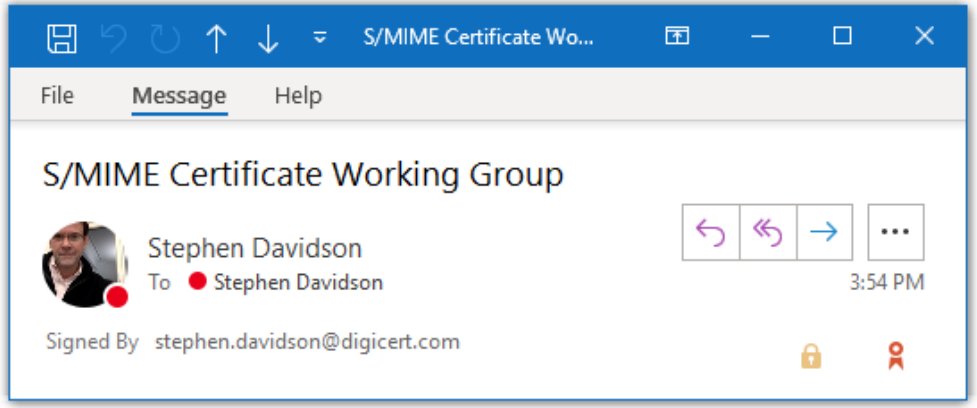
TeleTrusT-EBCA "PKI-Workshop" 2021

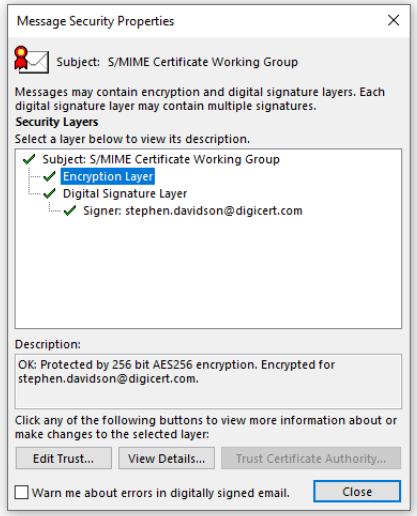
Berlin, 30.09.2021

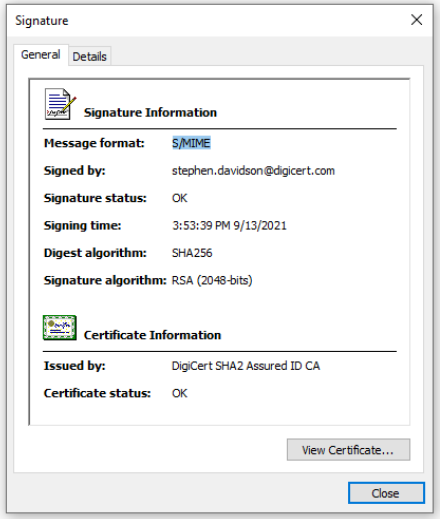
Establishing Global Baseline Requirements for Publicly-trusted S/MIME Certificates - Overview of the CA/Browser Forum S/MIME Certificate Working Group

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

S/MIME







SIGNING

- to protect integrity
- to assert origin and authenticity
- for content commitment or willful acts

ENCRYPTING

- to protect confidentiality

CA / Browser Forum

- An unincorporated association of digital certificate consumers, issuers, associate members (such as audit bodies), and interested parties
  - 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.

- The SMCWG is 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 will 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.

S/MIME Certificate Working Group

- Chartered by CABF ballot after lengthy discussion:
  - Framework where “reasonable assurance” may be provided to senders and recipients of email messages that the party identified in an S/MIME Certificate has control of the domain or email address being asserted. A variation of this use case is where an individual or organization digitally signs email to establish its authenticity and source of origin.
  - Rely on other CABF works where relevant.
  - Exercise care to avoid unintended adverse effects on overlap use cases.

- Working Group started tasks August 2020
  - Chair: Stephen Davidson, DigiCert
  - Vice Chair: Mads Henricksveen, BuyPass

S/MIME Membership

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

29 Certificate Issuers

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

6 Certificate Consumers

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

3 Associate Members

ACAB Council, U.S. Federal PKI, WebTrust

6 Interested Parties

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

What's Different

- Entanglement with document signing use case which may also use emailProtection
- Wide 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 existing standards outside RFC
  - Some overlap with browser requirements
  - Some standards 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

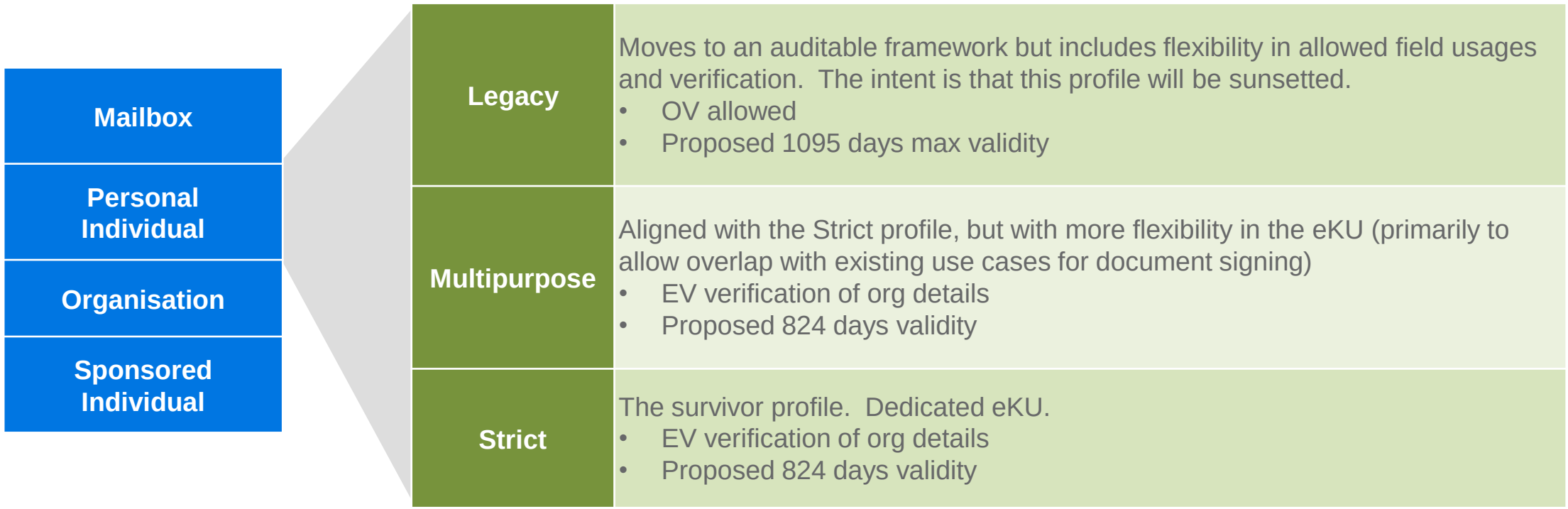
- Getting primary deliverable out
- New ideas later

Cert Profiles

- Will apply to “trusted” leaf certs with emailProtection EKU and at least one email address in Subject / SAN

Mailbox	The simplest S/MIME, including only email address. The same email control verification methods apply across all S/MIME types
Personal Individual	Includes personal details (for natural person)
Organisation	Includes Organization details (legal entity). Example uses include invoice or statement mailers, etc.
Sponsored Individual	Includes • personal details (for natural person, which may be validated by Enterprise RA for users with email addresses within the Enterprise's verified Domain Namespace) • in conjunction with Organisation details (validated by the CA)

Cert Profiles



Email Verification

- If Subject has DNemail, must be repeated as rfc822Name in SAN
- The CA shall not delegate email validation

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:*
   - Confirm control over each rfc822Name email address by sending a unique Random Value via email and then receiving a confirming response utilizing the Random Value

Things To Look Out For -1

- If Subject has DN email, must be repeated as rfc822Name (or otherName/id-on-SmtpUTF8Mailbox) in SAN
- CN must be 1) DN email or 2) O if Organisation or 3) givenName+surname if Individual
- Restrictions on allowed:
  - Subject attributes, which will have defined verification requirements
  - SAN types (such as dNSName, iPAddress, otherName, URI)
- serialNumber attribute remains available for Enterprise RA use (for uses such as customer ID or employee number)

Things To Look Out For - 2

- *Strict* profile has restrictions on allowed eKU and extensions
- *Org* and *Sponsored Individual* profiles include organisationalIdentifier verified by CA as defined in EVG 9.2.8 and Appendix H (similar to ETSI but modified for global)
  - 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)
- Allows additional algorithms (such as PSS) that are not generally allowed in TLS BR
- No stipulation on dual use vs split keys

Ideas welcomed

- Parking lot ideas for later versions:
  - CAA
  - ACME for S/MIME RFC 8823, etc.
  - Potential special extensions?
    - Enterprise RA
    - Keygen or Escrow by CA
    - Keygen and/or storage in other places (OS, browser, mobile app, email gateway, cloud user agent)
    - Private key protection (attestation by token/HSM)

Reminder: TeleTrusT is a SMCWG participant!

Links

- SMCWG Charter - https://cabforum.org/smcwg-charter/
- SMCWG Public Listserv – https://lists.cabforum.org/mailman/listinfo/smcwg-public
- Draft S/MIME Baseline Requirements - https://github.com/cabforum/smime/tree/preSBR
- Draft S/MIME Profiles - https://docs.google.com/spreadsheets/d/1gEq-o4jU1FWvKBeMoncfmhAUemAgGuvVRSLQb7PedLU/edit?usp=sharing

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 our eIDAS Qualified TSP and digital signature businesses.
- Co-founded QuoVadis, which became part of DigiCert in early 2019.
- Active in the CA/Browser Forum since 2006, currently Chair of S/MIME Certificate Working Group, writing the first baseline requirements for email signing and encryption certificates.