S/MIME Certificate Working Group

Antitrust Compliance

CA/BROWSER FORUM

“As you know, this meeting includes companies that compete against one another. This meeting is intended to discuss technical standards related to the provision of existing and new types of digital certificates without restricting competition in developing and marketing such certificates. This meeting is not intended to share competitively-sensitive information among competitors, and therefore all participants agree not to discuss or exchange information related to:

1. Pricing policies, pricing formulas, prices or other terms of sale;
2. Costs, cost structures, profit margins,
3. Pending or planned service offerings,
4. Customers, business, or marketing plans; or
5. The allocation of customers, territories, or products in any way.”

October 20

CA/BROWSER FORUM

Special meeting at CABF virtual face-to-face

1. Roll Call
2. Read Antitrust /Compliance Statement
3. Review Agenda
4. New members
   - Google
5. Discussion
   - Revisit progress and process
6. Any other business
7. Next call: October 28, 2020 at 11:00 am Eastern Time

Adjourn

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 36 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 visibility on use

Members

CA/BROWSER FORUM

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

3 Certificate Consumers

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

proposed
Certificate Consumer

Google

Use Cases

CA/BROWSER FORUM

SIGN

- signing mails to protect integrity
- signing mails to assert authenticity
- signing mails for content commitment or wilful acts
- Origin / authentication

ENCRYPT

- encrypting mails to protect confidentiality

KEYGEN AND/OR KEY STORAGE

- keygen by CA
- crypto token
- operating system (NSS, CAPI, etc)
- web browser (browser crypto)
- application (on iOS, Android, etc)
- enterprise email gateway
- cloud user agent

RELATED CONSIDERATIONS

- Protection of the private key; attestation
- Dual use or split keys
- Escrow / key archive considerations

Approach

CA/BROWSER FORUM

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

CA/BROWSER FORUM

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

- Split vs dual use
- Validity period, Algorithms, LDAP
- Certificate policy OID - what's useful for Relying Party?

Relying Party Interests

CA/BROWSER FORUM

What are our priorities?

- Simplest form of requirement - a literal baseline
- Or define parameters around the options?

What's the typical Relying Party and what might they want to know?

- Escrow by Issuer?
- Soft? Token?
- User agent (Cloud agent, gateway)?
- Validation (email vs identity)? Group control?