

TeleTrust-EBCA "PKI-Workshop" 2026

Berlin, 08.10.2026

Update CA/Browser Forum S/MIME and TLS

Stephen Davidson, DigiCert



digicert®

Stephen Davidson

stephen.davidson@digicert.com

Director – Trust Strategy
DigiCert Industry Standards

- CA/Browser Forum
 - Chair of *S/MIME Certificate Working Group*
 - Chair of *Server Certificate Working Group*
 - Chair of *Validation Sub-Committee*
- ETSI ESI
- PQ / Merkle Tree Certificates

—
14

TLS Baseline
Requirements

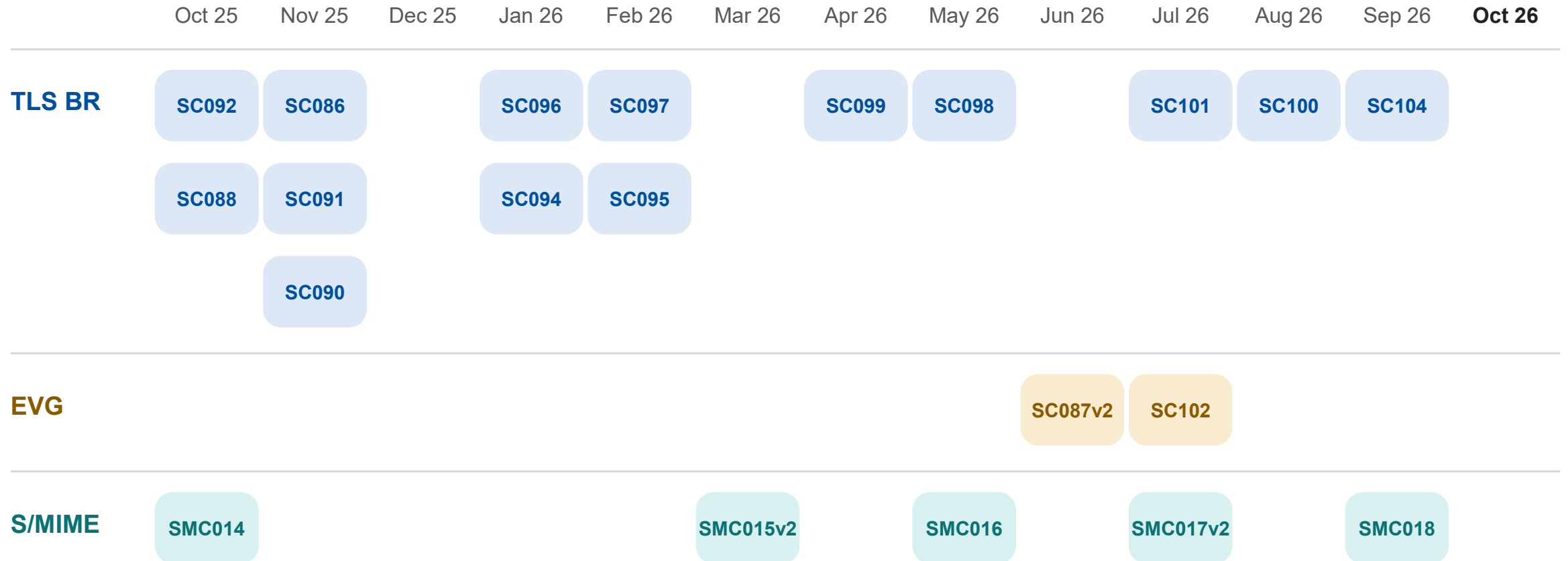
—
2

EV Guidelines

—
5

S/MIME Baseline
Requirements

Ballot Map



S/MIME Baseline Requirements

v1.0.12

13 Oct 2025, SMC014

DNSSEC for CAA lookups

Validation back to the IANA root for CAA lookups at the Primary Network Perspective, effective 15 March 2026. Mirrors SC085. Email DCV methods inherit the TLS BR 3.2.2.4 rules.

v1.0.13

27 Mar 2026, SMC015v2

Mobile driver's licence (mDL) for individual identity

mDL conforming to ISO/IEC 18013-5, verified per ISO/IEC 18013-7, from an issuing authority legally authorized by the relevant government.

v1.0.14

5 May 2026, SMC016

Equivalence with SC096 and SC097

DNSSEC logging carve-out and SHA-1 sunset. Unexpired Subordinate CA certificates issuing S/MIME with SHA-1 must be revoked.

v1.0.15

30 Jul 2026, SMC017v2

Larger RSA CA keys

RSA Root and Sub-CA keys created after 15 Sep 2026 must be 4096 bits. Subscriber minimum stays 2048. From 15 Sep 2027, no subscriber issuance from RSA Sub-CAs under 3072 bits.

v1.0.16

28 Sep 2026, SMC018

Cross-certificates and ECU realignment

CCADB Policy 6.3 cross-certificate requirements apply immediately. From 1 Jul 2027 only id-kp-emailProtection (mandatory) and id-kp-clientAuth (optional) are permitted in Sub-CA and subscriber certificates.

Big Themes for S/MIME

- Change in leadership
 - Stephen Davidson (DigiCert) and Martijn Katerbarg (Sectigo) rotate off
 - Rebecca Kelly (DigiCert) and Scott Rea (eMudhra) take over
- Apple Policy changes
 - Restrict Multipurpose to clientAuth and emailProtection
 - Dedicated CPS requirements
- Desire to streamline the options / promote agility
- SMC019 - Allow PQ Composite Certificates
 - ML-DSA and ML-KEM with legacy RSA / ECDSA
- SMC020 - drop BR version recording
- Machine readable certificate profiles

TLS Baseline Requirements: Oct 2025 to Feb 2026

v2.1.8

3 Oct 2025, SC092

Sunset of precertificate signing CAs

Ends use of Precertificate Signing CAs. Effective 4 Nov 2025.

v2.1.9

9 Oct 2025, SC088

Persistent DNS TXT validation

New DCV method 3.2.2.4.22: TXT record at _validation-persist with an accounturi.

v2.2.0

13 Nov 2025, SC086

Reverse zone names excluded

No certificates for names under in-addr.arpa or ip6.arpa from 15 Mar 2026.

v2.2.1

13 Nov 2025, SC091

Reverse lookup sunset, persistent TXT for IPs

Reverse address lookup ends 15 Mar 2027. New persistent TXT method for IP addresses.

v2.2.2

20 Nov 2025, SC090

Email, phone and crossover methods sunset

Email and phone DCV: SHOULD NOT from Mar 2026. Phone ends Mar 2027, email Mar 2028.

v2.2.3

15 Jan 2026, SC094

DNSSEC exception for email validation

MUST apply DNSSEC to queries that obtain the ADN, SHOULD on others.

v2.2.4

14 Jan 2026, SC096

DNSSEC logging carve-out

DNSSEC validation lookups fall outside logging and self-audit requirements.

TLS Baseline Requirements: Feb to Oct 2026

v2.2.5

24 Feb 2026, SC097

SHA-1 sunset

Removes all remaining SHA-1 signatures from certificates and CRLs. Effective 25 Feb 2026.

v2.2.6

27 Feb 2026, SC095

Clean-up 2025

Annual maintenance ballot. Also moved the EV Guidelines to v2.0.2.

v2.2.7

18 Apr 2026, SC099

Improved recording of validation method

Records which validation method was used. Proposed by Let's Encrypt (ISRG).

v2.2.8

13 May 2026, SC098

RFC 8657 CAA parameters

Process accounturi and validationmethods from 15 Mar 2027. Disclose the account URI format.

v2.2.9

2 Jul 2026, SC101

Authorization Domain Names clarified

Defines how the ADN is derived for each method. Proposed by Let's Encrypt (ISRG).

v2.3.0

6 Aug 2026, SC100

DNSSEC clarification and consolidation

All DNSSEC text moves to section 4.2.2.2. No new obligation. Proposed by DigiCert.

v2.3.1

3 Sep 2026, SC104

AIA extension set to SHOULD

Presence of the AIA extension in subscriber certificates is now SHOULD.

Upcoming Dates

- **15 Nov 2026** SC101 Authorization Domain Name derivation becomes mandatory for TLS DCV
- **15 Mar 2027** 100 day validity and 100 day DCV reuse. Phone, IP contact and reverse lookup methods end. RFC 8657 CAA parameter processing begins.
- **1 Jul 2027** S/MIME EKUs limited to emailProtection and optional clientAuth
- **15 Sep 2027** S/MIME: no subscriber issuance from RSA Sub-CAs under 3072 bits
- **15 Mar 2028** Email-based DCV methods end
- **15 Mar 2029** 47 day validity and 10 day DCV reuse

Four TLS themes



Retire weak validation, add automatable validation

Email, phone and crossover-prone methods get dated sunsets. A persistent DNS TXT method arrives.



Shorter lifetimes meet shorter reuse

The SC-081 schedule took its first step on 15 March 2026. Supporting ballots make automation realistic.



Precision over new obligations

Authorization Domain Names, logging, DNSSEC scope were clarified rather than expanded.



EV re-alignment

Start with squeezing out the overlaps, move on to modernizing the requirements

A Few Moving Forward Themes



Deprecate technically constrained Sub CAs

Chrome proposes to end the model where a Sub CA is limited by the nameConstraints extension.



Deprecate IV TLS

Individual-validated (IV) certificates for TLS would be retired.



Rewrite Section 7 as machine-readable profiles

Replace the cross-referenced tables with versioned, standalone certificate profiles that feed the CA and drive linting.



Create guardrails for AI in validation

Define allowable use of AI in validation tasks, and best practices for implementation.

Slimming down DCV

15 March 2026, in effect

IP Address method retired

- 3.2.2.4.8 can no longer be relied on
- Email and phone DCV: SHOULD NOT
- No certificates for names under in-addr.arpa or ip6.arpa (SC086)

15 March 2027

Phone and IP contact methods end

- 3.2.2.4.16 and 3.2.2.4.17
- 3.2.2.5.2 and 3.2.2.5.5
- 3.2.2.5.3 reverse address lookup (SC091)

15 March 2028

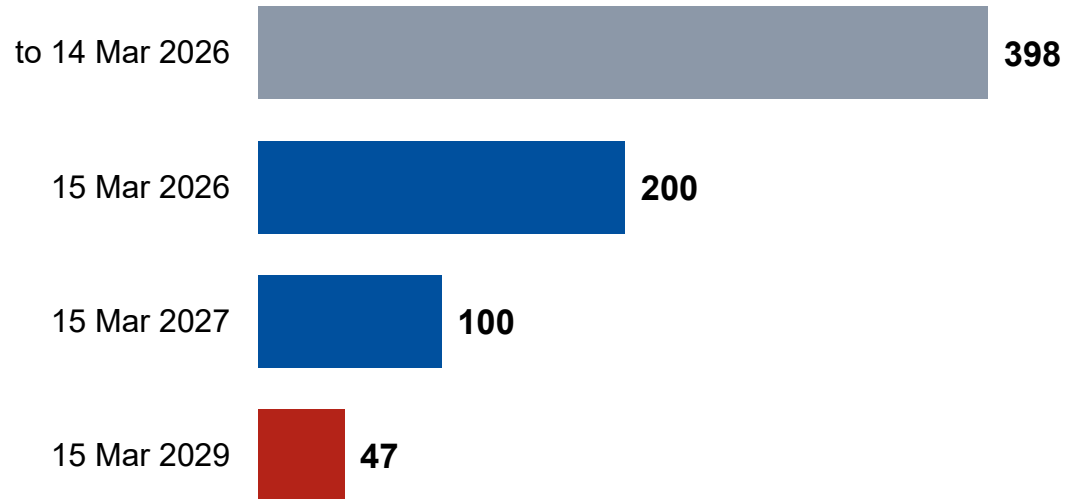
Email DCV ends

- 3.2.2.4.4 constructed email
- 3.2.2.4.13 email to CAA contact
- 3.2.2.4.14 email to DNS TXT contact

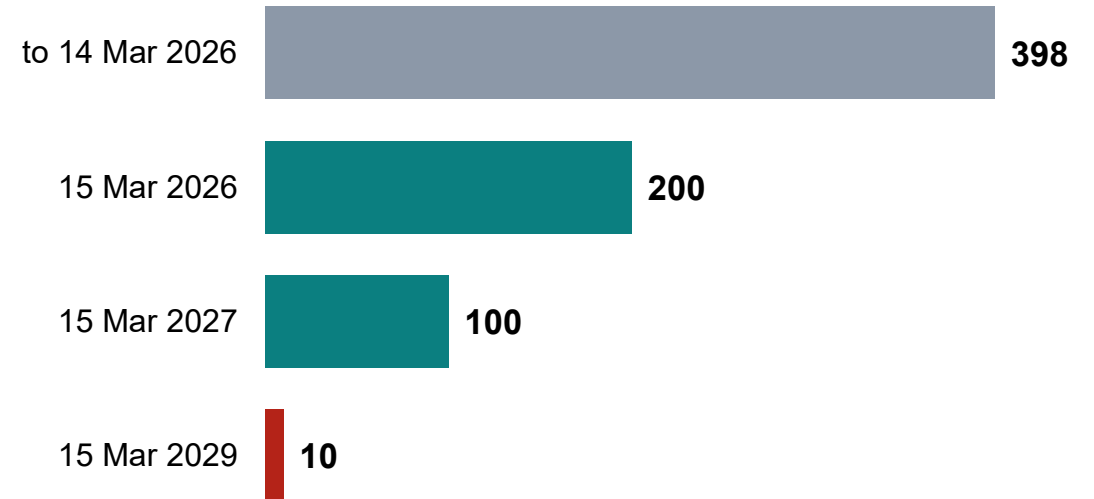
Added in the same period: 3.2.2.4.22, DNS TXT with persistent value (SC088). Record at _validation-persist, carries an accounturi, may carry persistUntil, 10 day maximum reuse. SC091 adds a persistent TXT approach for IP addresses.

The first SC-081 step landed, and tooling followed

Maximum subscriber certificate validity (days)



Domain and IP validation data reuse (days)



Subject Identity Information reuse stays at 398 days. Short-lived subscriber certificates are now 7 days or less. SC098 adds RFC 8657 accounturi and validationmethods processing from 15 March 2027, with CP/CPS disclosure of the account URI format for non-ACME accounts.

Merkle Tree Certificates replace chains with proofs

1

CA signs one tree

The CA batches many certificates into one Merkle tree and signs only the tree head, not each certificate.

2

Site sends a proof

The server presents a short inclusion proof instead of a signature chain. Proof size grows with the logarithm of the batch.

3

Browser verifies

The browser checks the proof against a tree head it already trusts. Certificate Transparency is built into issuance.

Why it matters: post-quantum signatures are large, and a certificate chain carries several. MTC keeps handshakes small. Chrome will not add post-quantum X.509 certificates to its root store and plans a separate MTC-only root store instead.

Browsers on MTC

Chrome

Clear stance

- Chrome PQC Root program will be the target program

Apple

Intent stated

- Largely matches Chrome
- Differs: third legacy-cipher log, domain transparency, 7-day cap
- Expect Chrome and Apple to align

Microsoft

Interested

- Browser and OS strategies may split
- Current TLS pilot: X.509 with pure PQC ciphers
- 2027 Composite pilot

Mozilla

No stated intent

- Monitoring



Automation

- Inventory your DCV methods
- Replace email, phone and IP-contact DCV
- Automate issuance and renewal with ACME
- Plan for 47-day certificates by 2029



PQ will have flavors

- **MTC:** compact proofs, Chrome's MTC-only root store
- **Pure ML-DSA:** plain X.509, large signatures
 - Private in Chrome
 - Public Pilot in Windows
- **Composite:** ML-DSA plus a classical signature; Microsoft's 2027 pilot is code signing only



Plan against the dates

- **15 Mar 2027:** 100-day certificates; phone and IP-contact DCV end
- **15 Mar 2028:** email DCV ends
- **15 Mar 2029:** 47-day certificates, 10-day validation reuse
- **S/MIME follows TLS**, so TLS ballots are the early signal