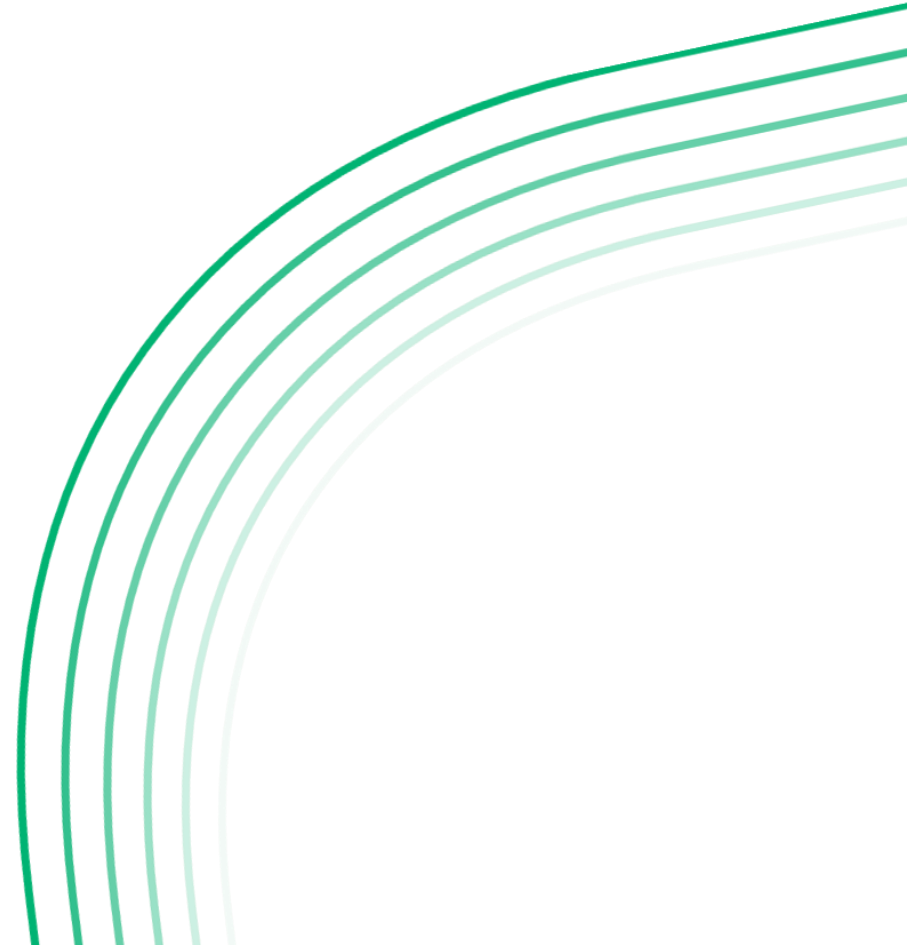


What's up CAs?

17th CA Day

September 25, 2025

Iñigo Barreira – CA Manager at Sectigo. ETSI ESI Vice-chair



Agenda

1. CA topics
 - a) 47 days validity and 10 days domain validation
 - b) PQC
 - c) Automation
 - d) clientAuth
 - e) OCSP vs CRLs
 - f) Multi-purpose CAs
 - g) Transparency in the EU
2. ETSI ESI update
3. CA/Browser Forum update
 - a) WGs update

CA Topics

47 days validity and 10 days domain validation – Why shorter TLS certificate lifecycles are a better choice

Enhanced security

Limiting outdated cryptographic standards

Operational efficiency

Agility and flexibility

Adoption of best practices

47 days validity and 10 days domain validation TLS term step-down

Effective date	Certificate term	DCV reuse period	Data reuse period
Today	398 days	398 days	825 days (EV 398 days)
March 15, 2026	200 days	200 days	398 days
March 15, 2027	100 days	100 days	398 days
March 15, 2029	47 days	10 days	398 days

47-day TLS means **12x** more work

47-Day Survival Checklist



Step 1: Awareness & Discovery



Step 2: Vendor technology inventory



Step 3: Automation mapping



Step 4: Rollout plan



Step 5: Crypto agility



August 2025

Know your inventory



Winter 2025

Compare vendors &
plan implementation



March 2026 & beyond

The first step down &
staying ahead



Fall 2025

Evaluate your automation
needs

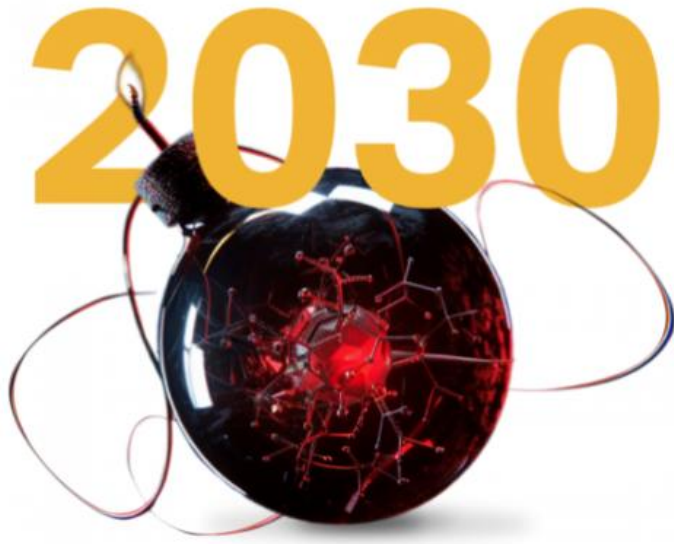


Spring 2026

Testing, training, and
transitioning



PQC - 2030: The ticking time bomb



- Quantum computing changes everything
- Threat to traditional encryption methods such as RSA and ECC
- Automation is the key to crypto agility in the quantum era



By 2029, advances in quantum computing will make conventional asymmetric cryptography unsafe to use."

2022 - Preparing for the Quantum World With CryptoAgility
Gartner

Automation

- Robotic and automated processes
 - Can lessen the IT skills gap
- Companies that are often particularly short on IT skilled staff, are those who aren't moving forward with IT automation
- Automation implementation also requires skills
- Existing staff refuse to automate, for fear of job security
- Project management is an extra project
 - A project might be difficult and more work before it pays off

Automation

- Skills gap are not solved by hiring/educating more people, but by looking and investing in automation.
 - Systemic innovation
- Automation in all IT aspects
- Still living with the technology but no longer in the environment that we used to (e.g., on premise)
- Competitive advantage: interconnectedness

clientAuth EKU in TLS certificates

- CAB TLS BRs allow the use of clientAuth EKU
- ETSI EN 319 412-4 references the CABF TLS BRs
- Chrome root program policy is not accepting the clientAuth EKU on TLS certificates
 - June 2025 for new applicants
 - June 2026 for already existing

OCSP vs CRLs - Issues with OCSP

- CRLs have significant advantages over OCSP but are not so good
- Privacy concerns
 - When someone visits a website using a software (e.g., browser) that checks for certificate revocation via OCSP, the Certificate Authority (CA) operating the OCSP responder immediately becomes aware of which website (in the case of web browsing) is being visited from that visitor's particular IP address. Even when a CA intentionally does not retain this information, CAs could be legally compelled to collect it. CRLs do not have this issue.
- Performance
 - The OCSP check is a HTTP request/response roundtrip on the network and there's time spent waiting for an answer from the OCSP Responder
- Availability
 - If the OCSP responder is down, usually clients skip the check and therefore do not verify the status of the certificate and accept as is, which then make the use of the OCSP useless as add no security
- Resources
 - Proxies (e.g., CDNs), specific systems (VAs), responders, URLs, etc.
 - personnel and infrastructure management

OCSP vs CRLs - Issues with OCSP

- Browsers not using/checking it or are implementing it in a way that provides no security benefits
 - CRLs have wide browser support and can provide privacy benefits to all sites, without requiring special web server configuration
- In 2023, the CAB Forum voted to make OCSP optional, CRLs mandatory and incentivize automation (ballot SC063) but some root programs still mandated the OCSP (this was removed end of 2024)
- Some CAs are deprecating its use
 - Let's encrypt: [Ending OCSP Support in 2025 - Let's Encrypt](#)
 - Example: Sectigo is serving billion OCSP responses daily
 - Potential issues for non-browsers applications

OCSP vs CRLs - Potential solutions

- CRLs sizes
 - Partitioned CRLs
 - CRLite: [crlite_oakland17.pdf](#)
 - Browsers: OneCRL (Firefox), CRLSets (Chrome)
- Short-lived certificates
 - <30 days

Multi-purpose CAs

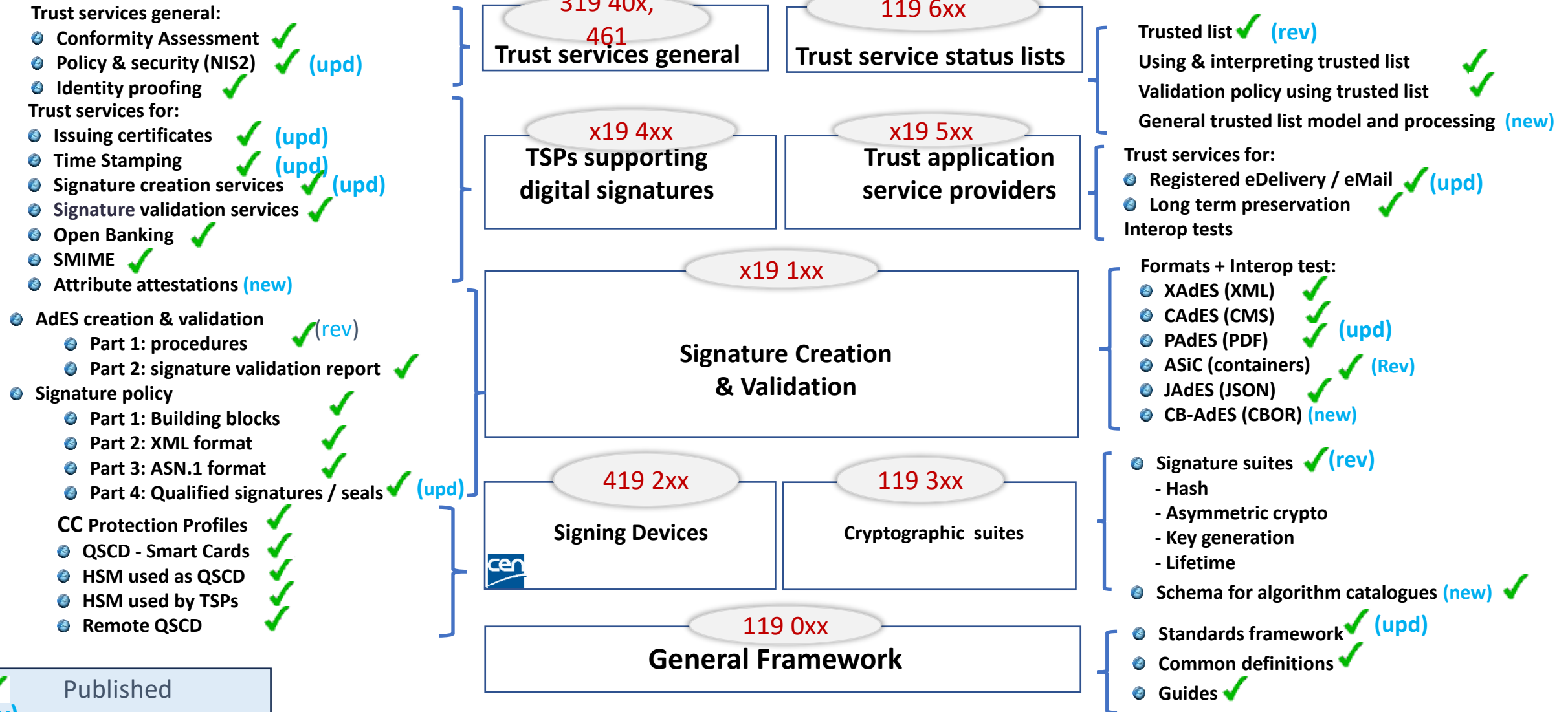
- Browser root programs require specific hierarchies based on certificate types, such as, TLS, S/MIME, Code Signing, etc.
- In the EUTL you can find several multi-purpose CAs for issuing Qcert for eSign/eSeal and QWACs
- Future phase-out of non-TLS hierarchies from the Chrome root store

EU Certificate Transparency Ecosystem

- Title
 - Requirements on a Certificate Transparency (CT) Ecosystem to make the issuing of certificates transparent and verifiable
- Scope and Field of Application
 - Report on existing Certificate Transparency approaches and on standardisation requirements for equivalent of Certificate Transparency as specified in RFC 6962 and concepts such as Static Certificate Transparency supporting log of certificates, as defined in amended Regulation (EU) 910/2014 (eIDAS 2)
- [CIR \(EU\) 2025/848](#)
 - Certificate transparency is mentioned in Annex IV for the WRP Access Certificates

ETSI ESI Update

ETSI & CEN Standards supporting eIDAS – the current picture



✓	Published
(Rev)	Recently revised
(Upd)	Update in progress
(New)	New

EU - ETSI Engagement Activities

- Monthly coordination activities + involvement in selected expert group focus meeting
 - 20+ updates to existing standards
 - 20+ new standards to be developed
- Main deliverables
 - Certificate policy for relying party wallet registration and access certificates
 - Certificate profile for public sector services signing certificate (Wallet issuer, PID Issuer, EAA Issuer)
 - Relying party authorisations
 - Interface for authentic sources
 - EAA Profiles general, Relying party access, PID/EAA Issuing
- 2 years (2026-2027)

CA/Browser Forum update

Servercert WG

- MPIC (Multi-Perspective Issuance Corroboration)
 - Defends against Border Gateway Protocol (BGP)
 - Requires DCV secrets be checked from multiple geographical locations (up to 7 in the next years)
 - Effective: March 15 monitoring, September 15 issuance in 2025
- WHOIS as email source is phasing out
 - Deprecates two arcane DCV methods
 - Email, Fax, SMS, or Postal Mail to Domain Contact
 - Phone Contact with Domain Contact
 - Effective: July 15, 2025
- Mass revocation planning
 - Effective: December 1, 2025
- DNSSEC for CAA and DCV lookups
 - Effective: March 15, 2026

S/MIME WG

- MPIC
 - Effective: May 15, 2025
- EUID as registration reference
- ACME for S/MIME
- Pre-issuance linting
 - Effective: September 15, 2025
- Introduction to PQC algorithms
- DNSSEC for CAA
 - Effective March 15, 2026

Code signing WG

- Timestamping
 - Protect Private Keys associated with its Root CA certificates and Subordinate CA certificates containing the “Time Stamping” EKU in offline Hardware Crypto Modules
 - Effective: April 15, 2025
- Reduction of code signing certificates validity period

Network Security WG

- Updates to CA Infrastructure scope, trusted roles, systems' applicability, etc.
 - Effective: July 3, 2025

