Remote Signature Creation Services Workshop – 13th June 2018

Report on Main points from Sessions

A number of presentations were given and two panel sessions were held at the remote signature creation services workshop held, as part of the ETSI Security Week, on 13th June 2018.
(see: http://www.etsi.org/etsi-security-week-2018/remote-signature-creation for agenda and presentations)

The following are a brief summary of the main points raised during the panel sessions, as well as other points raised in discussion following presentations:

- The following question was raised from the floor following the presentation from EU Commission. The presenter asked that this be sent in writing for a considered response.

  > *The statement can be found at the "Conclusion(s)" slide of the presentation: "Only qualified trust service providers that have been granted qualified status pursuant to Article 21 using trustworthy systems and products that meets the requirements of Article 24(2), in particular letter e) and f),* ***may generate or manage electronic creation data on behalf of the signatory****. "*
  >
  > *Electronic identities as defined in chapter II of eIDAS are being used in support of remote signing support of TSP supporting remote signing under chapter III of eIDAS. The eID may be used both for registration (as per article 24.1 b) and as an authentication means for assuring sole control of the signing key.*
  >
  > *Does the text marked in bold allow this practice?*

- It was considered that the protocol specification should be as simple as possible, limited to signature transactions as far as possible.
- There is a need to support signing unlimited batches of documents from applications operated under control of a legal person. It was suggested that to facilitate this there should be no 2nd factor authentication for generating qualified eSeals. Or at least that there would be some guidance on how 2nd factor authentication could be implemented in a machine to machine scenario.
- Many issues were raised concerning conformity assessment for identification and authentication systems. This included requirement for remote registration of users.
- It was suggested that certificates should contain information about the power of a natural person to act on behalf of an organization.
- When deploying remote server signing solutions the part that most commonly needs to be adapted for particular deployments is support for to authentication/authorization. Is it better not to include specific features for authentication in the protocol document.

- There was a discussion on “What you see is what you sign”. It was proposed in line with eIDAS annex II.2 that the reader should not be forced to view the content of any document to be signed, although this should not be prevented.
- ENISA reported that on two activities that were of direct relevance to the workshop:
    - ENISA are carrying assessment of CEN standards to consider their applicability to the QSCD for remote signing under implementing decision 2016/630. A draft is due to be available by September this year.
    - ENISA are reviewing TSP audit requirements taking into account the work of the CA Browser Forum and WebTrust. A draft is due to be available October this year.

  Note: ENISA is to confirm the correct understanding of these two activities.
- There were differing views expressed regarding the requirement for assuring sole control being the responsibility of the TSP or the QSCD. It was pointed out that recital 56 does not mention sole control, and Annex II only requires that the signing key “can be reliably protected by the legitimate signatory against use by others”. However, others pointed out that in order to achieve sole control “with a high level of confidence” (article 26) there needs to be direct security between the signatory and the control of the key in the QSCD. There was a general view that urgent clarity is needed in this area.
- Some views were expressed that without certification of the user device secure sole control is not sufficiently secure.
- A CAB reported that it was unclear which checks shall be done when doing assessment about QSCD management. It should be needed a clear method concerning how to manage such assessments.
- The current check list approach of the ETSI policy standards include too much fine detail to be checked without taking account of the need to look at the overall security of the system, using for example penetration tests.

  (Note however that general risk analysis and penetration testing are covered by references to EN 319 401).
- People agreed that it would be useful to have a checklist.
- When applying article 24.1 options for indirect registration, there are no clear requirements for identity checking. It would be useful to have some standardisation work on this, even if this does not mean that this would be accepted at national level.
- There needs to be more consistency regarding the maintenance of QSCD certification and whether this needs to be reviewed regularly.
- The ETSI protocols should support the generation of certificates “on-the-fly” at the moment of each signature request.