Post-Quantum

Cryptography Conference

ELI5: Implementing Digital Certificates for a Post-Quantum World

This presentation will focus on the pragmatic steps IT teams can take now to prepare for deployment of post-quantum cryptographic algorithms once it becomes practical. This conversation will directly connect the steps back to IT teams' day-to-day tasks, as it relates to certificate management, and help practitioners identify exactly what they need to do today to begin the process of being post-quantum ready. The presentation will go over: (1) the necessary steps for industry standards bodies to clarify requirements for the new NIST standards; (2) what software, hardware, and services vendors need to do to incorporate support and possible timelines for this support; (3) how enterprises can apply these updates, (4) what you, as an IT manager, can do today to begin the transformation to PQC, and (5) what a likely post-quantum certificate migration plan might look like, including the use of hybrid certificates.

Tim Callan
Chief Compliance Officer at Sectigo

SSL.com PQ SHIELD HID KEYFACTOR ENTRUST

January 15 and 16, 2025 - Austin, TX (US) | Online

SECTIGO®

PQC deployment and certificate agility

Tim Callan, Chief Compliance Officer at Sectigo

Real-world factors for implementation

What stands between us and implementation?

- Software readiness
  - Chrome 124, CloudFlare, breakage
- Certificate readiness
  - Inventory, automation, visibility
- Phase-in
  - Hybrid certificates
  - Public vs. private

Certificates…

1. Certificates will be a gating technology for most PQC
2. Certificates will be instrumental to PQC migration
3. Full PQC deployment requires full control of certificates
4. Most orgs have little control over their certificates

SECTIGO®

So when can I actually run PQC in production?

1. Algorithm selection
   - COMPLETE – 2023
2. FIPS standards
   - PARTIAL – 2024
3. IETF standards for certificates
   - End 2025 or early 2026 (?)
4. CABF standards for public CAs
   - Mid 2026 (?)

My best guess

- Earliest date for limited use case private CA using off the shelf components:

  Spring 2026

- Earliest date for public certificate issuance:

  Summer 2026

SECTIGO®

Most enterprises are not in control of their certificates

- Decentralized management
- Shadow IT
- Automation is lacking
- Tooling is missing or incomplete
- This technology is taken for granted

Impairs visibility, consistency, reliability, and agility

David Seferiadis ▾ New to Bugzilla
Comment 24 • 22 hours ago

From my experience at large enterprises supporting thousands of applications, Web PKI (E.g., CAB Forum, Bugzilla, etc.) does not effectively represent the enterprise. Enterprises often restrict public speaking, and our voice is primarily through our partner certificate authorities.

Enterprises are both subscribers and relying parties, as well as represent our customers as relying parties and through partners.

Web PKI is governed primarily by certificate authorities and browsers, yet the scope and impact of Web PKI is well beyond the browser and certificate authorities.

Despite having certificate lifecycle management platforms, complexity, scale, and legacy platforms still cause enterprises to manually manage too many certificates which is time consuming and error prone. Parts of the Enterprise are well modernized, but a sizable portion has limited or no automation.

Managing trust stores is another challenge. More work needs to be done on standardization, transparency, and automation of trust stores, particularly across partner ecosystems. This makes hierarchy changes difficult and high risk. In many cases you don't know in advance if using a new hierarchy will break connections.

There is certainly more Enterprises need to do to move away from Web PKI managed hierarchies for non-browser and internal use cases, drive automation and continue modernization - but today Enterprises have legacy environments where certificate rotations and hierarchy changes are often manual, non-trivial and error prone.

CAs must be held to a high standard, but unfortunately the impact of a potential action is borne largely by subscribers and relying parties. While I appreciate the merits of the technical conversation, from a business perspective, it would be hard to explain a potential revocation action which would have an Enterprise perception of disproportioned cost and risk.

It would be worthwhile to continue the conversation on how to improve Enterprise representation and trying to solve for the problems above.

"…certificate rotations and hierarchy changes are often manual, non-trivial and error prone."

SECTIGO®

What is certificate agility?

- The ability to replace any and all certificates
  - Error free
  - Immediate
  - Precise down to the individual certificate
  - Able to handle any volume
  - Verifiable
- Builds on the concept of crypto agility

What is hybrid encryption?

- Hybrid encryption support more than one encryption scheme at the same time using the same server
- This could be a hybrid certificate or two certificates side by side
- Each session can support the “best” scheme supported by the other side
- This allows for transition without requiring sudden universal change

Achieving certificate agility

1. Educate yourself
2. Inventory your PKI
   a. Public certificates
   b. Private CAs and certificates
   c. Watch out for “rogue” certificates
3. Achieve real-time visibility
4. Set automatic expiration actions (notification, renewal)
5. Automate DCV
6. Automate provisioning and deployment

Automation options

Several automation options:

- ACME
- Software agents
- APIs
- Other standards (EST, SCEP)

Automation platforms, AKA Certificate Lifecycle Management, play a key role

Q.U.A.N.T. – a strategic blueprint

- Transition to quantum-safe cryptography
- Become quantum resilient

Q	U	A	N	T
Quantum exposure inventory	Uncover risk	Assess and strategize	Navigate implementation	Track and manage

SECTIGO®

If you liked this conversation…

Available on these streaming services

Spotify

iHeart RADIO

STITCHER

iTunes

SOUNDCLOUD

Thank you very much!

https://www.sectigo.com/

Section Title Slide