HARICA

CA/BROWSER FORUM

CA/Browser Forum Updates and S/MIME Baseline Requirements

Dimitris Zacharopoulos

CA/Browser Forum Chair

The CA/Browser Forum

IS

- Global multi-stakeholder “Standards Defining Organization (SDO)” but not an incorporated entity,
- seeking consensus among members to create best practices and standards around the issuance of publicly-trusted digital certificates

IS NOT

- An adjudication/arbitration body
- A place to lodge complaints about Certificate Issuers or Consumers
- A place to ask for an exception to compliance with standards

The CA/Browser Forum

THE PRODUCT

- "Guidelines" which are incorporated into:
  - **WebTrust for CA Standards** by WebTrust Task Force
  - **ETSI Standards** by ESI (ETSI EN 319 411-1, 411-2, 411-6)
  - … other Standards/national policies

- Guidelines are licensed under Creative Commons Attribution 4.0

Current Governance

CA/B Forum Plenary → https://cabforum.org/

- Server Certificate Working Group
  - Validation Subcommittee
- Network Security Working Group
- Code Signing Certificate Working Group
- S/MIME Certificate Working Group

Each WG has some level of independence (via charter)

More Working Groups can be created depending on Industry interest

Latest News in Server Certificate WG

- Ballots since last CA Day
  - SC56: 2022 Cleanup (2022-11-30)
  - SC58: Require distributionPoint in sharded CRLs (2022-12-11)
  - SC61: New CRL entries must have a Revocation Reason Code (2023-04-03)
  - SC62: **Certificate Profiles Update (2023-04-24)**
  - SC63: Make OCSP optional, require CRLs, and incentivize automation (2023-08-17)
- Ballots under consideration
  - SC65: EV Guidelines in RFC 3647 format
  - Profiles cleanup
  - Subscriber agreement and terms of use consolidation

Latest News in Code Signing WG

- Ballots since last CA Day
  - CSC-17: Subscriber Private Key Protection enforcement extension (2022-10-28)
  - CSC-18: Update Revocation Requirements (2023-06-29)
  - CSC-19: Remove SSL BR References (2023-09-05)

- Ballots under consideration
  - Signing Service
  - Remove EV Guidelines References
  - High Risk

Latest News in S/MIME Certificate WG

- Ballots since last CA Day
  - SMC01: S/MIME Baseline Requirements adopted (2023-01-03)
  - SMC03: Clarification and corrections (2023-08-11)
- ETSI TS 119 411-6
  - Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates
  - Builds on ETSI EN 319 411-1 and 411-2
  - Incorporates S/MIME BRs by reference
- TSPs MUST be compliant for **activities starting 2023-09-01**
- Ask your ETSI auditor to **add the ETSI TS 119 411-6 in audit scope**

Scope of S/MIME Baseline Requirements

An S/MIME Certificate can be identified by:

1. the existence of an Extended Key Usage (EKU) for **id-kp-emailProtection** (OID: 1.3.6.1.5.5.7.3.4)

and

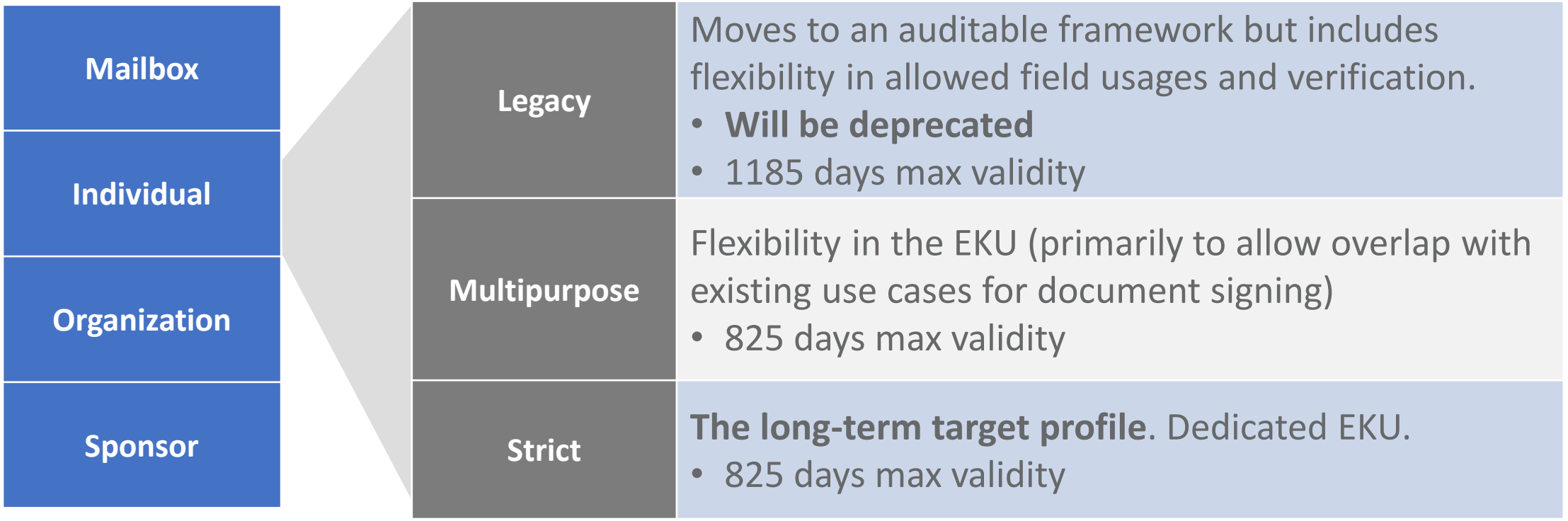
2. the inclusion of a ***rfc822Name*** or an ***otherName*** of type id-on-SmtpUTF8Mailbox in the ***subjectAltName*** extension

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.
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:



S/MIME BR OIDS

Certificate Type	Generation	Policy Identifier
Mailbox-validated	Legacy	2.23.140.1.5.1.1
	Multipurpose	2.23.140.1.5.1.2
	Strict	2.23.140.1.5.1.3
Organization-validated	Legacy	2.23.140.1.5.2.1
	Multipurpose	2.23.140.1.5.2.2
	Strict	2.23.140.1.5.2.3
Sponsor-validated	Legacy	2.23.140.1.5.3.1
	Multipurpose	2.23.140.1.5.3.2
	Strict	2.23.140.1.5.3.3
Individual-validated	Legacy	2.23.140.1.5.4.1
	Multipurpose	2.23.140.1.5.4.2
	Strict	2.23.140.1.5.4.3

A few things about S/MIME…

- *Org* and *Sponsored* profiles include **organizationIdentifier** 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) with minimal specification
- Some restrictions on SAN types (such as dNSName, iPAddress, otherName, URI)
- Some restrictions on certificateHold (suspending a certificate)
- Allows additional crypto algorithms (such as RSASSA-PSS, EdDSA/Curve25519 and Curve448)
- Light touch on dual use vs split keys, escrow
- OCSP is optional

Other resources

- Meeting minutes (including F2F) https://cabforum.org/category/minutes/
- Mailing-list archives (anyone can subscribe)
  - CABF Plenary public list https://cabforum.org/pipermail/public/
  - Server Certificate WG public list https://cabforum.org/pipermail/servercert-wg/
    - Validation Subcommittee public list https://cabforum.org/pipermail/validation/
  - NetSec WG public list https://cabforum.org/pipermail/netsec/
  - Code Signing Certificate WG public list https://cabforum.org/pipermail/cscwg-public/
  - S/MIME Certificate WG public list https://lists.cabforum.org/pipermail/smcwg-public/
- How to join the CA/B Forum
  - https://cabforum.org/information-for-potential-members/

Updates in the Apple Root Program

- Policy available here
  - **Effective September 1, 2023**, S/MIME CA providers must constantly maintain compliance with the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates (S/MIME Baseline Requirements)
  - S/MIME enabled root CAs and all subordinate CAs capable of issuing S/MIME certificates **must be audited annually**
  - CA providers must ensure all keys intended for use in a CA Certificate are included in lifecycle reports as part of their annual auditing procedures
  - **Effective April 15, 2024**, all CA providers applying to the Apple Root Program must submit only Root CA Certificates dedicated to a single purpose

Updates in the Apple Root Program (cont.)

- **Effective August 15, 2024**, TLS CA providers must support at least one of the domain validation methods from the TLS Baseline Requirements:
  - 3.2.2.4.7 DNS Change
  - 3.2.2.4.18 Agreed-Upon Change to Website v2
  - 3.2.2.4.19 Agreed-Upon Change to Website - ACME
  - 3.2.2.4.20 TLS Using ALPN
- **Additional Audit Obligations**
  - Apple reserves the right to require a CA provider to complete additional audit engagements.
  - Apple reserves the right to appoint or reject an auditor for a CA provider.
  - Apple reserves the right to require a detailed controls report from a CA provider.
    - A detailed controls report provides a thorough description of a CA provider's certification authority system and design as well as their implementation and operating effectiveness of PKI controls.
    - A detailed controls report may be a single report or a collection of artifacts which together provide the requisite information.

Updates in the Google Root Program

- Policy at https://g.co/chrome/root-policy Version 1.4
  - alignment with CCADB Policy Version 1.2 and the Baseline Requirements
  - clarify requirements related to the submission of annual self assessments
  - clarify requirements to better align with program intent (e.g., CA owner policy document freshness)
  - updated audit and incident reporting requirements to promote increased transparency
  - require subordinate CA disclosures in CCADB
  - clarify CA certificate issuance notification requirements
  - CCADB Self-Assessment

Updates in the Mozilla Root Program

- Policy 2.9. Redline from previous version
  - Provisions for S/MIME and S/MIME Baseline Requirements
  - A CA Operator MUST disclose a serious vulnerability or security incident in Bugzilla as a secure bug in accordance with guidance found on the Vulnerability Disclosure wiki page.
  - Annual self-assessment for server TLS certificate issuers
  - Certificate Revocation Reasons point to TLS Baseline Requirements
  - Root CA Lifecycles according to https://wiki.mozilla.org/CA/Root_CA_Lifecycles

HARICA

CA/BROWSER FORUM

Thank you

Dimitris Zacharopoulos

dzacharo@harica.gr