ATTRIBUTE AUTHENTICATION (ANONYMOUS AUTHENTICATION)

Martin Primas

13.4.2013

Example - access system into block of flats

I want to go home.

(~~Who are you?~~)
Do you live here?

Privacy and digital identity

- Identification is not necessary for many services
  - Access systems into block of flats
  - Library
  - Proving legal drinking age
  - Internet magazines with advance payment
- Protection of privacy
  - Anonymity - Identity should be published during the verification only with reason.
  - Untraceability - Service provider should not be able to trace issued token and verification sessions.
  - Unlinkability - Verification sessions of a single user should not be linkable.

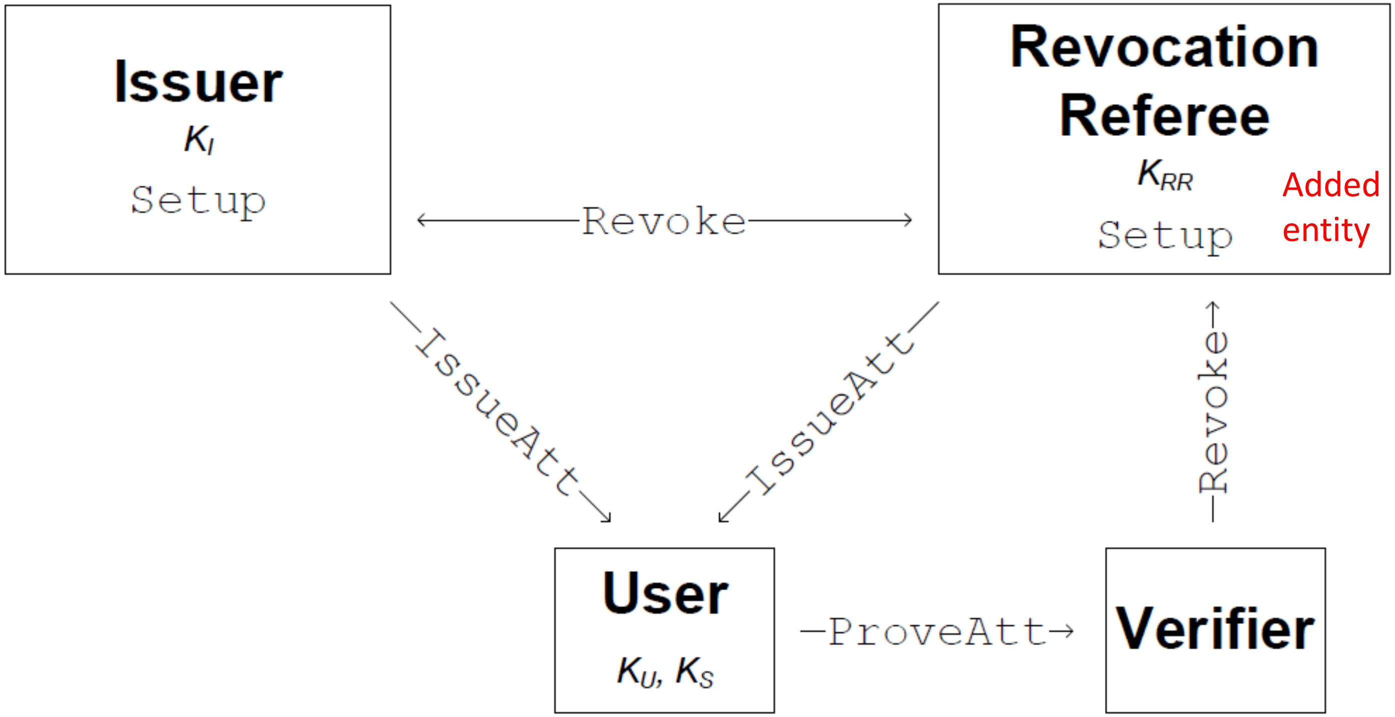
Attribute authentication

- Attribute authentication provide more privacy for users (described above).
  - Only necessary information about user is released in verification protocol.
- There is more possibilities for revocation (hard task to provide it):
  - Revocation of Unlinkability
  - Revocation of Credential (Untraceability / Access right)
  - Revocation of Anonymity

Known systems

- Known systems
  - U-Prove from Microsoft (missing Unlinkability)
  - Idemix (Identity Mixer) from IBM
- Missing in both systems
  - Revocation of Credential
  - Revocation of Anonymity (could be added)
- New system was described by VUT in Brno
  - OKsystem, where I worked, cooperated on review of the system and have started with developing on smart card.
  - **The system is described below.**

Communication scheme



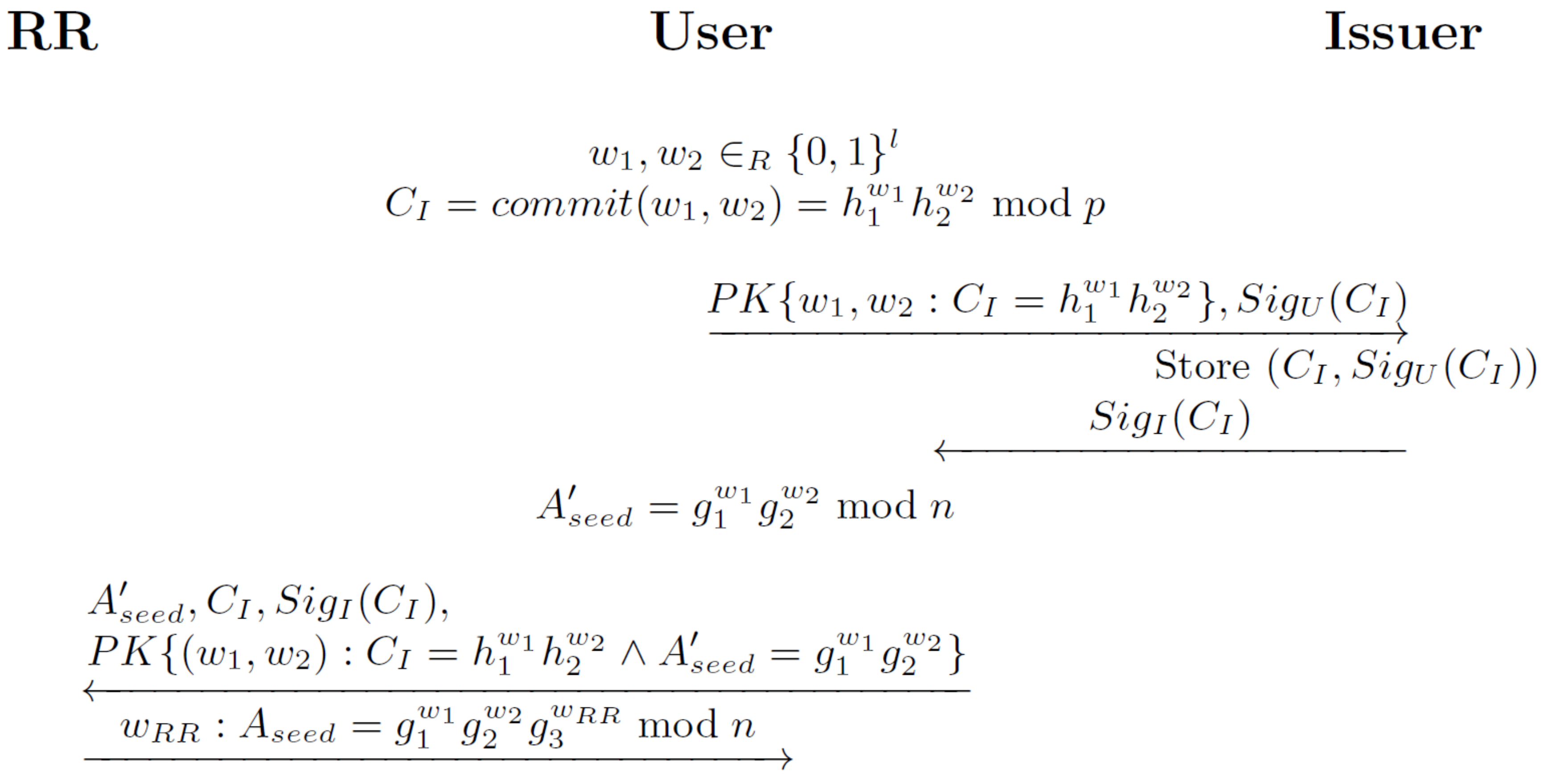
Entities

- Issuer
  - issues personal attributes to users
  - cooperates during the revocation of anonymity
- Revocation Referee (added entity)
  - works as a privacy guarantee
  - cooperates during the revocation of anonymity
  - cooperates with the Issuer during the attribute issuance
  - does not know private user information
- User
  - can anonymously prove the attribute ownership
- Verifier
  - verifies User's attribute ownership
  - can ask Revocation Referee for revocation

Used Cryptographic Primitives

- Okamoto-Uchiyama trapdoor one-way function
  - n = r^2s; r, s are large primes
  - g from Z_n; g mod r^2 is a primitive element of $Z^*_{r^2}$
  - Then **c = g^x mod n** is a trapdoor one-way function with r as a trapdoor: $$x = \frac{((c^{r-1} \bmod r^2) - 1)/r}{((g^{r-1} \bmod r^2) - 1)/r} \bmod r$$
- Discrete logarithm commitments
  - p : q|p-1 be a large prime and
  - g a generator of order q in Z_p.
  - Then **c = g^w mod p** is a simple commitment scheme with commitment w
- Proofs of knowledge of discrete logarithm
  - Notation: **PK{a: c = g^a}**

IssueAtt Protocol



RR **User** **Issuer**

$$w_1, w_2 \in_R \{0,1\}^l$$

$$C_I = commit(w_1, w_2) = h_1^{w_1} h_2^{w_2} \bmod p$$

$$\xrightarrow{PK\{w_1, w_2 : C_I = h_1^{w_1} h_2^{w_2}\}, Sig_U(C_I)}$$

Store $(C_I, Sig_U(C_I))$

$$\xleftarrow{Sig_I(C_I)}$$

$$A'_{seed} = g_1^{w_1} g_2^{w_2} \bmod n$$

$$\xleftarrow{A'_{seed}, C_I, Sig_I(C_I),\ PK\{(w_1, w_2) : C_I = h_1^{w_1} h_2^{w_2} \wedge A'_{seed} = g_1^{w_1} g_2^{w_2}\}}$$

$$\xrightarrow{w_{RR} : A_{seed} = g_1^{w_1} g_2^{w_2} g_3^{w_{RR}} \bmod n}$$

User master key for A_{seed}: $K_U = (w_1, w_2, w_{RR})$

ProveAtt Protocol in Camenisch-Stadler Notation

RR **User** **Verifier**

$$A_{seed} = g_1^{w_1} g_2^{w_2} g_3^{w_{RR}} \bmod n$$

$$K_S \in_R \{0,1\}^l$$

$$A = A_{seed}^{K_S} \bmod n$$

$$C_1 = g_3^{K_S w_{RR}} \bmod n$$

$$C_2 = g_3^{K_S} \bmod n$$

$$PK\{(K_S, K_S w_1, K_S w_2, K_S w_{RR}) : A = g_1^{K_S w_1} g_2^{K_S w_2} g_3^{K_S w_{RR}} \wedge A = A_{seed}^{K_S} \wedge C_1 = g_3^{K_S w_{RR}} \wedge C_2 = g_3^{K_S}\}$$

$$\xrightarrow{\hspace{10cm}}$$

- RR knows the trapdoor function, RR is able to
  - derive K_S from C_2 and then
  - derive w_{RR} from C_1 and from K_S

Revoke Protocol

- Unlinkability revocation
  - RR can calculate w_{RR} and w'_{RR} from two transcripts of the ProveAtt protocol
  - If $w_{RR} = w'_{RR}$, then the session has been carried out by the same User.
- Credential revocation
  - RR can publish revocation information $rev = w_{RR}$ on a public blacklist
  - Each Verifier is able to check if the User is blacklisted or not by checking $C_1 = C_2^{rev} \bmod n$.
- Anonymity revocation
  - RR can reveal w_{RR} and corresponding C_I since both values are linked by the IssueAtt protocol
  - C_I is then forwarded to Issuer who can de-anonymize the User

Thank you for attention.

Any questions?