



European Forum on Electronic Signature
ELECTRONIC SIGNATURE and PKI
GLOBAL TRENDS, EXPERIENCE AND EXPECTATIONS



TRUST & SECURITY ON DIGITAL SINGLE MARKET

12th Edition of the Conference, June 04-06th, 2012

Międzyzdroje, Poland

**Electronic signature - simply, long-term, safely and in
accordance with Commission Decision 2011/130/EU**

Peter Rybár

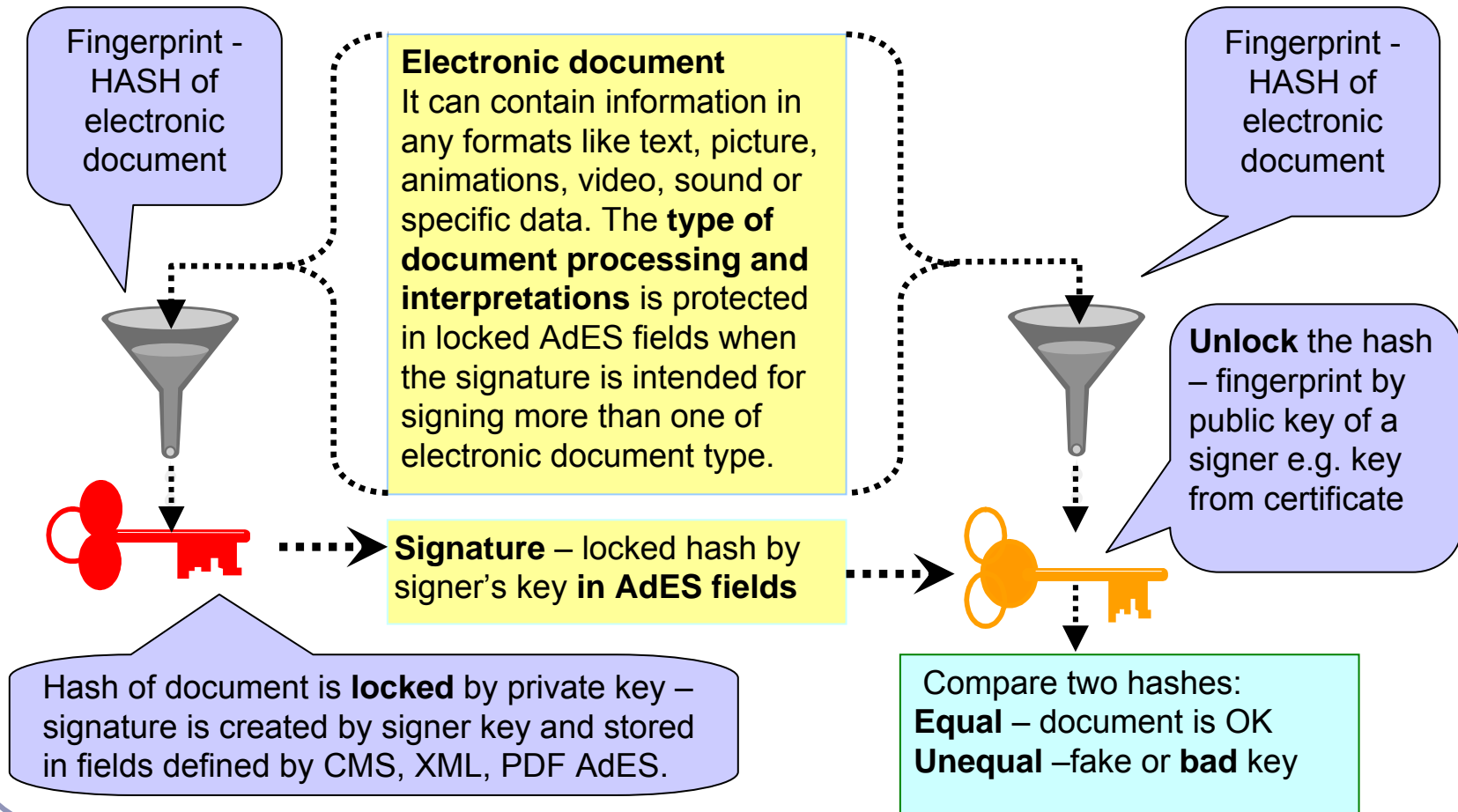
National Security Authority

Information Security and Electronic Signature Department

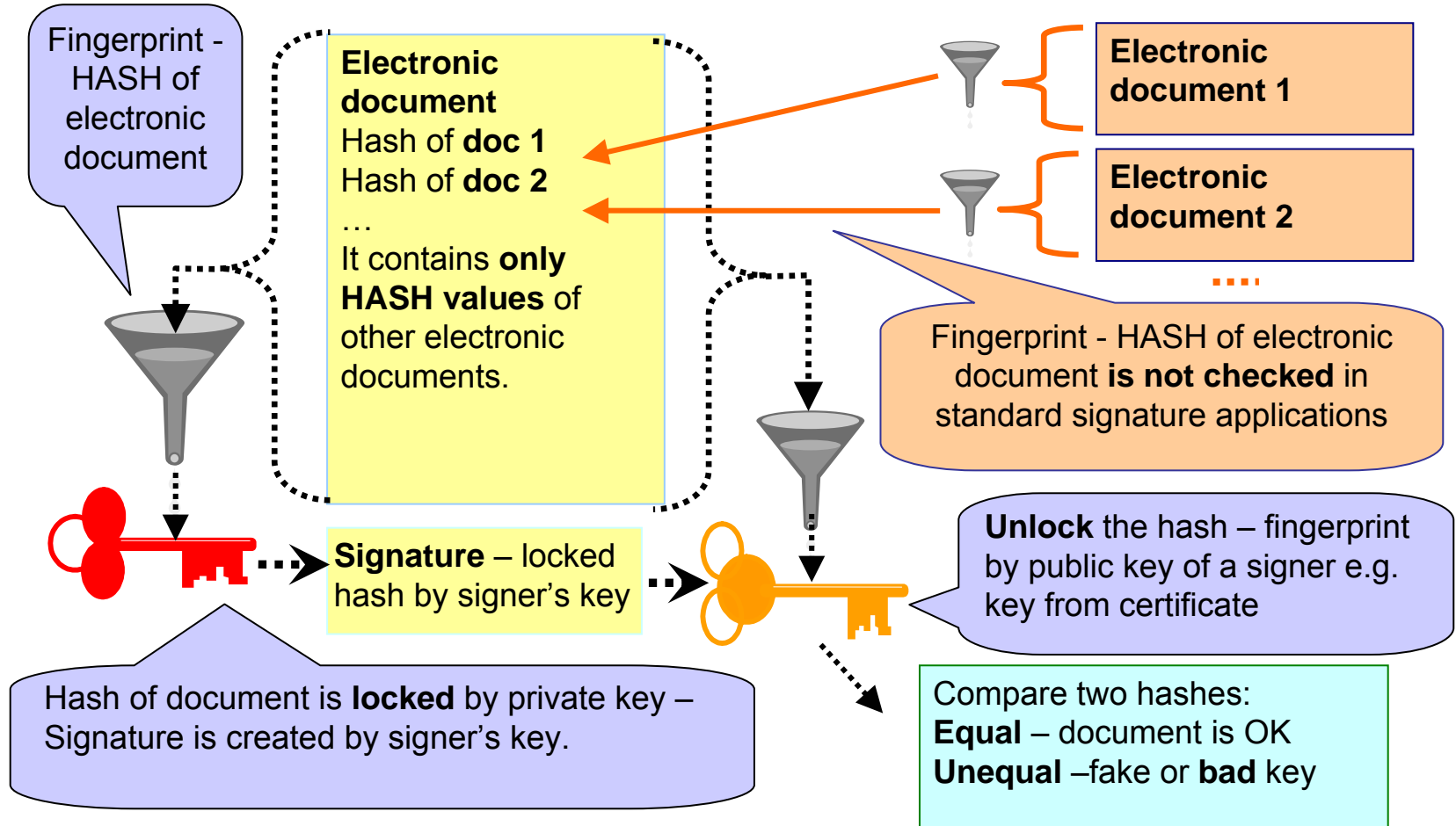
Budatinska 30, 850 07 Bratislava 57, Slovak Republic

<http://www.nbusr.sk/> e-mail: podatelna@nbusr.sk

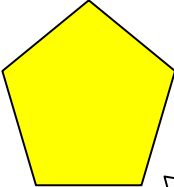
Interoperability - signatures according to CD 2011/130/EU e.g. included in ASiC-S container



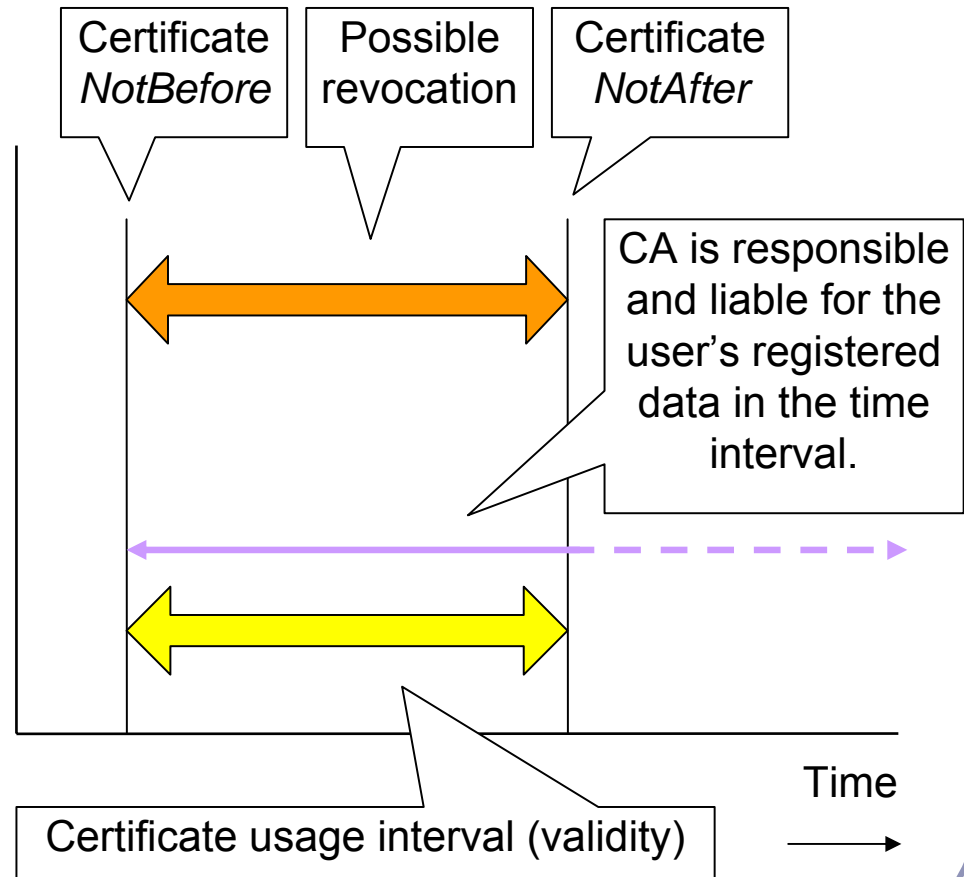
Variety of specific signature formats which are not according to CD 2011/130/EU e.g. as defined in ASiC-E or when the Manifest is used.



The certificate validity period Rec. ITU-T X.509 | ISO/IEC 9594-8:2008



Certificate: validity?
Usage interval is (**notBefore** - **notAfter**) -possible revocation. There is an interval of the CA/RA responsibility and liability of the user's registration data archiving.
This data can be used e.g. in the legal actions.
After the certificate(s) for a public key have expired, a signature verifier **cannot rely on compromises being notified via CRLs**.



Certificate - What do we expect in the long-term validation?

1. Integrity protection

- public key, hash value protected with e.g. archive time-stamp or Positive OCSP response

2. Public key connected with identity

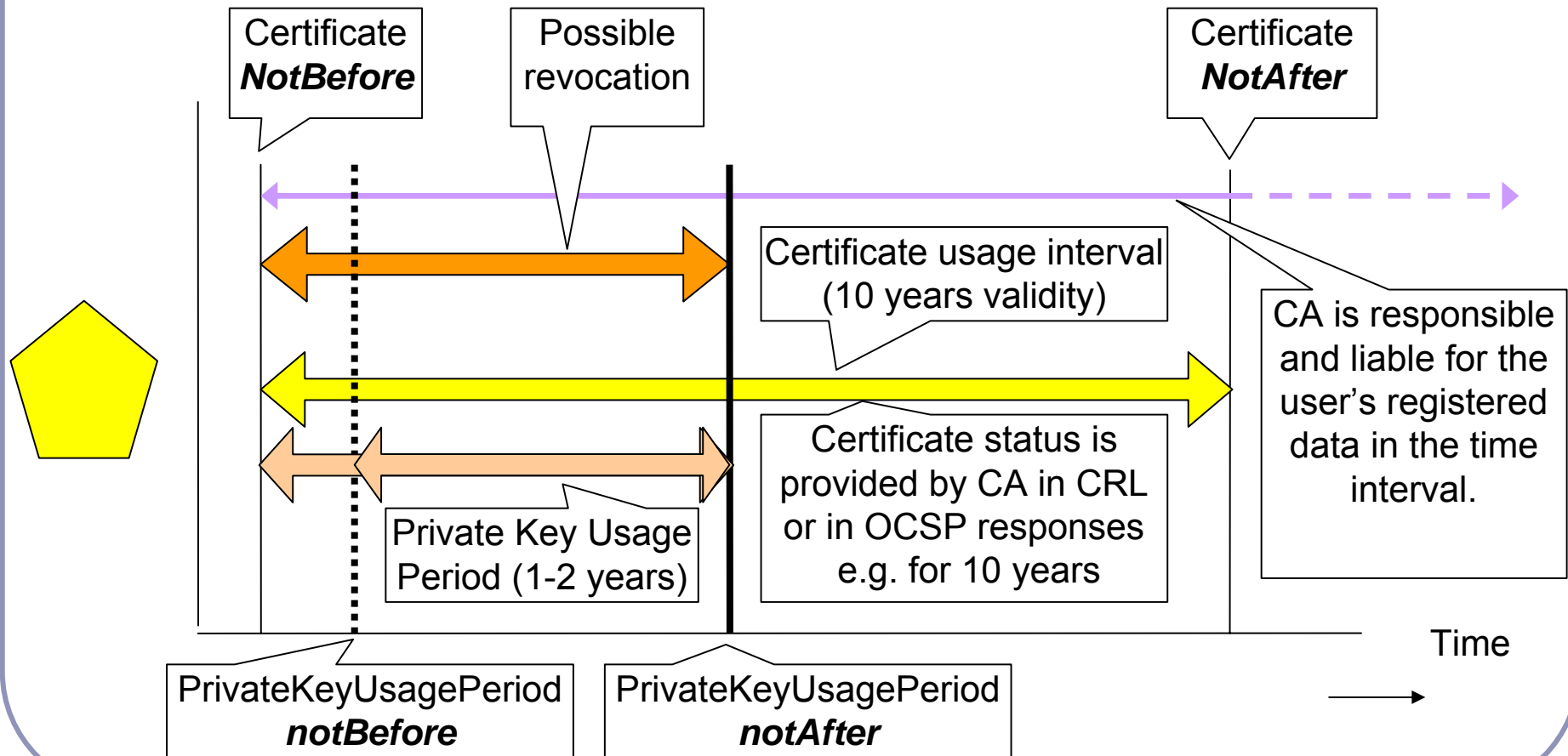
- How long is CA responsible and liable for identify connection in certificate?
- How long can we rely on CA registration database containing identity information usable in e.g. legal proceedings? For 10 years?

ITU-T Rec. X.509: 8.2.2.5 Private key usage period extension

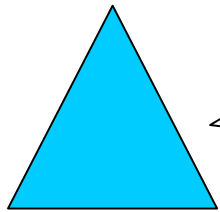
PrivateKeyUsagePeriod ::= SEQUENCE {
 notBefore [0] GeneralizedTime OPTIONAL,
 notAfter [1] GeneralizedTime OPTIONAL }

This field indicates the period of use of the private key corresponding to the certified public key. It is applicable only for digital signature keys.

Private key is used for e.g. 2 years! Signed e-invoice is archived for 10 years and it can be directly validated in 10 years certificate validity period!



Revocation and Update of revocation information in CRL or OCSP

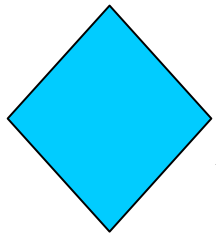


CRL is issued in a regular interval e.g. 12 hours or immediately after revocation.
Retrospective revocation before the time from thisUpdate CRL field **is not possible**.

Certificates statuses are stable in the interval.

CRL-***ThisUpdate***

Time



OCSP is issued immediately after requesting at *ProducedAt*.
Retrospective revocation before the time from thisUpdate of OCSP field **is not possible**.

OCSP-***ThisUpdate***

OCSP-*ProducedAt*

Time

Certificate status is stable in the interval.

Long-term validation with OCSP Single Extensions - CertHash

The **CertHash extension** (Positive Statement) is used in indirect OCSP response as a positive statement that OCSP responder **knows the status** of the certificate and also provides the **integrity protection of** the certificate if the **certificate is already expired** and **algorithms** used in the certificate **could be weak**. The **CertHash extension** (Positive Statement) adopted from Common PKI Optional SigG-Profile is designed to be included in the OCSP singleExtensions of SingleResponse(RFC 2560).

Common PKI Object Identifiers: 1.3.36.8.3.13

```
CertHash ::= SEQUENCE {  
    hashAlgorithm AlgorithmIdentifier,  
        -- The identifier of the algorithm that has been used  
        -- the hash value below.  
    certificateHash OCTET STRING  
        -- The hash over DER-encoding of the entire PKC or AC  
        -- (i.e. NOT a hash over tbsCertificate).  
}
```

Long-term validation with OCSP

Single Extensions - ProofOfExistence

The OCSP response with **ProofOfExistence** extension of signer's signature can be used as a secure time-mark with the **same functionality** as expected from **the signature time stamp**. The ProofOfExistence extension is designed to be included in the singleRequestExtensions of OCSP(RFC 2560) and the same ProofOfExistence must be included in the singleExtensions of SingleResponse(RFC 2560).

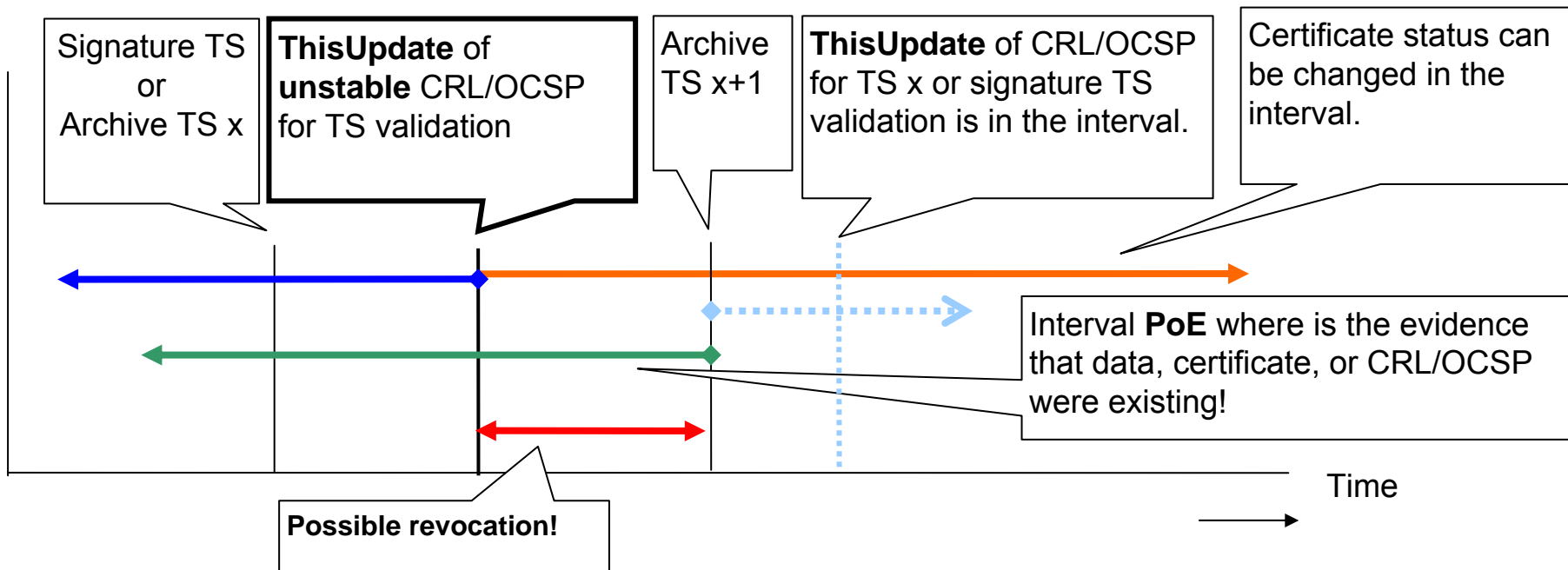
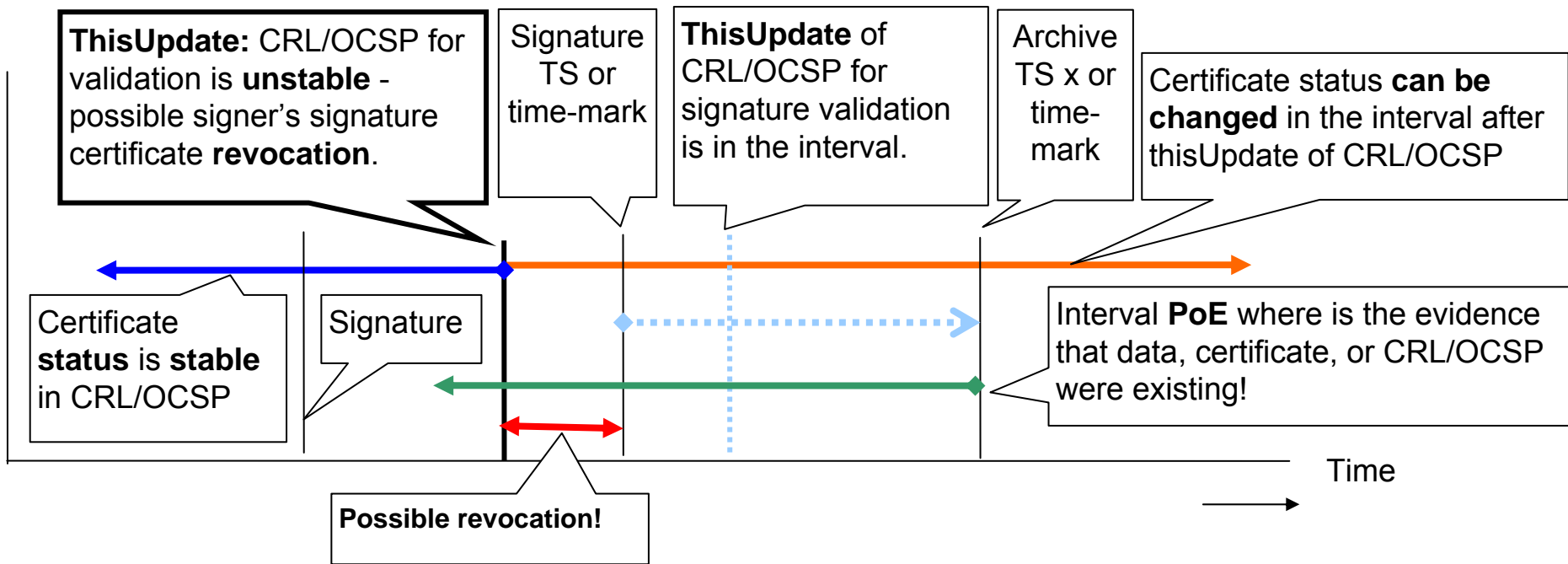
Object Identifiers: 1.3.6.1.4.1.38655.1.4

```
ProofOfExistence ::= SEQUENCE {  
    poEType PoEType DEFAULT poESignerSignatureBinOctets,  
    poE MessageImprint  
}  
PoEType ::= INTEGER { poESignerSignatureBinOctets(0), poEAnyDATA(1) }  
  
MessageImprint ::= SEQUENCE {  
    hashAlgorithm      AlgorithmIdentifier,  
    hashedMessage      OCTET STRING  
}
```

The long-term validation

The long-term validation must use only information which was **updated after the time to which we validate** the certificate.

Information updated before that time is not stable and **later** could be **changed**. Selection of CRL or OCSP response must be according to ***thisUpdate*** time whose time value must be later than the signature verification time (signature time-stamp or signature time-mark). Any new certificate revocation time must be with a time value after ***thisUpdate*** time of the latest CRL or OCSP. It means before the time value ***thisUpdate*** of CRL or OCSP the new revocation must not be realized as a basic rule because a backward revocation is not permitted.



Proof of Evidence (PoE)

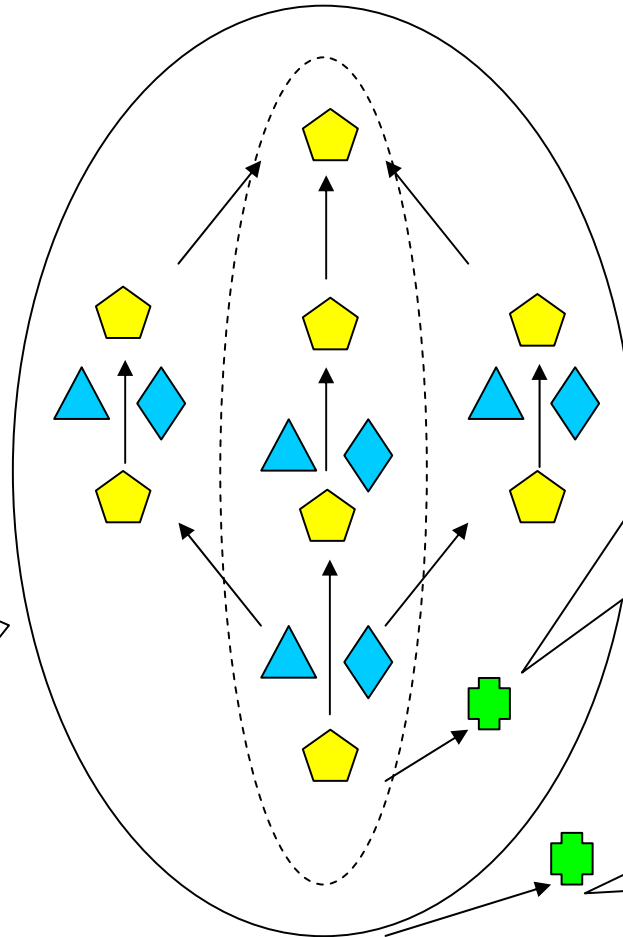
When the usage of the signed document and the signature is expected for the long-term perspective then there must exist a provable evidence that a particular object existed at a particular time.

The object which can be used as a proof of evidence (PoE) of particular object existence in the past is e.g. an archive timestamp (ATS) or time mark where at least two types of information are present: the protection of data and the protection of time when such protection of data was realized.

PoE protects from the usage of fake objects created e.g. now with algorithms broken now, claiming that the object was created in the past.

Complex X.509 PKI validation

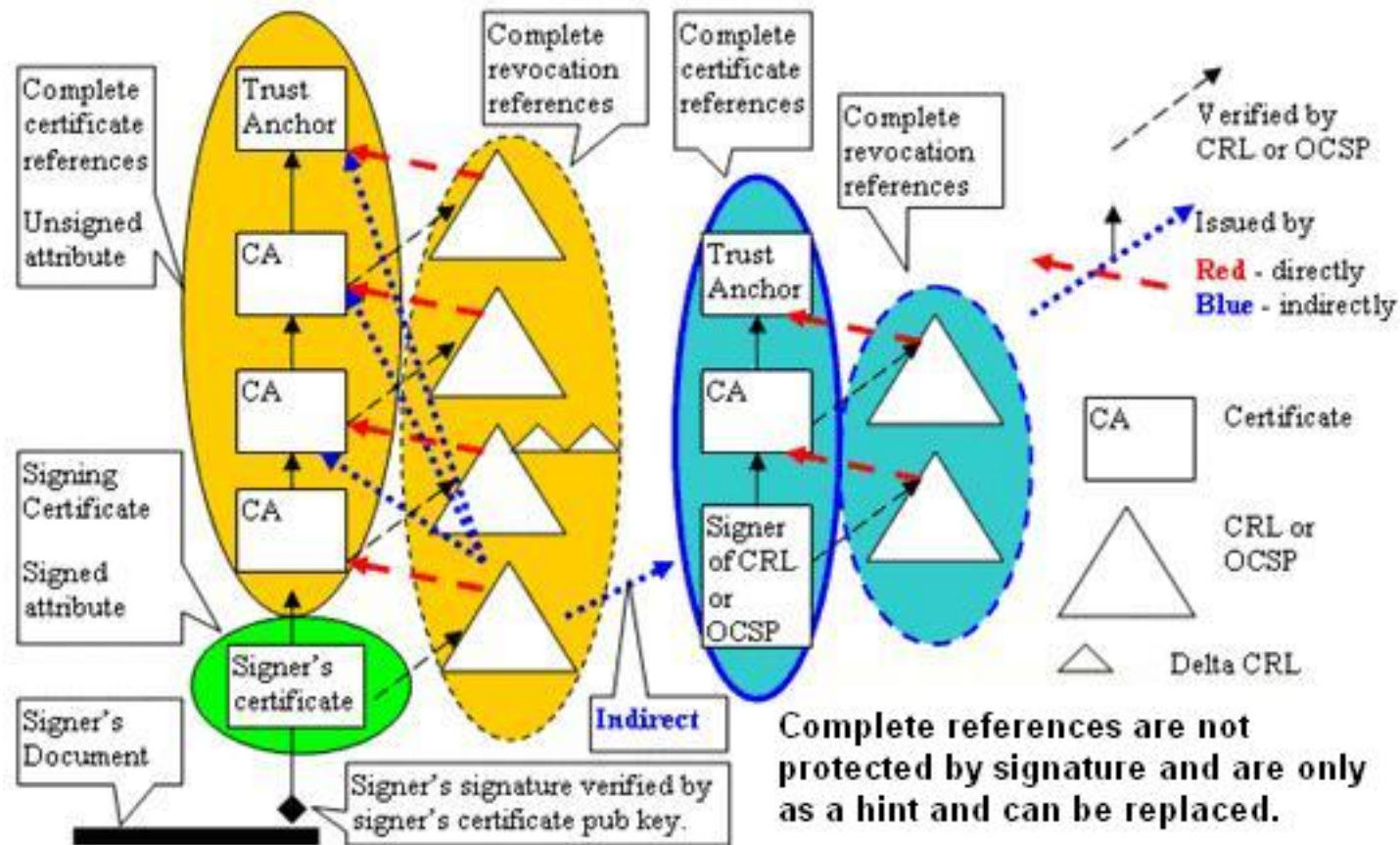
Time of the validation moment of CRL or OCSP signature is according to the actual time or interval in the past before **archive time-stamp (PoE)**. If the actual time is used then *thisUpdate* is the max bound of the time to which the verification was realized (possible revocation after *thisUpdate*).



Time of the validation moment of the signer's certification path is according to the **signature time-stamp**

(Archiving)
Time-stamp
protects the
data (PoE).

ETSI ESI deprecates long-term formats
in chapter 8 ETSI TS 103 173 V2.1.1
(2012-03) and requires a new one

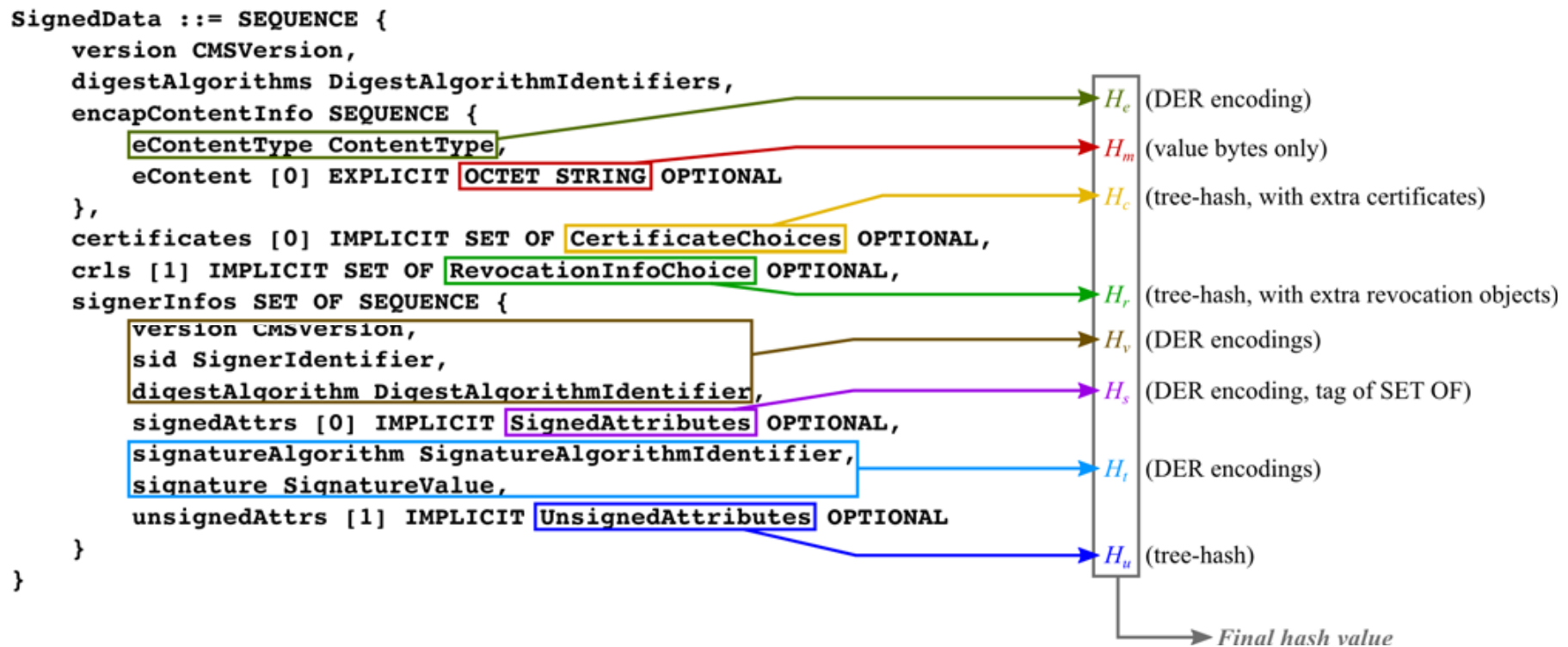


CAdES version 2.1.1 defines a new long-term-validation attribute to replace old validation material attributes

The archive attributes ATS, ATSp2 and a new long-term-validation attribute defined in [CAdES version 2.1.1](#) have at least the following interoperability problems and limitations:

- ATS, ATSp2 and a new long-term-validation attribute are not backward compatible with CMS.
- When parallel CMS signatures are used then new parallel signature must be included only before adding of any ATS, ATSp2 and a new long-term-validation attribute in any parallel signature because by including a signer's certificate the hash of archiving attributes will be destroyed.
- CMS validation systems are not able to locate Certificates, CRLs and OCSP responses in many attributes defined by ETSI ESI.
- CMS UnsignedAttributes are usually BER encoded to achieve a one-pass processing but ETSI TS 103 173 V2.1.1 requires only DER what causes complicated attribute processing with dangerous limitations and forbids to use many of CAdES implementations created according to CD 2011/130EU.
- Requirements of ETSI TS 103 173 V2.1.1 are inconsistent in some chapters. In chapter 8 (LT-Level) there is deprecated the use of old long-term attributes but in chapter 6 there is required as mandatory DER encoding for the old long-term attributes – DER is expected only for ATS. DER encoding of UnsignedAttributes is irrelevant for a new mandatory long-term-validation attribute required in ETSI TS 103 173 V2.1.1 and mandatory DER requirements have dangerous impact on existing implementations.

New hash processing requires ordering but does not ensure a selection of particular attributes (intended for e.g. parallel CMS signatures) by CADES ETSI TS 103 173 V2.1.1 (2012-03) and ETSI TS 101 733 V2.1.1 (2012-03).



Proposal of a new ATSV3 was registered on ETSI ESI to achieve interoperability and backward compatibility with CMS

The new ATSV3 together with a new ATS attribute ATSHashIndex will fix all mistakes and dangerous limitations mentioned in previous slides of previous archiving attributes and a new ATS attribute ATSHashIndex determines the presence and the order of objects included in ATS hash computations what is a way how to achieve a backward compatibility with the present ATS and provide the evidence which objects like certificates, CRL or OCSP responses were protected by ATS in PoE interval (Proof of Existence). The new ATSV3 defines new rules where only objects of CertificateSet, RevocationInfoChoices and UnsignedAttributes are included in ATS hash calculations. There is also a proposal to include a new signature policy attribute where the machine processable signature policy will be stored for the long-term validations.

The archive-time-stamp-v3 attribute

The archive-time-stamp-v3 attribute is a time-stamp token. To achieve a backward compatibility with CMS and to protect the signature when parallel signatures are used from redundant objects presence, certificates are included in **SignedData-certificates**, CRLs are included in **SignedData-crls** and **OCSF** responses are included in SignedData-crls-[1] where SignedData-crls-[1]otherRevInfoFormat MUST contain **OID id-pkix-ocsp-basic** (1.3.6.1.5.5.7.48.1.1) and **SignedData-crls-[1]otherRevInfo** MUST contain **BasicOCSPResponse**. The BasicOCSPResponse is defined in RFC 2560 and when is used for the long-term validation it MUST contain at least OCSF signer's certificate in BasicOCSPResponse-certs when the certificate is not included in SignedData-certificates.

id-aa-ets-archiveTimestampV3 OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) nbu-sk(38655) pkiattribute(1) 5 }

ArchiveTimeStampToken ::= TimeStampToken

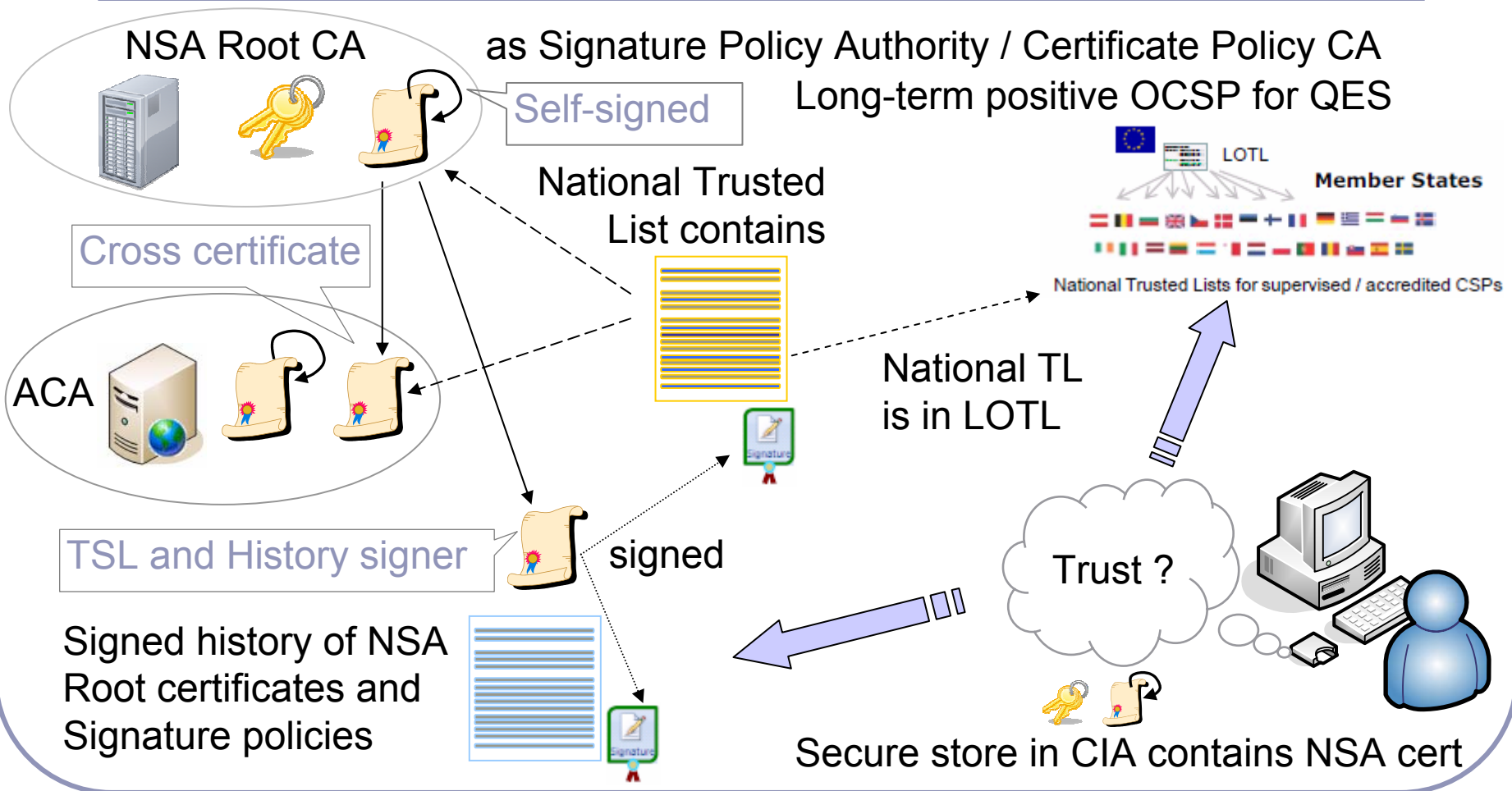
The ATSHashIndex unsigned attribute of ATSV3

The ATSHashIndex attribute is designed to be included in the archive time-stamp (ATS) as an unsigned attribute to allow indexing of hashed objects of SET of signedData-certificates, SignedData-crls and the unsigned attributes of the signature which is archive time-stamped. It means this attribute fixes interoperability problems concerning ordering of BER encoded SET attributes and problems with identification of objects which must not be included in ATS hash calculation (e.g. objects included after ATS).

id-aa-ATSHashIndex OBJECT IDENTIFIER ::= { iso(1) org(3) dod(6) internet(1) private(4) enterprise(1) nbu-sk(38655) pkiattribute (1) 6 }

```
ATSHashIndex ::= SEQUENCE {  
    hashIndAlgorithm AlgorithmIdentifier  
    DEFAULT {algorithm id-sha256},  
    certificatesHashIndex SEQUENCE OF Hash,  
    crlsHashIndex SEQUENCE OF Hash,  
    unsignedAttrsHashIndex SEQUENCE OF Hash  
}  
Hash ::= OCTET STRING
```

One key of NSA Root CA for QES





Thank you for your attention!

Sources:

Interoperability - National profile according to CD 2011/130/EU:

<http://www.nbusr.sk/en/electronic-signature/verification/index.html>

<http://www.nbusr.sk/en/electronic-signature/signature-policies/index.html>

Freeware application LockIt created mainly for SK NSA in English, German, Russian and... languages to sign any documents in ZIP package ASiC-S with CAdES, XML Trusted List, PDF and History List of the NSA Root CAs and Signature policies

<http://lockitin.webnode.sk/products/produkt-1/>

Ing. Peter Rybár e-mail: peter.rybar@nbusr.sk