The Qrypto-Con 2026

ENCRYPTION CONSULTING

Call for Speakers

Two days. One global stage for cryptography, PKI, and quantum readiness.

NOVEMBER 18 & 19

Learn Hands-on

Connect Globally

Watch Experts

Advance Quicker

Speak at Qrypto-Con

Qrypto-Con is Encryption Consulting's virtual conference for the people who build, run, and secure the world's cryptography. Over two days, practitioners and leaders share what's working in PKI, key management, certificate lifecycle automation, cryptographic discovery, and the migration to quantum safe cryptography.

We're inviting speakers to lead sessions of 24 to 30 minutes. Whether you have a hard won implementation story, original research, or a contrarian point of view, we want to hear it. If you have an idea that matters but isn't listed in the tracks below, just contact us and we'll make room for it.

Why speak at Qrypto-Con

Reach a focused, senior audience of PKI, cloud security, and cryptography practitioners.

Build your authority on the topics defining the next five years of enterprise security.

Present from anywhere. We record your session and you join live for audience Q&A.

The tracks at a glance

Submit your abstract under any of the six tracks below. Topics within each track are prompts, not limits. The questions are there to spark your angle.

- Cryptographic Discovery & Inventory
- PKI & Certificate Lifecycle Management
- Post Quantum Cryptography & Crypto
- Cloud & Multicloud Key Management
- Encryption in Practice
- Emerging & Future

Key dates & format

Abstract deadline	**September 15, 2026**
Acceptance notice	**October 15, 2026**
Conference dates	**November 18 & 19, 2026** Virtual
Session length	**24 to 30 minutes, plus live Q&A**
Submit to	**info@encryptionconsulting.com**

Note: dates shown are this year's schedule. Please confirm against your final event calendar before publishing.

TRACK 1

Cryptographic Discovery & Inventory

You can’t protect, rotate, or migrate what you can’t see. This track is about making enterprise cryptography visible and keeping it that way.

Building a Cryptography Bill of Materials (CBOM)

What is a CBOM and how does it differ from an SBOM? How do you build a continuously updated inventory of every key, certificate, algorithm, and protocol across cloud, HSMs, databases, source code, and trust stores? What belongs in a CBOM, and how do you keep it current?

Automated Cryptographic Discovery

How do you discover cryptographic assets across hybrid and multicloud estates without manual spreadsheets? What are the tradeoffs and coverage gaps between discovery with agents and discovery without them? How do you find cryptography hidden in source code, binaries, containers, and CI/CD pipelines?

From Inventory to Risk: Scoring & Prioritization

Once you have an inventory, how do you score assets for risk? How do you flag weak ciphers, key reuse, expiring certificates, and quantum vulnerable algorithms, and separate dormant cryptography from what’s actually in production?

Open Standards & Interoperability

Why does CycloneDX matter as a CBOM export format? How do you avoid vendor lock in and feed cryptographic inventory into your wider security and compliance tooling?

TRACK 2

PKI & Certificate Lifecycle Management

The backbone of enterprise trust, designed, automated, and kept compliant at scale.

Public Key Infrastructure (PKI)

What architecture should you implement and why? How do you protect your PKI and manage Root of Trust at scale? What are the automation capabilities and business value of modern PKI? How do you expand PKI to secure critical infrastructure?

Certificate Lifecycle Management (CLM)

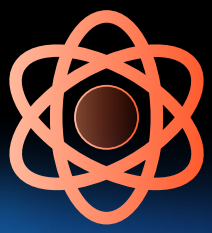
Why is automation essential as certificate volumes explode? How do you discover certificates, vulnerabilities, and compliance gaps across your network and remediate them? Best practices, trends, and bottlenecks in CLM, plus staying compliant with NIS2.

Cloud and Hybrid PKI Design

Migrating PKI from on premises to cloud or virtual environments raises real questions. What are the options, benefits, and limitations? How do you move an existing PKI between cloud service providers without breaking trust?

Code Signing & Document Signing

How do you use code signing to secure the software supply chain? CI/CD integration, use cases, and CA/Browser Forum requirements. Why does document signing matter, and how widely is it adopted?



TRACK 3

Post Quantum Cryptography & Crypto Agility

NIST finalized its first post quantum standards in 2024 and CNSA 2.0 sets milestones through 2030. The clock is running.

The NIST Post Quantum Standards in Practice

What do the new NIST standards (FIPS 203, FIPS 204, and FIPS 205) mean for real deployments? How do you evaluate and implement a quantum safe solution, and build quantum safe PKI and digital certificates?

Inventory Led PQC Migration Planning

Why does quantum migration start with discovery? How do you use a cryptographic inventory to find quantum vulnerable RSA, DH, ECDH, and ECDSA in production, then build a phased, dependency aware migration roadmap and track quantum safe adoption over time?

Crypto Agility

What is crypto agility and why is it the foundation of quantum readiness? How do organizations achieve and maintain the ability to swap algorithms without rearchitecting? What does an agile cryptographic estate look like in practice?

TRACK 4

Cloud & Multicloud Key Management

One key estate across many clouds, integrated, governed, and under control.

AWS, Azure & Google Cloud Key Management

How do you integrate AWS KMS, Azure Key Vault, and GCP KMS with your PKI and cloud HSMs? What encryption and key types are supported, and what services integrate natively? Pros and cons of integrating cloud HSM for CMK generation.

Multicloud Key Management

What is multicloud key management and why is it needed? How do you gain a single, policy evaluated view of keys across Azure, AWS, and GCP, and detect the same key appearing across clouds?

Bring Your Own Key (BYOK)

What's the need for BYOK, and the real advantages and disadvantages? When is it good practice, and what are the most useful use cases?

TRACK 5

Encryption in Practice

Where the theory meets production systems: HSMs, data protection, IoT, and incident response.

Hardware Security Modules (HSMs)

Why use an HSM and what security does it provide? What compliance does it satisfy? Where are vendors and users taking HSM technology next?

Data Protection & Data Loss Prevention

What is data protection due diligence, and how do you identify and address risks, including during mergers and acquisitions? How do you identify sensitive data and build a robust DLP framework that holds up in the cloud?

PKI for IoT Security

How can PKI secure IoT deployments at scale? Best practices and requirements for reliable, secure solutions. Are standards such as NIST ready for manufacturers to depend on?

Cryptographic Incident Response

When a CA is compromised or an algorithm is deprecated overnight, how fast can you find every affected asset? How do you query an inventory by algorithm, issuing authority, or attribute to identify blast radius in minutes rather than days?

TRACK 6

Emerging & Future

The frontier of what's coming next for cryptography, identity, and defense in the AI era.

Zero Trust Security Model

What does Zero Trust really require, and what problems does it solve? Best practices for implementation, plus the honest limitations and challenges.

Homomorphic Encryption

What is homomorphic encryption, where is it genuinely useful, and what are its real limitations and drawbacks today?

Generative AI & Cryptographic Security

How does GenAI fit into an organization's cybersecurity model? What are its capabilities, risks, and limitations? And how can AI and advanced encryption serve as defenses in modern cyber conflict?

Passwordless Authentication

What is passwordless authentication, what makes it hard to implement, and how does it improve security posture?

Standards & Compliance

What do current regulations, standards, and frameworks require for PKI, encryption, and key management? Where do existing standards fall short, and what should improve?

What to include in your abstract

- Session title and the track it fits best.
- A three to five sentence summary of your talk and its key takeaways.
- Who it's for (for example, security architects, PKI admins, CISOs) and the level: intro, intermediate, or advanced.
- A short speaker bio and your availability for live Q&A on November 18 or 19.

The Qrypto-Con 2026

Send us your abstract: a short title and a few sentences on what you'll cover and why it matters. The speaker schedule fills quickly, so submit as soon as possible.

Submit to: info@encryptionconsulting.com

Register Now

ENCRYPTION CONSULTING