



S/MIME Certificate Working Group



Redmond #59 CABF Face to Face – June 2023



Update

- New Cert Issuer member: Logius PKI overheid
- Primary focus on answering questions arising from CAs implementing the S/MIME BR
 - Clarification and correction ballot pending



Clarification & Correction Ballot



- Clarification of Enterprise RA capabilities
- Clarification of Mailbox Address definition
- Clarification of Pseudonym references
- Correction of some numbering and typo issues
- Correction of missing keyUsages for EdDSA Certificates
- Correction of LEI roles
- Correction of ISO code in organizationIdentifier
- Clarification of ETSI audit requirements to include 411-2



Update

- Release by DigiCert of PKILINT as OSS. Includes lints for the S/MIME BR.
- Externally: working with ETSI on TS 119 411-6 on implementation standard mapping ETSI CP with the S/MIME BR
- Tomorrow: discussion of ICA transition for effective date
- After September:
 - Topics relating Enterprise RA
 - CAA
 - How to create bluesky between S/MIME and Signing?

All participants are reminded that they must comply with the CA/Browser Forum anti-trust policy, code of conduct, and intellectual property rights agreement, which can be found in Section 1.3 of the Bylaws and cabforum.org.

Please contact the chair with any comments or concerns about these policies.



Agenda

- Transition for Issuing CAs at Effective Date
- Erratum ballot ([link](#))
- ETSI audit requirements

As time permits...

- Question relating to organizationIdentifier ([link](#))
- Question relating to private key protection



Transition for Issuing CAs



- Certificate Consumer desire for transition plan for S/MIME ICAs to be determined by SMCWG ballot rather than root store policy
- Need to get this done ASAP!



Transition for Issuing CAs

1. Allow transition period for existing CAs
 - How long?
 - Any restrictions?
2. Same Keys: Allow reissue of existing CAs
 - Add CP OIDs where needed
 - Any restrictions?
3. New Keys: Force new compliant CAs as of Effective Date



Clarification & Correction Ballot



- Clarification of Enterprise RA capabilities in 1.3.2.1
- Updated Mailbox Address definition in 1.3.3
- Updated Pseudonym reference in 3.1.1, 3.1.3, 7.1.4.2.2 (a), and 9.4.2
- Enterprise RA reference clarifications in 3.2.4, 3.2.4.2 (6), and 3.28
- Cleaning up of numbering in 4.9.1.1
- Addition of keyUsages for EdDSA Certificates in 7.1.2.3 (e)
- Clarification of LEI in 7.1.2.3 (l)
- Clarification of ISO code in organizationIdentifier in 7.1.4.2.2 (a)
- Clarification of ETSI audit requirements in 8.4



ETSI TS 119 411-6



- Current text in section 8.4 will be updated by Erratum ballot to allow ETSI audits even if ETSI standard not ready
- When ready will update SBR reference to new ETSI TS 119 411-6
 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates
- Allow coexistence of ETSI EN 319 411-1 and ETSI EN 319 411-2 with the S/MIME BR
- Liaison draft will be shared with CABF in coming weeks



ETSI TS 119 411-6



- Approach similar to used for QWACs...
 - All the applicable requirements for the certification policy supported, as identified in the S/MIME Baseline Requirements (SBR) [1], shall be applied.
 - In case of conflict between any requirement in the current version of the present document, the latest version of the SBR takes precedence, unless a requirement in ETSI EN 319 411-1 [2] or EN 319 411-2 [3] is more stringent, in which case it remains applicable.



ETSI TS 119 411-6



SBR	ETSI
Mailbox-validated	[LCP]
Organization-validated	[LCP] or [NCP] or [NCP+] or [QCP-I] or [QCP-I-qscd]
Sponsor-validated	[LCP] or [NCP] or [NCP+] or [QCP-n] or [QCP-n-qscd]
Individual-validated	[NCP] or [NCP+] or [QCP-n] or [QCP-n-qscd]



Private Key

Current text SBR#6.1.2:

If the CA or a Delegated Third Party generates the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber, then the entity generating the Private Key SHALL either transport the Private Key in hardware with an activation method that is equivalent to 128 bits of encryption or encrypt the Private Key with at least 128 bits of encryption strength.

Example methods include using a 128-bit AES key to wrap the Private Key or storing the key in a PKCS 12 file encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport.

Proposed amended text (changes in yellow):

If the CA or a Delegated Third Party generates the Private Key on behalf of the Subscriber where the Private Keys will be transported to the Subscriber, then the entity generating the Private Key SHALL either encrypt the Private Key with at least 128 bits of encryption strength or transport the Private Key in hardware with an activation method that is at least equivalently secure.

Example methods include using a 128-bit AES key to wrap the Private Key or storing the key in a PKCS 12 file encrypted with a randomly generated password of more than 16 characters containing uppercase letters, lowercase letters, numbers, and symbols for transport. When using hardware with additional security measures, e.g. smartcards with a limited number of PIN entry attempts, these additional measures should be taken into account and e.g. shorter PINs or passwords may be used.