S/MIME Certificate Working Group
Members

25 Certificate Issuers
Actalis, Asseco Data Systems (Certum), BuyPass, CFCA, Chunghwa Telecom, Comsign, DigiCert, D-TRUST, eMudhra, Entrust DataCard, GDCA, GlobalSign, HARICA, iTrusChina, MSC Trustgate.com, SecureTrust, SECOM Trust Systems, Sectigo, SHECA, SSC, SSL.com, SwissSign, TrustCor, TWCA, OISTE Foundation

4 Certificate Consumers
Google, Microsoft, Mozilla/Thunderbird, Zertificon

3 Associate Members
ACAB Council, U.S. Federal PKI, WebTrust

5 Interested Parties
Arno Fiedler, PSW, TeleTrusT, Vigil Security, Nathalie Weiler
Background

The SMCWG is chartered to work on requirements applicable to CAs that issue S/MIME certificates used to sign, verify, encrypt, and decrypt email.

- Currently 37 members
- Just starting work: 7 meetings (including startup meetings to form the WG)

S/MIME varies from some other CABF focus areas:

- Wide variety of deployment modes
- Most standards specific to user groups
- Tolerant processing by Certificate Consumers
- Little broad visibility on use
Use Cases

SIGN
● to protect integrity
● to assert authenticity / origin
● for content commitment or wilful acts

ENCRYPT
● to protect confidentiality

KEYGEN AND/OR KEY STORAGE
● keygen by CA
● crypto token
● operating system (NSS, CAPI, etc)
● web browser (browser crypto)
● application
● remote (email gateway, cloud agent)

RELATED CONSIDERATIONS
● dual use or split keys
● protection of the private key; attestation
● escrow / key archive considerations
● Alternate algorithms
Approach

The SMCWG is chartered to work on requirements applicable to CAs that issue S/MIME certificates used to sign, verify, encrypt, and decrypt email.

- Certificate profiles for S/MIME certificates and Issuing CA certificates
- Verification of control over email addresses
- Key management, certificate lifecycle, etc.
- CA operational practices, physical/logical security, etc.
- Identity validation for natural persons and legal entities
S/MIME Certificate Profile

https://docs.google.com/spreadsheets/d/1gEq-o4jU1FWvKBeMoncfmhAUemAgGuvVRSLQb7PedLU/edit?usp=sharing

Reviewing known public reqs/stds such as Mozilla, Gmail, US Federal, ETSI, etc.

Adopt practices from BR where possible

Areas of discussion:

- Considerations for split vs dual use
- Validity period, Algorithms, LDAP
- Certificate policy OID - what’s useful for Relying Party to know about the cert?