TeleTrusT-EBCA "PKI-Workshop" 2024

Berlin, 10.10.2024

"S/MIME Baseline Requirements – updates on S/MIME standardization"

Stephen Davidson, DigiCert, Chair of "S/MIME Certificate Working Group" in the "CA/Browser Forum"

Standards Personalities

eIDAS

- Trusted Lists EUTL
- Supervisory Bodies
- Conformity Assessment Bodies (CABs)
- ETSI standards

WebPKI

- Browser Root Programs
- CA/Browser Forum
  - S/MIME Baseline Requirements
  - TLS Extended Validation Guidelines
  - TLS BR
  - Network and Certificate System Security Requirements
  - Code Signing BR

S/MIME

- CABF S/MIME Certificate Working Group (SMCWG)
- Baseline Requirements for CAs that issue S/MIME certificates used to sign, verify, encrypt, and decrypt email
  - Working now ~5 years
  - Chair: Stephen Davidson (Digicert), Vice Chair: Martijn Katerbarg (Sectigo)
- Diverse membership
  - 34 Certificate Issuers
  - 7 Certificate Consumers
  - 15 Associate Members and Interested Parties

S/MIME Market

- Situation was Wild Wild West
- Little visibility on “real world” use
- Few dominant standards
- Wider variety of deployment modes
  - Common use of Enterprise RAs
  - Desktop vs gateway vs web/cloud
  - Key handling (soft vs token/hsm, local vs server/escrow)
- “Tolerant” processing by Certificate Consumer software
- Entanglement with document signing use case which may also use emailProtection

Looking back

Version	Ballot	Description	Date
1.0.0	SMC01	S/MIME Baseline Requirements adopted	January 01, 2023
1.0.1	SMC03	Clarification and corrections	August 11, 2023
*	*	Implementation date	September 01, 2023
1.0.2	SMC04	Addition of ETSI TS 119 411-6	December 8, 2023
1.0.3	SMC05	Introduction of CAA for S/MIME	February 20, 2024
1.0.4	SMC06	Post implementation clarification and corrections	May 11, 2024
1.0.5	SMC07	Align logging requirement, key escrow clarification	July 15, 2024
1.0.6	SMC08	Deprecate Legacy Generation and minor updates	August 29, 2024

Bugs!

- More than 30 already reported in Bugzilla
- Some have required revocations!
  - Email domain validation issues
  - subjectDN formatting mistakes, like CN muddles, OrgID
  - Characters and SAN issues
  - Disallowed keyUsages
  - CP OID mixups
  - OCSP failures
- More expected under audit regime
- Active “rollup” ballots to improve the standard

Linting

- Many issues are preventable!
- PKILINT has support for:
  - PKIX
  - CABF S/MIME
  - CABF TLS BR
  - CABF EV
  - ETSI - QWAC
  - CRL, OCSP response
  - Cert chaining
- https://github.com/digicert/pkilint

Coming Next

Ballot SMC09

- Require pre-linting of leaf end entity Certificates starting September 15, 2025
- Require WebTrust for Network Security for audits starting after April 1, 2025
- Clarify that multiple certificatePolicy OIDs are allowed in end entity certificates
- Clarify use of organizationIdentifer references
- Update of Appendix A.2 Natural Person Identifiers

Coming Next

Ballot SMC10

- S/MIME BR rely on TLS BR Domain Control Validation (DCV) methods
- TLS BR perceive threats to DCV from BGP hijack etc
- Adoption of Multi-Perspective Issuance Corroboration (MPIC)
- Will require CAs to conduct DCV and CAA from up at least 5 remote, diverse perspectives by 2026
- SMC10 will adopt MPIC for S/MIME
  - Delayed start because there are CAs that may not have been aware of MPIC discussion

Coming Next

- Most S/MIME is enterprise! Your feedback is welcomed!

- Expect changes to TLS BR domain control validation methods
  - Deprecation of WHOIS
- Automation?
- Shorter validity?

Stephen Davidson
stephen.davidson@digicert.com

- Principal Strategist in DigiCert's Industry Standards team with a focus on standards and accreditations related to eIDAS Qualified TSP and digital signature businesses.
- Co-founded QuoVadis, which became part of DigiCert in early 2019.
- Active in ETSI ESI and the CA/Browser Forum; Chair of S/MIME Certificate Working Group