**Comments on Draft « SBR\_Discussion\_Draft\_20220509 »**

**S/MIME certificates;**

**Baseline Requirements**

| **Team name** | **Clause/ Subclause** | **Paragraph Figure/ Table** | **Type of comment** (General/ Technical/Editorial) | **COMMENTS** | **Proposed change** | **RESOLUTION**on each comment submitted |
| --- | --- | --- | --- | --- | --- | --- |
| Compliance | 3.1.3 | Second paragraph | General | This language implies that SV certificates may only use a pseudonym field when it is issued through an Enterprise RA | Remove “approved by an Enterprise RA and “  |  |
| Compliance | 3.1.4.1 | First paragraph | General | The SHOULD implies we’re o.k. with software bugs and are implementing a method to circumvent | Replace SHOULD with MAY as an indicator |  |
| Compliance | 3.2.2.3 | Second pard | General | “... the CA shall use only the approved methods in section 3.2.2.4 of the TLS BRs...” | Not sure or don´t understand if all methods stated in 3.2.2.4 can be valid for this if we have already confirmed the FQDN. Suggest replace “when confirming” to “to confirm”. And remove the “approved” word. |  |
| Compliance | 3.2.2.4 |  | General |  | Can this section be “no stipulation”? |  |
| Compliance | 3.2.3.3 |  | Noteworthy | Noteworthy that third party databases are still allowed to be used but only if they get their data from government sources, and they must be disclosed publicly, just as we currently do with QGIS sources | Clarify that not all sources have to be disclosed, only QGIS |  |
| Compliance | 3.2.4 | 1 | General | “...which SHOULD be current names...” | “...which SHALL be current names...” |  |
| Compliance | 3.2.4.2 |  | General | Text does not specify if evidence reuse is allowed if the validation period of the ID has expired since its original validation | As example: If an identity is verified using an ID that has 6 months remaining until expiry: Is the reuse of this data allowed for 6 months, or 825 days? | TBD |
| Compliance | 4.9.6 |  | General | This section is a copy-paste from the TLS BRs which indicates “no stipulation” | Add “no stipulation” |  |
| Compliance | 6.1.6 |  | General | There´re no key parameters generation for EdDSA key pairs | Add the correspondent to EdDSA key pairs, if needed |  |
| Compliance | 7.1.2.2 | a | General | The certificates policies shall be present but does not specify if there´s any prohibited value. | Is it needed a clarification? |  |
| Compliance | 7.1.2.3 | b | General | Why is CRL required on S/MIME Subscriber certificates? | Replace SHALL be present with MAY be present |  |
| Compliance | 7.1.2.4 | 2 | General | This language is unclear. The smart card EKU is not allowed unless CA can verify key protection, but there is not key protection guidelines within the S/MIME BRs | Remove everything behind the parenthesis |  |
| Compliance | 7.1.4.2.4 & .5 |  | General | Subject:countryName is currently MAY. I would like to always set this to MUST / SHALL | Change MAY to SHALL on OV and SV |  |
| Compliance | 8.1 | First para | General | Certificates that are capable of being used to issue new certificates … is this referring to CA certificates? Why is the sentence so complicated? Is this related to frequency or circumstances of assessment? | CA certificates that are capable …A CA certificate is deemed as capable …Or reword the whole paragraph to clarify the intention or move to another section related to technically constrained CAs |  |