Technical and Legal Meaning of "Sole Control" – Towards Verifiability in Signing Systems

Mirosław Kutyłowski[1] Przemysław Błaśkiewicz[1]
Łukasz Krzywiecki[1] Przemysław Kubiak[1]
Wiesław Paluszyński[2] Michał Tabor[2]

Wrocław University of Technology

Trusted Information Consulting, Warsaw

LIT 2011

Outline

1. Advanced Electronic Signatures
   - Motivation
   - EU Directive
2. Black-Box SSCD
3. Attacks and Threats
4. Verifiability
5. Feasibility
6. Proposed Framework
   - Common Criteria
   - Security Levels
   - Evaluation Rules

Electronic signatures - legal idea

Idea of advanced electronic signature

- a signature linkable with its signatory
- technically, signing is performed by some (yet unspecified) electronic means controlled by the signatory
- no undetected changes in a document possible after signing

EU legal concept of electronic signatures

EU Directive 1999/93/EC, Art. 2

”advanced electronic signature” means an electronic signature which meets the following requirements:

(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) **it is created using means that the signatory can maintain under his sole control**; and

(d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

EU legal concept of electronic signatures

EU Directive 1999/93/EC, Art. 2

certificate: a) it is uniquely linked to the signatory;

certificate: b) it is capable of identifying the signatory;

secure device: c) it is created using means that the signatory can maintain under his sole control; and

cryptography d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

can maintain – sloppy behavior of the signatory does not reduce his responsibility

EU legal concept of electronic signatures -SSCD

SSCD

- ”signature-creation device” means configured software or hardware used to implement the signature-creation data;
- ”secure-signature-creation device” . . . meets the requirements laid down in Annex III;

EU legal concept of electronic signatures -SSCD

ANNEX III

1. Secure signature-creation devices must, by appropriate technical and procedural means, ensure at the least that:
   (a) the signature-creation-data used for signature generation can practically occur only once, and that their secrecy is reasonably assured;
   (b) the signature-creation-data used for signature generation cannot, with reasonable assurance, be derived and the signature is protected against forgery using currently available technology;
   (c) the signature-creation-data used for signature generation can be reliably protected by the legitimate signatory against the use of others.
2. Secure signature-creation devices must not alter the data to be signed or prevent such data from being presented to the signatory prior to the signature process.

Concepts for SSCD

Generic solutions: smart card

- carefully designed and limited operating system,
- the keys can be used to generate a signature, but not read by the card holder,
- tamper resistant
- some (weak) authentication of the user against the card

Generic solutions: keys locked on a server

- no electronic device hold by the user, the keys stored on a secure server
- keys used after rather reliable authentication of the user
- successful in practice!

where to keep the money: in a bank or in a pocket?

SSCD - checking properties

Certification concept

Devices checked by special institutions/companies:

- confidential information checked, so it cannot be open for inspection by public
- specialized know-how and labs for testing
- independence from the manufacturer – no personal, economic, . . . connections

Certification limitations

- a manufacturer can know more tricks than an inspector
- inspection by a check-list only
- instead of trusting the manufacturer we have to trust a certification authority

Attacks - geopolitic situation

Cyber-war

- attack methods: may be see only the top of an iceberg
- strong financing of cryptanalysis in some countries, state control over research results

Generic attacks

1. low quality randomness
2. using random parameters as hidden channels
3. tricks with key generation
4. hardware trapdoors

E2E verifiability

The concept

- no expert knowledge is required to evaluate relevant security mechanisms,
- evaluation results should be self-evident and undeniable,
- effectiveness of security mechanisms can be checked while the system is running and not only as a prior inspection,
- no assumption is made about honesty of any party of the protocol, it concerns in particular the manufacturers and supervision authorities.

E2E verifiability

The concept

- no expert knowledge is required to evaluate relevant security mechanisms,
- evaluation results should be self-evident and undeniable,
- effectiveness of security mechanisms can be checked while the system is running and not only as a prior inspection,
- no assumption is made about honesty of any party of the protocol, it concerns in particular the manufacturers and supervision authorities.

E2E verifiability

The concept

- no expert knowledge is required to evaluate relevant security mechanisms,
- evaluation results should be self-evident and undeniable,
- effectiveness of security mechanisms can be checked while the system is running and not only as a prior inspection,
- no assumption is made about honesty of any party of the protocol, it concerns in particular the manufacturers and supervision authorities.

E2E verifiability

The concept

- no expert knowledge is required to evaluate relevant security mechanisms,
- evaluation results should be self-evident and undeniable,
- effectiveness of security mechanisms can be checked while the system is running and not only as a prior inspection,
- no assumption is made about honesty of any party of the protocol, it concerns in particular the manufacturers and supervision authorities.

Solutions alternative to SSCD

Some examples

- Fail-Stop Signatures
- Mediated Signatures
- Validation and Authorization Service
- Floating Exponents
- Two-Head Dragon
- hash based trees of one-time signatures

Two-Head Dragon protocol

A SSCD with a Two-Head Dragon

1. a good dragon with two heads lives in a smart card, one head per side
2. a signature is created by one of sides, selected at random
3. during signature creation the head from the active side says a half of a magic formula
4. once the whole formula is said, the secret keys are revealed

If the keys get compromised and used, then whp the secret keys are revealed to the public.

Idea

An adversary holding the secret key cannot use them!

A framework for “sole control”

Common Criteria Approach

Methodology

1. find questions for key issues,
2. define security levels for possible answers
3. examine a solution and assign it appropriate level

- it is not generally true that we need the highest level in each category
- we do not have to be paranoid - we need to adjust the solutions to real risks!

A framework for “sole control”

Key Issues

1. to what extent does the signatory depend on honesty of the third parties? What are the potential consequences of malicious behavior of these parties?
2. In what way can the signatory transfer the sole control to other parties, if he wishes to do so (or is coerced to do so)?
3. Is the sole control evident to the signatory, or is it merely a technical fact that can be checked by third parties?

A framework for “sole control”

Key Issues

1. to what extent does the signatory depend on honesty of the third parties? What are the potential consequences of malicious behavior of these parties?
2. In what way can the signatory transfer the sole control to other parties, if he wishes to do so (or is coerced to do so)?
3. Is the sole control evident to the signatory, or is it merely a technical fact that can be checked by third parties?

A framework for “sole control”

Key Issues

1. to what extent does the signatory depend on honesty of the third parties? What are the potential consequences of malicious behavior of these parties?
2. In what way can the signatory transfer the sole control to other parties, if he wishes to do so (or is coerced to do so)?
3. Is the sole control evident to the signatory, or is it merely a technical fact that can be checked by third parties?

Criteria for “sole control”

Trust levels

TRUST-0 : the signatory has to trust blindly the system providers

TRUST-1 : it suffices to trust certification and auditing bodies supervising the system of digital signatures

TRUST-2 : the signatory does not have to trust any third party

Criteria for “sole control”

Transferability of control

TRANSFER-0 : the signatory may transfer the possibility of creating signatures to a third person without substantial effort

TRANSFER-1 : transfer of sole control is detectable with substantial probability

TRANSFER-2 : transfer of control is impossible neither by technical nor organizational means

Criteria for “sole control”

Quality guarantees

GUARANTEE-0 : “sole control” is based on a declaration of the system provider

GUARANTEE-1 : “sole control” is confirmed by certification bodies and runtime audits

GUARANTEE-2 : “sole control” is self-evident in the sense that any breaches can be recognized at least by the signatory and are undeniable

Criteria for “sole control”

Signatory’s control over the keys

level CONTROL-0 : the signatory has no record about usage of signature creation data, especially those created without his consent

level CONTROL-1 : the signatory has access to data indicating actual usage of the signature creation data

level CONTROL-2 : the signatory has access to data proving actual usage of the signature creation data in undeniable way

Evaluation rules

Proposed methodology

1. Evaluation does not need to be performed by bodies that are independent. In fact, the reliable search for weaknesses is done by competition that has strong interest in detecting any security flaws.
2. Evaluation result may not depend on secret mechanisms: “no security by obscurity” just as elsewhere in cryptography.
3. Evaluation should be performed in public, and all results must be available for potential users. EU may contribute a lot ....

Evaluation rules

Proposed methodology

1. Evaluation does not need to be performed by bodies that are independent. In fact, the reliable search for weaknesses is done by competition that has strong interest in detecting any security flaws.
2. Evaluation result may not depend on secret mechanisms: “no security by obscurity” just as elsewhere in cryptography.
3. Evaluation should be performed in public, and all results must be available for potential users. EU may contribute a lot ....

Evaluation rules

Proposed methodology

1. Evaluation does not need to be performed by bodies that are independent. In fact, the reliable search for weaknesses is done by competition that has strong interest in detecting any security flaws.
2. Evaluation result may not depend on secret mechanisms: “no security by obscurity” just as elsewhere in cryptography.
3. Evaluation should be performed in public, and all results must be available for potential users.
   EU may contribute a lot ....