Mediated Signatures - Towards Undeniability of Digital Data in Technical and Legal Framework

Przemysław Kubiak[1], Mirosław Kutyłowski[1], Anna Lauks-Dutka[1], Michał Tabor[2]

Institute of Mathematics and Computer Science[1], Wrocław University of Technology

Trusted Information Consulting[2], Warsaw

LIT 2010, May 3

Outline

1. Advanced Digital Signatures
   - Qualified Signatures
   - Validity of the Signature
   - Standard Implementation
   - Risk Issues
   - Reasons of Failure
2. Mediated Signatures
   - Cryptographic Description
   - Mediated RSA Example
   - Application Scenario
   - Legal Framework

Outline

The Concept of Qualified Signatures

signature creation data (**secret key**)

signature verification data (**public key**)

The Concept of Qualified Signatures

signature creation data (**secret key**)

signature verification data (**public key**)

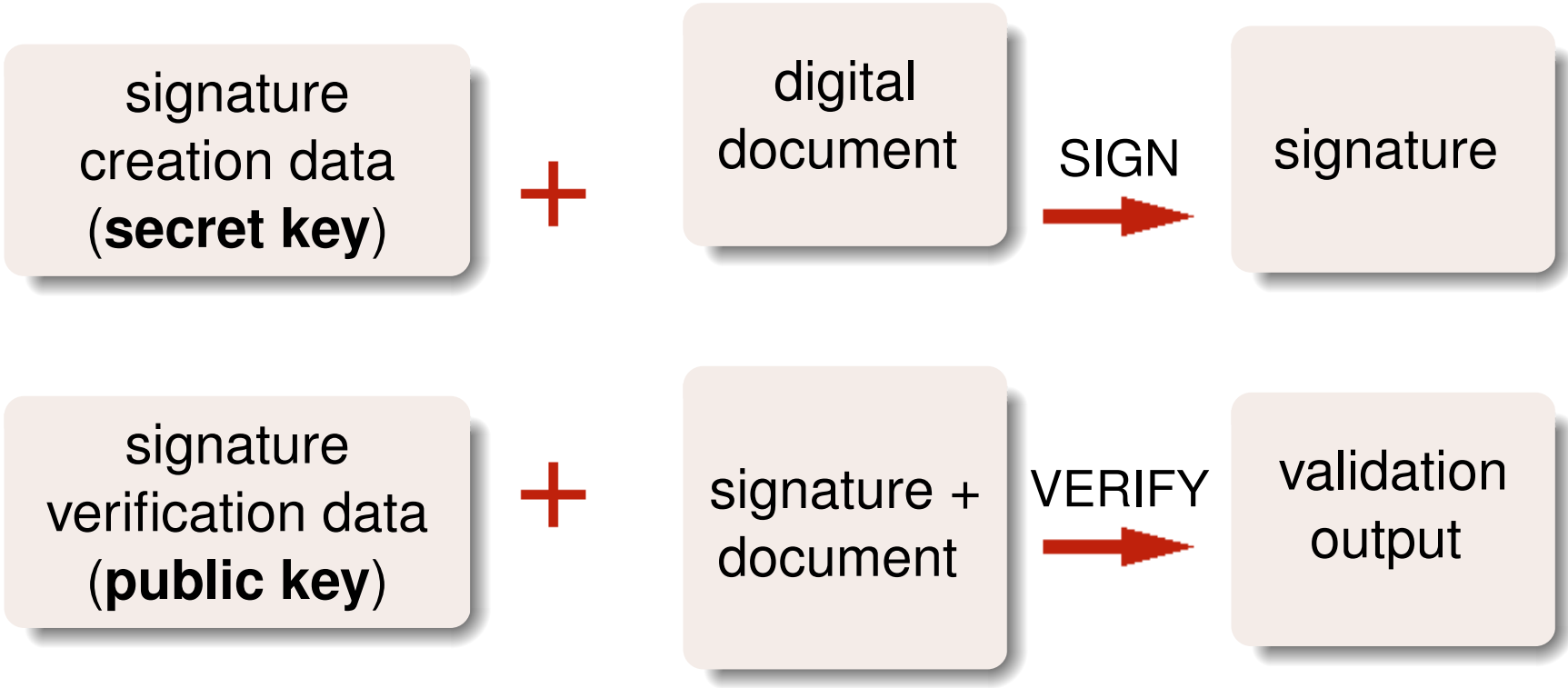
Qualified Certificate

1. certificate issuer
2. date of issue and expiration
3. ID of the certificate holder:
   - family name: Kutyłowski
   - given name: Mirosław
   - personal number (PESEL):

   ...
4. 2048 RSA public key: 0x00308187028181 ...
5. signature of the issuer

⋮

The Concept of Qualified Signatures



Checking the Signature

1. **Verification of the signature**
   (using the public key from the certificate)
2. **Verification of the identity of the key holder**
   – checking the certificate

Checking the Signature

1. **Verification of the signature**
   (using the public key from the certificate)
2. **Verification of the identity of the key holder**
   – checking the certificate

Cryptographic Point of View

If signature verifies correctly then:

- it was created with the proper signing key, or
- the signing scheme has been broken

Checking the Signature

1. **Verification of the signature**
   (using the public key from the certificate)
2. **Verification of the identity of the key holder**
   – checking the certificate
   - problem: the signing key can be: stolen (with a smart card), retained by the certification provider, leaked (trapdoor), smart card can be misused, ...

Cryptographic Point of View

If signature verifies correctly then:

- it was created with the proper signing key, or
- the signing scheme has been broken

Additional Mechanisms

Each certificate:

- has limited validity period
- can be revoked by issuer / signer

Standard Implementation – Properties

A secret (signing) key :

- stored on a cryptographic smart card
- access secured with a PIN number

Status of the certificate can be checked with :

- OCSP (Online Certificate Status Protocol)
- recent CRL (Certificate Revocation List) – risky for the verifier

Standard Implementation – Properties

Key idea :

- enable signing offline

Reality :

- verification must be performed online
- signing time unknown

Risk Issues

1. loosing control over a signature creation device

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)
3. kleptography ($\Leftarrow$ malicious manufacturer)

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)
3. kleptography ($\Leftarrow$ malicious manufacturer)
4. retaining the key ($\Leftarrow$ if generated by a provider of the certification cervices)

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)
3. kleptography ($\Leftarrow$ malicious manufacturer)
4. retaining the key ($\Leftarrow$ if generated by a provider of the certification cervices)
5. revoking certificates ($\Rightarrow$ for complicating the legal situation)

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)
3. kleptography ($\Leftarrow$ malicious manufacturer)
4. retaining the key ($\Leftarrow$ if generated by a provider of the certification cervices)
5. revoking certificates ($\Rightarrow$ for complicating the legal situation)
6. signatures based on qualified certificate but not on a secure signature creation device

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)
3. kleptography ($\Leftarrow$ malicious manufacturer)
4. retaining the key ($\Leftarrow$ if generated by a provider of the certification cervices)
5. revoking certificates ($\Rightarrow$ for complicating the legal situation)
6. signatures based on qualified certificate but not on a secure signature creation device
7. decline of mathematical/technical strength

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)
3. kleptography ($\Leftarrow$ malicious manufacturer)
4. retaining the key ($\Leftarrow$ if generated by a provider of the certification cervices)
5. revoking certificates ($\Rightarrow$ for complicating the legal situation)
6. signatures based on qualified certificate but not on a secure signature creation device
7. decline of mathematical/technical strength
8. standards and obscure technical requirements

Risk Issues

1. loosing control over a signature creation device
2. poor randomness ($\Rightarrow$ cryptographic compromise)
3. kleptography ($\Leftarrow$ malicious manufacturer)
4. retaining the key ($\Leftarrow$ if generated by a provider of the certification cervices)
5. revoking certificates ($\Rightarrow$ for complicating the legal situation)
6. signatures based on qualified certificate but not on a secure signature creation device
7. decline of mathematical/technical strength
8. standards and obscure technical requirements

Many of above problems can be eliminated by adopting:

Mediated Signature Architecture

Reasons of Failure of Qualified Signatures

Some Critical Issues

single technical point of failure: secure signature creation device

Reasons of Failure of Qualified Signatures

Some Critical Issues

single technical point of failure: secure signature creation device

based on trust and not technical measures: use of randomness, key generation services

Reasons of Failure of Qualified Signatures

Some Critical Issues

single technical point of failure: secure signature creation device

based on trust and not technical measures: use of randomness, key generation services

signing time unclear: after creating the signed data, **before** - requires additional mechanisms

Reasons of Failure of Qualified Signatures

Some Critical Issues

single technical point of failure: secure signature creation device

based on trust and not technical measures: use of randomness, key generation services

signing time unclear: after creating the signed data, **before** - requires additional mechanisms

no way to block temporarily: impossible to disable signing possibility temporarily (like a credit card) or apply a signing policy

Reasons of Failure of Qualified Signatures

Some Critical Issues

single technical point of failure: secure signature creation device

based on trust and not technical measures: use of randomness, key generation services

signing time unclear: after creating the signed data, **before** - requires additional mechanisms

no way to block temporarily: impossible to disable signing possibility temporarily (like a credit card) or apply a signing policy

legal problems: Poland: impossible to check legal status of a signature at the time of verification, it is possible to check validity for the past

Outline

Mediated Signature Architecture

Background

1. there are at least two parties of the protocol:
   - user
   - security mediator
2. creation of a single signature is possible if **all** the necessary parties are involved (by using the appropriate cryptographic material)

Mediated Signature Architecture

User

(1) creates a pre-signature S_1, using his private key K_1:

$$S_1 = \mathrm{SIG}(K_1, \mathrm{Hash}(M))$$

S_1 →

← S

Mediator

(2) finalizes the signature, using the appropriate keying material K_2:

$$S = \mathrm{FIN}(K_2, S_1)$$

Mediated Signature Architecture

User

(1) creates a pre-signature S_1, using his private key K_1:

$$S_1 = \mathrm{SIG}(K_1, \mathrm{Hash}(M))$$

S_1 →

← S

Mediator

(2) finalizes the signature, using the appropriate keying material K_2:

$$S = \mathrm{FIN}(K_2, S_1)$$

- there is **one** public key K related to the secret key pair (K_1, K_2)
- S is the signature of M

RSA Based Mediated Signature

Keys

- $n = pq$, $d \cdot e = 1 \bmod \varphi(n)$
- splitting the key d:
  - for mediator: $d_1 := \mathrm{HSM}(K, ID_{signer})$
  - for the signer: $d_2 := d - d_1$

RSA Based Mediated Signature

Keys

- $n = pq$, $d \cdot e = 1 \bmod \varphi(n)$
- splitting the key d:
  - for mediator: $d_1 := \mathrm{HSM}(K, ID_{signer})$
  - for the signer: $d_2 := d - d_1$

Signature Creation

signer: $s_1 := (\text{hash+padding}(M))^{d_1}$

mediator: $s_2 := (\text{hash+padding}(M))^{d_2}$

signature: $s := s_1 \cdot s_2 \bmod n$

Signature Verification

as usual

RSA Based Mediated Signature

Extended Scenario

- one key on a smart card
- the second key on the laptop
- the third key on a server

Attack

creating a signature by the adversary requires

- stealing the smart card, and
- stealing the laptop, and
- breaking into the server

RSA Based Mediated Signature

Extended Scenario

- one key on a smart card
- the second key on the laptop
- the third key on a server

Attack

creating a signature by the adversary requires

- stealing the smart card, and
- stealing the laptop, and
- breaking into the server

For Paranoids

split the key into even more pieces and put them on independent devices

Main Features

Revocation

The signer can block signing possibility for any time, any reason, ... :

- block the card used in his office for vacation time and holidays
- block the card during a stay in a hospital
- block the card for the time 23:00-6:00 every day
- ...

in this case the signature WILL NOT BE CREATED

Monitoring

Mediator can monitor the signing activities and refuse to finalize if something suspicious is going on

Main Features II

Signing Time

Mediator can implement hash chaining and provide undeniable and verifiable evidence of the signing time

Verification

- no adjusting the software necessary - no special time stamps, ... that need to be interpreted well
- in fact, Mediator performs pre-validation of a signature, making it easier for the recipient of the document

Risks

- we do not depend solely on security of smart cards!
- two weaker but independent mechanisms are better than a single strong one

Public Administration Case Study

Signing documents exchanged between citizens and public authorities:

- single point of contact as a favorable solution: it can be integrated with Mediator
- privacy: the public bodies know anyway these documents
- signature can be created by ID cards even if thousands of them are stolen or lost (security does not depend solely on ID cards) the smart cards do not require the best possible protection and can serve for a longer time
- automatic and provable date of signing - elimination of frauds and legal disputes

Use in Corporations

- full control over signing activities, disabling a single user immediate
- excellent tool for controlling document flow in a heterogeneous IT environment

Compatibility with EU Directive

1. signature creation data are still in hands of the signer

Compatibility with EU Directive

1. signature creation data are still in hands of the signer
2. Mediator runs security mechanism that are fully compatible with the Directive,
   the Directive does not prohibit to use further cryptographic keys to improve security

Compatibility with EU Directive

1. signature creation data are still in hands of the signer
2. Mediator runs security mechanism that are fully compatible with the Directive,
   the Directive does not prohibit to use further cryptographic keys to improve security
3. the whole systems really satisfies the security requirements from Annex III,
   affordable smart cards do not fulfill these requirements, if we take them seriously

Foresight

Future

- the concept of qualified electronic signatures based on classical X.509 architecture is technically obsolete
- the future belongs to distributed security mechanism supported by online mechanisms

Thank you for attention!