The Standards People

Signature formats & verification procedures

Presented by: **Juan Carlos Cruelas (UPC), Andrea Röck (Universign)**

For: **ETSI Standards Training Webinar**

01.06.2021

Signature formats

Agenda

- AdES signatures and ASIC containers specifications
- What AdES are all about?
- Some hints on the AdES attributes
- AdES life cycle: an example
- ASiC Containers
- Signature creation and validation (ETSI EN 319 102-1)
- Validation procedure
- Signature validation report (ETSI TS 119 102-2)
- Signature (validation / creation / augmentation) policy
- Signature validation service
- Cryptographic Suites (ETSI TS 119 312) “Algo paper”Subject 2

AdES signatures and ASIC containers specifications

- Signatures standardised by ESI receive the generic name of AdES signatures.
- They build on the major digital signature standards for different syntaxes (underlaying standards hereinafter)
  - ASN.1: CAdES (EN 319 122-1 and 2) builds on CMS IETF RFC 5652.
  - JSON: JAdES (TS 119 182-1) builds on JWS IETF RFC 7515
  - PDF: PAdES (EN 319 142-1 and 2) builds on PDF signatures
  - XML: XAdES (EN 319 132-1 and 2) builds on W3C XML Signatures
- EN 319 162-1 and 2 (ASiC) specify a container that encloses CAdES, XAdES signatures, or time-stamp tokens, and detached signed data or time-stamped objects (in files).
- Reminder: every underlaying digital signature standard supports the capability for adding additional data objects (attributes/qualifying properties) either covered by the digital signature itself (signed attributes) or not (unsigned attributes).

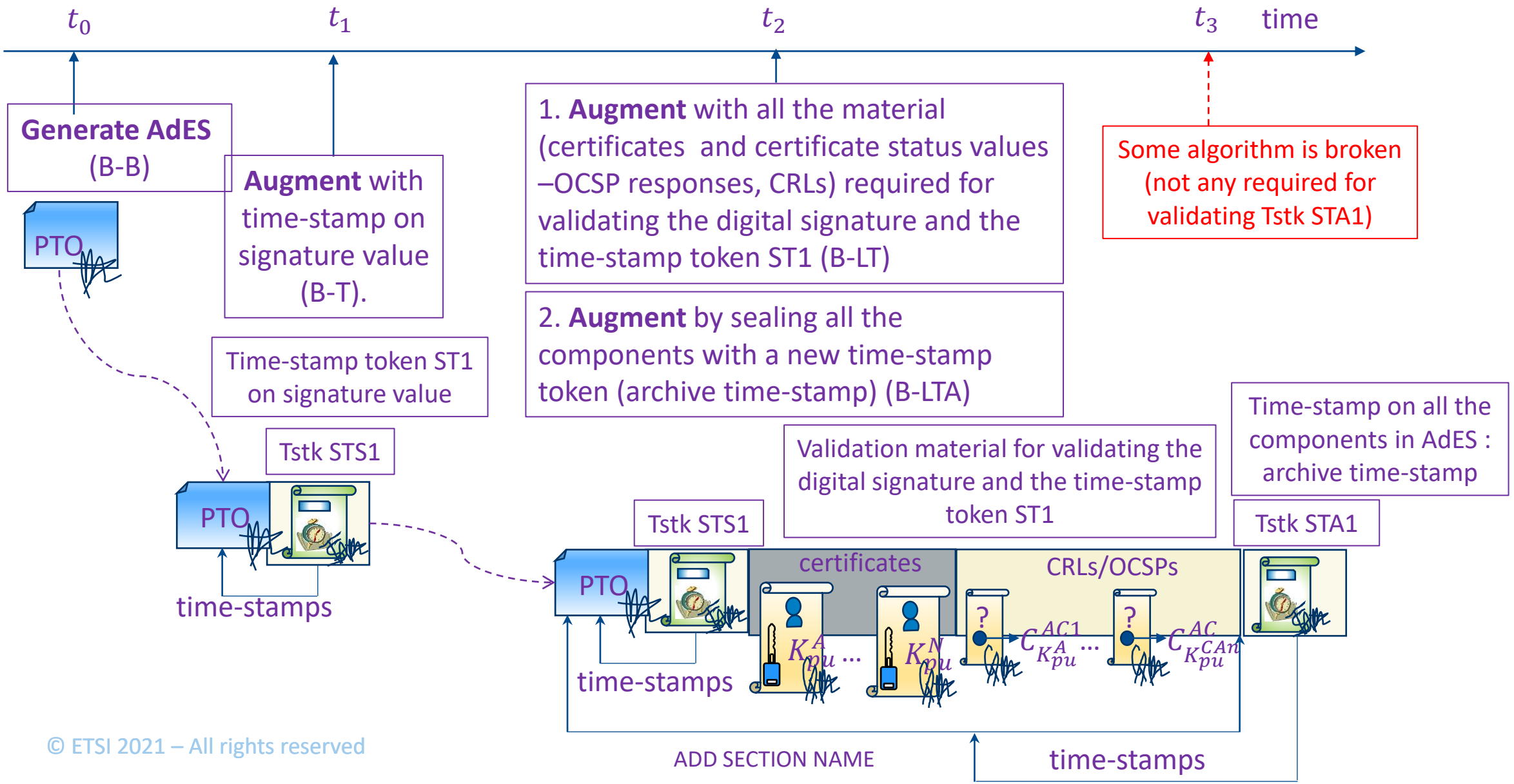
What AdES are all about?

- Each AdES standard:
  - Has two specifications (except JAdES, for the moment):
    - Building blocks and Baseline (parts 1)
    - Extended formats (parts 2)
- Building blocks and Baseline specifications:
  - Define a number of data types (attributes/qualifying properties) in the corresponding syntax
  - Define, for each attribute, whether it is secured by the digital signature itself (signed attributes) or not (unsigned attributes). This determines how each one is incorporated into the AdES signature.
  - Define several combinations of attributes (called levels) that reduce to the minimum possible the degree of optionality (**baseline signatures**) and offer different features, namely B-B, B-T, B-LT, and B-LTA.
  - Each part 2 defines another set of combinations of attributes (E-XX levels) where the degree of optionality is higher tan in baseline signatures and offer other features.

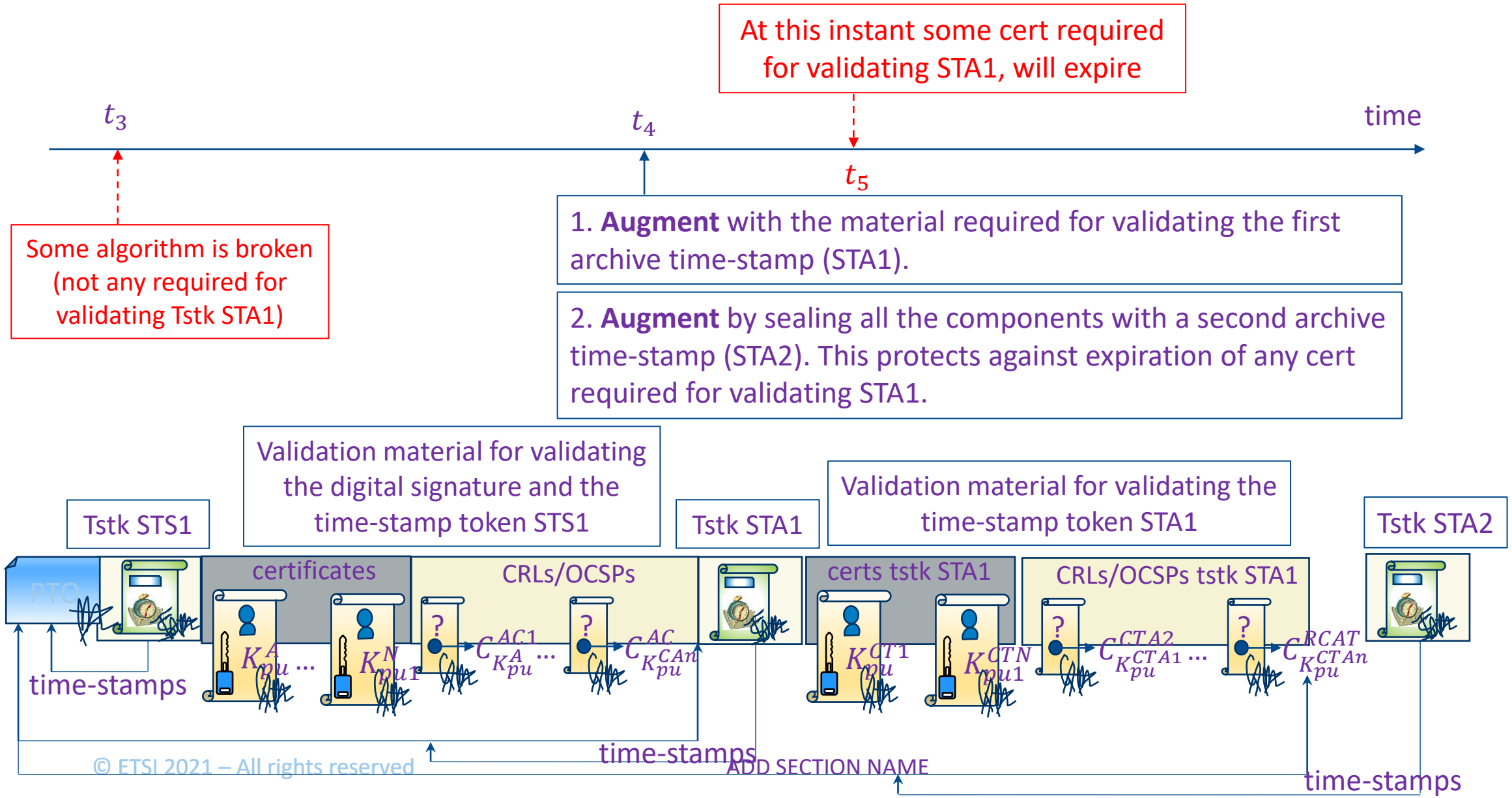
Some hints on the AdES attributes

- Some interesting signed attributes:
  - Attributes owned by the signer:
  - Time-stamp tokens on the signed data objects(s);
  - Commitment type taken by the signer when signing.
- Some interesting unsigned attributes:
  - The ones allowing to achieve long-term digital signatures (signatures whose validation can be re-stated long time after their generation)
    - Time-stamp tokens on the digital signature itself for proving the time when the AdES signature was generated
    - Validation data, including certificates in the cert path, as well as status certificates data (OCSP responses and CRLs), for allowing to proceed to validation time after the generation of AdES signature.
    - Time-stamp tokens on all the components of the AdES signature (archive time-stamps). They prove that these components have not been altered since the instant when they were produced and incorporated.
- Terminology: to **augment** AdES signatures means to incorporate unsigned attributes.

AdES life cycle: an example

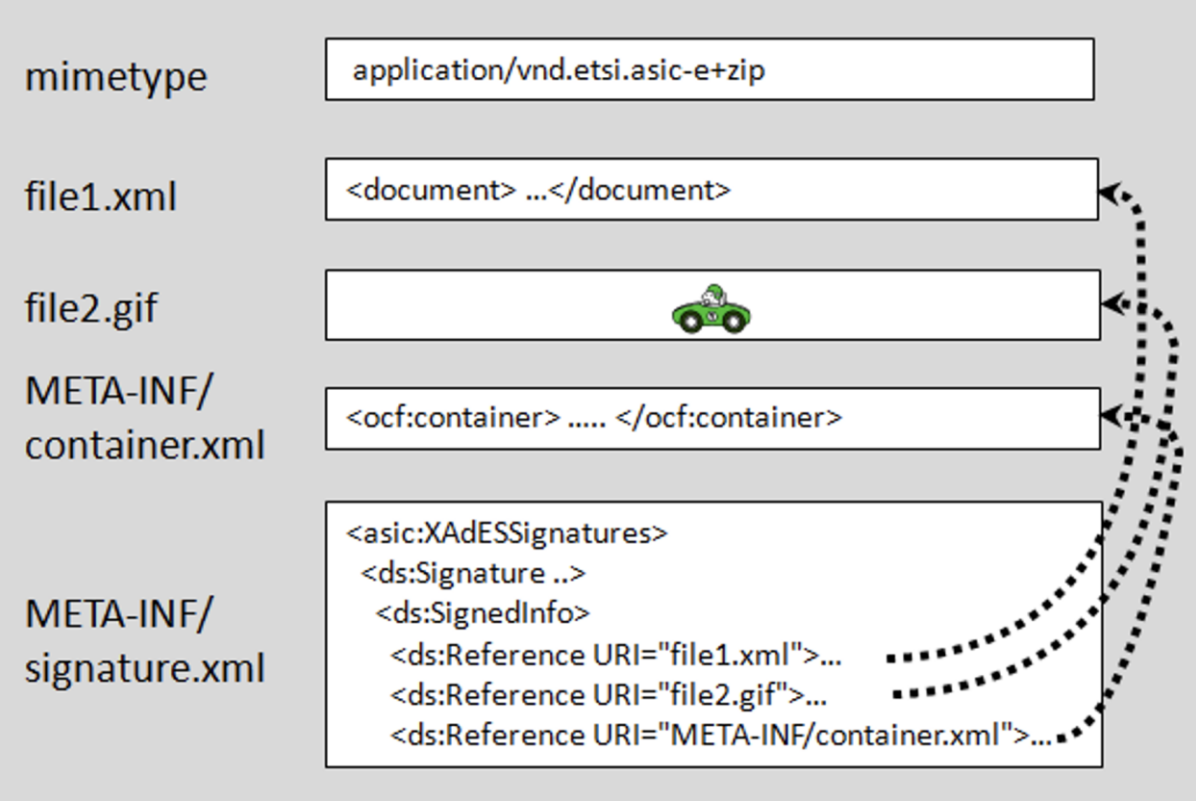


AdES life cycle: an example (continued)



ASiC Containers

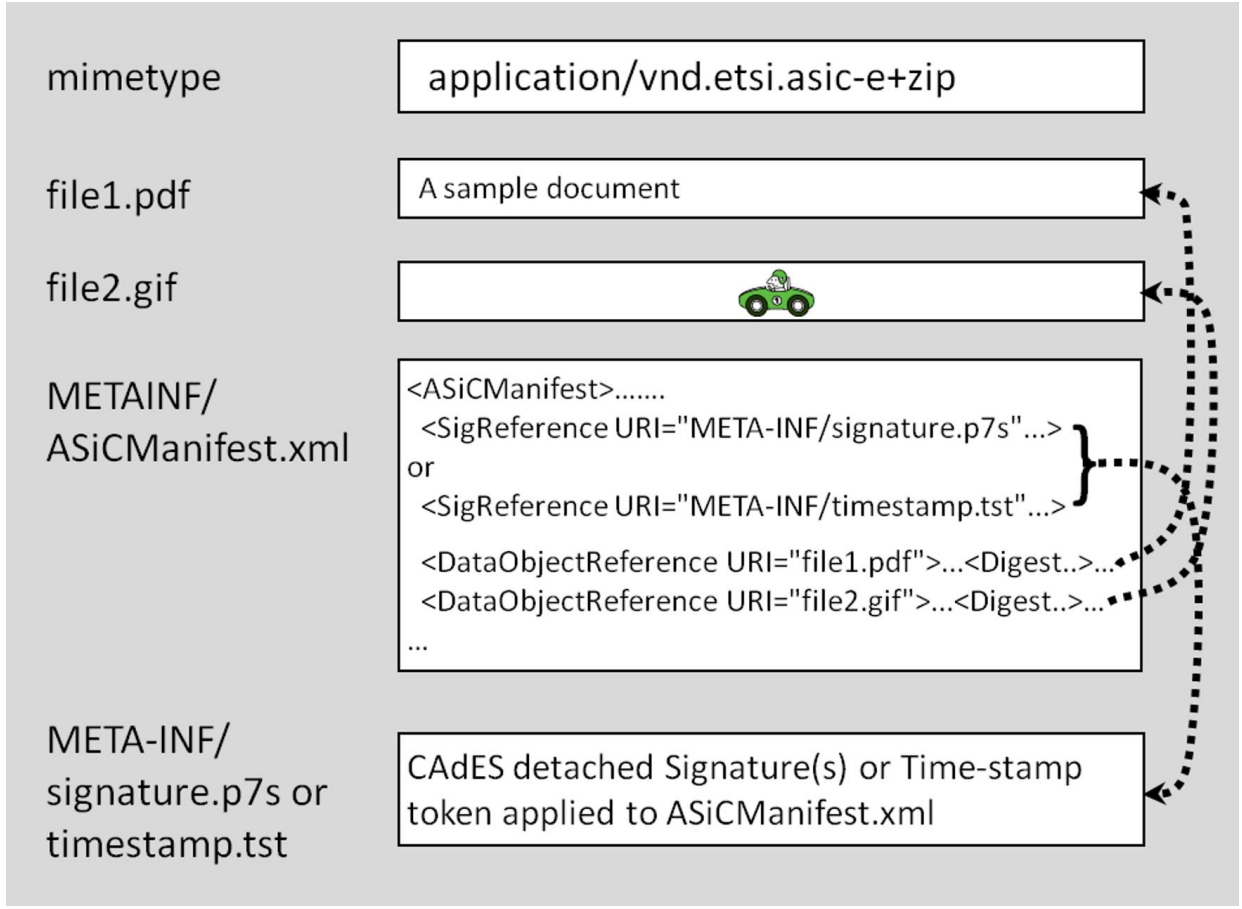
- ASiC containers may enclose several signed files and detached AdES signatures



ASiC container with several XAdES signatures

- XAdES signatures have mechanisms for explicitly referencing the signed documents through URIs

ASiC Containers



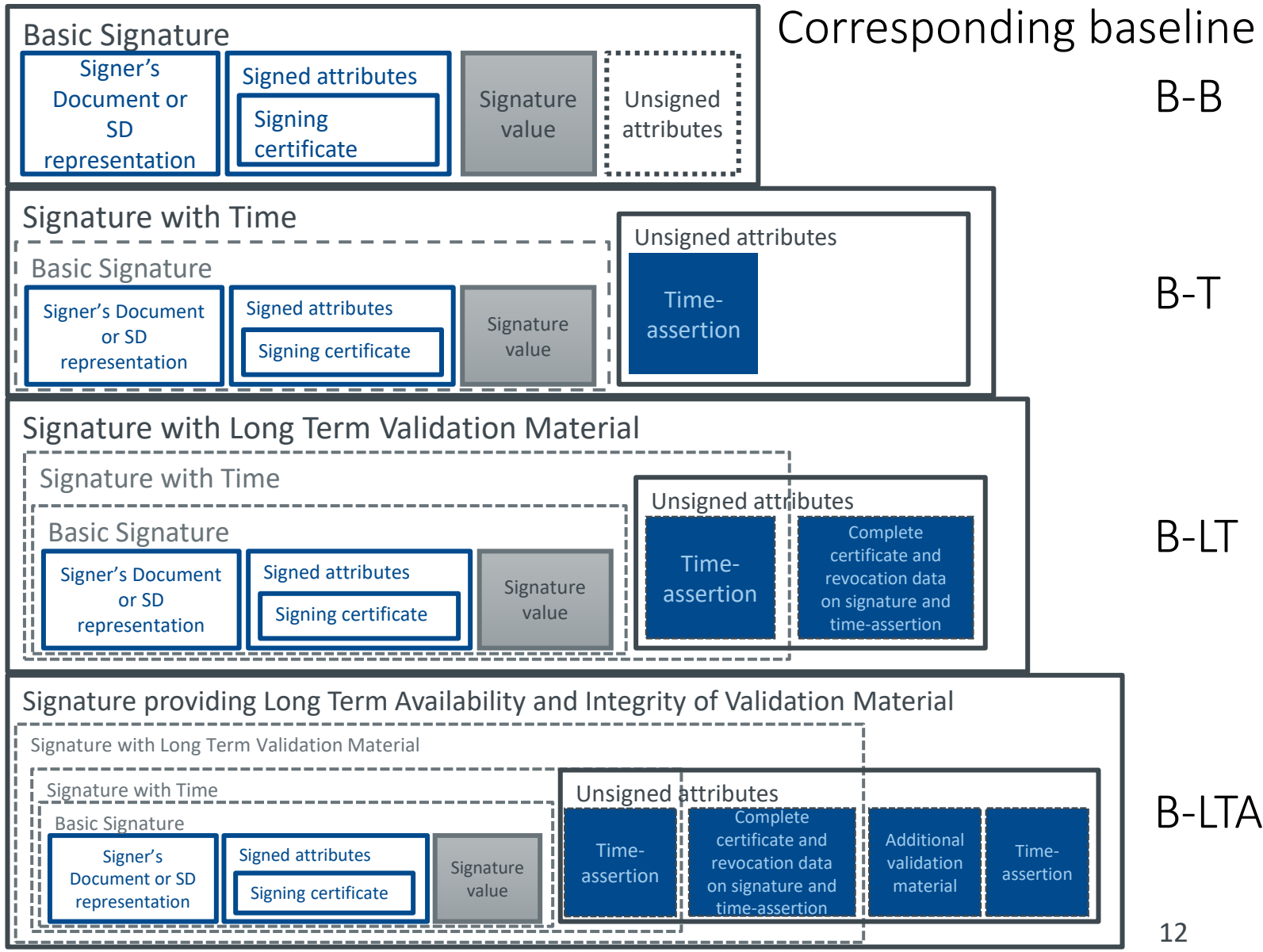
ASiC container with a CAdES signature or a time-stamp token

- Neither CAdES nor RFC3161 time-stamp tokens have mechanisms for explicitly referencing the signed/time-stamped files, so a separated file (ASiCManifest.xml) is signed/time-stamped.
- This manifest contains explicit references to the signed/time-stamped files and their digest values: indirect signing/time-stamping.
- If there are more than one CAdES or time-stamp tokens: one ASiCManifest file for each.

Verification procedures

Signature creation and validation (ETSI EN 319 102-1)

- Defines 4 signature classes:
- Signature levels B-xx, E-xx are format specific implementations of the different signature classes



Validation procedure

- Based on building blocks which are combined to three main validation procedures
  - For basic signatures
  - For signatures with time and signature with long-term validation material
  - For signatures providing long term availability and integrity of validation material
- Result will be TOTAL-PASSED, TOTAL-FAILED, INDETERMINATE
- Required that for the same input have same output as the algorithm (validation time is one input)
- The process is controlled by constraints that can be set by a signature validation policy, explicitly in the validation system, or implicitly by the implementation, e.g.:
  - X.509 validation constraints
  - Cryptographic constraints
  - Signature elements constraints

Signature validation report (ETSI TS 119 102-2)

- Provides a general structure and XML implementation of signature validation report
- Information on
  - The result (general and detailed)
  - The signature
  - The signed document
  - The elements used in the validation
- Might be signed
- To be used for example by a validation service

Signature (validation / creation / augmentation) policy

- Has four different parts
  - ETSI TS 119 172-1: Building blocks and table of contents for human readable signature policy
  - ETSI TS 119 172-2: XML format for signature policies (machine readable)
  - ETSI TS 119 172-3: ASN.1 format for signature policies (machine readable)
  - ETSI TS 119 172-4: Signature validation policy for European qualified electronic signatures/seals using trusted lists
    - Based on ETSI TS 119 615 Procedures for using and interpreting EU Member States national trusted lists
  - Part 1 and part 4 contain signature creation / validation / augmentation constraints and applicability rules
  - Machine readable policies consider only technical constraints on digital signatures, but no pure applicability rules

Signature validation service

- **ETSI TS 119 441**: Policy requirements for TSP providing signature validation services
  - Main part defines requirements for a general signature validation service
  - Annex defines requirements aimed for qualified validation services for qualified electronic signature and seals based on main part
- **ETSI TS 119 442**: Protocol profiles for trust service providers providing AdES digital signature validation services
  - Defines a main structure of the protocol
  - Provides two different bindings, with XML and JSON syntax
  - Based on DSS-x core v2.0

Cryptographic Suites (ETSI TS 119 312) “Algo paper”

- Provides a list of recommended algorithms needed for signatures
  - Hash functions
  - Signature algorithms
  - Key generation
- Based on recommendations in “SOG-IS Crypto Evaluation Scheme - Agreed Cryptographic Mechanisms” which is updated every two years
- Contains **recommended** and **legacy** mechanisms
- Non-recommended algorithms are not contained