‘Notary Services’ Requirements Review
&
Data Structures for Certifications

A. Schmidt, W. Schneider, Fraunhofer SIT

Requirements for Data Validation and Certification Services
draft-ietf-ltans-notareqs-02.txt
Requirements Review 1/3

- Use cases are very generic, necessary to cover the wide range of potential applications
- Accordingly, requirements remain yet mostly at a conceptual, non-technical level
- Difficulty
  - Demarcation of the scope of LTANS standardisation of certification services – what part of reqs to be turned into specs?
- More input needed
  - More reqs that make contact to specs (5.1-5.4 don't seem to suffice)
  - More operational & security reqs outside specs proper to delineate scope *and give users a hint how to apply the specs safely*

Requirements Review 2/3

From work on electronic conversions/transformations we distilled some fundamental requirements – some may be applicable to ltans-notareqs

1.Technical solutions desirable

Complex operations on/workflows with E-Docs are to be attested – standardised technical proceedings should be used to mitigate human error
-> Fits Sec. 1 or 2 (motivational)

2. Agreement of contents

Particular to transformations/format conversions/partial copies/attested translations, the certification asserts agreement of source with target contents
-> Enhances and specifies 5.1; the assertion must qualify its meaning (here ‘contents agree to the desired level’)
-> Operational; The necessary degree of agreement/correlation is determined in the context of the use-case, again one needs a space to note it

3. Authentication of authorship

Signers of originals must be authenticated – auth. results recorded in the certification
-> present in 5.4,
-> Hardly ever done in the context of notarisation of paper docs, maybe take note that necessity arises with use of otherwise anonymous technical services
-> Operational; Use-case determines verific. policies - need space to record them (-> 5.4)

4. Data Integrity -> present in Sec. 7;

Requirements Review 3/3

5. Attribution of certification and authorisation of the certifier

What is attested must be authenticated by a signature; Additionally, *identity, role, and authorisation of the certifier* can be of importance (e.g. notary public/authorised translator/public official), proper credentials are determined by use-case

-> presently buried in 5.1 last sentence; maybe better explicate/expand

-> Application of attribute certificates suggests itself; should capabilities to handle them and a space to contain them be technical reqs?

6. Data protection and secrecy

Personal and other data must be collected in the course of operation of cert. services; not to be disclosed; sometimes necessary to keep records; encryption where possible

-> some points for Sec. 7

7. Retraceability and logging

a) The certification must keep a record of proceedings (esp. for transformations) to enable forensic evaluation; b) integrity of the protocol to be assured during proceedings; c) Retraceability must be possible *independently* of the cert. service

-> a), b) Sec. 5, not yet present

-> c) rather important operational requirement

8. Independent evaluation and certification (sic) of certification services

Given the complexity and high security demands, this seems an important req for the trust in such services -> possibly a high-level note for Sec. 7, maybe outside scope

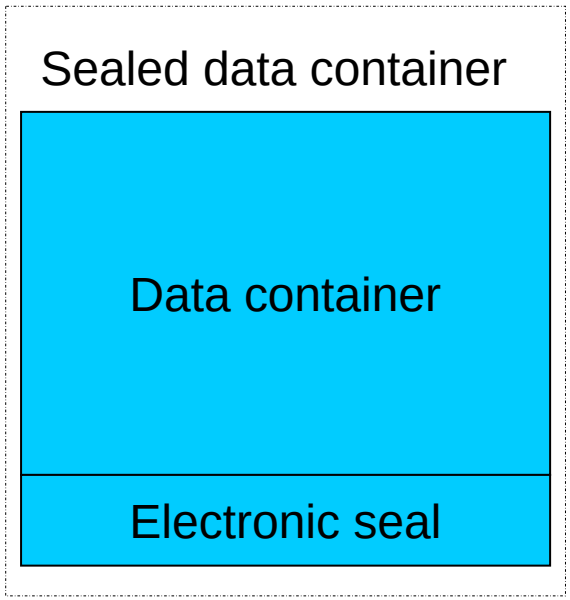
Data Structures for Certifications 1/4

General requirements for data structures:

- Generic, application independent data structure meeting the above mentioned requirements for conversion / transformation
- Flexible and extendable to support further certification services and security levels
- Able to represent the assertion of a certification service including
  - e.g. identity of participants, credentials of certification service, etc.

Data Structures for Certifications 2/4

Solution concept: **Sealed data container**



Sealed data container consists of

- **Data container** containing data to be attested
- **Electronic seal** attesting the integrity and authenticity of the data container's content and the correctness of the data / data proceeding

Data Structures for Certifications 3/4

Content of data container:

- **Final results**
  - consists of e.g.
    - Documents like contracts, agreements, oaths, etc
- **Report data**
  - consists of e.g.:
    - Documentation of the operations over the data, like data processing protocols, used components, acting parties, …
    - Intermediate results, like signature verification and authentication results, incl. used validation policies
  - provides
    - Retraceability of data processing and communication between parties
    - Authentication of authorship (signers)

Data Structures for Certifications 4/4

Content of seal:

- **Annotation**
  - consists of e.g.:
    - Name of signers of documents, incl. the authentication results
    - Credentials of the certification service and its operators, authorisation & role
    - Date and time that the service was performed
    - Information what is attested, e.g. correctness of transformation
- **Signature**
  - Signs annotation and data container
  - Consists of e.g.:
    - Electronic signature, Certificate, Attribute certificate

Seal provides

- Meaning of the assertion, e.g. all parties agreed to a final document
- Trustworthiness of the assertion
- Data integrity and authenticity of the annotation and the data container