Secure Signature Creation Devices (SSCDs)

…from different approaches

Dr. István Zsolt BERTA
istvan.berta@microsec.hu
Microsec Ltd.

e-SZIGNO

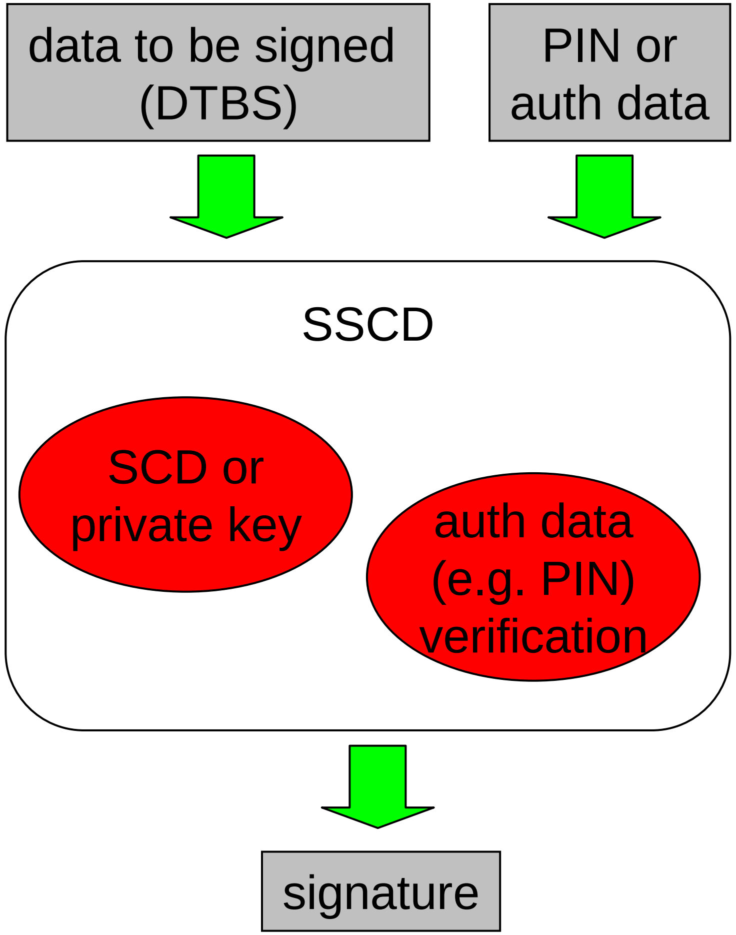
Requirements for SSCDs

Annex III of the e-Signature Directive, in plain words:

1. SSCDs must ensure that the signature creation data:
   (a) is secret and unique;
   (b) the signature is protected vs. forgery;
   (c) is reliably protected, only the signatory can use it.
2. SSCDs must not
   - alter the data to be signed;
   - prevent the data to be signed from being presented to the signatory.

Very high level requirements.
More or less common sense.

SSCD as a crypto token



- Stores the private key of the signatory
- Capable of authenticating the signatory
- Outputs a signature if the signatory is authenticated only
- Private key or auth data cannot be retrieved from it

- Small and simple enough to be secure
- Usually it is a piece of hardware

Conformity assessment of SSCDs

- A device is considered an SSCD if its conformity had been assessed by a designated body.
- Lower level criteria for assessment:
  - **Common Criteria, SSCD PP, EAL4+**
  - other criteria based on FIPS 140-X or ITSEC
  - or anything that fulfills the criteria in Annex III of the Directive
- An SSCD assessed in one Member State is to be recognized in all other Member States

Different approaches to SSCDs

- Personal devices (e.g. smart card, USB token)
- Solutions based on a central server
- Solutions for mass creation of signatures
- Solutions based on mobile phones

etc…

Let’s take a look at some examples!

Smart card

- Standardized device ☺
- People can relate to cards ☺ (as they use credit cards)
- Can be personalized ☺
- Needs a card reader ☹
- Driver problems, lack of support on various platforms ☹☹
- CSPs have little or no bargaining power vs card manufacturers ☹☹

USB token

- A personal crypto token, just like a smart card
- No card reader required ☺
- It is harder for people to relate to it ☹
- PIN pad readers cannot be used
  → they are less secure ☹ (?)
- Can be combined with a USB drive ☺/☹
- Same driver problems as smart cards ☹☹☹

Hardware Security Module (HSM)

- Personalized HSM storing the private key of one signatory
  - mass signing, great performance ☺
  - expensive ☹ → for large organizations only
- Multiple signatories have their keys in an HSM of a central server
  - I do not own my private key ☺
  - how do I authenticate to the HSM???
- Not accepted in every member state ☹

Pure software SSCD, without hardware?

- Why not? ☺ It works everywhere! ☺☺
- It is possible to backup the private key ☺/☹
- My experience: a natural person CANNOT take care of a software based private key ☹
- Questionable degree of security ☹☹

- Can be a viable solution for large organizations who can protect a software key ☺☺
- Why the signatory cannot choose the solution that fits her the best?

Mass signing with multiple smart cards

- Sometimes, in some legal environments…
  - mass signing is needed
  - qualified signatures are required
  - an HSM cannot be used as an SSCD

- Solution: A device containing multiple SSCD smart cards is used for mass creation of signature
  Such a device is:
  - such a device should not exist ☹ ☹
  - a circumvention of legislation ☹ ☹
  - a logical response to bad regulation ☹ ☹

Mobile phones (1)

A mobile phone can be viewed as a personal device. ☺

How can we sign using mobile phones?

- SIM card as an SSCD
  - depends on the telco operator ☹
  - depends on the phone ☹
- Additional hardware SSCD connected to the phone
  - heavily depends on the phone ☹☹
  - at least the same driver & compatibility issues as hardware SSCDs in PCs ☹

Mobile phones (2)

- Software on the mobile phone, so the mobile phone becomes the SSCD
  - ❑ depends on the phone ☹
  - ❑ is it really secure? ☹☹
  - ❑ phones change a lot, hard to evaluate ☹☹
- Server-based solution, phone as authentication
  - ❑ does not depend on client platforms ☺☺
  - ❑ I do not have my private key in my pocket ☹
  - ❑ can a rouge telco operator sign on my behalf? ☹

Myths, fairy tales, urban legends (1)

- A QES must be extremely secure!
  - No, it is equivalent with handwritten signatures; a handwritten signature is not secure at all
  - it should be usable; otherwise it shall never be used
  - mass signing: a way of saving money
- QES is so important that it must be strictly separated from everything else!
  - the same card/PIN cannot be used for anything else?
  - this is unrealistic, and makes signatures unusable
- The signatory must view and accept the document before signing it!
  - this does not happen with handwritten signatures in over 90% of the cases

Myths, fairy tales, urban legends (2)

- A PIN must be provided for each QES created!
  - what about mass signing?
- An SSCD MUST establish a secure cypto channel…
  - with what? with the human signatory???
  - with the application? (rules out most applications)
  - with the driver? (what’s the point in that?)
- Security assessment provides additional security
  - evaluation takes LONG, costs a lot of money
  - PC software are complex, there:
    assessed product = product with known vulnerabilities
  - SSCDs are more simple; is their case different?

Myths, fairy tales, urban legends (3)

- ? Smart card readers with PIN pads are more secure
  - PIN pad reader ←→ crypto channel
- ⚡ The document must be hashed on the SSCD for security
  - does not protect the signatory at all
  - but: it may prevent the signatory from using encryption
- ? It is more secure to authenticate the signatory using biometry
- ? CEN SSCD PP is a common ground for SSCDs
  - it focuses on crypto tokens only
  - it has many-many different interpretations
  - in encourages circumvention and ‘evaluation tweaking’

Conclusions & Recommendations

- e-Signing should be simple, otherwise users will not accept it. Signing is not the purpose of existence, people have other things to do.
- Mass creation of e-signatures (or e-seals) is a requirement from the market.
- Natural persons cannot relate to software keys, they can handle a hardware device much better.
- SSCD PP is suits personal crypto tokens the most. It is often blocking innovation and is often circumvented.
- The current regulation or current situation with SSCDs is one of the obstacles blocking the market.
- Relax the requirements, make the technology usable!

Thank you very much! ☺