S/MIME Certificate Working Group

October 25, 2022
Berlin F2F

CAB CA/BROWSER FORUM

S/MIME Update

Process to get to S/MIME BR v1.0.0

- 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!

Two years of work - extensive final discussions of draft

30	Cert Issuers
6	Cert Consumers
7	Associate Members
7	Interested Parties

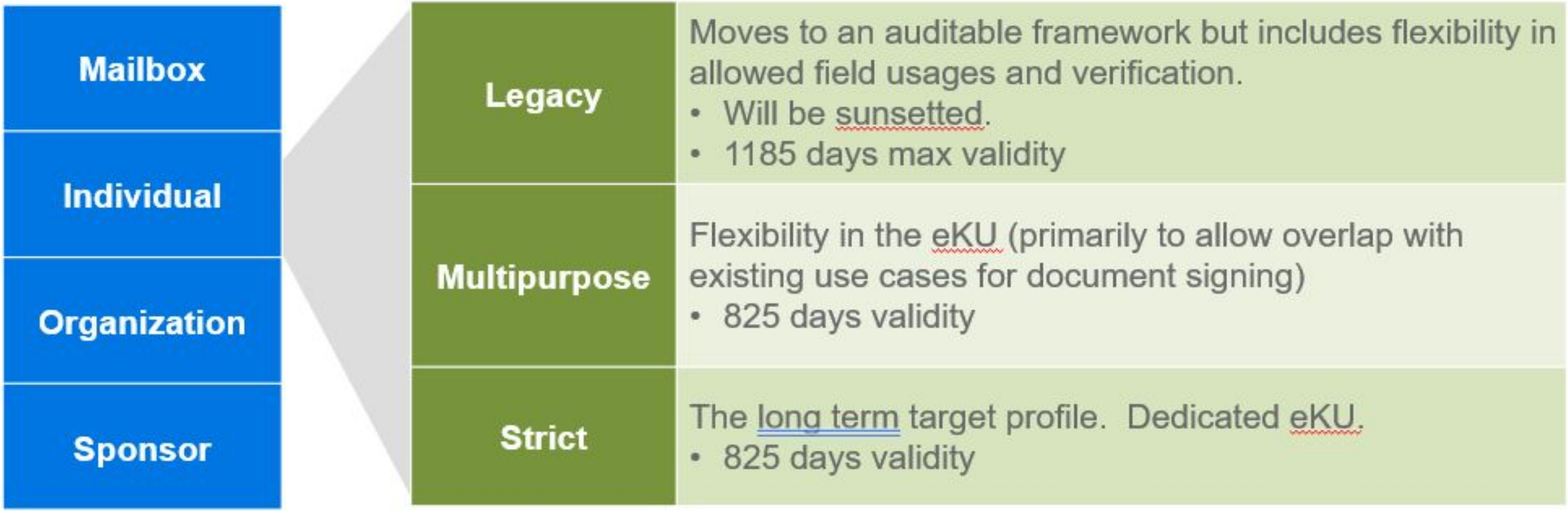
S/MIME Update

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.

S/MIME 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.

S/MIME Generations



- Mailbox
- Individual
- Organization
- Sponsor

Legacy	Moves to an auditable framework but includes flexibility in allowed field usages and verification. • Will be sunsetted. • 1185 days max validity
Multipurpose	Flexibility in the eKU (primarily to allow overlap with existing use cases for document signing) • 825 days validity
Strict	The long term target profile. Dedicated eKU. • 825 days validity