Digital Signatures for e-Government – a Long-Term Security Architecture

Przemysław Błaśkiewicz, Przemysław Kubiak, and Mirosław Kutyłowski

Wrocław University of Technology

e-Forensics, Shanghai, 11 Nov. 2010

Challenges for electronic signatures

Advantages

- Electronic signatures based on asymmetric techniques are relatively strong and easy to verify by anybody.
- Electronic signatures are suitable for wide scale flow of documents, providing strong proofs for:
  - authorship of a document signed
  - integrity of the document and lack of modifications after signing

However ...

... a strong mathematical algorithm is not enough to ensure security of signatures.

Challenges for electronic signatures

some crucial threats

Problem: leaking secret keys

the signatures can be forged when secret keys are revealed to a third party.
How do we know that the secret keys are only in the signing device of the signer?

Problem: erosion of cryptography

advances of cryptanalysis are unpredictable.
How do we know that nobody knows how to break the signature scheme? A real forger will always deny his capabilities.

Challenges for electronic signatures

some crucial threats

Problem: dishonest service providers

a service provider can

- retain secret information (when generating the keys),
- insert trapdoors in software and hardware delivered,
- ...

How can we trust that certification processes and audits are effective enough?
How do we know that the controlling body does not collude with the service provider?

Challenges for electronic signatures

how to deal with the threats

Desired properties

1. security of the system should not be based on the assumption that a certain party is honest. A misbehavior should be inevitably detectable.
2. security properties should be self-evident as much as possible, security evaluation should not require high expertise.

Such assumptions adopted by e-voting community as fundamental design rules.

Challenges for electronic signatures

dangerous assumptions

PKI today

- PKI today assumes honesty of *Trusted Third Parties*. Failure of this assumption is critical to the system.
- In European legal systems it is not necessary to prove honest behavior in order to act as TTP.
- Even worse, sometimes public bodies are obliged by law to accept such services.

so may be reluctance of business and citizens for PKI today is well founded?

Our goal

1. provide solutions that are immune against misbehavior,
2. make PKI system less dependent on certification and audit, provide tools for public verifiability

Our techniques:

1. **strong RSA**: an RSA signature with DL based internal signature,
2. **Floating key**: a strong mediated signature with clone detection
3. **hash** based PKI?

mRSA - the core of the system

algorithm

The key idea (Boneh, Ding, Tsudik 2001, 2004):

- the secret key is split between two “parties”: the user and the central server (mediator):
- none of the two parties can alone make a signature.

Mediated RSA in detail:

- public key: e, N,
- private key d is split: $d = d_1 + d_2$,
- signature generation under message m:
  1. $h(m)$, Δ :=PSS-padding($h(m)$), are calculated,
  2. $s_1 := \Delta^{d_1} \bmod N$,
  3. $s_1, \Delta, h(m)$ are sent to the mediator,
  4. the mediator checks status of user’s id-card,
  5. $s_2 := \Delta^{d_2} \bmod N$,
  6. $s := s_1 \cdot s_2 \bmod N$ is now verified using $h(m)$.

mRSA - the core of the system

key management

Key splitting - example procedure:

- the mediator generates d_2 in a way independent from generation of n and d
- n, e and d are calculated by a dealer (e.g. in a distributed manner)
- $d_1 := d - d_2$ transferred (distributivelly or as a single Paillier ciphertext) to the signing device
- neither the mediator nor the signing device alone has data to factorize n

Security of mRSA versus security of RSA

- if there is an effective cryptanalytic attack on mRSA, then by simulating data for mRSA protocol having RSA data we will obtain an effective attack on RSA.
- so: *cryptanalytically mRSA is at least as strong as RSA*

Why mediated signatures?

The aim of mediated signatures:

Fast revocation of user’s public key in case the private key has been compromised – the pre-signatures of the card are no more finalized.

Drawbacks of currently deployed protocols:

- CRL: the list is refreshed in time intervals, if the list is large - some applications abandon status checking,
- OCSP: executed at the time the signature is verified, hence many repeated executions,
- validation service:
  - for the signer – it is not compulsory,
  - for a verifier – additional service she would pay for; if many copies of a document distributed by the signer - many validations.

Floating exponents

detection of cloned signature creation devices

Strengthening - mediated signatures

- update d_1 and d_2 after each key usage, public key unchanged
- the updates are unpredictable - a (pseudo)random process
- when a cloned card is used, it changes the key d_2 on the mediator's side, afterwards the legitimate card cannot create a valid signature and cloning becomes detected!

Floating exponents

detection of cloned signature creation devices

Floating exponents -details:

the exponents d_1 and d_2 might float:

- there is a dynamic offset, say h, of the exponents:
  - the signature creation device holds $d_1 + h$
  - the server holds $d_2 - h$
- during each interaction a small number c is agreed between the signature device and the server, and the offset is updated $h := h + c$.

if two devices with the same key interact with the server, then the offset becomes de-synchronized: this leads to detection of clones!

Strong mRSA

motivation

Generation directly on a signature creation device

1. if randomness not really random, then the keys might be really weak ...
2. ... but it is hardly possible to check that the randomness is really good
3. all kinds of kleptographic techniques apply

External generation

1. source of randomness could be of very good quality
2. easy to control and protect against installing trapdoors in the keys
3. **... as long as trapdoors are not a feature of the system!**

Strong mRSA

motivation

Dilemma:

Whom to trust:

1. a manufacturer?
2. or a service provider?

Nested signatures for RSA

Internal signature:

- RSA uses the hash value of the message to be signed padded by some number of bits,
- a *salt* in PSS-padding might itself be a signature!
- in *salt* there is enough space for e.g. BLS (Boneh, Lynn, Shacham 2001) signature,
- internal deterministic signature causes RSA-PSS to be deterministic, but with unpredictable *salt* .
  So there is no room for a covert channel.

Strong RSA

key generation options

Example scenario:

- the keys for RSA are generated by a service provider and loaded into a signing device
- the keys for internal signature are generated by a signing device

Strong RSA

security features

Security features:

- key generation:
  - the service provider can potentially forge the RSA signatures but not the internal ones
  - the manufacturer of the devices potentially can forge internal signatures but not RSA
- cryptanalytic erosion:
  - failure of one of the algorithms does not immediately lead to forge-ability of signatures
  - the external and internal signatures are based on different algebraic problems (factorization and discrete logarithm)

Strong RSA

implementation issues

Compatibility:

standard verification software unaware of internal signature can still work as the format of the signature is unchanged

Hash based signatures

an alternative for RSA and DL?

Hash based signatures – basic facts:

- one time signatures
- conversion to multiple-signatures possible with Merkle trees approach

Extended features:

- the mechanism for extending the number of signatures (hierarchical approach) can be used to change the hash function without changing the public keys
  ⇒ so weakening a hash function does not lead to change of the public keys
- a mediated version of hash based signatures is easy to construct

Acknowledgement

- supported by Polish Ministry of Science and Higher Education and by Foundation for Polish Science
- work done in cooperation with Trusted Information Consulting and CryptoTech companies