

Anonymous k -show Credentials

Mohamed Layouni Hans Vangheluwe

School of Computer Science, McGill University, Canada

Fourth European PKI Workshop: Theory and Practice
June 2007

Anonymous Credentials: High-level Overview

- Assertions made by some Certification Authority about the identity (attributes) of a user
- These assertions are embedded in a digital token
- The embedded information can be selectively disclosed by the credential holder (unlike X.509 certificates). E.g., subset disclosure, Boolean predicates, interval proofs...
- Additional properties such as unlinkability and untraceability...

General workflow & parties involved

- Three parties :
 - An Issuer (Certification Authority)
 - A User (credential holder)
 - A Verifier
- Workflow :
 - The CA issues a credential to the User (Issuing protocol)
 - The User shows¹ his credential to a verifier (Showing protocol)
 - Optionally, the Verifier deposits the showing transcript back at the CA.

¹Showing = proving token validity + predicates on embedded attributes w/o necessarily disclosing actual values.

Setting up the context

Properties of interest

Security properties

- Unforgeability (of tokens, showing transcripts)
- Framing-resistance (wrt. to showing)
- Revocability etc.

Privacy properties

- Selective disclosure
- Untraceability. Is a token untraceable?
- Unlinkability. Are multiple tokens unlinkable?
- Multi-show Unlinkability for one token?
- Multi-show Untraceability
- ...

The case of Idemix

Security & Privacy properties

- Unforgeability ✓
- Framing-resistance ✓
- Revocability ✓

Privacy properties

- Selective disclosure ✓
- Unlinkability. Are multiple tokens unlinkable? ✓
- Multi-show Unlinkability/untraceability for one token?
 - One-show untraceable
 - ∞ -show unlinkable/untraceable with Revocability

This work...

proposes a **k -show untraceable** version of the Idemix credentials (for $k > 1$):

- k -show credentials can be spent k times without being linked to the instance of the issuing protocol that generated them, or to the identity of their owner.
- The identity of the owner is revealed only if the credential is spent more than k times.

Setting up the context

Outline

- 1 Introduction
- 2 Overview of the Idemix credentials
- 3 The proposed k -show credentials
- 4 Conclusion

System parameters

- Each Issuing organization O chooses a safe prime product modulus n_O and keeps the factorization secret.
- O also chooses random elements $a_O, b_O, d_O, g_O, h_O, v_O, z_O \in QR_{n_O}$ and publishes them along with n_O .
- Each User U has a secret master key x_U .
- Each User U has a local secret key $x_{(U,O)}$ associated with each organization O .

Assumptions

- Strong RSA assumption (in $\mathbb{Z}_{n_O}^*$)
- Discrete Logarithm assumption (in QR_{n_O})

Establishing a pseudonym

U obtains a pseudonym $N_{(U,O)}$ and a validating tag $P_{(U,O)}$, s.t.,

$$P_{(U,O)} := a_O^{x_U} b_O^{s_{(U,O)}} z_O^{t_{(U,O)}}$$

where $s_{(U,O)}$ and $t_{(U,O)}$ are jointly chosen at random by O and U, but known only to U.

Credential Issuing

- 1 U shows valid $(N_{(U,O)}, P_{(U,O)})$ to O, and proves its well-formedness
- 2 O issues to U a credential pair $(c_{(U,O)}, e_{(U,O)})$, s.t.,

$$c_{(U,O)}^{e_{(U,O)}} = P_{(U,O)} d_O \pmod{n_O}, \text{ for prime } e_{(U,O)}$$

Credential Showing (one-time show mode)

User U

Public Info

Organization O

$$n_O, \{a_O, b_O, d_O, g_O, h_O, v_O, z_O\} \in QR_{n_O}$$

$$r_1, r_2 \in_R \{0, 1\}^{2\ell_n}$$

$$A := c_{(U,O)} h_O^{r_1}$$

$$B := h_O^{r_1} g_O^{r_2}$$

$$H_{(u,O)} := h_O^{t_{(u,O)}}$$

$$\xrightarrow{A, B, H_{(u,O)}}$$

SPK $\{A, B, H_{(u,O)}\}$ well-formed &
 A corresponds to a certificate issued by O

- Multiple showings detected through $H_{(u,O)}$
- Verifiable encryption of x_U at time of issuing, allows for abuser identification by the Revocation Manager.

Establishing a pseudonym (with local & global revocability)

User U

Public Info

Organization O

$$n_O, \{a_O, b_O, d_O, g_O, h_O, v_O, z_O\} \in QR_{n_O}$$

jointly choose $N_{(U,O)}, s_{(1,U,O)}, t_{(U,O)}$

$$P_{(U,O)} := a_O^{x_U} b_O^{s_{(1,U,O)}} z_O^{t_{(U,O)}} v_O^{x_{(U,O)}}$$

$$Y_{(U,O)} := g^{x_{(U,O)}}$$

$$Y_U := g^{x_U} \text{ (if } O=\text{Revocation Manager)}$$

SPK{ $P_{(U,O)}, Y_{(U,O)}$ (alternatively Y_U) are consistent/well-formed}

U stores

$$N_{(U,O)}, P_{(U,O)},$$

$$s_{(1,U,O)}, t_{(U,O)},$$

$$Y_U, Y_{(U,O)}$$

O stores

$$N_{(U,O)}, P_{(U,O)},$$

$$Y_U \text{ or } Y_{(U,O)}$$

Issuing a k -show credential

- 1 U shows valid $(N_{(U,O)}, P_{(U,O)})$ to O, and proves its well-formedness
- 2 O issues to U a credential pair $(c_{(U,O)}, e_{(U,O)})$, s.t.,

$$c_{(U,O)}^{e_{(U,O)}} = P_{(U,O)} d_O Q_{(k,U,O)} \pmod{n_O},$$

where $Q_{(k,U,O)} := \prod_{i=2}^k g_{O,i}^{s_{(i,U,O)}}$, for random $s_{(i,U,O)}$ jointly chosen by O and U, and known only to U.

The tuple $(Q_{(k,U,O)}, c_{(k,U,O)}, e_{(k,U,O)})$ is U 's k -show credential with organization O .

Showing a k -show credential

User U

Public Info

Verifier V

$$n_O, \{a_O, b_O, d_O, g_O, h_O, v_O, z_O\} \in QR_{n_O}$$

if $\text{cnt}(U, O) \geq k$ then quit

else $r_1, r_2 \in_R \{0, 1\}^{2\ell_n}$

$$A := c_{(k,U,O)} h_O^{r_1}, B := h_O^{r_1} g_O^{r_2}$$

$$H_{(u,O)} := h_O^{t_{(u,O)}}$$

$$\xrightarrow{A, B, H_{(u,O)}}$$

$$\xleftarrow{c}$$

$$c \in_R \{0, 1\}^{\ell_c}$$

$$r := x_{(u,O)} + \sum_{i=1}^k s_{(i,U,O)} c^i$$

r

SPK $\{A, B, H_{(u,O)}, r$ consistent/well-formed & A corresponds to a certificate issued by $O\}$

increment counter

store transcript

$$\text{cnt}(U, O) := \text{cnt}(U, O) + 1$$

for later checkings

Over-showing detection and local revocation

- Issuing organization O checks if $H_{(u,O)}$ appeared more than k times (showing transcripts are unforgeable)
- If yes, interpolate $k + 1$ challenge/response pairs (c, r) to recover $x_{(u,O)}$, and thus $Y_{(u,O)}$.
- Given $Y_{(u,O)}$, find $N_{(u,O)}$ in local users database. Find corresponding $H_{(u,O)}$.
- Add $H_{(u,O)}$ on a blacklist of revoked users.

Global revocation

- At the time of showing, User U verifiably encrypts Y_U , under the Revocation Manager's public key, and sends it to the verifying organization O .
- The encryption specifies a deanonymization condition L , agreed-upon by U and O .
- The Revocation manager reveals the user's identity if L is satisfied.
- The recovered identity Y_U is then added to a global blacklist of revoked users.
- Users may be asked to (privately) prove that their hidden Y_U 's are not this blacklist.

Achieved properties

- Showing unlinkability to Issuing protocol:
At the time of showing, the Verifier sees only a perfectly blinded version of $c_{(k,U,O)}$, and nothing else linkable to Issuing Organization's view. Hence, unlinkability holds even in case of collusion between Issuer & Verifier.
- Showings k -time untraceable to User's identity:
The identity of the credential holder ($x_{(U,O)}$) remains hidden as long as the credential is shown no more than k times.
- Unforgeability,
- Framing-resistance,
- Selective Disclosure...

Summary

- Showings of a credential untraceable to the instance of the issuing protocol that generated it.
- When shown no more than k times, credential showings are untraceable to the identity of the credential holder.
- Credentials are locally revocable. Optionally, global revocability can be enabled with the help of a TTP.
- To detect over-showings, the Issuing organization is able to link the showings of the same credential to each other.

Open question

Is it possible to have k -show untraceability without linkability and without an Escrow party?

Thank you! Questions?