## Public Review: resolution of public comments on Draft ETSI EN 319 411-2 V2.0.2 (2015-01)

| **Organization name** | **Clause/ Subclause** | **Paragraph Figure/ Table** | **Type of comment** (General/ Technical/Editorial) | **COMMENTS** | **Proposed change** | **RESOLUTION** on each comment submitted |
|---|---|---|---|---|---|---|
| A | | | General | No comments. | NA | NA |
| B | 2 | 2.1 | General | IETF RFC 3647 should be included in the Normative references. | To facilitate trust mappings, include the RFC Clause/Subclause/Paragraph number in parentheses next to each Clause/Subclause/Paragraph in this document. Where this document introduces new requirements that do not appear in RFC 3647, note that fact as well. At the very least each Clause and Subclause should display the relevant RFC 3647 Clause/Subclause number. | Agreed with changes – 411-1 and 2 document to be restructured in line with RFC 3647. However, conformance to the RFC is not considered to be mandatory since it is only a guidance document identifying “candidate topics for inclusion in a detailed CP or CPS.” |
| C | 7.4.1 | Registration | Editorial | Item 3) [QCP-w] must start on a new line | Jump to next line | Accepted |
| D | 7.4.6 | a) | Technical | The standard requires that “Revocation status information shall be made available beyond the validity period of the certificate” but does not state in which form should information shall be available.<br>Is a manual offline method accepted or should revoked certificates remain on CRLs until CA termination. The latter may be impractical in large infrastructures? | Any requirements to the format of the information should be specified or it should be noted if there are no requirement to the format.<br>It should not be required to have all revoked certificates in the CRLs even beyond the validity period of the certificate. | No change<br>A separate work item is planned to provide standard for use of CRL / OCSP for handling revocation information including after the expiry. Currently, no specific requirements are stated in the policy. |
| E | 7.4.6 | a) and b) | Technical | *“The requirements specified in EN 319 411-1[2], clause 7.4.6* | | Agree that the current text mandates OCSP “forever” without |

| Organization name | Clause/ Subclause | Paragraph Figure/ Table | Type of comment (General/ Technical/Editorial) | COMMENTS | Proposed change | RESOLUTION on each comment submitted |
|---|---|---|---|---|---|---|
| | | | | ***shall apply.***<br>***In addition the following particular requirements apply:***<br>***Revocation status***<br>***a) Revocation status information shall be made available beyond the validity period of the certificate.***<br>***b) The TSP shall document precisely in its practices statements and in its terms and conditions how requirement a)***<br>***is met, including TSP termination (see clause 7.5.9).***<br>***NOTE 1: There are plans for further standardization activities for handling revocation status beyond the validity period of the certificate."***<br>**Issues:**<br>**1. ETSI EN 319 411-2 leaves open the question on how the TSPs should implement the new requirement**<br>**2. the new requirement seems to put major restrictions on OCSP response validation** | | **providing a way-out after deadlines such as expiry of CA key or CA services termination.**<br>**Notes added:**<br>**NOTE 2: The obligation from ETSI EN 319 411-1 [2] to support OCSP is not applicable after the certificate expiry.**<br>**NOTE 3: There are plans for further standardization activities for handling revocation status beyond the validity period of the certificate.** |

| Organization name | Clause/ Subclause | Paragraph Figure/ Table | Type of comment (General/ Technical/Editorial) | COMMENTS | Proposed change | RESOLUTION on each comment submitted |
|---|---|---|---|---|---|---|
| | | | | **options when we look at RFC 6960 (section 2.2), because after the expiry of the CA key which has been signed the certificate in question the only viable OCSP response validation option would be a "Trusted responder". This cannot be good.** | | |