Steps of the supervisory body to minimalize impacts of known attacks on validation trust services and services based on validation

PDF, ASiC and XML signature vulnerabilities

COL Peter Rybár
Deputy Director
Regulation and Supervision Department
National Security Authority
Slovak Republic

How to break PDF Signatures

The signed PDF document can be constructed in such a way that its appearance can be changed without necessarily invalidating the signature.

For more information see, e.g.:

http://pdfsig-collision.florz.de/

https://www.pdf-insecurity.org/

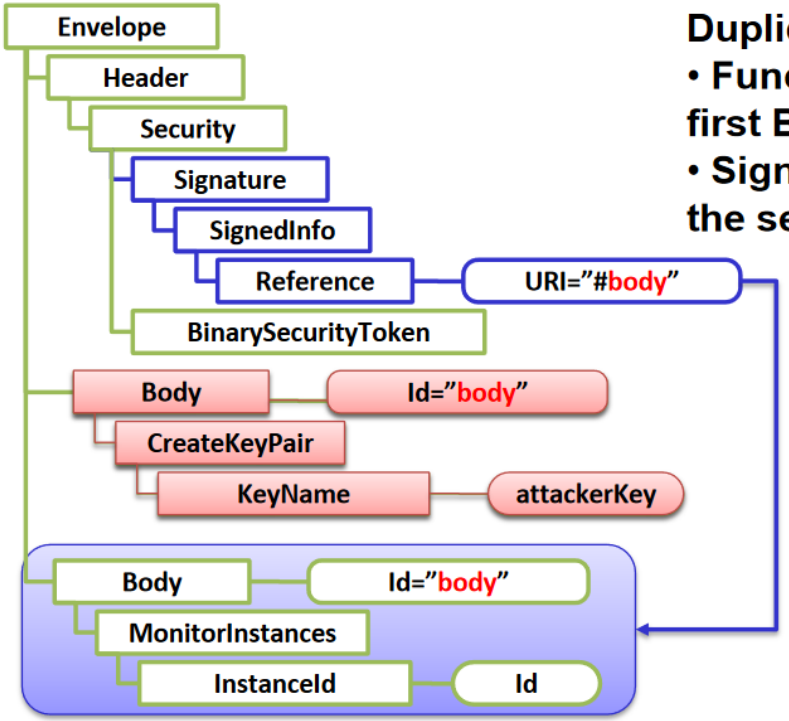
https://www.pdf-insecurity.org/signature/signature.html

https://web-in-security.blogspot.com/2019/02/how-to-spoof-pdf-signatures.html

XML Signature attacks (ASiC is based also on XML signature)

XML Signature Element Wrapping attacks – source https://owasp.org/

Solution: CMS AdES (e.g. http://tl.nbu.gov.sk/kca/tsl/tsl.xml.**p7s**) can be used for the XML file, e.g. for the trusted list file (http://tl.nbu.gov.sk/kca/tsl/tsl.xml) and also CMS AdES can be used for the implementation of **ASiC**.



Duplicate the Body element:
- **Function invocation from the first Body element**
- **Signature verification over the second Body element**

The same attack on the Timestamp!

External CMS AdES for detections of freshness of XML, e.g. for TL XML

To solve some attacks on XML and to enable the automatic verification of the up-to-date status of the trusted list, the NSA publishes together with the XML file of the trusted list (TL XML) also the advanced electronic seal of the TL XML file on the same web page and with the same file name that is concatenated with the string ".p7s" added at the end of the file name of TL XML. The seal of the trusted list is in the format CMS AdES, where for the validation the same certificate is used as is used for TL XML and where **the necessity to reload** the trusted list is detected if

1. the signed signing time attribute value (included in CMS AdES) is later than the trusted list issue date (included in XML TL) and
2. the signed hash value of the TL XML (included in CMS AdES) is not equal to the computed TL XML file hash value.

Note: *later than the trusted list issue date* to prevent reply attack on .p7s

See: http://tl.nbu.gov.sk/kca/tsl/tsl.xml**.p7s** – CMS AdES of TL XML

http://tl.nbu.gov.sk/kca/tsl/tsl.xml – XML trusted list

How to prevent becoming a victim of attacks on signatures

The validation service must:

- Be able to uniquely select the signer signature if there is more than one.
- Must not export unprotected version or parts of the document with unprotected data of the document (e.g. skipped by canonicalization or other transformation).
- According to the selected signature, export only signed content (e.g. version of the signed PDF document) or signed documents included in the ASiC container or files nested in the nested containers in ASiC like signed PDF stored in ASiC or another ASiC containers stored in ASiC.
- According to the selected signature, export content with metadata which provides correct type of interpretation of the signed documents.

Identifier of the signature of the signed document (documents) - DSId

Electronic document may be secured independently or jointly with other electronic documents, namely through several or one qualified electronic signature, qualified electronic seal or qualified electronic time-stamp.

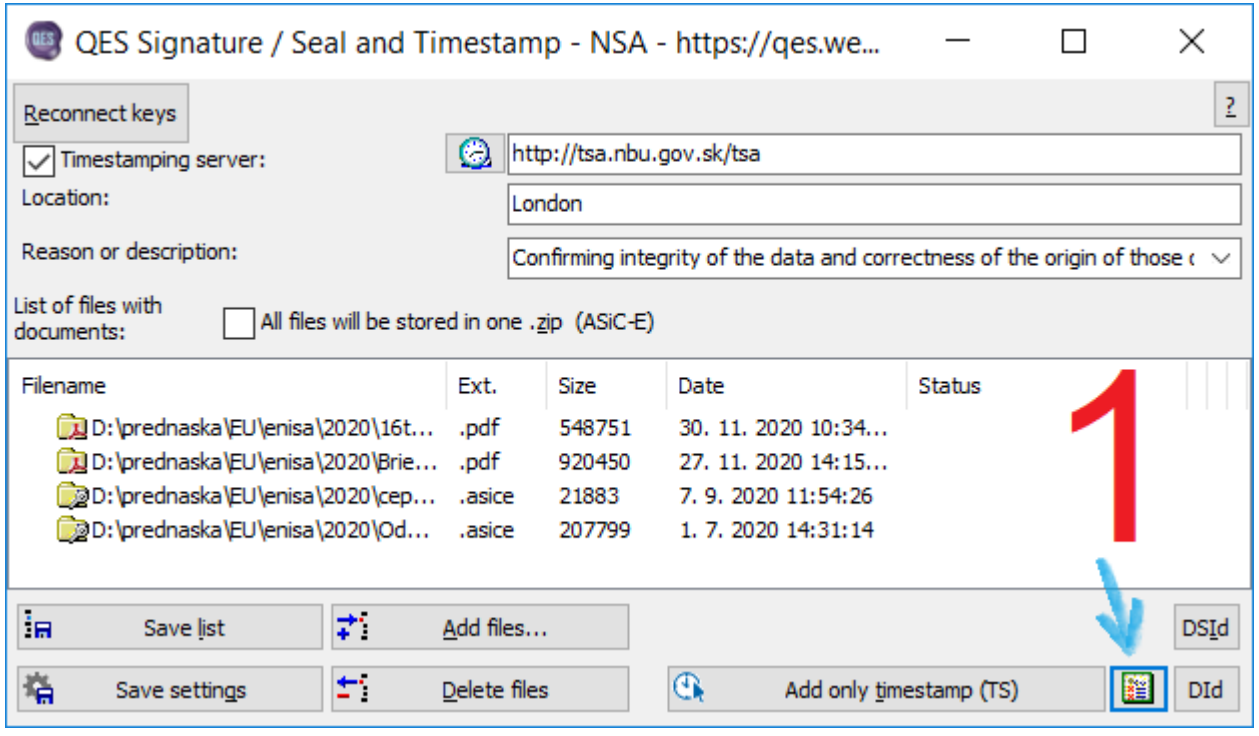
Secured electronic document (documents) is identified based on the identifier of the signature of the signed document (documents) marked **DSId**, whose value (defined in Clause 3.3 in ISO 14533-4) contains hash from the digital signature (DER encoded result of the asymmetric function of signing – the result is stored in the field of advanced electronic signature, it is **unchangeable** in time and **unambiguous** for every signature).

The relying party may only work with the electronic document that was secured by

- the person indicated in the electronic document as signer/seal creator or
- the person, to whom the securing through signature/seal was forwarded from the context of electronic signature usage of the particular document.

Signature validation reports and upgrade with time-stamps, CRL or OCSP

If you want to create a validation report for each signature, click on the button in the figure below, which will be displayed by checking the timestamp server, which will create a separate ZIP for each signature (DSId as the ZIP file name) containing signed files and their signature validation report.
Time-stamps, CRLs or OCSP responses, used in the validation procedure, will be also included in the PDF and ASiC files listed in the QES application.



Timestamp and validation report.

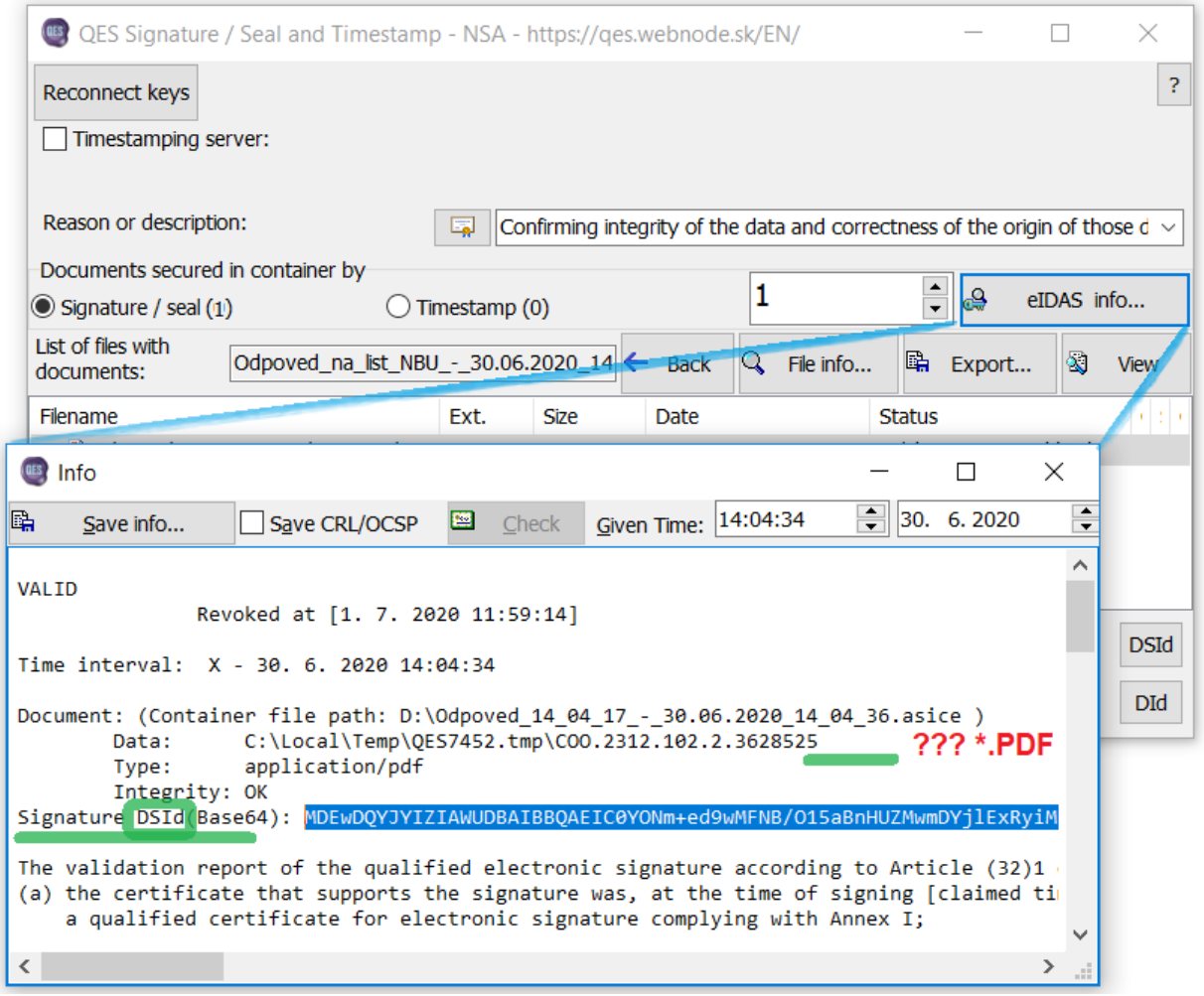
Signature identifier of the signed document(s) DSId

Signature identifier of the signed document(s) DSId. Example of command line usage of the DSId file defined in ISO 14533-4:2019.

```
QES.exe /p "doc.pdf"      /DSId "doc.pdf.DSId"
QES.exe /a "ATest.asice" /DSId "ATest.asice.DSId"
```

A registry or document management system can uniquely identify a document(s) that has been signed by a specific person based on a DSId file, even if there are more signatures in PDF / ASiC container.
Selected **blue** value in the figure can be stored in the text file *.DSId e.g. in the Notepad.

https://qes.webnode.sk/en/



Article 46 of Regulation (EU) No 910/2014

In accordance with Article 46 of the Regulation (EU) No 910/2014 an electronic document shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form.

Definitions - Article 3(35) of the Regulation (EU) No 910/2014, *electronic document* means any content stored in electronic form, in particular text or sound, visual or audiovisual recording.

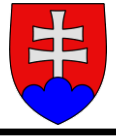
To support the legal effect of the electronic document Regulation (EU) No 910/2014 defines rules enabling to secure

- **integrity** of the electronic document,
- link to the **identity** of the person, who secured it through qualified electronic signature, qualified electronic seal or qualified electronic time-stamp and
- correct **interpretation** of the content of the electronic document.

Correct interpretation of the content of the electronic document

An electronic document (file) is just a sequence of numbers (BYTEs).

94E7365FBC59B89CC322816292E4BEF8F26E82 ....

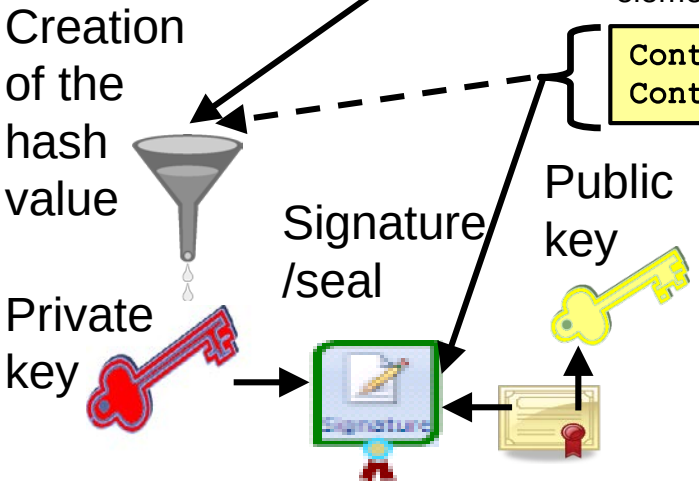
Header  Payment in EUR http://frame1.sk

It is not enough to provide only the message, but the signature / seal must also ensure the correct interpretation of the individual values in the individual BYTE of the message, otherwise a completely different content may be displayed.

Metadata protected by QES / QESeal.

The type of interpretation of the electronic document / message data is protected in attribute ***(CMS AdES)*** `id-aa-contentHint` in `contentDescription` or in element ***(XML AdES)*** `DataObjectFormatd` in `Description`:

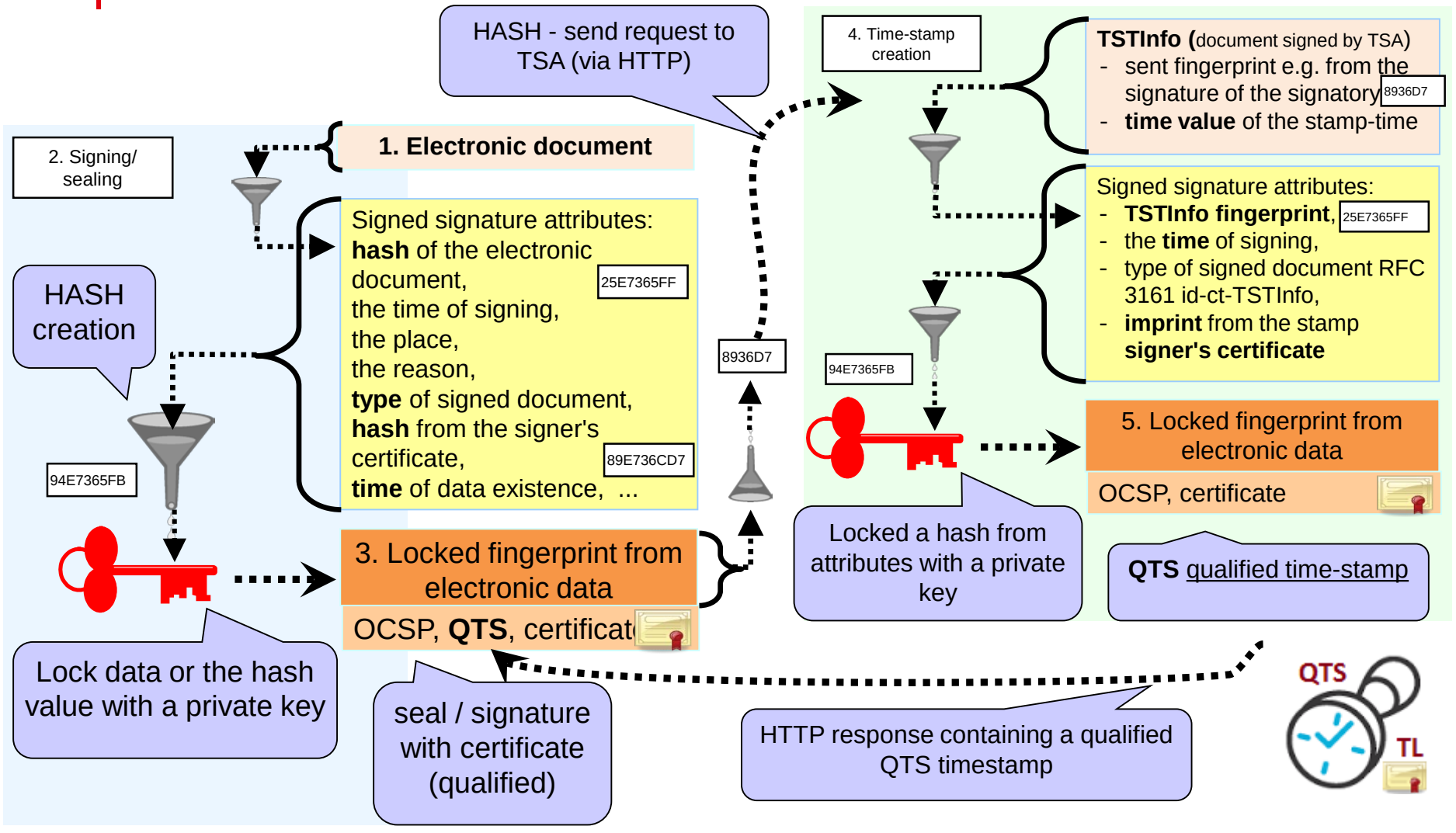
```
Content-Type: text/plain; charset=UTF-8; name="Document.txt"
Content-Disposition: attachment; filename="Document.txt"
```



Example: http://elpi2.szm.com/priklad.htm

NATIONAL SECURITY AUTHORITY

Electronic document signed with the AdES with a time-stamp



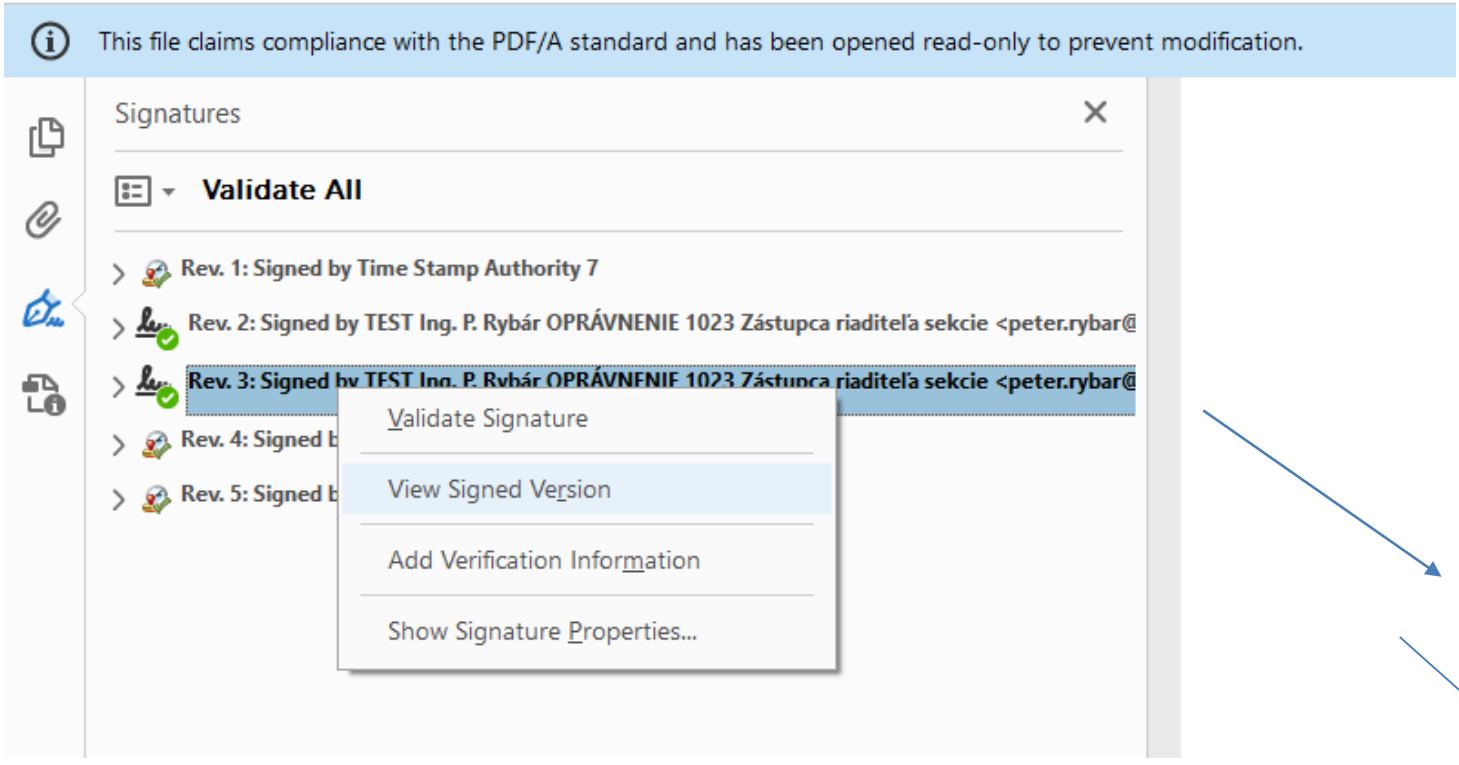
NATIONAL SECURITY AUTHORITY

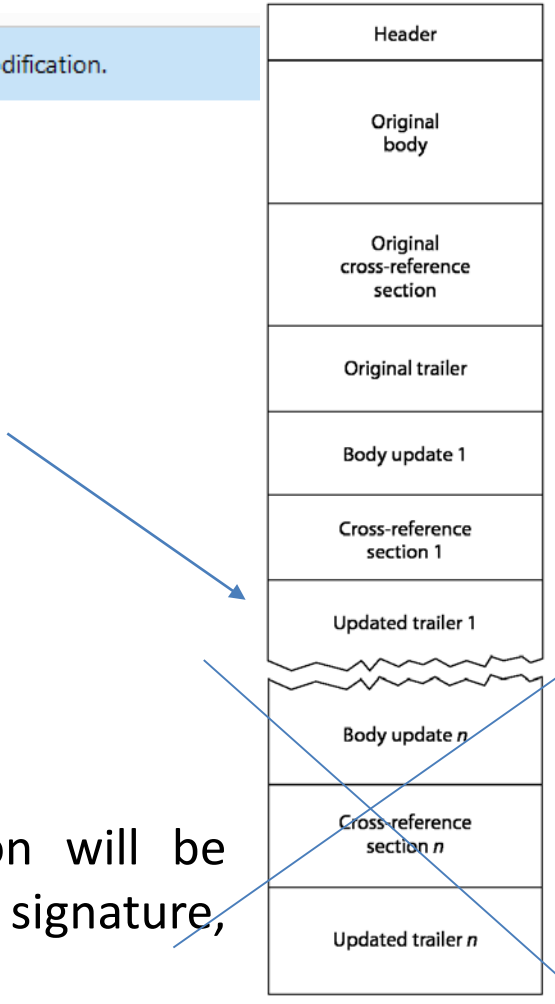
Several PDF document versions

The pdf file may encompass several PDF document versions and only the version identified based on **DSId** may be worked with, secured by the person identified in accordance with Clause 5.1.3.3 of Supervision Scheme of qualified trust services defined by the supervisory body.

By using DSId the signature of one PDF document version is identified or one signature from ASiC container, or one signature from nested containers in ASiC, while ASiC may encompass a huge number of signatures of one or several various documents or PDF document versions, if PDF is signed by a PDF signature and is stored in ASiC (PDF is nested in ASiC).

Adobe PDF



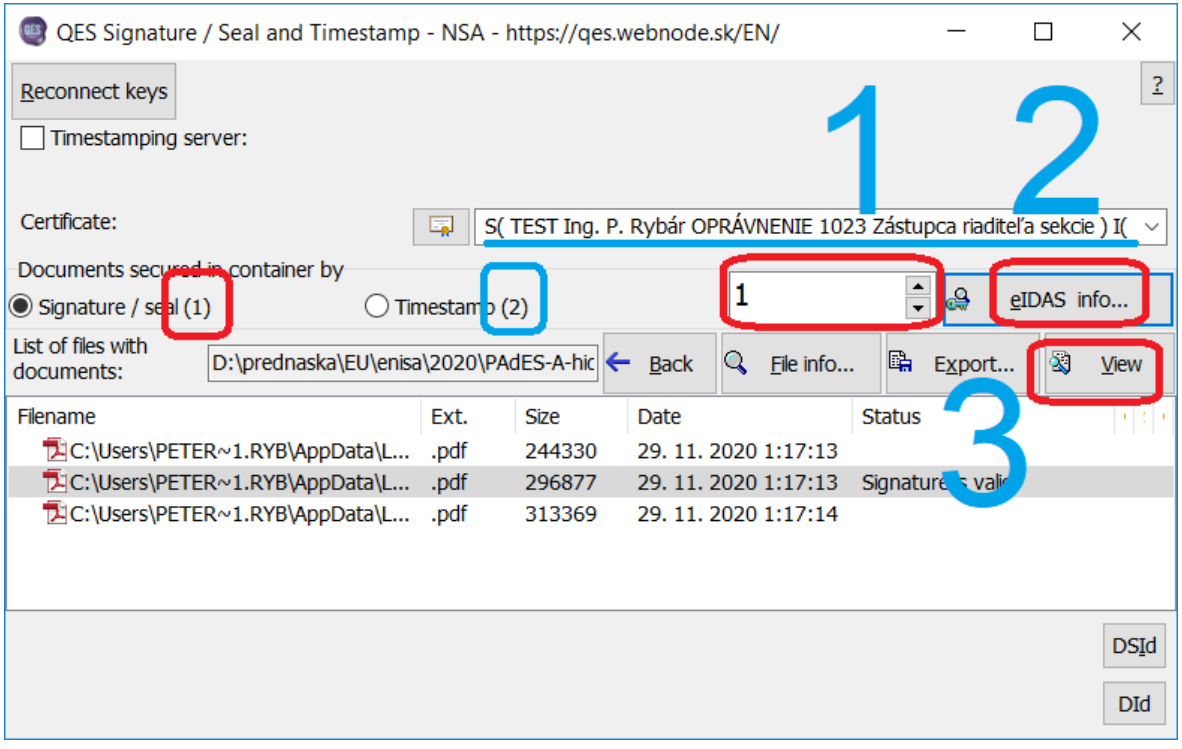


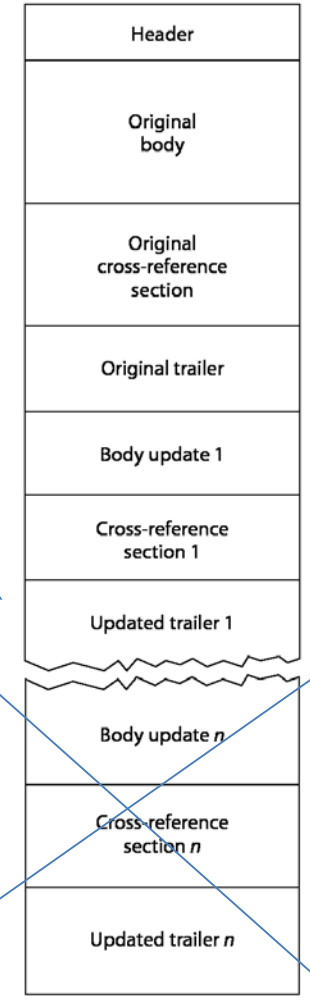
After opening the PDF document, the latest version will be displayed, which could have been changed after the last signature, and therefore the signed version is not displayed !!!

Always work only with a version signed **by a specific person !!!**

NATIONAL SECURITY AUTHORITY

Free QES Application - https://qes.webnode.sk/en/



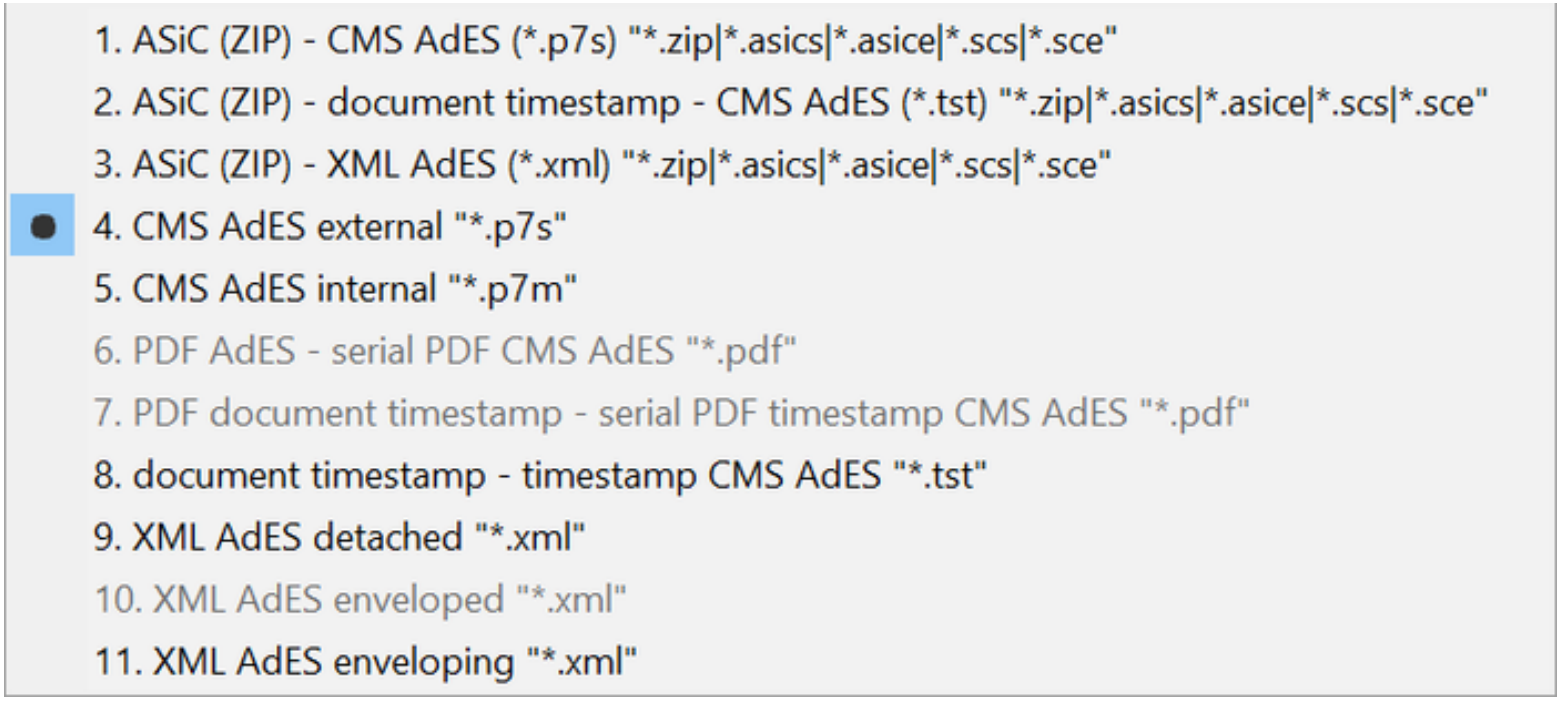


After opening the PDF document (click on the "File info" button), the number of eIDAS signatures and PDF timestamps will be displayed - **the unsecured version will not be displayed**. Enter the signature/time stamp number to select the PDF version.
Always work only with a version signed **by a specific person !!!**

NATIONAL SECURITY AUTHORITY

Annex of the Commission Implementing Decision (EU) 2015/1506

Regulation (EU) No 910/2014 requires a public sector body to be able to accept all 4 signature formats, which form 11 categories of file security. You can use them e.g. in the QES application:



https://qes.webnode.sk/en/

CID (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014

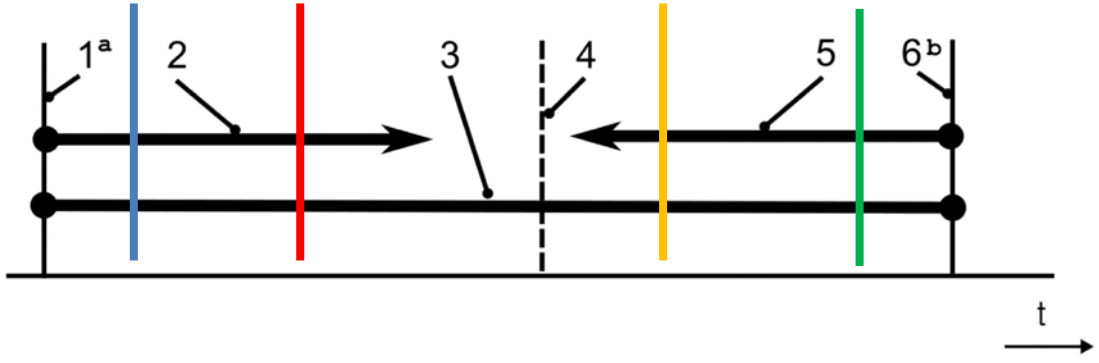
NATIONAL SECURITY AUTHORITY

The time of signing

The time of signing the qualified electronic signature or of creating the qualified electronic seal is indicated as ***given-time***. A procedure of its determination is shown in Figure *given-time* (4) in a Proof of Existence (PoE) of the closed interval <1[a], 6[b]> in accordance with Annex E in ISO 14533-4:2019 or Clauses 5.1.3.1 and 5.3.2 of Supervision Scheme.

If it is necessary to determine the date and the time, in which could occur securing of electronic document, e. g. if the electronic document is multiply secured.

From the available qualified electronic time-stamps, which are covered (protected) by the electronic document signature or cover (protect) the signature value, shall be selected the one with the smallest date and time value interval <red, orange>.



ISO 14533-4:2019 Annex E (normative) Use of the PoE objects

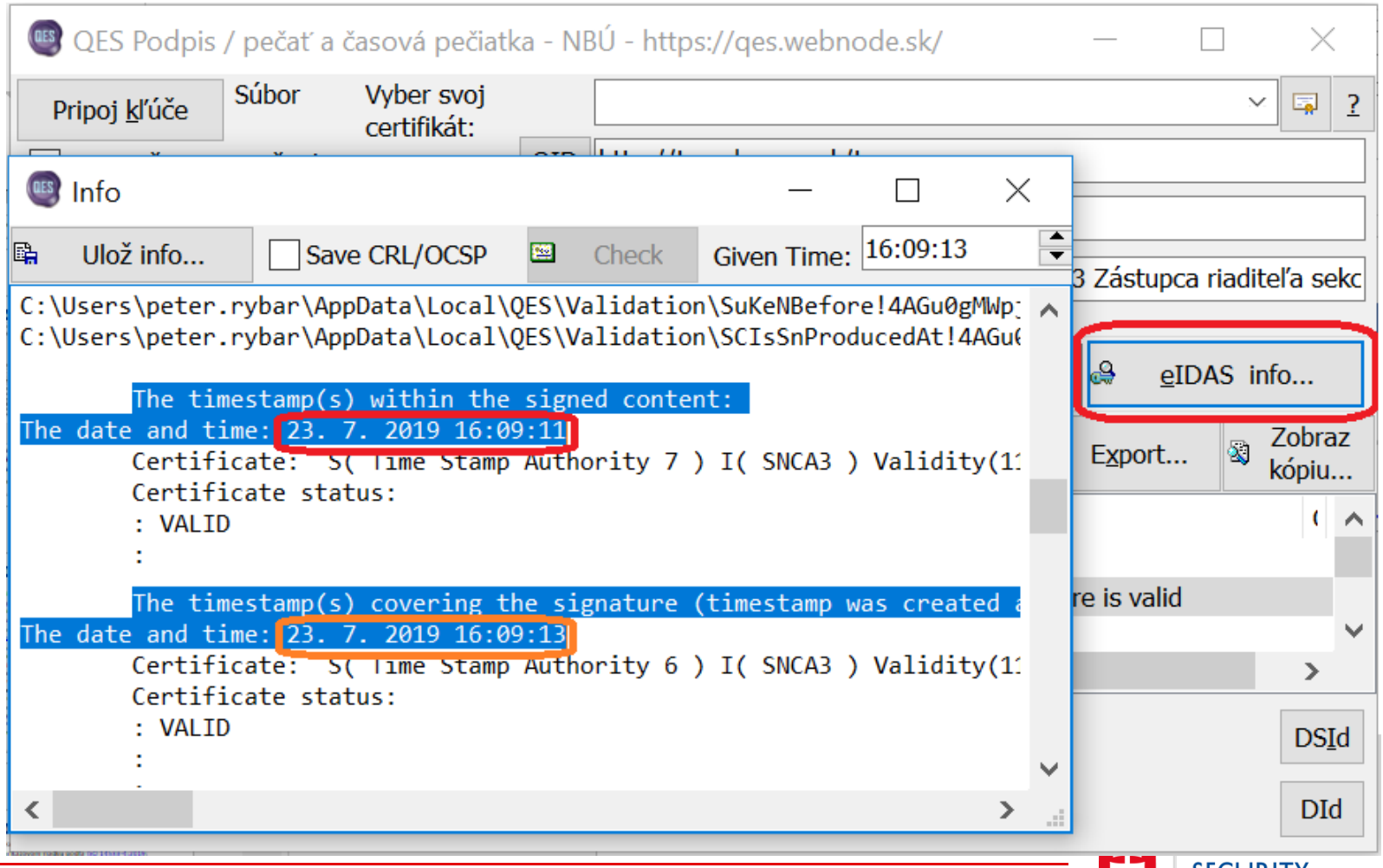
NATIONAL SECURITY AUTHORITY

The time of signing

If it is necessary to specify the date and time of the interval after and before which the authorization took place according to ISO 14533-4:2019

The **last** timestamp included in the **signed content** - in the document.

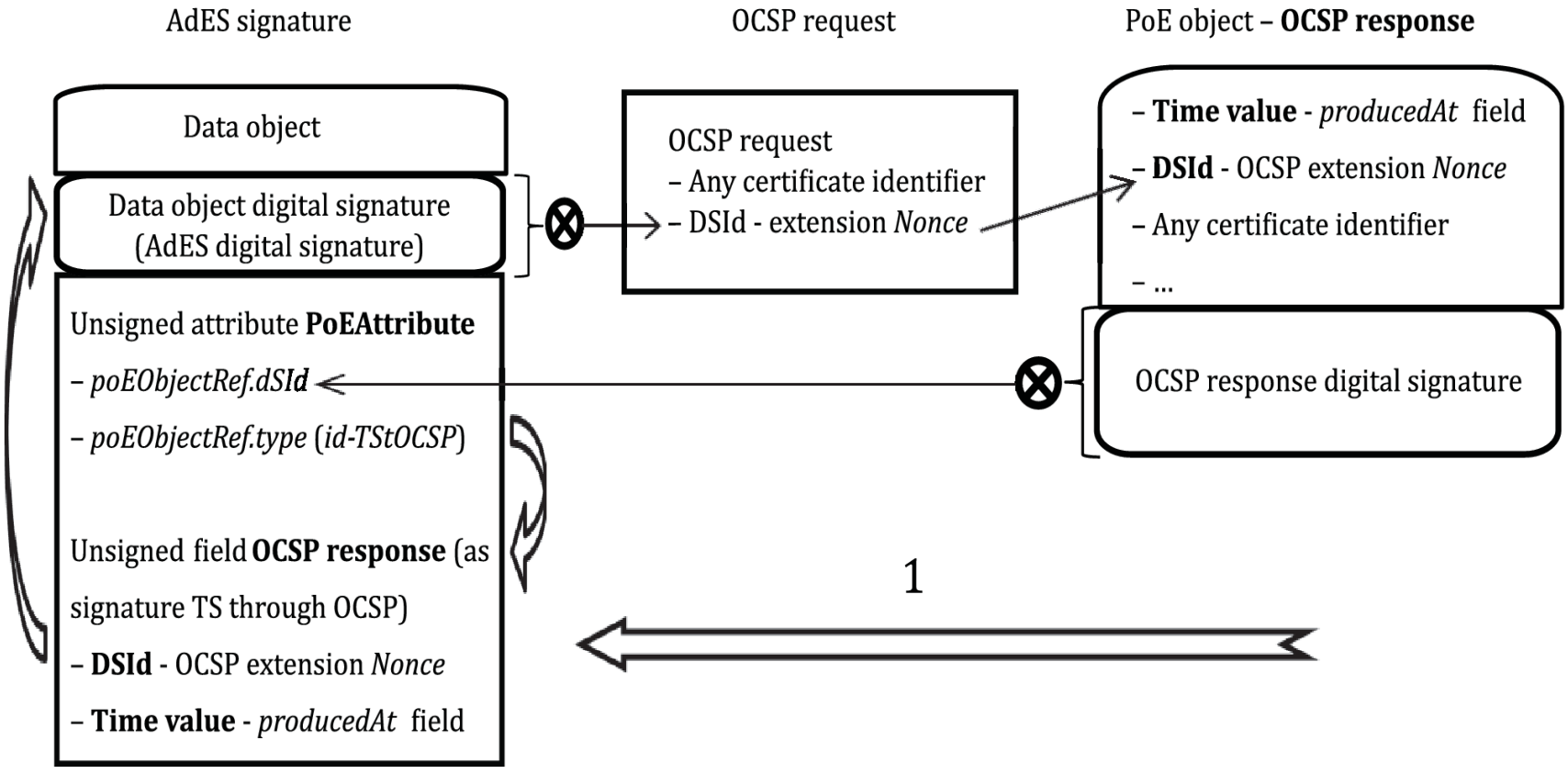
The **first** time stamp covering the signature.



Clause 5.1.3.1 Supervision Scheme:

Annex C (normative) Signature timestamp as a timestamp through OCSP

ISO 14533-4:2019



1 **external PoE object is included in the signature**

NOTE **OCSP extension Nonce contains the hash value of the signature**

NATIONAL SECURITY AUTHORITY

THANKS FOR YOUR ATTENTION