# TeleTrusT-EBCA "PKI-Workshop" 2025

**Berlin, 18.09.2025**

## "Update S/MIME Certificate Working Group"

**Stephen Davidson, DigiCert, Chair of "S/MIME Certificate Working Group" in the "CA/Browser Forum"**

# S/MIME Certificate Working Group

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

| S/MIME BR | Ballot | Subject |
|---|---|---|
| **1.0.7** | SMC09 | Update to WebTrust requirements, require linting, minor edits |
| **1.0.8** | SMC010 | Introduction of Multi-Perspective Issuance Corroboration (MPIC) |
| **1.0.9** | SMC011 | Add EUID as Registration Reference |
| **1.0.10** | SMC012 | ACME for S/MIME Automation |
| **1.0.11** | SMC013 | Introduction of PQC Algorithms |
| **1.0.12** | SMC014 | DNSSEC for S/MIME |

# Pre-issuance Linting

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Cleans out profile issues
- Required starting 20250915
- Open-source PKILINT has complete coverage of the S/MIME BR
  - https://github.com/digicert/pkilint

# MPIC

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Multiple Perspective Issuance Corroboration
- Required when conducting Domain Control Validation (DCV) and Certification Authority Authorization (CAA) checks.
- Defense against network-level attacks like Border Gateway Protocol (BGP) hijacking.
- Quorum of agreement between Primary Network Perspective and Remote Perspectives.
  - Phased launch starting earlier this year
  - Enforcement starting 20250915

# DNSSEC

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- SMC014 = SC085
- DNSSEC adds an optional layer of security to DNS by enabling cryptographic validation of DNS resource records.
- CA required to validate DNSSEC, when present, in the course of retrieving CAA records or performing DCV-related DNS lookups from Primary Network Perspectives.
- Effective date of March 15, 2026
- Adoption rate of DNSSEC is fairly low today, but domains that do use DNSSEC will benefit from improved security.

# Post Quantum

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Introduces specifications for the use of two PQC algorithms, as standardized by the U.S. NIST:
  - ML-DSA, a digital signature scheme; and
  - ML-KEM, a key encapsulation mechanism.
- Specifies single-key/non-hybrid PQC certificates that do not rely upon pre-quantum algorithms.
- Intended to enable experimentation by Certificate Issuers with PQC certificates.
- Additional requirements on the use of PQC may be imposed by Root programs.

# S/MIME BR ongoing discussion

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Pseudonyms
  - Tagging when repeated in CN
  - Better handling of corporate “role names”
- Mobile Driver Licenses
- PQC updates (such as composite)

# Server Certificate Working Group

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

| TLS BR | Ballot | Subject |
|---|---|---|
| **2.1.2** | SC080 | Strengthen WHOIS lookups and Sunset Methods 3.2.2.4.2 and 3.2.2.4.15 |
| **2.1.3** | SC083 | Winter 2024-2025 Cleanup Ballot |
| **2.1.4** | SC084 | DNS Labeled with ACME Account ID Validation Method |
| **2.1.5** | SC081 | Introduce Schedule of Reducing Validity and Data Reuse Periods |
| **2.1.6** | SC085 | Require Validation of DNSSEC (when present) for CAA and DCV Lookups |
| **2.1.7** | SC089 | Mass Revocation Planning |

# DCV Methods

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Browser draft ballot to sunset “manual” methods
  - Methods relying on email and phone:
    - 3.2.2.4.4 (Constructed Email to Domain Contact)
    - 3.2.2.4.13 (Email to DNS CAA Contact)
    - 3.2.2.4.14 (Email to DNS TXT Contact)
    - 3.2.2.4.16 (Phone Contact with DNS TXT Record Phone Contact)
    - 3.2.2.4.17 (Phone Contact with DNS CAA Phone Contact)
    - 3.2.2.5.2 (Email, Fax, SMS, or Postal Mail to IP Address Contact)
    - 3.2.2.5.5 (Phone Contact with IP Address Contact)
  - Method that enables crossover attacks:
    - 3.2.2.4.8 (IP Address)
- Focus on automated methods

# Shrinking Time

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Driving home automation

| | Maximum Validity | DCV Reuse | Subject |
|---|---|---|---|
| **Until March 15, 2026** | 398 days | 398 days | 825 days |
| **As of March 15, 2026** | 200 | 200 | 398 |
| **As of March 15, 2027** | 100 | 100 | 398 |
| **As of March 15, 2029** | 47 | 10 | 398 |

# Mass Revocation Plans

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- Mozilla requirement, added to TLS BR
- Communicate revocation obligations to Subscribers
- Reinforce through legal agreements
- Planning for mass revocation
  - Testing
  - Under audit
- Emphasis on the use of automation, continuous improvement
  - Not just revoke: replace!

**Stephen Davidson**
stephen.davidson@digicert.com

DigiCert Industry Standards, Europe
Co-founder of QuoVadis QTSP

- CA/Browser Forum TLS and S/MIME
- ETSI ESI
- C2PA