Welcome to the World of Standards

ETSI

World Class Standards

Wrap-up

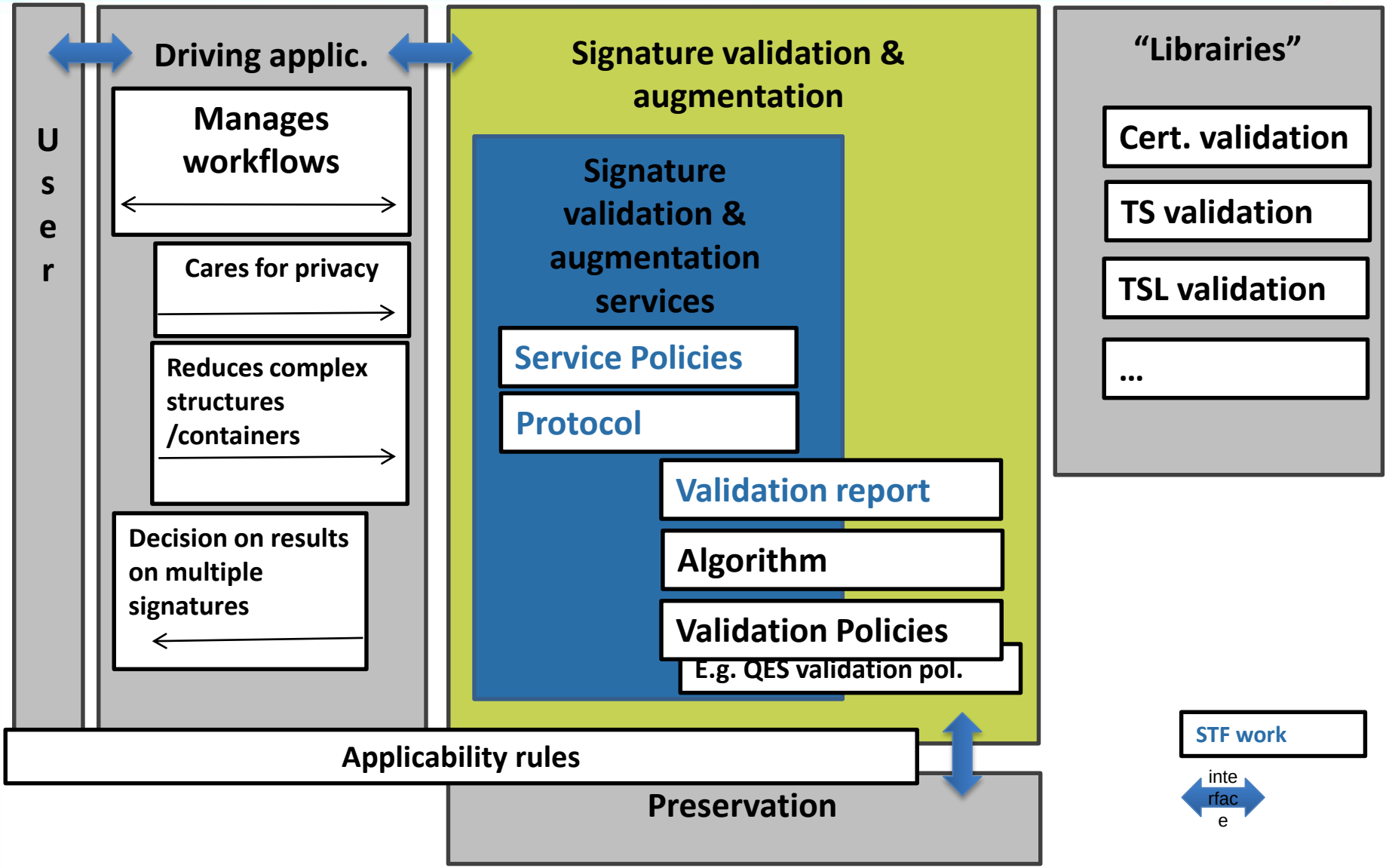
eSignature and eSeal validation workshop, Jan 10 2018

STF 524, interfaces, context

Several comments point the fact that signature validation frames within a more global context:

- SVSP or user application will probably complete the validation service trough the driving application for handling applicability rules beyond the validation. This is a.o for:
  - Reducing complex structures, containers, or workflows:
    - into more granular elements that can be handled by the validation service, knowing that the validation service may handle counter- or parallel- signatures, and could handle ad-hoc signature validation policies requested for each signature (see session 4 below)
    - in such a way that only non-confidential info is passed to the validation service
  - Interpreting the signature validation report(s) in the perspective of complex workflow where multiple signatures have different meaning
  - …
- The signature validation and augmentation service needs to be able to interface and to be positioned w.r.t preservation services
- A series of buidling blocks defined in the framework of validation are of general interest and could be specified independly (see session 3 below).

STF 524, interfaces, context



Session 2 - other standardisation initiatives

- Some fears were expressed about having a document (ETSI) based on another (OASIS), ETSI rules make it clear that it is not possible to copy in an ETSI document pieces of other documents from other organizations but ETSI can refer to a particular version of a document.
- Andreas Kuehne from OASIS explained that new elements (e.g. from 119 102-2) can be swiftly integrated into OASIS specs
- There is a liaison between OASIS and ETSI that ensures flexibility

Session 3 - feed-back from the field

- Plug tests are expected by the audience
- A library of signature validation reports corresponding to use-cases (esp. AES_QC, QES cases) is wished for TSP to test their implementations (see also session 5 below)
- The validation algorithm should cover the need for “modern” validation e.g. key controlled or validity assured certificates, etc.
- The validation report could be a P.O.E per se
- “universal” building blocs could be specified separately: TSL handling, certificate(s) validation, time-stamp(s) validation, …

Session 4 – validation report

- The work on the validation report included a mapping exercise from the DSS OASIS validation report
  - OASIS – DSS “comprenhensivity” is discussed (may be more in the sense of “understandability” then “completeness”). It is difficult to assert whether it is better to do something from the scratch or not
  - The XML part of the validation report should not be mandatory as some implementers do no use OASIS DSS
  - although the attendees do not like in general the idea of having a document based on another, ETSI rules make it clear that it is not possible to copy in an ETSI document pieces of other documents from other organizations.

Session 4 – protocol (1/2)

- The audience is in favor of an individual treatment of signatures in the following aspects:
  - it should be possible that the protocol allows to validate not all the signatures present in the request, but some of them, and clearly identify which ones.
  - it should be possible that the protocol allows to request to validate a certain signature against a certain signature validation policy.
  - it should be possible that the protocol allows to request to augment a certain signature to a certain technical level.
- There is a strong request of allowing that in the case of PDF and PAdES signatures, the document is not necessarily sent to the server but a digest of the document, detached from the signature. Regarding what has to be sent from the signature, it seems that the CMS/CAdES signature present within the Signature PDF dictionary instead the Signature PDF dictionary itself seems reasonable.

Session 4 – protocol (2/2)

- ETSI should consider in a second phase enlarge the protocol for allowing to request validation of contents of an ASiC container.

(note that the STF 524 works on signature validation, even if this does no prevent to consider this work in a braoder scope)

Session 5 - Policies & supervision (1/2)

- The policies need to address the security of the communication protocol (or submission channel) to avoid m-in-m attacks / validation report interception (e.g. one could impose or recommend SSL/TSL, propose smth for async. communication)
- The checklist is welcome
- The current list of documents seem to be quite clear and their structure aligned with other ETSI dels is appreciated
- 119 172-4 could be imposed for QES validation, at least when offered by a QSVSP, to avoid discrepancies in validation results between validation providers, and it should be clear how this maps to the requirements in the regulation

Session 5 - Policies & supervision (2/2)

- We need to think if we want to keep a « shall » for the reference to EN 319 102-1 for the algorithm
  - It will be difficult to proof that a service is compliant to a specific algorithm.
  - It would be nice to have a extensive set of "test signatures" with expected results at least for the EU case. This might be created partly after the plugtest, however, such as set and the corresponding validation result need to be controlled actively since the status of the signatures can change (e.g. if there is no signature time-stamp and the certificates expires).
- Use of Q-TS is suggested for QES (cf. recent event infineon)

Other

- Regarding constraints it is important to separate business constraints (or rules) from signature constraints. Signature validation constraints are to be processed by the SVA and business rules by the DA (or the verifier beyond).
- There is a strong demand for evolving 102 038 and its ASN.1 countepart, as there are strong difficulties for building implementations based on these specs.
  - To be done under the light of 119 172-1 and its evolution, as this document should be slightly updated to reflect applicability rules versus signature validation constraints.