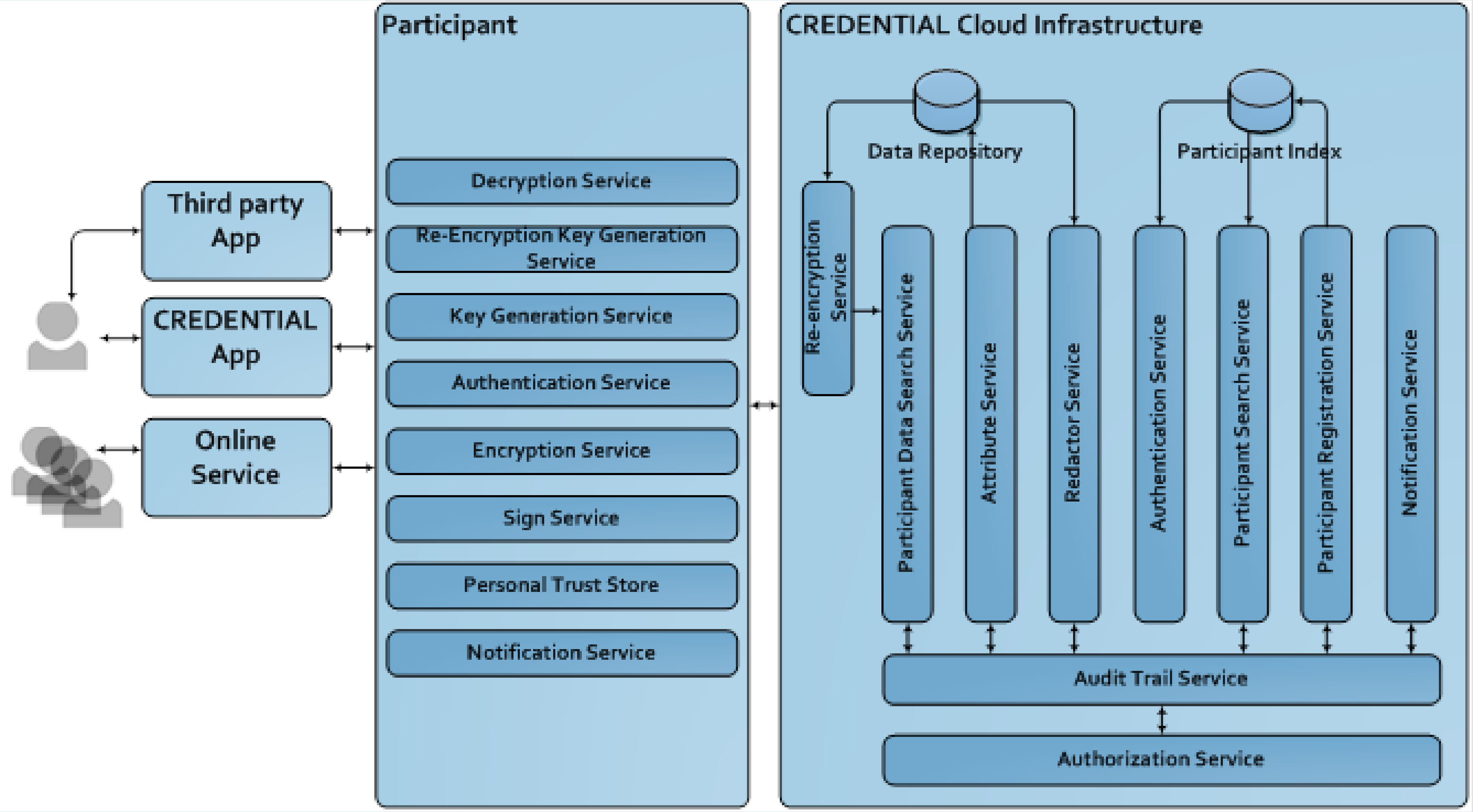
Functionalities

- **Account Management**
  - **Enabling users to create a new account** that involves the creation of its proxy-re-encryption enabled key material and an account association on the CREDENTIAL Wallet.
  - **Users can perform various management functionalities** *(e.g., showing an activity protocol on its data or delegate access rights to its data).*
- **Identity Management**
  - **Integrating identity data stored within the CREDENTIAL Wallet in the authentication mechanisms towards other service providers.**
  - **Securely sharing the identity data** in the CREDENTIAL Wallet.
- **Data Sharing**
  - **Storing, reading, sharing of user data** that is assigned to the CREDENTIAL Wallet.

Services

- ✓ **Cryptographic Services:** Related to the management of cryptographic material and its usage to protect data.
- ✓ **Data Management:** Management of the data and the policies to access it.
- ✓ **Account and Identity Management Services:** Credentials, accounts and identity and attributes management.
  - o *Account management:* Handling the life-cycle of CREDENTIAL accounts.
  - o *Access management:* Controlling the access to the users' data by managing and evaluating requests against user-defined policies.
- ✓ **Auditing & Notification:**
  - o *Auditing:* Stores information regarding attempted access and authorizations to access stakeholders' data, in compliance with current legislation framework and privacy requirements.
  - o *Notification:* Recognizing events happening on the CREDENTIAL Wallet and notifying users according to their preferences (*customize notification settings*)s

Services *(cont.)*



Conclusions & Future Work

- ✓ **Main functionalities of the CREDENTIAL system, as well as the overall logical and physical architecture, to provide a *privacy-preserving data sharing platform*.**

Future work:

- ➢ **Functionality and added-value services** will be showcased by concrete pilots from the domains *of eGovernment*, *eHealth*, and *eBusiness (currently under deployment).*
- ➢ **Further elaboration on mapping CREDENTIAL features into acceptance factors** to explain *how the technology is perceived*.

Thank you very much for your attention!

Dr. Alexandros KOSTOPOULOS

Research Programs Section, Fixed

Research and Development Department, Fixed & Mobile
Technology Strategy & Core Network Division, Fixed & Mobile

Hellenic Telecommunications Organization S.A. (OTE)

1, Pelika & Spartis Street
15122 Maroussi-Athens,
Greece

Tel.:   +30-210-6114671
Fax: +30-210-6114650

E-Mail: alexkosto@oteresearch.gr