TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-EBCA "PKI-Workshop" 2023

Berlin, 21.09.2023

"S/MIME Baseline Requirements - Challenges from Ballot to Effective Date"

Stephen Davidson, DigiCert

Chair of S/MIME Certificate Working Group

Stephen Davidson

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Focus on standards and accreditations related to DigiCert Qualified Trust Service Provider and digital signature-related businesses.
- Co-founder of QuoVadis.
- Active in the CA/Browser Forum and ETSI ESI-Electronic Signatures & Infrastructures.
- Chair of the S/MIME Certificate Working Group.

S/MIME Certificate Working Group

- In 2020 chartered by CA / Browser Forum
  - 30 Certificate Issuers, 6 Certificate Consumers, 14 Associate Members and Interested Parties
- Baseline Requirements applicable to CAs that issue S/MIME certificates used to sign, verify, encrypt, and decrypt email:
  - Verification of control over email addresses
  - Key management and certificate lifecycle
  - Certificate profiles for S/MIME certificates and Issuing CA certificates
  - CA operational practices, physical/logical security, etc.
- Rely on other CABF works where relevant. Exercise care to avoid unintended adverse effects on overlap use cases.

S/MIME Market

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Little broad visibility on “real world” use
- Entanglement with other use cases
  - document signing
  - clientAuth
- Wider variety of deployment modes
  - Common use of Enterprise RAs
  - How keys are generated and stored (soft vs token/hsm, local vs server/escrow)
  - Desktop vs gateway vs web/cloud
- Few dominant standards outside RFC
  - Some overlap with browser requirements
  - Some influential policies specific to user groups
- “Tolerant” processing by Certificate Consumer software

S/MIME BR

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

When	What
November 1, 2022	SMC 01 Ballot passed!
January 1, 2023	End of 60-day IPR Review
July, 2023	SMC 03 Carification Ballot
September 1, 2023	Effective Date
September 15, 2024	Replacement of “extant” S/MIME CAs
September, 2024	Coverage in audit reports: • WebTrust for S/MIME • ETSI TS 119 411-6

CA/BROWSER FORUM

Scope

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

An S/MIME Certificate can be identified by

1. Extended Key Usage (EKU) for id-kp-emailProtection

   and

2. the inclusion of a *rfc822Name* or

   an *otherName* of type id-on-SmtpUTF8Mailbox

   in the *subjectAltName* extension

Cert Profile Types

Mailbox-validated	Subject is limited to (optional) subject:emailAddress and/or subject:serialNumber attributes.
Individual-validated	Includes only Individual (Natural Person) attributes in the Subject.
Organization-validated	Includes Organization details (legal entity) in Subject. Example uses include invoice or statement mailers, etc.
Sponsor-validated	Organization certificate that also includes “sponsored” Individual (Natural Person) attributes. Often issued via an Enterprise RA.

Cert Profile Generations

- Each Type will have Generations:

Mailbox	**Legacy**	Moves to an auditable framework but includes flexibility in allowed field usages and verification. • Will be sunsetted • 1185 days max validity
Individual	**Multipurpose**	Flexibility in the eKU (primarily to allow overlap with existing use cases for document signing) • 825 days validity
Organization	**Strict**	The long term target profile. Dedicated eKU. • 825 days validity
Sponsor		

Cert Profile Types

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

	Mailbox Control Section 3.2.2	Organization Identity Section 3.2.3	Individual Identity Section 3.2.4
Mailbox	YES	-	-
Individual	YES	-	YES
Organization	YES	YES	-
Sponsor	YES	YES	YES

Vetting

Section 3.2.2 Mailbox control must be performed by the CA

1. *Validating Applicant's authority over email address via domain:*
   - Only the approved methods in Section 3.2.2.4 of TLS BR
   - Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate
   - Suitable for Enterprise RA

2. *Validating control over email address via email:*
   - Unique Random Value sent via email to each Mailbox Address in request

3. *Validating applicant as operator of associated mail server(s):*
   - Confirm control of the SMTP FQDN to which a message delivered to the Mailbox Address should be directed

Vetting

- Section 3.2.3 – Org vetting
  - Org vetting is mainly “OV plus”
  - Legal name based on government records
  - ETSI-style organisationIdentifier attribute in Subject
- Section 3.2.4 – Individual vetting
  - CA options: Physical ID, Digital ID (such as eMRTD), eID
  - Government eID (such as eIDAS “notified”, and future EUDI Wallet)
  - Allows reliance on Enterprise RA records
  - Attestations (from company for affiliation, or from authorized sources as supplementary)
  - Allows pseudonym per Section 3.1.3

A few things …

- The rules are defined:
  - Certificate Profiles
  - Content of fields, well as verification requirements
- For example, commonName is restricted:

Mailbox	Mailbox Address
Individual	Personal Name, Pseudonym, or Mailbox Address
Organization	organizationName or Mailbox Address
Sponsor	Personal Name, Pseudonym, or Mailbox Address

A few things …

- *Org* and *Sponsored* profiles include organisationIdentifier verified by CA
  - VATDE-123456789 vs NTRUS+CA-12345678
  - serialNumber attribute remains available for Enterprise RA use (for uses such as customer ID or employee number) with minimal specification
- Some restrictions on SAN types (such as dNSName, iPAddress, otherName, URI)
- Some restrictions on certificateHold
- Allows additional algorithms (such as RSASSA-PSS and EdDSA/Curve25519 and Curve448)
- Light touch on dual use vs split keys, escrow
- OCSP is optional

Lessons from implementing

- Request from implementers to include transition rules in new standards
  - Lead time for ballots
- Spread of CAs across Legacy -> Strict
- Enterprise RA is very dominant
- In ERAs, broad use of Pseudonyms
  - “Uniqueness” questions
  - Grey area between Org-validated and Sponsor-validated profiles
- OrgID jurisdiction level-setting
- Complexity of separating emailProtection from documentSigning use cases

A few future things …

- WebPKI moves towards pure hierarchies, shorter Root and ICA lifecycles
- CAA using a new flag “issuemail”
- Legacy generation will fade away
- Automation!
- Liiiiiinting!

Linting

- Automated compliance checking
- Started with the TLS BR
  - certLint, ZLint and X509lint
- DigiCert released next-gen pkilint as OSS
  - ASN.1 parser, allowing deeper dives
  - Can look at other PKI structures like CRL, OCSP
  - Rich validation logic (allows test variables)
- Growing library of test frameworks
  - S/MIME BR profiles (Ballot SMC01 and SMC03)
  - New TLS BR profiles (Ballot SC62)
- pkilint repository on GitHub

- CABF Meeting minutes (including F2F) https://cabforum.org/category/minutes/
- CABF General public list https://cabforum.org/pipermail/public/
- Server Certificate WG public list https://cabforum.org/pipermail/servercert-wg/
  - Validation Subcommittee public list https://cabforum.org/pipermail/validation/
- Code Signing Certificate WG public list https://cabforum.org/pipermail/cscwg-public/
- S/MIME Certificate WG public list https://cabforum.org/pipermail/smcwg-public/
- NetSec WG public list https://cabforum.org/pipermail/netsec/

Audit Standards

- WebTrust for CAs - S/MIME
- ETSI TS 119 411-6 “Requirements for trust service providers issuing publicly trusted S/MIME certificates”
  - Mapping of the ETSI CP OIDs to the CABF OIDs