Signing with Multiple ID's and a Single Key

Mirosław Kutyłowski (speaker)
Jun Shao

Wrocław University of Technology, Poland
Zhejiang Gongshang University, P.R.C.

IEEE CCNC 2011, Las Vegas, 10.1.2011

Electronic personal ID cards, personal data protection

Personal identity cards

European Community

1. in a near future: national identity cards as smart cards
2. functionalities:
   - online authentication,
   - digital signature,
   - health insurance card,
   - ...
3. intended:
   - contacts with public authorities online,
   - secure electronic business for citizens

Personal data protection

Problems

1. electronic data flow make it easy to collect data violating personal data protection rules
2. European personal data protection standards: permission of the person involved or an explicit legal rule are necessary to allow processing given personal data
3. building IT systems according to these rules is hard, privacy aware design of cryptographic primitives is necessary

Sectors

Sector

A separate area of activity. Examples:

- health authority
- insurance
- law enforcement

Sector separation rule

Authentication in one sector should be unlinkable with authentication in another sector. That is:
person X in sector A must not be linkable with person Y in sector B, if pseudonyms X and Y correspond to the same physical person

Implemented concepts:

Bürgerkarte (A), Restricted Identification (D, PL)

Signatures in different sectors

Goal

1. use a different electronic signature in each sector
2. for signatures designated for sectors A and B it should be unfeasible to say if they come from the same person

A trivial solution?

for each sector a different key pair

wrong! we cannot afford it: the memory space on a smart card is very limited, only a limited number of sectors possible (just a few)

Signatures in different sectors

Detailed goal

design a signature scheme such that one private key can be used for an arbitrary number of sectors
but the signatures created for different sectors remain unlinkable

remark

this solves the problem since the public keys and their certificates may be stored outside the smart card.

Our Solution

Sector
setup

System parameters

- a group G of a prime order, where Decisional Diffie-Hellman Problem is hard,
- a generator g of G,
- a secure hash function $H_G : \{0,1\}^* \to G$

Parameters for a sector A

- public key

$$g(A) := H_G(A)$$

where A stands for the legal name of sector A

- (no private key)

Person
setup

Electronic personal identity card

Person B holds an ID card obtained by ID-Authority:

1. the ID card generates and stores x_B, the private key of B
2. $y_B := g^{x_B}$ is the public key for B
3. the ID card holds a certificate for y_B issued by ID-Authority

Registering into a sector

Person B registering to sector A

B appears at ID-Authority

1. the ID card generates $p(A)_B := g(A)^{x_B}$
2. the ID card presents $p(A)_B$ to ID-Authority and proves in a zero-knowledge way that its discrete logarithm with respect to $g(A)$ is the same as discrete logarithm of p_B with respect to g,
3. ID-Authority issues a certificate for $p(A)_B$ for sector B the certificate contains only a restricted subset of personal data of B

Signatures of B for sector A

Creating a signature of m by B

1. choose $r \in [1, q-1]$ uniformly at random, compute
$$R := (g(A))^r$$
2. $$S := H_q(g(A), p(A)_B, R, m) \cdot x_B + r \bmod q$$

(R, S) is the signature of m, it comes together with the certificate of $p(A)_B$

Signature verification

1. public key $p(A)_B$ retrieved from the certificate
2. verification test:

$$g(A)^S \stackrel{?}{=} (p(A)_B)^{H_q(g(A),p(A)_B,R,m)} \cdot R$$

Security features

Unforgeability

If the multi-sector signature scheme can be forged in the random oracle model, then the Discrete Logarithm Problem can be solved for G.

Privacy

Public keys $P(C)$, $P'(D)$ from sectors C and D are presented (together with some signatures).
Question: Are $P(C)$, $P'(D)$ are assigned to the same person?
If we can answer this question in the random oracle model, then Decisional Diffie-Hellman Problem can be solved for G.

Security features II

Unlinkability

Given the public keys of Alice and Bob, and two public keys X and Y for sector A. We know that they belong to Alice and Bob.

Question: which of them belongs to Alice and which to Bob?

If this question can be solved in the random oracle model, then Decisional Diffie-Hellman Problem can be solved for G.

*R*emark: the question is related but different from DDHP.

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.wroc.pl
2. http://kutylowski.im.pwr.wroc.pl
3. +48 71 3202109, fax: +48 71 320 2105