UNIVERSITAT ROVIRA i VIRGILI

PRESENTATION ON
U-PROVE
&
IDEMIX

Francisco Javier Rodrigo Ginés

MESIIA – Privacy Protection

Index

1. Introduction

- Organizations are increasingly looking to securely identify individuals who access their services, both online and offline.
- More and more they also seek to learn other identity-related information about individuals that is held by other organizations.
- This authentication need are driven by cost and efficiency considerations, by new business models, and by the rise of phishing, identity theft, and other security threats.
- This need leads us to attribute-based credentials technologies.

1. Introduction

- "*ABCs allow a user (prover) to securely and privately prove ownership of an attribute to a service provider (verifier). Attributes are stored in credentials, which are similar to certificates of attributes issued by one or more authorities.*"
- For example: the government is an authority trusted for age and nationality.
- Both U-Prove and IDEMIX are attribute-based credentials (ABCs).

1. Introduction

- There are two main strategies of developing ABCs: Using credentials only once or using the credentials multiple times.
- In using the credentials only one time strategy, the provers request a new credential with the same set of attributes each time they want to reveal an attribute from the credential. U-PROVE is an ABC that only use credentials once.
- In the multi-use strategy, the provers uses zero-knowledge proofs (ZKPs), so they can prove the possession of an attribute without revealing it. IDEMIX is an ABC that use multi-use credentials.

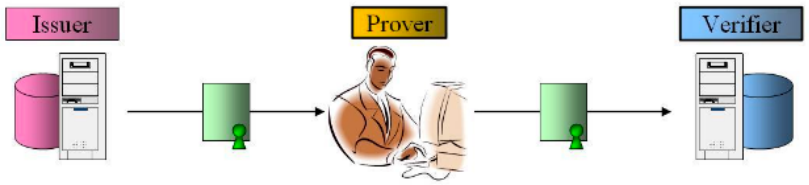
2. U-Prove

- U-Prove is a digital attribute-based credential technology originally developed by Credentica and later acquired by Microsoft in 2008.

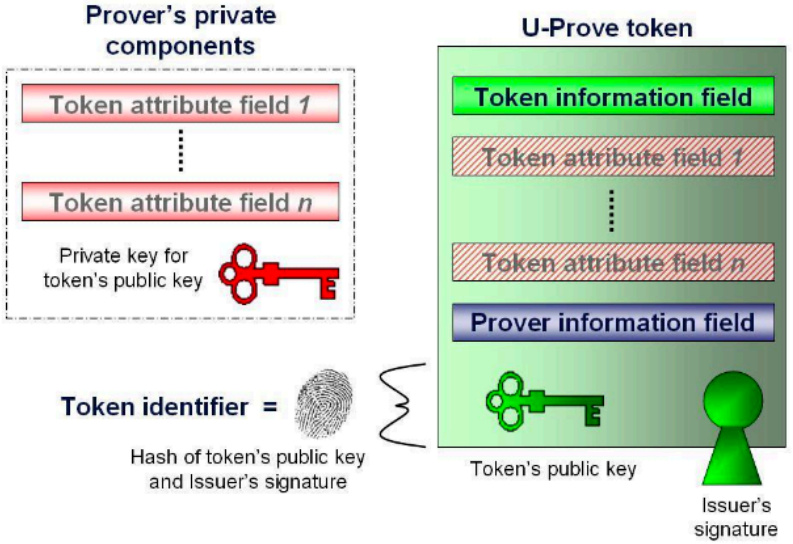
- U-Prove is based on the U-Prove token. This token is the collection of attributes cryptographically protected (by public-key cryptography). It is issued by an authoritative source to a user via an issuance protocol.

- Because a U-Prove token is just a binary string it can be issued and presented over any electronic network. To perform the U-Prove protocols, all participants require computing devices that function on their behalf.

2. U-Prove



U-Prove issuance and presentation protocols

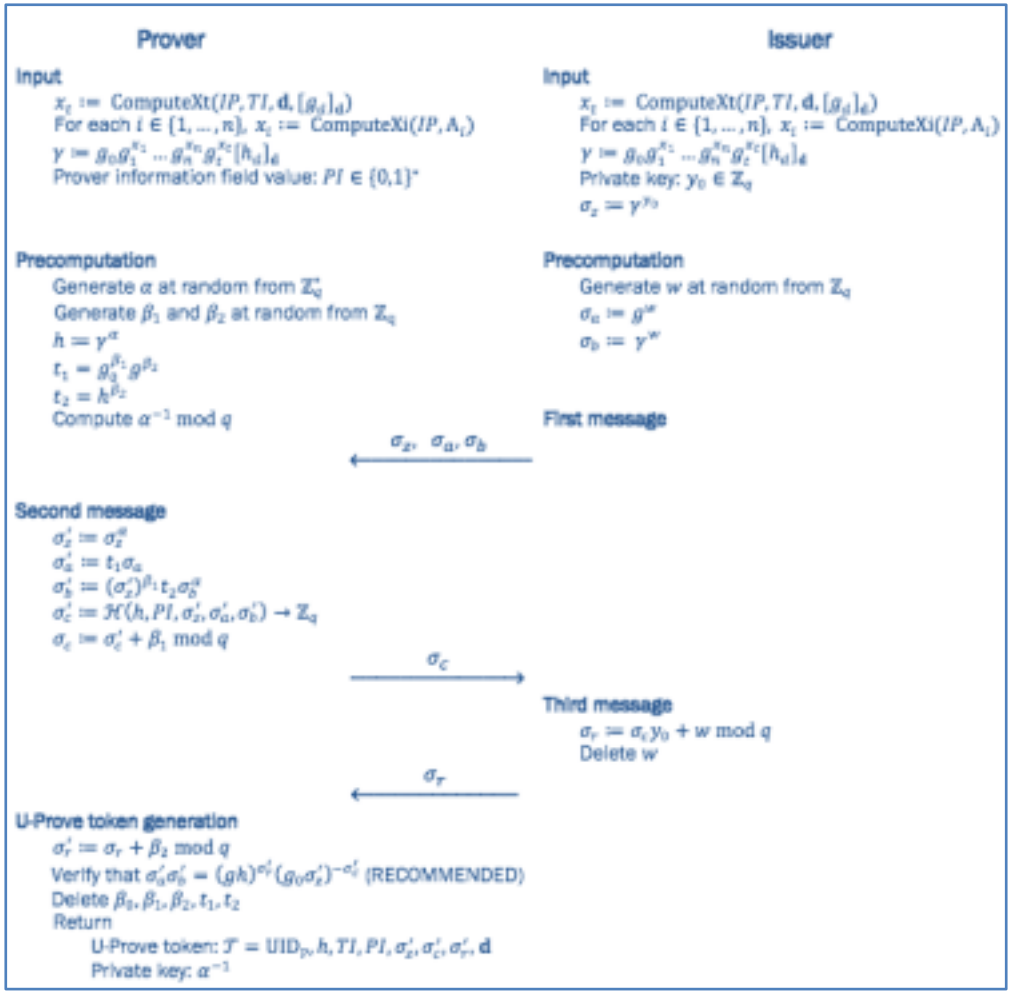


Structure of an U-Prove token

2. U-Prove

- A prover, in order of getting an U-Prove token, must engage along with the issuer in the U-Prove issuance protocol. This protocol takes the attributes as input in order of encoding it.

- This issuance protocol is a three-leg interactive protocol that enables the prover to hide some of the attributes from the issuer.



Issuance protocol

2. U-Prove

- The U-Prove issuance protocol allows the issuer to protect the tokens against unauthorized manipulations.

- The protocol ensure that two basic protections are always in place:

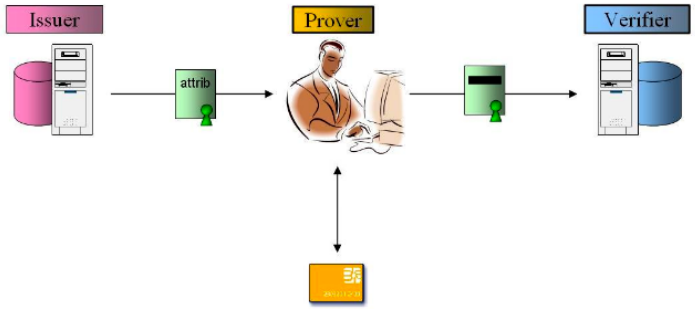
- **Integrity and source authenticity**: Each issued U-Prove token contains an unforgeable digital signature of the issuer using its private key. It enables anyone to verify that the U-Prove token was issued by the issuer and that its contents have not been altered.

- **Replay attack prevention**: Each issued U-Prove token also contains a public key that is known only to the prover. The prover randomly generates it during the issuance protocol, together with the corresponding private key for the U-Prove token. This private key is not part of the U-Prove token.

2. U-Prove

- Optionally, an Issuer can issue tokens to a prover so the private key of each U-Prove token is split between the prover's own device and a trusted device. The resulting U-Prove tokens cannot be used without the assistance of the trusted device.

- This trusted device can be a tamper-resistant computing device (such as a smart card or a USB key with a CPU), a tamper-resistant chip (such as a TPM), a software-only emulation, a mobile smartphone, or an on-line service.



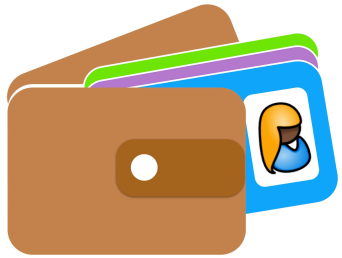
Device-protected U-Prove token

2. U-Prove

- Status of deployment (according to a report published in 2010):

- *" Microsoft on Tuesday released a community technology preview (CTP) of its U-Prove cryptographic tech, and opened up its patented crypto algorithms under the company's Open Specification Promise (OSP). The Redmond software maker also open sourced two SDKs (C# and Java editions) under the Free BSD license for integrating U-Prove into open-source identity selectors. The release will be accompanied by preview code integrating U-Prove with ActiveDirectory Federation Services v2, Windows CardSpace v2 and Windows Identity. "*

3. IDEMIX



- Identity Mixer (IDEMIX) is a digital attribute-based credential technology developed by IBM.

- Identity Mixer works in a similar way as a classical PKI but with two main differences:

- **The public keys are flexible:** Provers can have many independent public keys, called pseudonyms, for the same secret key.

- **Credentials are also flexible:** The credentials that certify the prover's attributes can be transformed into valid tokens for any of the prover's pseudonyms.

3. IDEMIX

- IDEMIX' elements:

- The **prover,** he/she gets the credentials from issuers and controls which attribute is revealed.

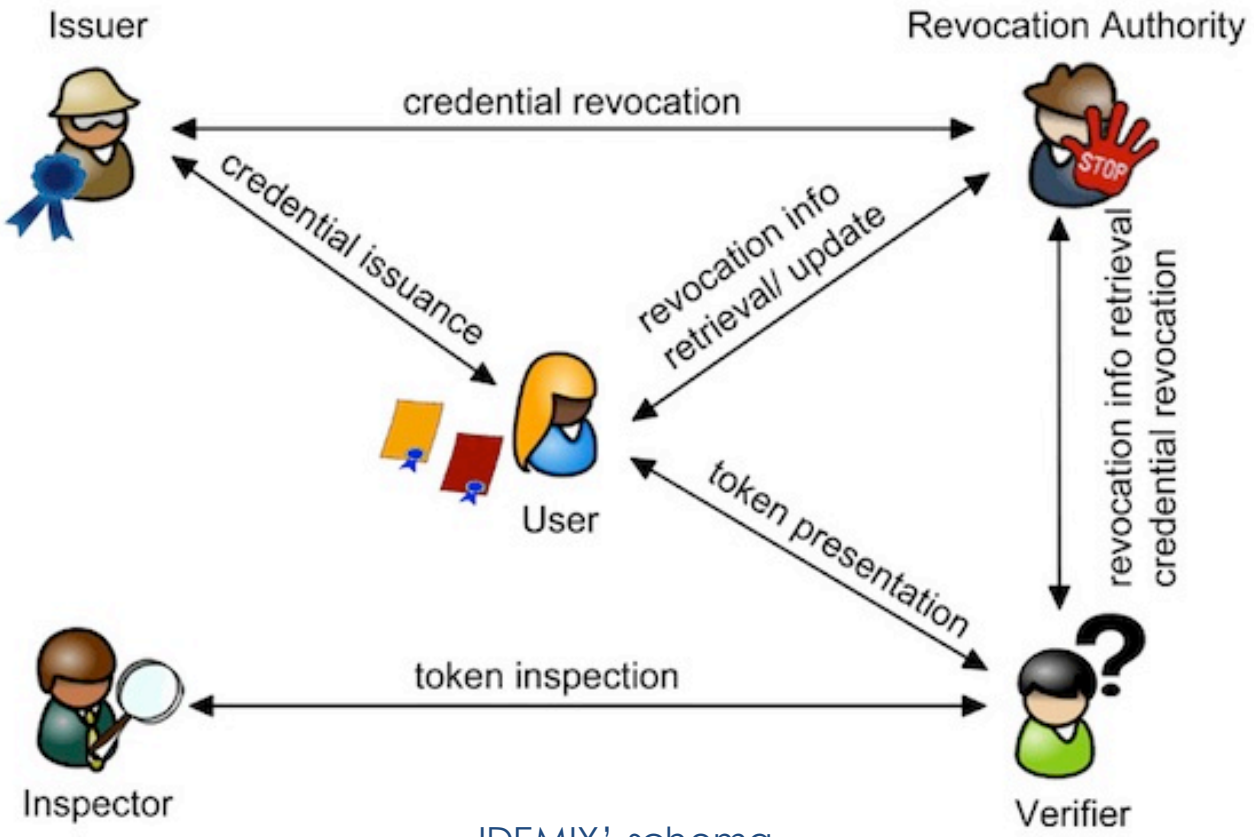
- The **issuer** creates credentials and gives them to provers. An issuer generates a secret issuance key and publishes the corresponding public verification key.

- A **verifier** protects access to a resource or service that a prover wants to get.

- A **revocation authority** (optional) is responsible for revoking issued credentials, so that these credentials can no longer be used.

- An **inspector** (optional) is a trusted authority who can de-anonymize presentation tokens under specific circumstances.

3. IDEMIX



IDEMIX' schema

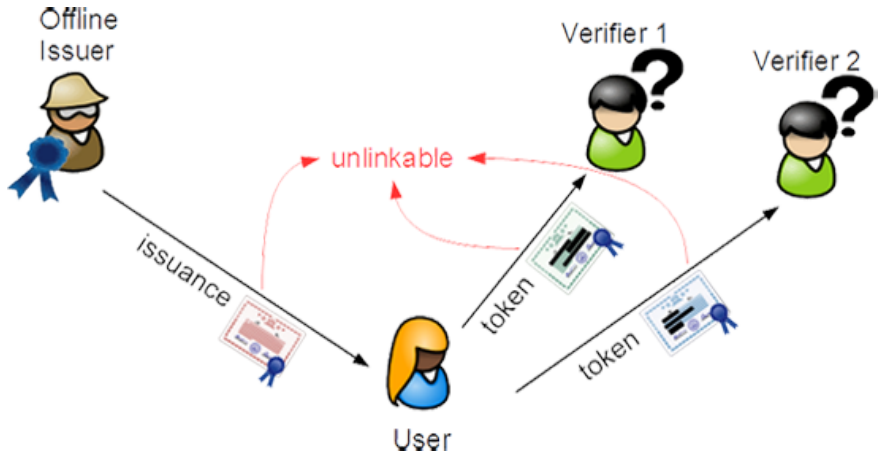
3. IDEMIX

- In IDEMIX, a credential is a CL signature by the issuer on the user's secret key and on the attribute values. The only way of transforming the credential into a token is that the user creates a zero-knowledge proof showing that he knows a valid CL signature on the attribute values.

- For creating a token, the user encrypts an attribute with the public key of the inspector, so only that inspector can decrypt it.

3. IDEMIX

- Identity Mixer offers a solution that U-Prove can't give: Issuers can be offline during authentication, but at the same time, users can reveal only those attributes that are required by the verifier and can do it privately and without being linkable across other transactions.



IDEMIX' Issuance protocol

3. IDEMIX

- Status of deployment (according its web):

- *" An open-source reference implementation of IBM Identity Mixer is freely available for commercial and non-commercial use. The Privacy-ABC Engine language framework acts as an abstraction layer on top of the cryptographic routines of IBM Identity Mixer and Microsoft U-Prove, allowing application developers to use the technology without needing to understand the cryptographic details. It is available from GitHub under an Apache 2.0 license. The core cryptographic routines are published separately under a proprietary license that allows commercial as well as non-commercial use. "*

4. Conclusions

- U-Prove is highly efficient, IDEMIX is more complex and so, les efficient.
- In U-Prove the proves must be online in order of obtaining new credentials, in IDEMIX proves can use the credentials multiple times online and offline.
- In U-Prove proves may reveal some of its attributes, this doesn't happen in IDEMIX.
- The difference between these two technologies allows you to choose the technology that fit better for your project.

5. Bibliography

- Course slides, pages 37 – 50.
- Wikipedia: U-PROVE
- Microsoft research: U-PROVE
- Pomcor: Pros and cons of U-PROVE for NSTIC
- IBM research: Identity Mixer (IDEMIX)
- Identity Mixer (IDEMIX)
- Pomcor: Pros and cons of IDEMIX for NSTIC

Links checked on March 7th

Any question