Electronic Signature

István Zsolt BERTA
istvan@berta.hu

Electronic Signatures - Contents

Electronic Signature

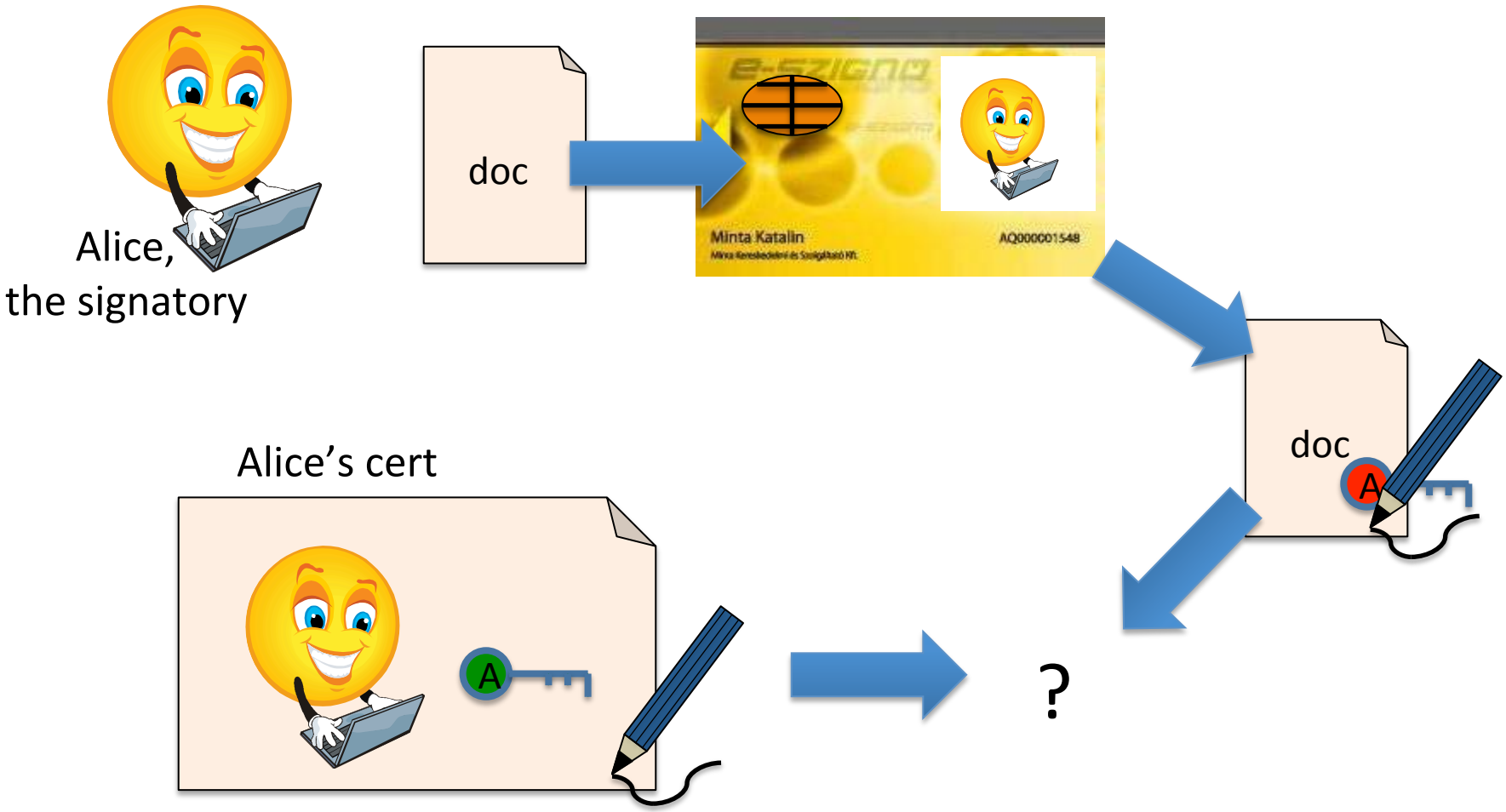
1. What is an electronic signature? E-signature laws
2. Electronic signature creation
3. Time stamping
4. Electronic signature verification
5. Long-term validity of the e-signature

What is an electronic signature?

Electronic signature

- Electronic signature means ‘authenticating’ an electronic document in an electronic way
- so that it can be ‘proven’ who signed it and what had been signed
- Electronic signatures are recognized by law
- Certain forms of electronic signatures can be considered equivalent with handwritten signatures
  - depending on the legislation
  - examples: encoding or adding info about the signatory
- This allows e.g. contracts / declarations to be made in a purely electronic format, without the use of paper

Digital signature



- Encoding with Alice's private key,
  anyone can verify it with Alice's public key in her cert

Electronic signature vs Digital signature

- Electronic signature is a **legal** term – used for electronic authentication recognized by law
- Digital signature is a **technical** term – used for encoding with one's private key
- Not all electronic signatures are digital signatures
  - example: writing one's name at the end of an e-mail message
- Not all digital signatures are electronic signatures
  - example: usage of private key in case of a TLS authentication

- Electronic signatures are not necessarily based on PKI and digital certificates – but the most 'advanced' ones are

EU directive 1999/93/EC (current, until 2016)

- Directive 1999/93/EC of the European Parliament and of the Council – on a Community framework for electronic signature
- Defines key terms:
  - electronic signature
  - certification service provider (CA)
  - advanced electronic signature
  - certificate
  - qualified certificate
  - secure signature creation device
- Electronic signature based on a qualified certificate, created with a secure signature creation device (=qualified electronic signature)

EU directive 1999/93/EC (current, until 2016)

Advanced electronic signature shall meet the following requirements:

"(a) it is uniquely linked to the signatory;

(b) it is capable of identifying the signatory;

(c) it is created using electronic signature creation data that the signatory can, with a high level of confidence, use under his sole control; and

(d) it is linked to the data signed therewith in such a way that any subsequent change in the data is detectable."

Advanced electronic signature based on a qualified certificate and created using a secure signature creation device
(= qualified electronic signature)

EU directive 1999/93/EC (current, until 2016)

- Public service providers are under supervision in each Member State of the EU
- Legal effect:
  - qualified electronic signature: equivalent with a handwritten electronic signature
  - qualified electronic signature: cross-border, recognized in all Member States
  - signature cannot be rejected solely because it is electronic or because it is not qualified
- CSP (CA) is liable for the electronic signatures
- CSP may limit the usability of the certificate (QCStatements extension)

EU regulation (new, from 2016)

- Regulation of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC – full text
- Regulation, not just a directive; comes into effect 1st of July, 2016
- Electronic identification schemes – Member States shall define how they identify their citizens, and share this information with other Member States
- Cooperation, breach notification
- Trust services lists
- Multiple trust services

EU regulation (new, from 2016)

- Trust services
  - electronic signatures (natural persons)
    - » certificates for QES
    - » validation service
    - » preservation service
  - electronic seals (legal persons)
  - time-stamping
  - electronic registered delivery
  - website authentication
- Trust services can be provided as qualified or non-qualified
  - qualified trust services providers need to prove in court that they had not been negligent
  - qualified trust services enjoy a presumption that they are provided 'well'; the opposite needs to be proven

Qualified vs Non-Qualified

- The difference is mostly legal, the cryptographic technology behind them is the same
- Differences are:
  - probative force
  - cross-border acceptance
  - service provider's liability
  - requirements on key management

Qualified signature

- Is it more secure → not necessarily
- Qualified means it is equivalent with a handwritten signature
- As a Relying Party you have more info on what applies to the qualified signature, e.g.:
  - Face-to-face registration
  - Supervised CA
  - CA is liable for the certificate
  - Secure Signature Creation Device
- It is ‘more straightforward’ to accept qualified signatures

US law

- Electronic Signatures in Global and National Commerce Act ("ESIGN")
  - a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforce-ability solely because it is in electronic form
  - contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation

- No direct mention of PKI or digital signatures
- Detailed requirements on what the consumer has to be informed of, and what the requirements are for obtaining the consumer's consent, and what information has to be retained

E-signed document

- A document with a(n advanced) electronic signature is authentic
- where authenticity is provided by its encoding

- Thus are all copies of the signed document also ‘original’

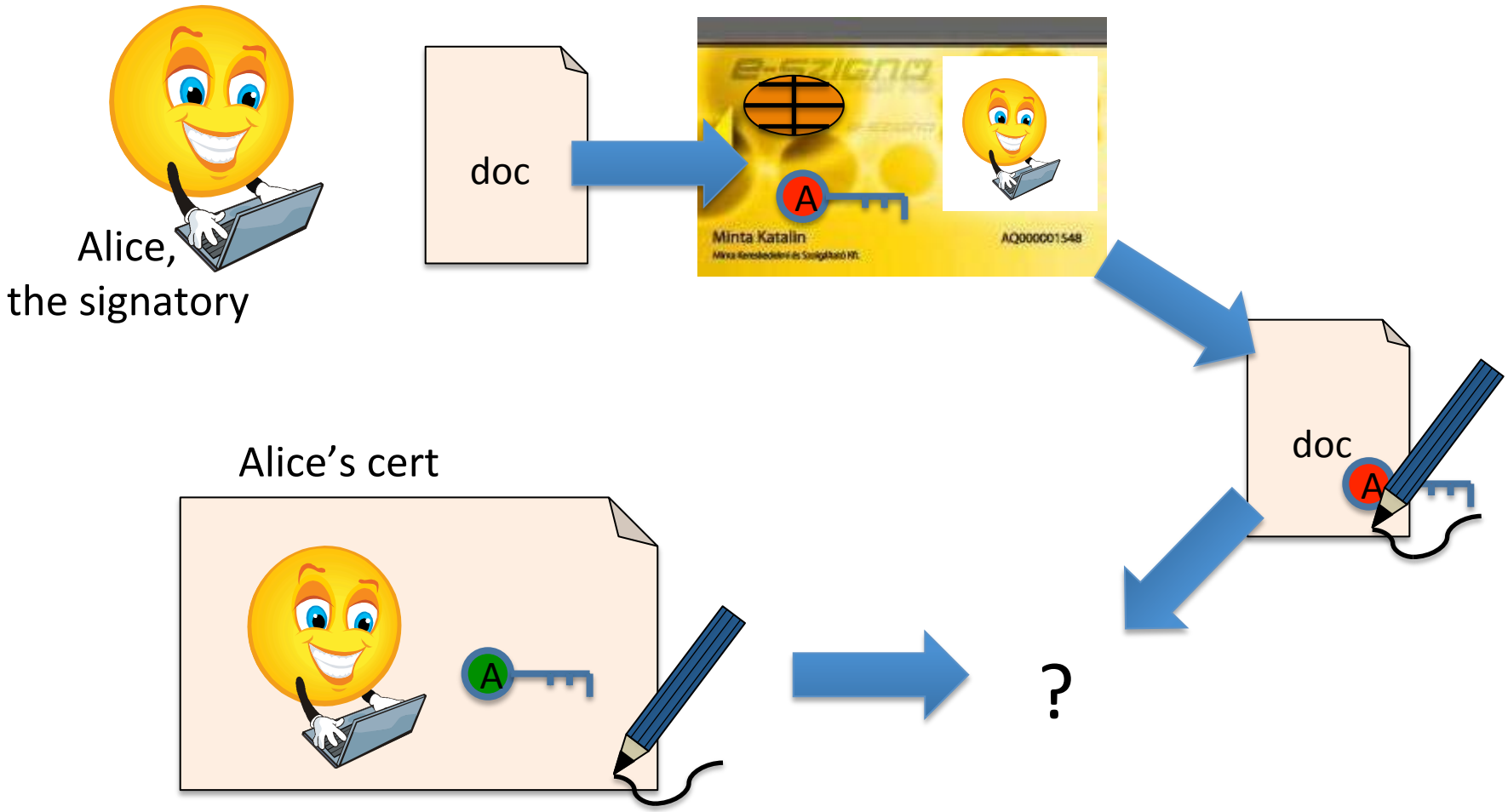
Non-Repudiation

- Electronic signature is commonly associated with non-repudiation
- Laws do NOT use this term, they use:
  - probative force
  - presumption
- if the signature is valid
- Technical verification of the signature:
  - is the signature created with the user's private key?
  - was the user's certificate valid at the time of signing?
- Legal questions:
  - did the signatory sign the document?
  - did he/she understand it and intend to sign it? was there consent?
  - meeting of the minds

→ Non-repudiation is just a technical term

Electronic signature creation

Electronic Signature creation

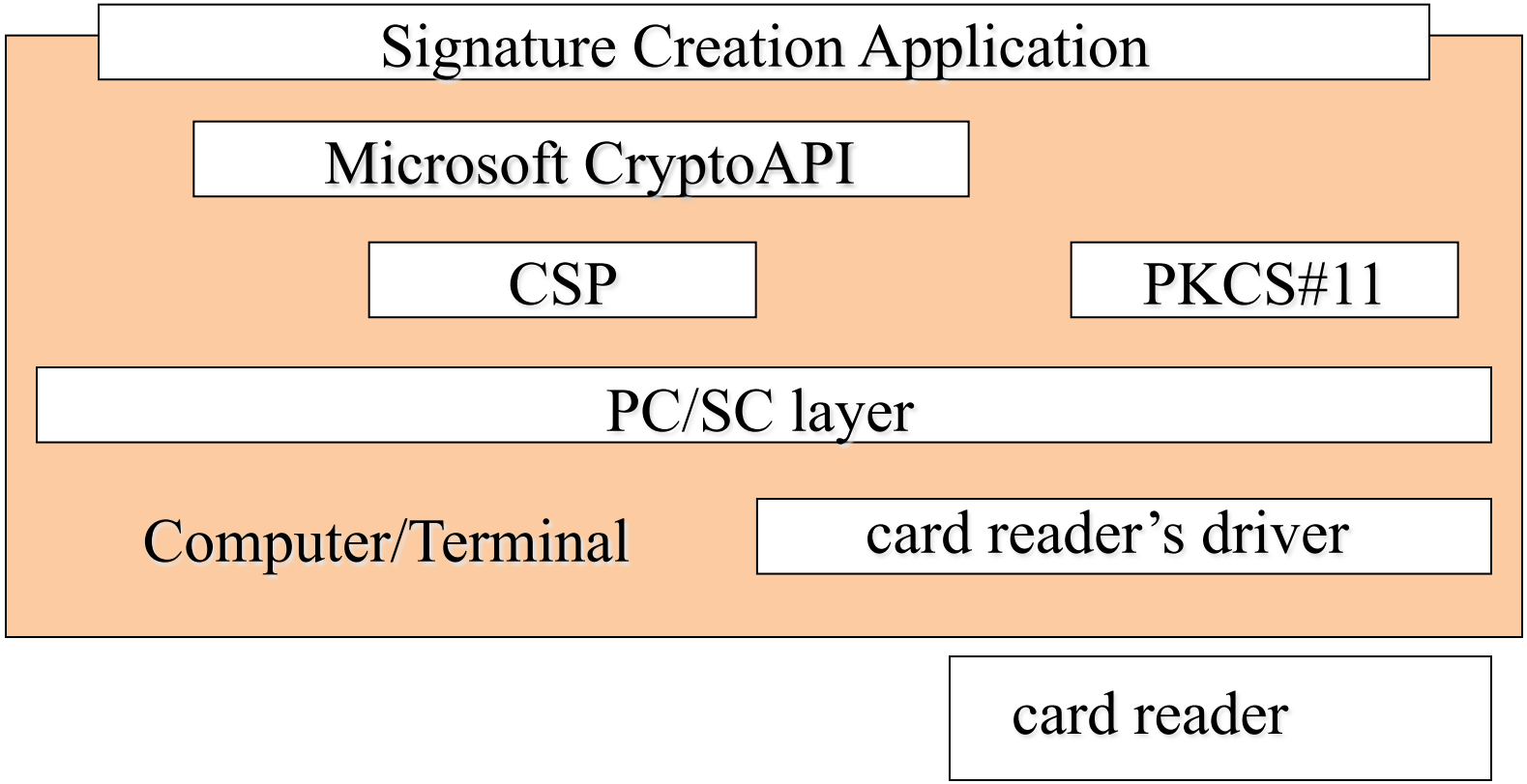


- Henceforth, we consider at least advanced electronic signatures only

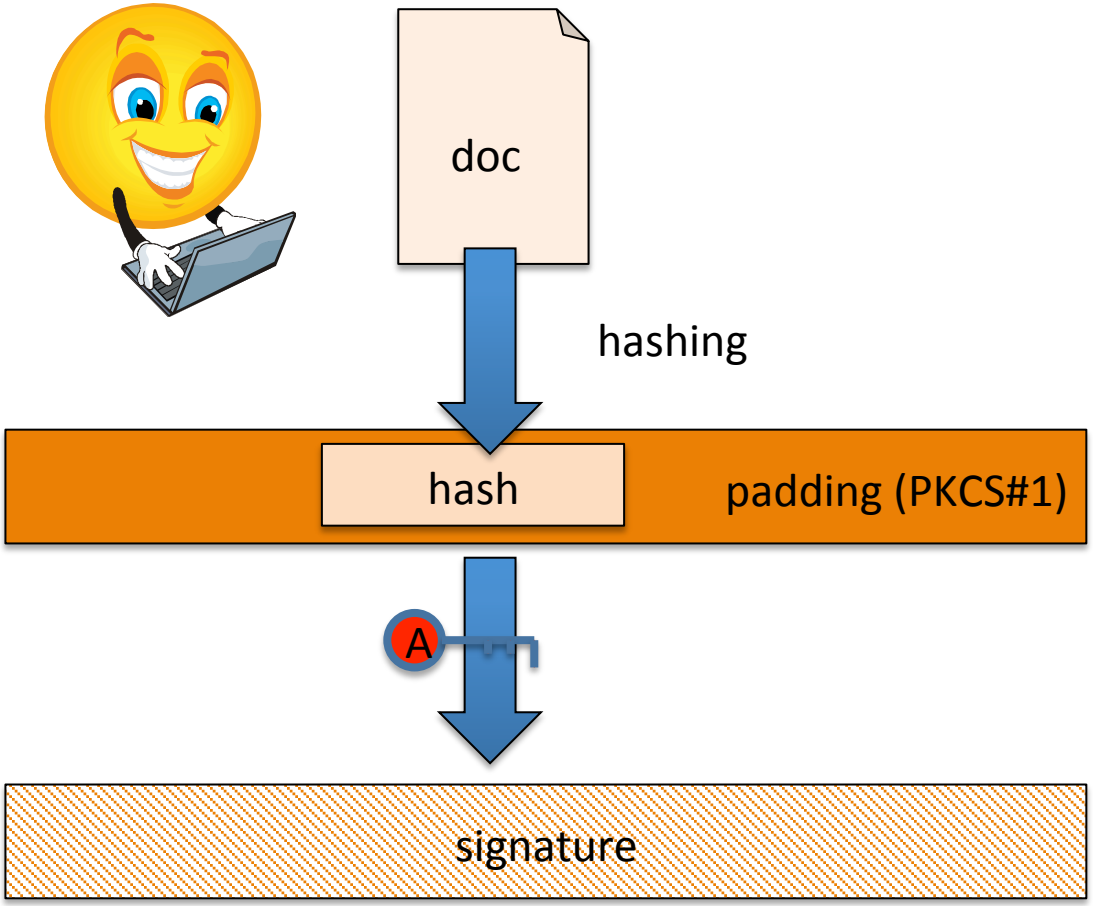
Signature creation

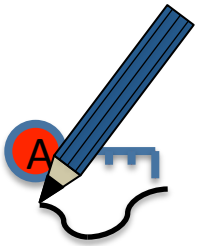
1. The signatory reviews a document and decides to sign it
2. The signatory gives the document to a Signature Creation Application
3. The Signature Creation Application computes a hash of the document and sends the hash to a (Secure) Signature Creation Device
4. The Signature Creation Device computers the signature using the private key and sends it back to the Signature Creation Application, who appends it to the document

Communication with a smart card

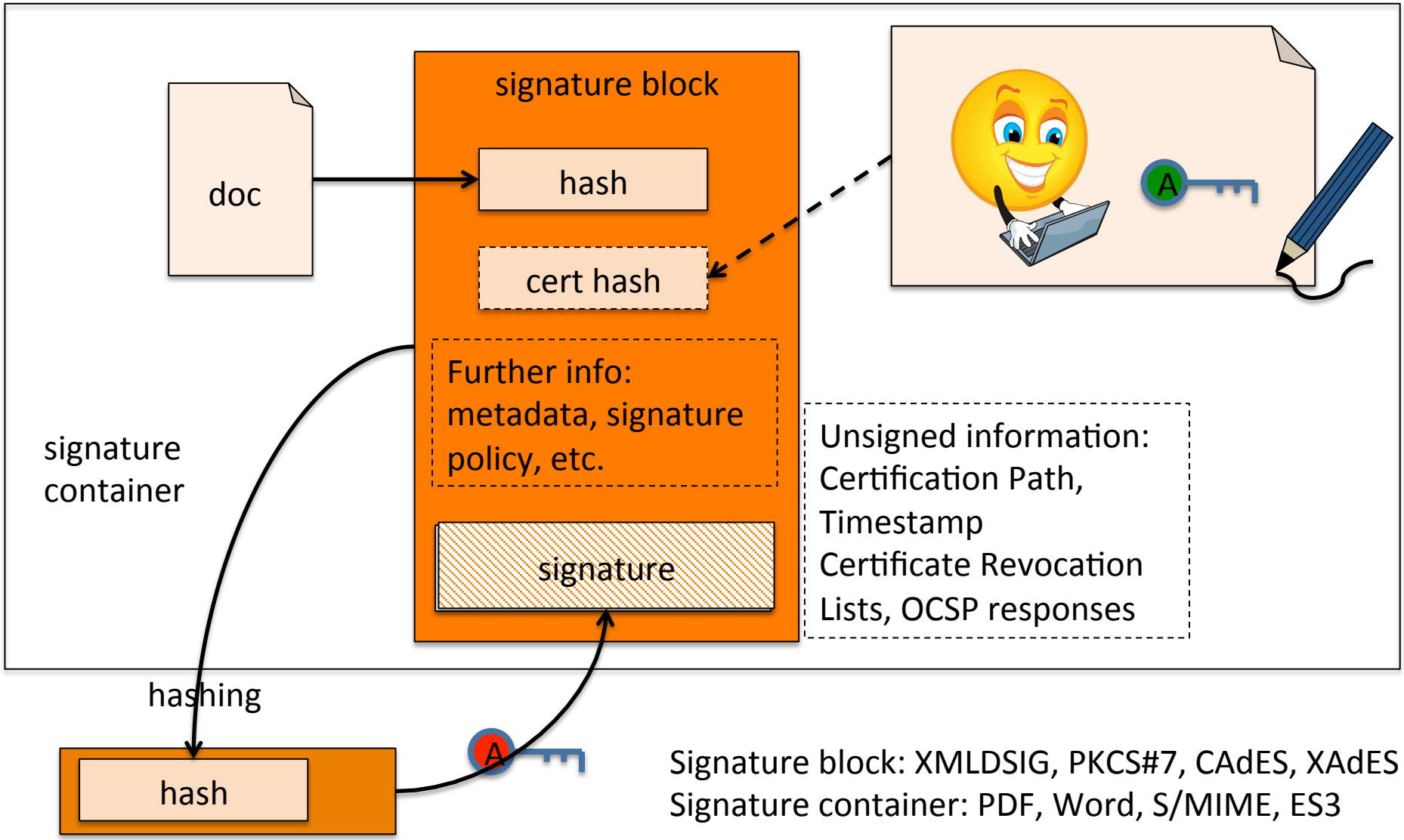


Signature creation





Signature Creation (detailed)



Signature block: XMLDSIG, PKCS#7, CAdES, XAdES
Signature container: PDF, Word, S/MIME, ES3

Signature formats

- In practice, signature is not computer over a hash of the document but over a signature block (which contains the hash of the documents)
- ASN1-based formats
  - PKCS#7, CMS
  - CAdES (ETSI extension)
- XML-based formats
  - XMLDSIG
  - XAdES (ETSI extentsion)
- Signature format: describes how the signature was created, refers to policies, contains paths, CRLs, etc
- Container format: helps you find what was signed, helps you when opening the signed doc, helps you manage multiple signature

XMLDSIG signature

```
<ds:Signature>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="..." />
    <ds:SignatureMethod Algorithm="..." />
    <ds:Reference Id="..." URI="...">
          <ds:Transforms> ... </ds:Transforms>
          <ds:DigestMethod Algorithm="..." />
          <ds:DigestValue>...</ds:DigestValue>
     </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue ...> ... </ds:SignatureValue>
  <ds:KeyInfo ...> ... e.g. signer's cert ... <ds:KeyInfo>
    ...
</ds:Signature>
```

XADES Signature

```
<ds:Signature>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="..." />
    <ds:SignatureMethod Algorithm="..." />
    <ds:Reference Id="..." URI="..."> ... </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue ...> ... </ds:SignatureValue>
  <ds:KeyInfo ...> ... <ds:KeyInfo>
  <ds:Object><xades:QualifyingProperties>
        <xades:SignedProperties> signature policy ref;
    location and time of signature, ...
    </xades:SignedProperties>
        <xades:UnsignedProperties> timestamp, revocation
    information, ...</xades:UnsignedProperties>
    </xades:QualifyingProperties></ds:Object>
</ds:Signature>
```

Signature & Signed document

- Detached signature – two separate files
  - you should NEVER lose connection
- Signature format is also a container
  - e.g. Word or PDF
  - easy to open
  - difficult to enforce a signature/verification policy
- Container is also a signature format
  - e.g. enveloping XAdES signature or ES3 dossier
  - easy to verify signatures with a unified policy
  - signatures need to be unpacked before verification

PDF signature

- Document + signature container at once
- Contains PKCS#7 or CAdES signatures
- Supports visible signatures
- Straightforward: one document, one signature
- Not-so-straightforward: multiple signers, archive signatures, signatures over non-PDF files
- ETSI 102 788 - PAdES

ES3 dossier (widely used in Hungary)

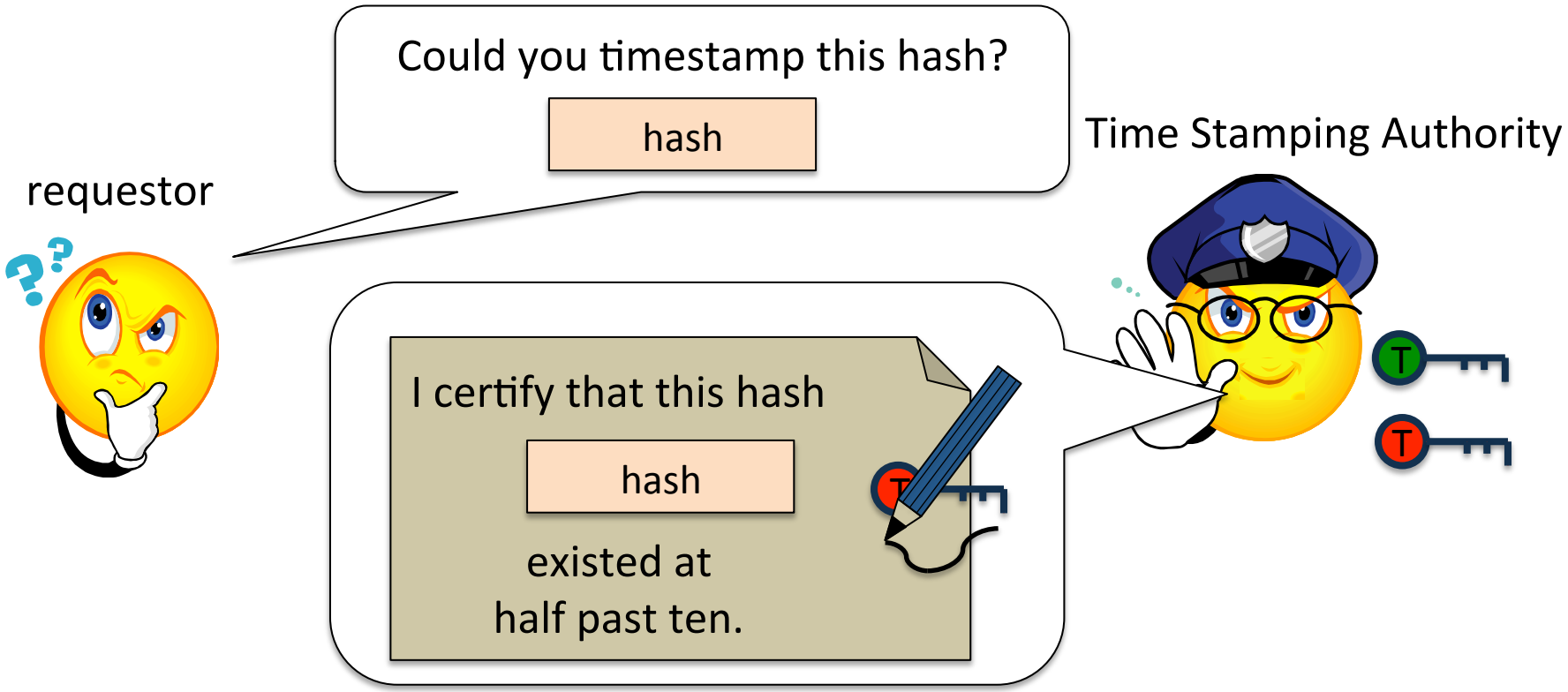
- See specification here
- XML container format
- May contain multiple documents and multiple XAdES signatures over them
- Metadata for documents
- Supports workflows
- Signatures can be time stamped and/or archived

OpenOffice signatures

- ZIP file with a fixed structure
- the file META-INF/documentsandsignatures.xml may contain multiple signatures
- XMLDSIG signatures only, they can be XAdES too…
- Problems: no timestamps, compatibility issues

Time stamping

Time stamping



- Online question, online answer with a secure time
- TSA is required to maintain a secure clock
- Provides signed answers
- RFC 3161

Time stamping as a trust service

- Provides a secure time
- Links the secure time to a document
- Has probative force
- Has a standard format

Why time stamp?

- A signed document's lifetime may significantly exceed that of the certificate
- Signatures must remain valid even if the signatory's certificate
  - expires
  - is revoked
- In order to verify a signature, we need a secure point in time when we can be sure the signature already existed
- Time stamps provide this source of time

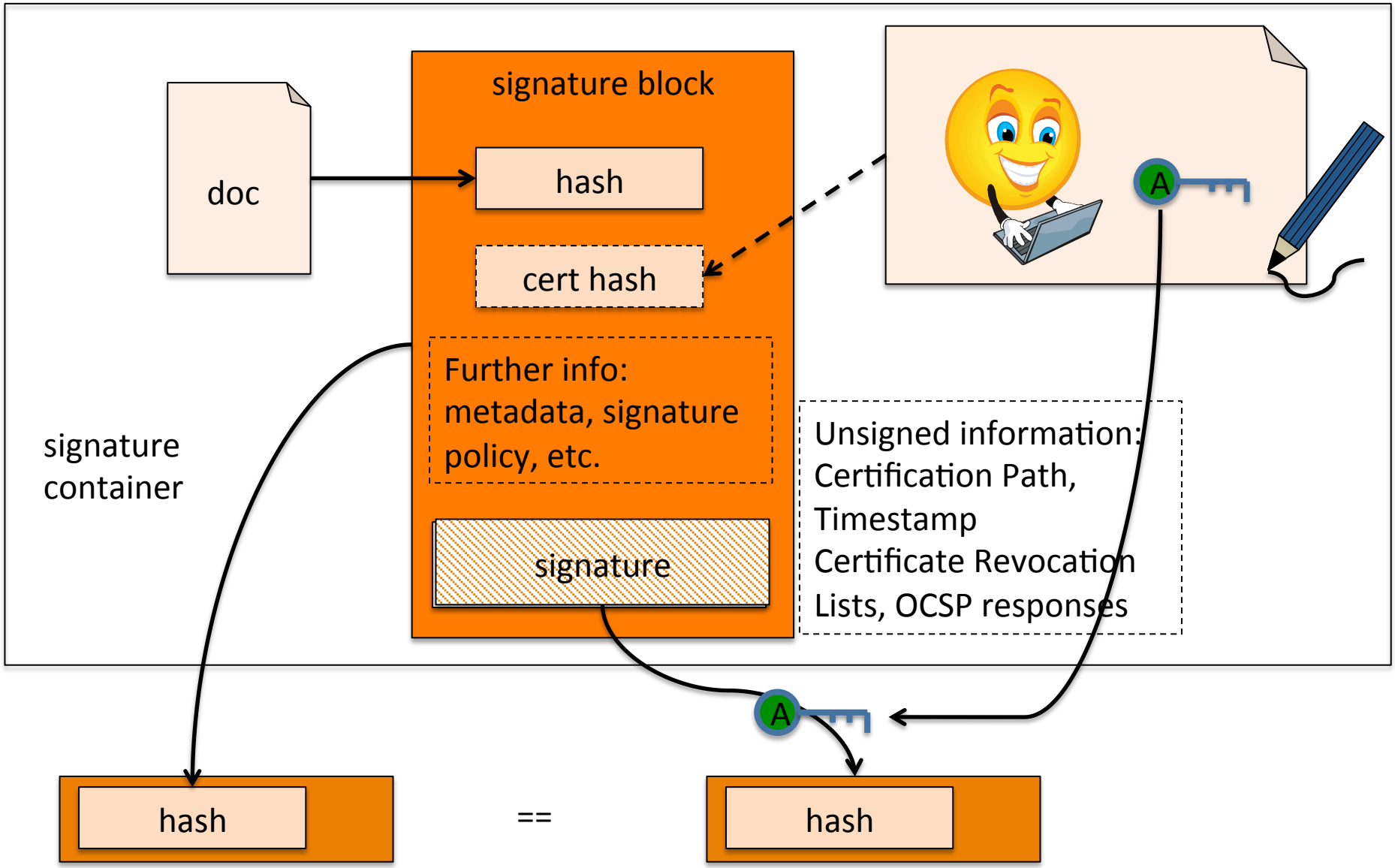
- Signature verification is usually based on time stamps

Signature verification

Signature verification

- Verify technical validity
  - cryptographic verification - does the required relation exist between the document, the public key and the signature?
  - was the signatory's certificate valid at the time of signing?
- Is the signature acceptable in the given legal & organizational context?
  - level of security of the signature
  - was the signer authorized to sign?
  - how sure am I in the validity of the signature?
  - signature policy?
  - did the signer mean to sign the document?
  - was it the signer (person) who signed the document?

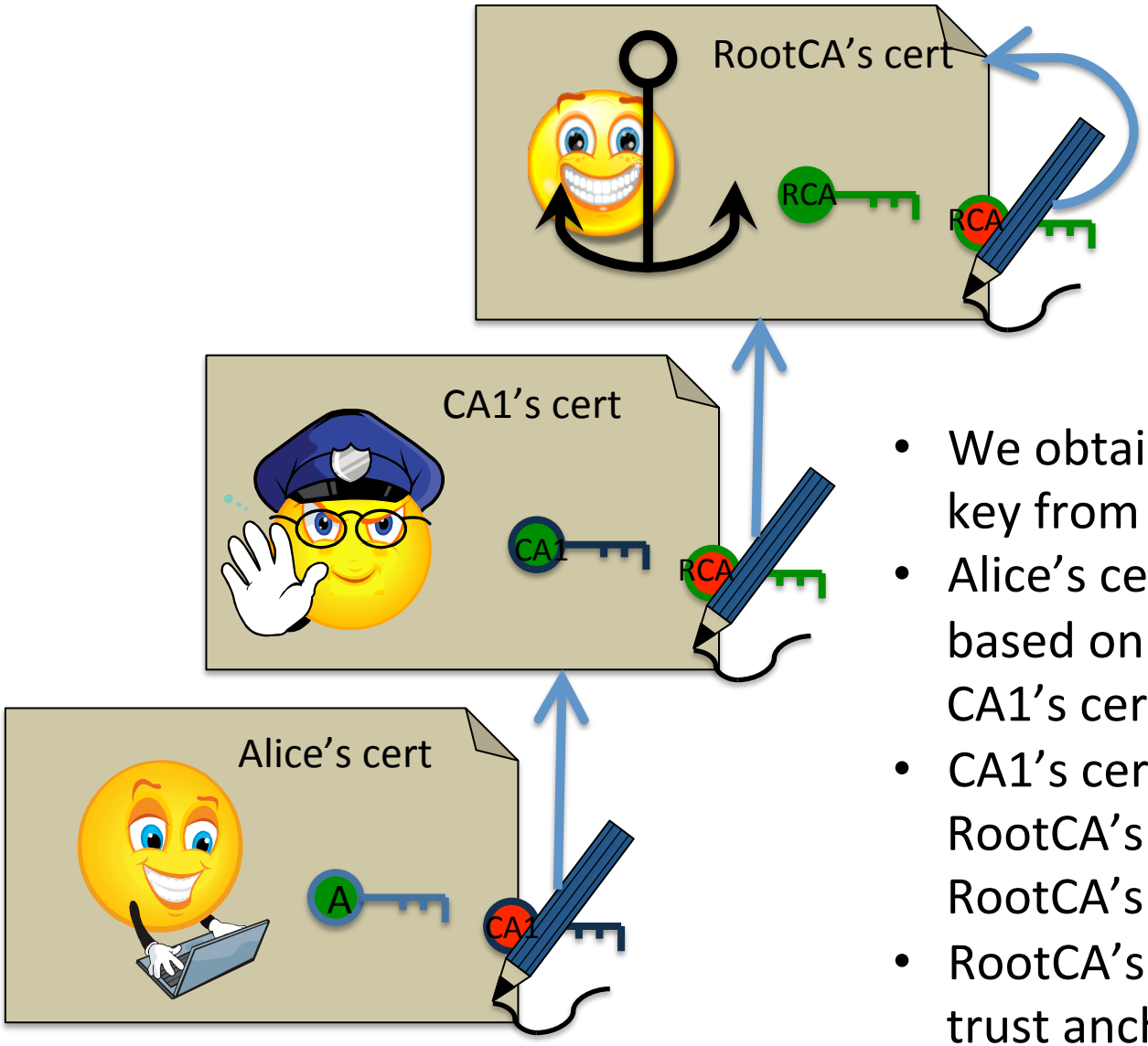
Cryptographic verification



Was the singer's cert valid at the time of signing?

- When was the signature created?
  - is there a timestamp?
  - do I have any other evidence?
- Can the signer's cert be chained to a trusted root?
  - with respect to the time of signing…
  - there can be multiple roots and/or multiple chains
- Were all certificates in the chain valid at the time of signing?
  - unexpired?
  - unrevoked?

Certification Path



- We obtain user Alice's public key from Alice's cert
- Alice's cert can be verified based on CA1's public key in CA1's cert
- CA1's cert can be verified by RootCA's public key in RootCA's cert
- RootCA's key/cert is a trust anchor

Relevant revocation info

- Revocation information **relevant to the time of signing** can be used as evidence only
  - the CRL must relate to the cert
  - the CRL must be relevant to the time of signing
  - can a CRL earlier than the time of signing be used as evidence?

Grace period

- CRLs at the time of signing might mean unsuitable evidence, because
  - the user needs time to detect key compromise
  - the user needs time to report key compromise
  - the CA needs time to update its registry about the key compromise and publish the new revocation status
  - it takes time until new revocation status information propagates and all relying parties are notified

  - it may take time until someone can obtain **positive** confirmation of a signature's validity
  - … up the whole certification chain…

Addressing grace period

1. Use the most recent revocation information (neglect grace period)
2. Apply grace period for end-entity certs, but do not apply it for CA/TSA certs
3. Apply grace period at every level
4. Apply grace period at ever level, use real-time revocation checking
   - via OCSP – to get immediate positive confirmation
   - OCSP responses need to apply to current time
   - each OCSP response must be fresh
   - how to validate the OCSP responder's cert?

Validating a signature

- Obtain ‘control time’, i.e. the point of time we use for signature validation
  - if there is (one or more) time stamp, use that
  - if there is any other evidence, use that
  - worst case: use time of validation
- With respect to the ‘control time’:
  - build a certification path
  - validate signature on all certs in the path → recursion
  - collect evidence for revocation status of all certs in the path, and validate the signature on all such evidence → recursion
  - apply grace period as per signature policy

Result of Signature Validation

- VALID: The validity of the signature can be **proven** based on the available information, according to the signature policy
- INVALID: The signature is **proven** to be invalid based on the available information, according to the signature policy
- UNFINISHED: There is no evidence for the signature being invalid, but we have no positive evidence either; we need to wait until relevant revocation information is published

If a signature is technically valid

- Note that it does not necessarily mean that it will be accepted in court or is not necessarily suitable for a given purpose

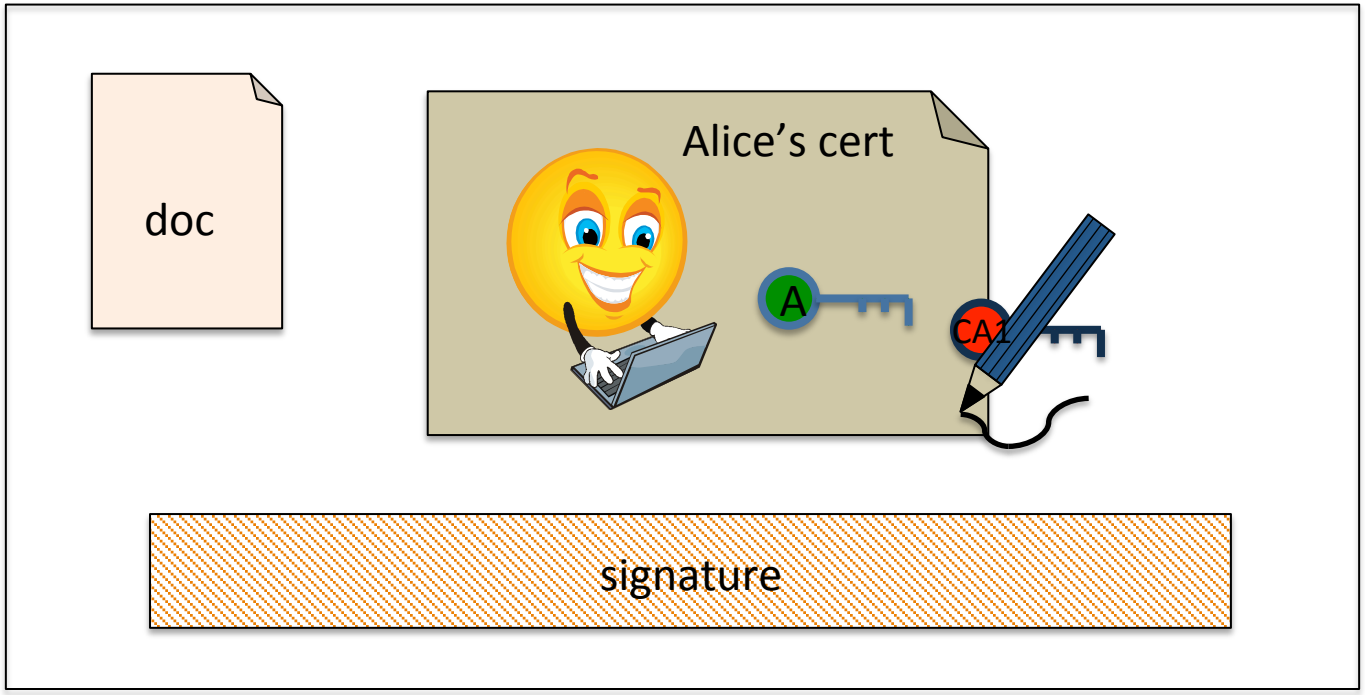
Long-term validity of signatures

How long does a signature remain authentic?

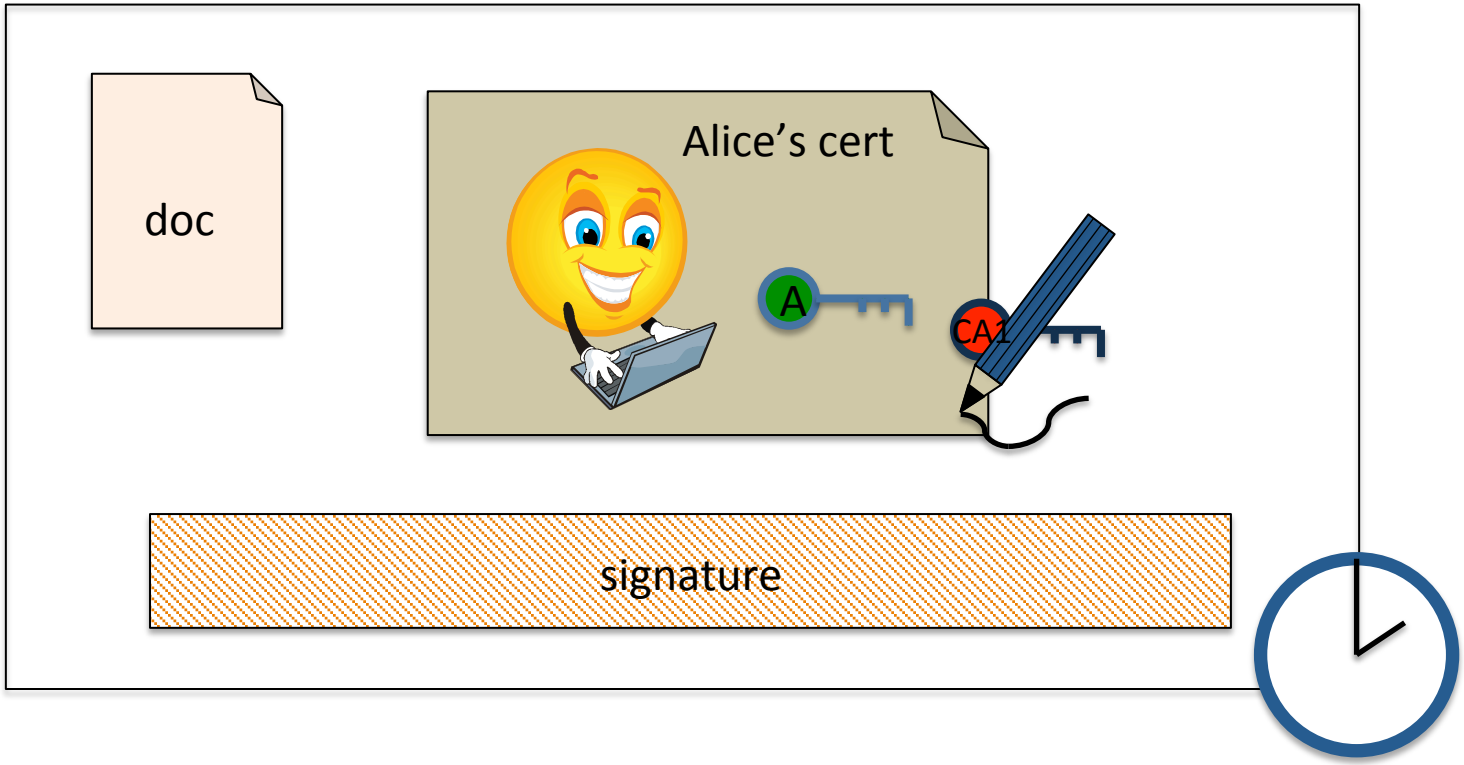
- From legal point of view, the validity of the signature does not fade away with time
- From technical point of view it may become difficult to prove that a signature had been valid at a previous point of time

- Signature without timestamp? → as long as the signer's cert is valid
- Signature with timestamp? → as long as the TSA's cert is valid
- If you want more, the signature needs to be **archived**, it needs to be time stamped at regular intervals

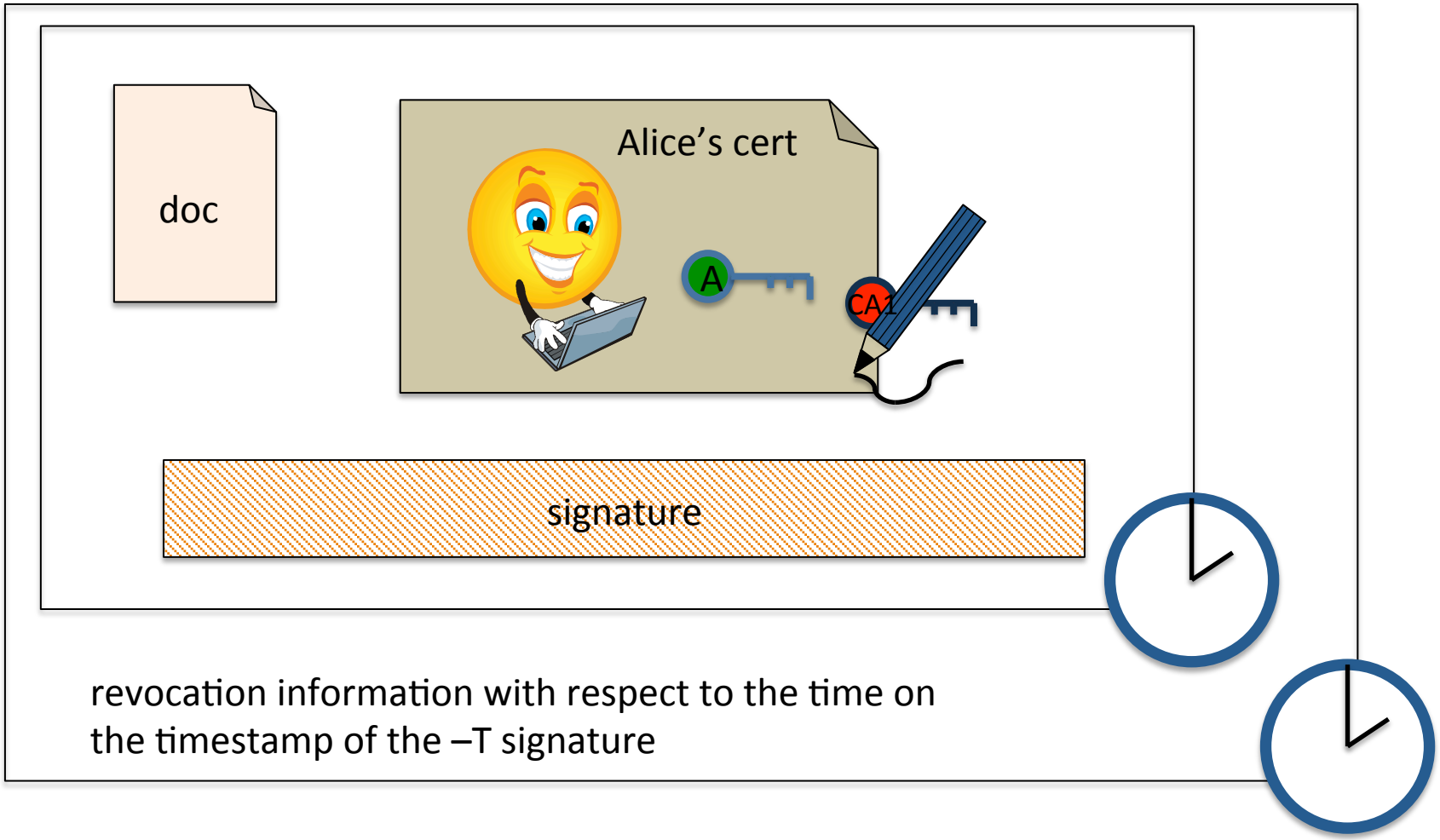
XAdES-BES (basic electronic signature)



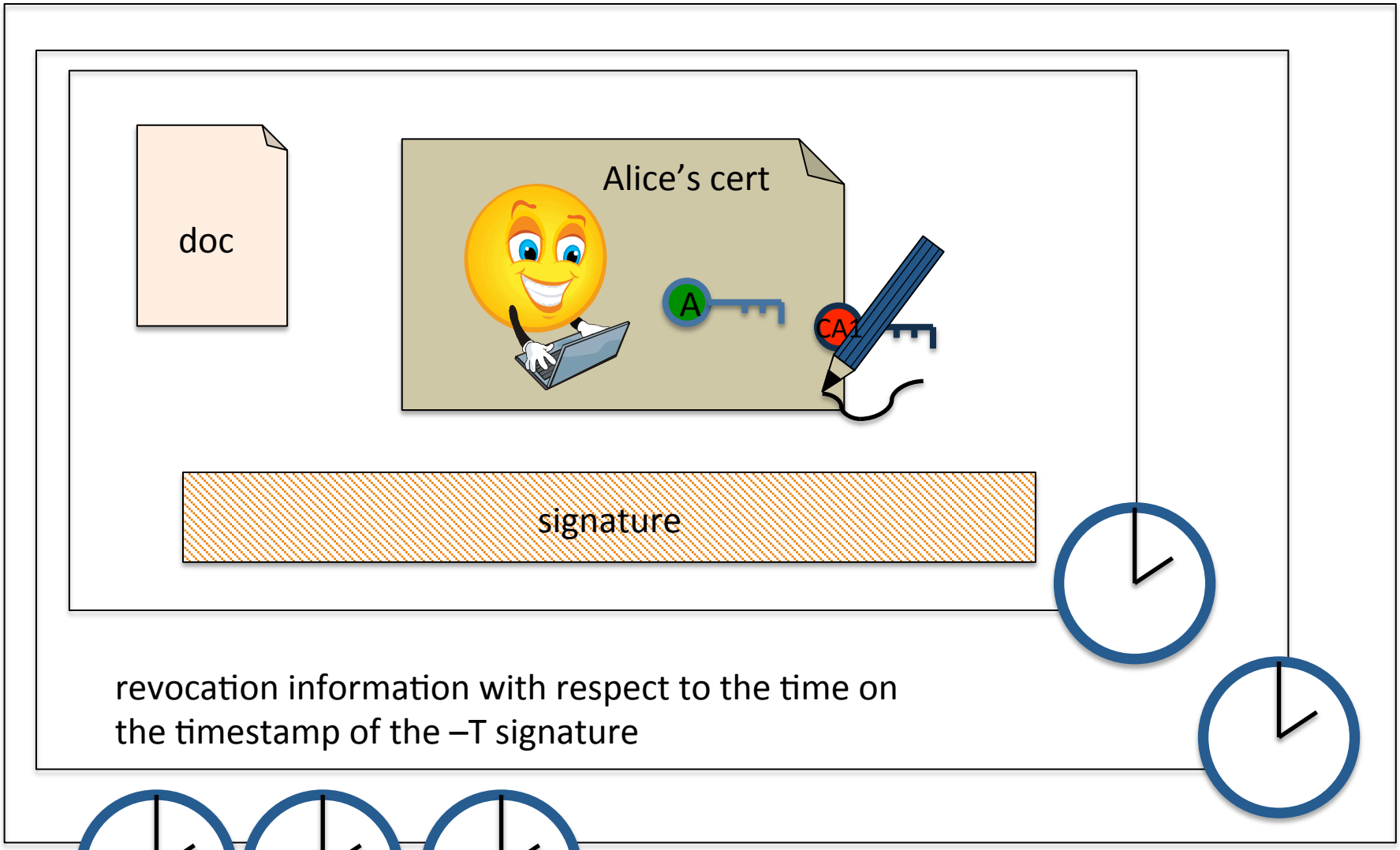
XAdES-T (… with Time)



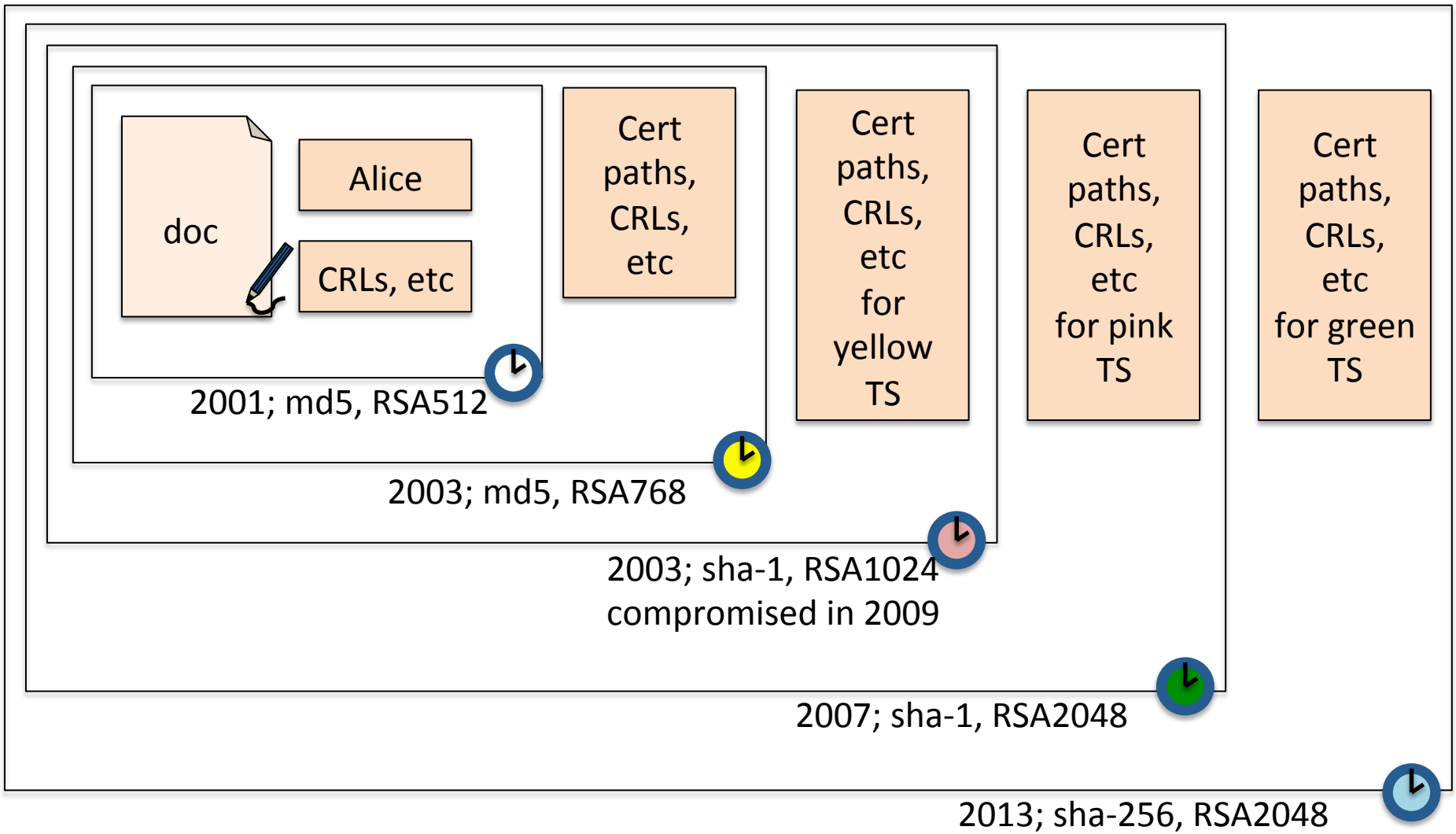
XAdES-C or –X-L


doc
Alice's cert
A
CA1
signature
revocation information with respect to the time on
the timestamp of the –T signature

XAdES-A


doc
Alice's cert
A
CA1
signature
revocation information with respect to the time on
the timestamp of the –T signature

XAdES-A validation, in 2010



Signature Policy

- A signature's validity is not objective, it depends on the policy we use for signature validation
- The signature policy may include
  - roots
  - algorithms
  - timings
  - timestamps
  - revocation information
  - grace periods
  - etc…
- A signature's validity can be discussed in context of a policy only

Summary

- Electronic signature is a legal term for e-signatures recognized by law; they are not necessarily based on crypto or PKI
- Digital signature is a crypto operation, its result is not necessarily accepted by court
- EU legal systems define certain PKI-based (qualified) signatures as equivalent with handwritten ones; US legal systems do not emphasize PKI, they emphasize the circumstances
- A PKI signature is obtained by encoding the hash of the document (or a signature block) with the private key
- To verify a signature, you need to verify if the signature, the public key and the doc correspond to each-other and that the signatory's cert was valid at the time of signing
- Security of signatures is often based on time stamps

Recommended reading

- EU and US e-signature laws
- Thomas Fleiner: Common law vs Continental law
  tipsheet | full paper
- Summary of US e-Sign act
- XAdES specification