TeleTrusT-EBCA "PKI-Workshop" 2022

Berlin, 29.09.2022

Update on the S/MIME Baseline Requirements

Stephen Davidson, DigiCert
Chair of S/MIME Certificate Working Group

Stephen Davidson
stephen.davidson@digicert.com

- Senior Manager in DigiCert's Global Governance, Risk and Compliance 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; currently Chair of S/MIME Certificate Working Group, writing the first baseline requirements for email signing and encryption certificates.

CA / Browser Forum

- Unincorporated association of digital certificate consumers, issuers, and other (non-voting) interested groups
  - Started by aiming to create standard certificate profiles for TLS
  - Expanded to broader topics of interest to webPKI
- Auditable standards:
  - TLS Extended Validation Guidelines
  - TLS Baseline Requirements
  - Network and Certificate System Security Requirements
  - Code Signing Baseline Requirements

S/MIME Certificate Working Group

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

- Chartered to work on requirements applicable to CAs that issue S/MIME certificates used to sign, verify, encrypt, and decrypt email.

- S/MIME Baseline Requirements to address:
  - 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 Membership

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

30 Certificate Issuers

AC Camerfirma, Actalis, Asseco Data Systems, BuyPass, CFCA, Chunghwa Telecom, Comsign, DigiCert, D-TRUST, eMudhra, Entrust, GDCA, GlobalSign, GlobalTrust, HARICA, IdenTrust, iTrusChina, MSC Trustgate.com, OISTE Foundation, SECOM Trust Systems, Sectigo, SecureTrust, SHECA, SSC, SSL.com, SwissSign, Telia, TrustCor, TWCA, Visa

6 Certificate Consumers

Apple, Google, Microsoft, Mozilla/Thunderbird, rundQuadrat, Zertificon

7 Associate Members

ACAB Council, CertiPath, CPA Canada/WebTrust, tScheme, U.S. Federal PKI, Zone Media

7 Interested Parties

Arno Fiedler, KPMG Korea, PrimeKey, PSW, TeleTrusT, Vigil Security, Nathalie Weiler

S/MIME Market

- Entanglement with document signing use case which may also use emailProtection
- Wider variety of deployment modes
  - Common use of Enterprise RAs
  - How keys are generated and stored (soft vs token/hsm, local vs server/escrow)
  - Crossover with other use cases (clientAuth, document signing)
  - 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
- Little broad visibility on “real world” use

Approach

- Discussion of use cases
- Identification and review of relevant standards (such as Moz, Gmail, ETSI, US Gov)
- Verification of control over email addresses
- Discussion and drafting of leaf profiles

- Ongoing drafting of S/MIME BR v1
- Audit considerations
- Identity vetting steps

- Getting primary deliverable out
- New ideas later

S/MIME Approach

- Started tasks August, 2020
  - Chair: Stephen Davidson, DigiCert
  - Vice Chair: Mads Henricksveen, BuyPass
- Process
  - Discussion of use cases
  - Identification and review of relevant standards
  - Verification of control over email addresses
  - Discussion and drafting of leaf profiles
  - Operational practices and audit considerations
  - Identity vetting steps
- New ideas in future versions!

S/MIME BR Ballot

- We are on the edge of the ballot of SBR v1.0.0

- Process
  - 7 day discussion
  - 7 day ballot
  - 60 day Intellectual Property review
    = Adoption Date
  - 8 months implementation per section 1.2.1
    = Effective Date
  - Coverage in audit reports after Effective Date

Scope

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

An S/MIME Certificate can be identified by the existence of

an Extended Key Usage (EKU) for id-kp-emailProtection (OID: 1.3.6.1.5.5.7.3.4)

and 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	Effectively an 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

	Mailbox Control	Organization Identity	Individual Identity
Mailbox	Section 3.2.2	NA	NA
Individual	Section 3.2.2	NA	Section 3.2.4
Organization	Section 3.2.2	Section 3.2.3	NA
Sponsor	Section 3.2.2	Section 3.2.3	Section 3.2.4

Email Verification

- 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

- More to come…

Org and Individual Verification

- Org vetting is mainly OV except organisationIdentifier

- Individual vetting has options:
  - Physical ID
  - Digital ID (such as eMRTD)
  - eID (such as eIDAS “notified”)
  - Digital signature under formal frameworks (still to be approved)
  - Enterprise RA records
  - Attestations (from company for affiliation, or from authorized sources as supplementary)

Things To Look Out For -1

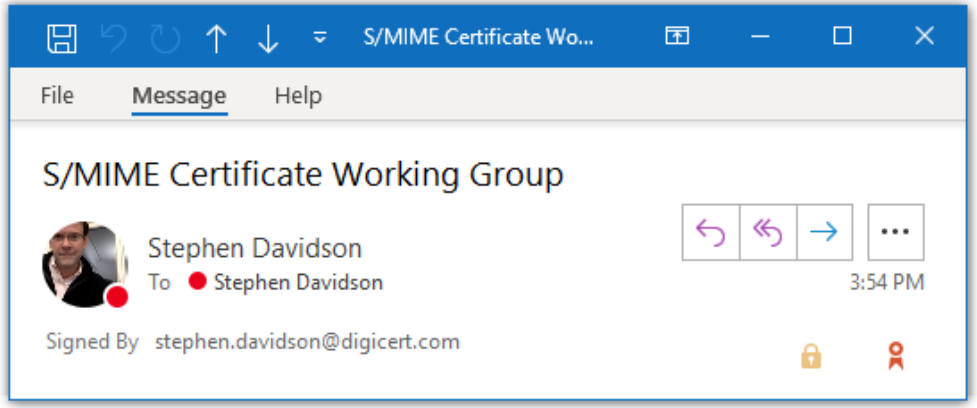
- The rules are defined:
  - Certificate Profiles
  - Content of fields, well as verification requirements
- For example, commonName is restricted:

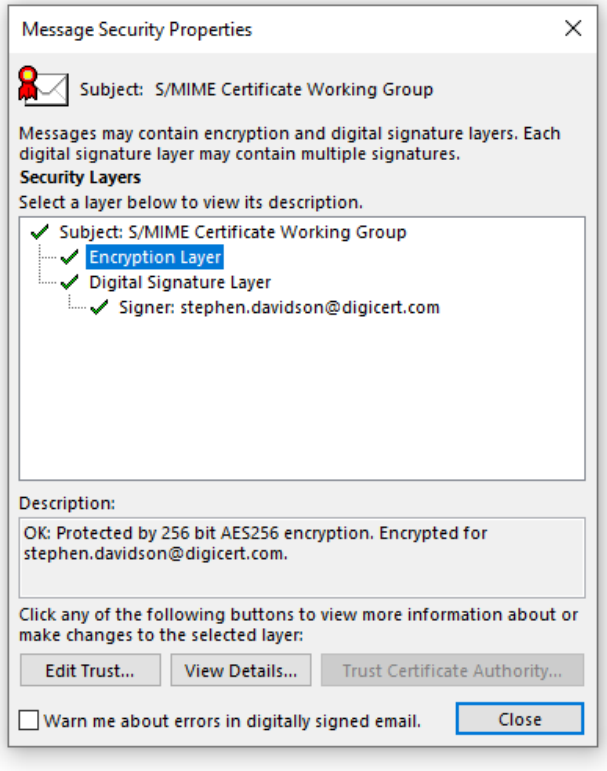
Mailbox	Mailbox Address
Individual	Personal Name, subject:pseudonym, or Mailbox Address
Organization	subject:organizationName or Mailbox Address
Sponsor	Personal Name, subject:pseudonym, or Mailbox Address

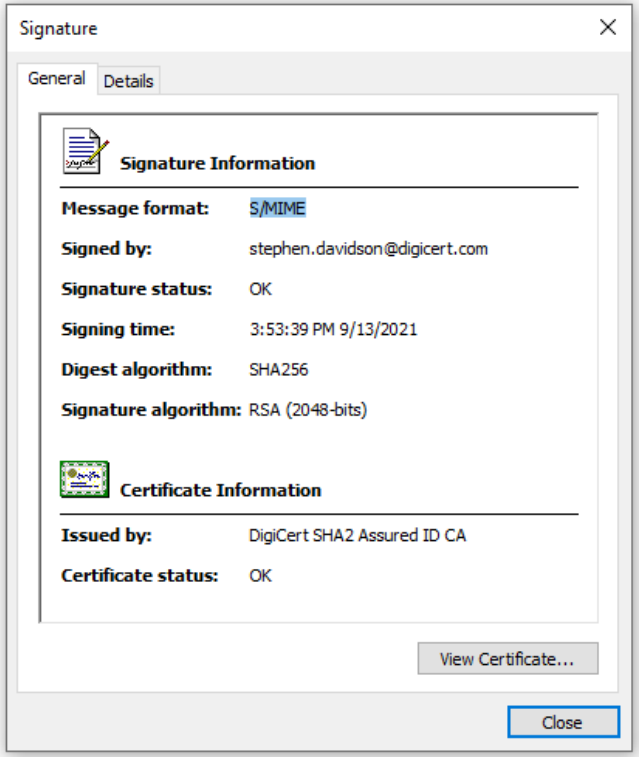
Things To Look Out For - 2

- *Org* and *Sponsored* profiles include organisationIdentifier verified by CA
  - VATDE-123456789 (VAT Scheme, Germany, Unique Identifier at Country Level is 12345678)
  - NTRUS+CA-12345678 (NTR Scheme, United States - California, Unique identifier at State level is 12345678)
- serialNumber attribute remains available for Enterprise RA use (for uses such as customer ID or employee number)
- Some restrictions on SAN types (such as dNSName, iPAddress, otherName, URI)
- Some restrictions on certificateHold
- Allows additional algorithms (such as RSASSA-PSS and EdDSA)
- Light touch on dual use vs split keys, escrow
- Ongoing debate over OCSP

Questions?


S/MIME Certificate Wo...
File
Message
Help
S/MIME Certificate Working Group
Stephen Davidson
To Stephen Davidson
3:54 PM
Signed By stephen.davidson@digicert.com


Message Security Properties
Subject: S/MIME Certificate Working Group
Messages may contain encryption and digital signature layers. Each digital signature layer may contain multiple signatures.
Security Layers
Select a layer below to view its description.
Subject: S/MIME Certificate Working Group
Encryption Layer
Digital Signature Layer
Signer: stephen.davidson@digicert.com
Description:
OK: Protected by 256 bit AES256 encryption. Encrypted for stephen.davidson@digicert.com.
Click any of the following buttons to view more information about or make changes to the selected layer:
Edit Trust...
View Details...
Trust Certificate Authority...
Warn me about errors in digitally signed email.
Close


Signature
General
Details
Signature Information
Message format: S/MIME
Signed by: stephen.davidson@digicert.com
Signature status: OK
Signing time: 3:53:39 PM 9/13/2021
Digest algorithm: SHA256
Signature algorithm: RSA (2048-bits)
Certificate Information
Issued by: DigiCert SHA2 Assured ID CA
Certificate status: OK
View Certificate...
Close

Links

- SMCWG Charter - https://github.com/cabforum/servercert/blob/e6ad111f4477010cbff409cd939c5ac1c7c85ccc/docs/SMCWG-charter.md
- SMCWG Public Listserv – https://lists.cabforum.org/mailman/listinfo/smcwg-public
- Draft S/MIME Baseline Requirements - https://github.com/cabforum/smime/tree/preSBR