A Secure Channel for Attribute-Based Credentials

Gergely Alpár   Jaap-Henk Hoepman

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

November 8, 2013

Overview

ABCs and IRMA

Secure Channel

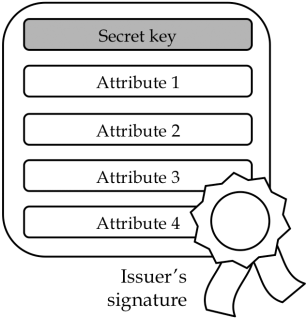
Protocol 1: ICA

Protocol 2: ABCDH

Conclusion

Attribute-Based Credential (ABC)

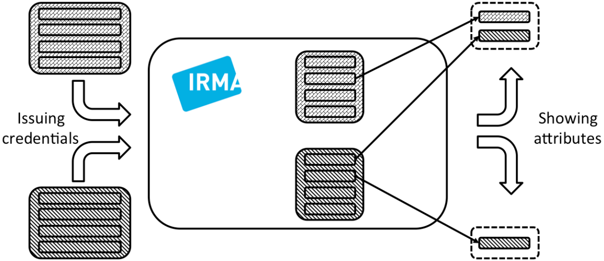
- Attributes
- Credential



Main Functions

Credential carrier is a smart card.

- Issuing
- Selective disclosure (SD)



(High-Level) Selective Disclosure

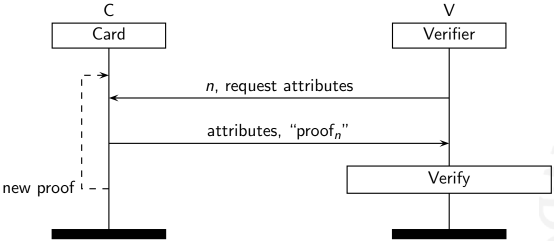


Figure: Selective disclosure for each credential.

Security and Privacy of ABCs

- Security
  - Authenticity of issuer
  - Unforgeability of credentials
  - Non-transferability of attributes (credentials, user's device)
  - (Hiding of attributes)
- Privacy
  - Issuer (a.k.a. IdP) is not included in the verification
  - Issuer unlinkability
  - Multi-show unlinkability
  - Only attributes and their issuers reveal information

I Reveal My Attributes (IRMA)

Based on an *efficient*, *full* smart-card implementation [VA13] of Idemix [CL01, Sec12]

- MULTOS (Infineon SLE78)
- Issuing (5 attributes): 2.6 s
- Selective disclosure (5 → 0 attributes): 0.95 → 1.45 s
- Several credentials may be on a card
- No attribute property proofs (speed, simplicity)
- No equality proof (owing to the small RAM)
    - No proof of equal secret keys

To bind SD proofs, we need a secure channel.

Required: Secure Channel

There are a few requirements:

- Confidentiality, to hide
  - Selectively disclosed attributes
  - Requests from a verifier
  - Issuers of credentials
- Binding (without equality proof)
  - To bind proofs
  - To bind verification and issuance
- Authentication (for the key exchange)
  - Verifier's terminal

    public-key certificate: pk, "allowed attributes"
  - Card

BUT: the card *shouldn't* be identified!

Authentication Without Identification

- Selective disclosure (one credential):

$$\mathrm{SD}\left((a_i)_{i\in\mathcal{D}}; n\right) := \mathrm{SPK}\left\{\text{secret in } C : (a_i)_{i\in\mathcal{D}} \in C\right\}(n)$$

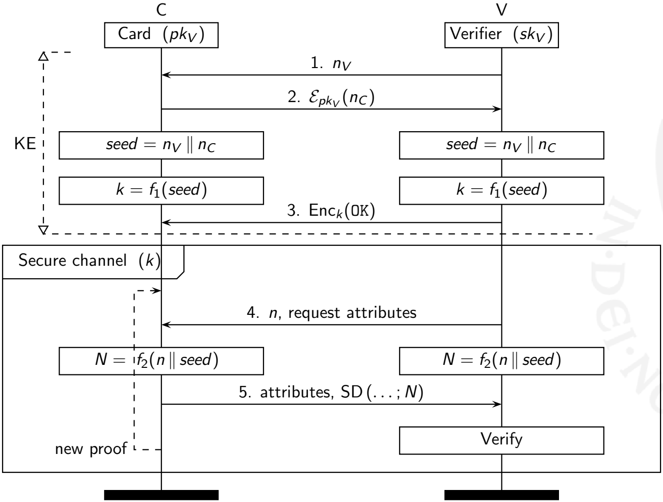
- Preserving anonymity (only attributes reveal information)
- Verifying card validity
- Binding this validity proof to the channel
- Valid card options:
  - A *"validity"* attribute; *e.g.*,

$$\mathrm{SD}\left((a_1); n\right),$$

  - A credential; possibly "empty proof"

$$\mathrm{SD}\left(\emptyset; n\right),$$

Implicit Card Authentication (**ICA**)



C

V

Card (pk_V)

Verifier (sk_V)

1. n_V

2. $\mathcal{E}_{pk_V}(n_C)$

KE

$seed = n_V \,\|\, n_C$

$seed = n_V \,\|\, n_C$

$k = f_1(seed)$

$k = f_1(seed)$

3. $\mathrm{Enc}_k(\mathtt{OK})$

Secure channel (k)

4. n, request attributes

$N = f_2(n \,\|\, seed)$

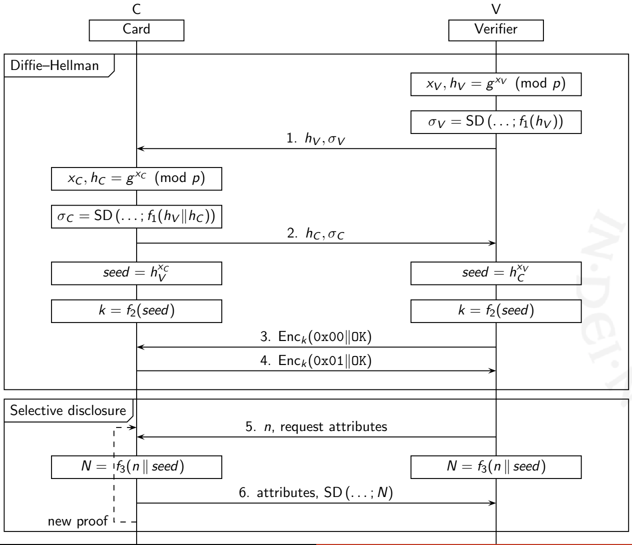
$N = f_2(n \,\|\, seed)$

5. attributes, SD $(\ldots; N)$

Verify

new proof

Diffie–Hellman Channel Protocol (**ABCDH**)



C

Card

V

Verifier

Diffie–Hellman

$x_V, h_V = g^{x_V} \pmod{p}$

$\sigma_V = \mathrm{SD}\,(\ldots; f_1(h_V))$

1. h_V, σ_V

$x_C, h_C = g^{x_C} \pmod{p}$

$\sigma_C = \mathrm{SD}\,(\ldots; f_1(h_V \| h_C))$

2. h_C, σ_C

$seed = h_V^{x_C}$

$seed = h_C^{x_V}$

$k = f_2(seed)$

$k = f_2(seed)$

3. $\mathrm{Enc}_k(\texttt{0x00}\|\texttt{OK})$

4. $\mathrm{Enc}_k(\texttt{0x01}\|\texttt{OK})$

Selective disclosure

5. n, request attributes

$N = f_3(n \,\|\, seed)$

$N = f_3(n \,\|\, seed)$

6. attributes, $\mathrm{SD}\,(\ldots; N)$

new proof

Conclusion

- A secure channel between an anonymous card and a verifier
- A security model
- Two protocols
- Implicit: ideal revocation
- Yet to develop efficient revocation techniques for ABCs
- Non-identifying authenticity
- Interacting with (potentially) untrusted entities (M2M, H2H)

Thank you for your attention!

Gergely Alpár
http://www.cs.ru.nl/~gergely
gergely@cs.ru.nl

IRMA project: https://www.irmacard.org

References

Mihir Bellare and Phillip Rogaway, *Entity authentication and key distribution*, Advances in Cryptology—CRYPTO'93, Springer, 1994, pp. 232–249.

Jan Camenisch, Nathalie Casati, Thomas Gross, and Victor Shoup, *Credential authenticated identification and key exchange*, Advances in Cryptology–CRYPTO 2010, Springer, 2010, pp. 255–276.

Jan Camenisch and Anna Lysyanskaya, *An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation*, Advances in Cryptology — EUROCRYPT 2001 (Birgit Pfitzmann, ed.), LNCS, vol. 2045, Springer Berlin / Heidelberg, 2001, pp. 93–118.

Security Team, IBM Research, *Specification of the Identity Mixer Cryptographic Library, version 2.3.4*, Tech. report, IBM Research, Zürich, February 2012.

Pim Vullers and Gergely Alpár, *Efficient Selective Disclosure on Smart Cards Using Idemix*, Policies and Research in Identity Management (IDMAN) (Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell, eds.), IFIP AICT 396, Springer, 2013, pp. 53–67.