

2024

Call for Speakers

Encryption Consulting
Virtual Conference



NOVEMBER 7 & 8, 2024



We are thrilled to invite you to speak at the Encryption Consulting Virtual Conference 2024. If you have an idea that you believe is important but is not on the list, please feel free to contact us. We will have it added.

Note:- Just so you know, the deadline for submission of your abstract is August 30th, 2024. We will confirm acceptance by September 7th, 2024. Presentation time is set to be 24-30 minutes.

Encryption Consulting will help record your presentation, but the speaker will be expected to be available online for questions and answers during the virtual conference.

CONFERENCE

FOUNDATION

Public Key Infrastructure (PKI)

What is PKI? What encryption is used in PKI? What architecture should be implemented and why? What are the challenges solved by PKI? What are the automation capabilities of PKI? What are the benefits of automating your PKI? How do you protect your PKI? How do you protect critical infrastructure using PKI? How do you expand PKI capabilities and business values? How to manage Root of Trust at scale?

Google Cloud Platform Services

What are the features available in GCP KMS? How do you integrate GCP KMS with your PKI? What types of encryption and keys are supported by GCP KMS? What services are integrated with GCP KMS? Other services are offered by GCP.

Data Protection

What is Data Protection Due Diligence? How do you identify data protection risks and address them? How do you frame the potential data protection risk exposure during mergers and acquisitions?

Cloud Agnostic/enabler PKI design

Migrating from On-Prem to Cloud/virtual environment, what are the options for Enterprise? What are the benefits and limitations of PKI on On-Prem and Cloud? What are the options to move Existing PKI to other Cloud service providers?

Hardware Security Modules

Why should we use HSM? What security is provided by HSM? What Compliance does HSM follow? What do HSM vendors and users think about HSM's future developments and cutting-edge technology?

Microsoft Azure Services

What are the features available in Microsoft Azure KMS? How do you integrate Microsoft Azure KMS with your PKI? What types of encryption and keys are supported by Microsoft Azure KMS? What services are integrated with Microsoft Azure KMS? Other services offered by Microsoft Azure. What is Azure Key Vault? How to integrate Azure Key Vault with Azure HSM and the benefits and limitations of integrating Azure HSM with Azure Key Vault.

AWS Services

What are the features available in AWS KMS? How do you integrate AWS KMS with your PKI and AWS cloud HSM? What types of encryption and keys are supported by AWS KMS? What services are integrated with AWS KMS? How can AWS KMS be integrated with cloud HSM for CMK generation? What are the pros and cons of integrating Cloud HSM with AWS KMS? What features are provided by the AWS Certificate Manager? Other services provided by AWS.

Standards and Compliances

What are different Regulations, Standards, and Compliance? What are the recommendations regarding PKI, encryption, key management, and more? We would also like to review the limitations of existing standards or suggestions for improvements.

Multi-Cloud Key Management

What is Multi-Cloud key management? What is the need for Multi-Cloud key management? What features are provided by Multi-Cloud key management? What are the benefits of Multi-cloud Key Management?

Zero Trust Security Model

On what basis does the Zero Trust Security model work? What are the requirements of the Zero Trust Model? What are some best practices for implementing the Zero Trust Security model? What problems are solved by the Zero Trust Security model? What are the limitations or challenges to the Zero Trust Security Model?

Data Loss Prevention

How to identify sensitive data and the risks of unauthorized data exfiltration? How to build a robust data loss prevention framework? How to prevent unauthorized data exfiltration in the cloud?

Code-Signing

What is code-signing? Importance of DevOps CI/CD integration. How do you use code-signing to secure the software supply chain? Use cases of code-signing. Compliances in code-signing, including CA/ Browser forum requirements.

Post-Quantum Cryptography

What is the NIST Post-Quantum Cryptography Standard? What are NIST-approved public-key encryption, key-establishment, and digital signatures algorithms? The need for post quantum assessment in your organization. Expert insights on building a roadmap and strategy for the quantum era. Evaluating the Post Quantum Cryptographic Solution Implementation and the need for PQC training in organizations. How do you build post-Quantum PKI and digital certificates? How to achieve quantum-ready security for future?

Certificate Lifecycle Management

Why is automation important in certificate lifecycle management? How are the growing number of certificates becoming a burden for organizations? Challenges in issuing certificates from different certification authorities, maintaining them, and being mindful of renewing them. Discovering certificates, vulnerabilities, and compliance issues on your organization's network and how to mitigate them. Best practices for CLM. Trends in certificate management. Staying compliant with standards regulations with a CLM solution. Bottlenecks in the automation of certificate management. Compliance with NIS2.

PKI IN PRACTICE

PKI for IoT Security

How can PKI secure IoT deployments? What are the best practices for implementing PKI to secure IoT deployments? What are the requirements for delivering IoT solutions that are both reliable and secure? Are the standards, such as NIST, ready for manufacturers to depend on?

Document Signing

How often is document signing implemented in organizations? Why is Document signing important?

Code Signing

How does PKI help in Code Signing? Why is Code Signing important? What are your experiences with code signing?

MULTI-CLOUD KEY MANAGEMENT IN PRACTICE

Bring Your Own Key (BYOK)

What is the need for BYOK? What are the advantages of BYOK? What are the disadvantages of BYOK? Is it a good practice to use BYOK? Different use cases of BYOK.

| FUTURE

Crypto Agility

What is Crypto Agility? Why is Crypto-Agility important? How can organizations achieve and maintain Crypto-Agility?

Homomorphic Encryption

What is Homomorphic Encryption? What is the need for Homomorphic Encryption? What are the applications of homomorphic encryption? Limitations and Drawbacks of Homomorphic Encryption.

Generative AI

How does GenAI works? What are the capabilities, risks, and limitations of GenAI? How GenAI fits with organization's cybersecurity models?

Artificial intelligence and super-encryption

How Artificial intelligence and enhanced encryption technologies can be used as primary defense mechanisms in cyber warfare?

Passwordless Authentication

What is passwordless authentication* What are the challenges in implementing passwordless authentication? How it can be used to improve security?



CONTACT ENCRYPTION CONSULTING

Please submit your interest on info@encryptionconsulting.com as soon as possible because the speaker schedule is filling up soon.

[Click here for registration](#)