Post-Quantum

Cryptography Conference

Opening

Paul van Brouwershaven
Chair PKI Consortium

Albert de Ruiter
Vice Chair PKI Consortium and Policy Authority PKI Dutch Government (Logius)

KEYFACTOR CRYPTO4A SSL.com ENTRUST HID

October 28 - 30, 2025 - Kuala Lumpur, Malaysia

PKI Consortium

PKI Consortium

Welcome

Post-Quantum Cryptography Conference

Connexion Conference & Event Centre

Paul van Brouwershaven

Chair, PKI Consortium
& the PQC Working Group

Owner of Digitorus

digitorus

PKI Consortium

CAB CA/BROWSER FORUM

ETSI

IETF

PKI Consortium

Albert de Ruiter

Vice chair, PKI Consortium

Policy Authority, Logius (Dutch Government)

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

PKI Consortium

QVC-NL

HAPK!DO

PKI Consortium

Quantum computers can solve <u>certain problems</u> all at once

PKI Consortium

Quantum Computing will support **revolutionary breakthroughs**

PKI Consortium

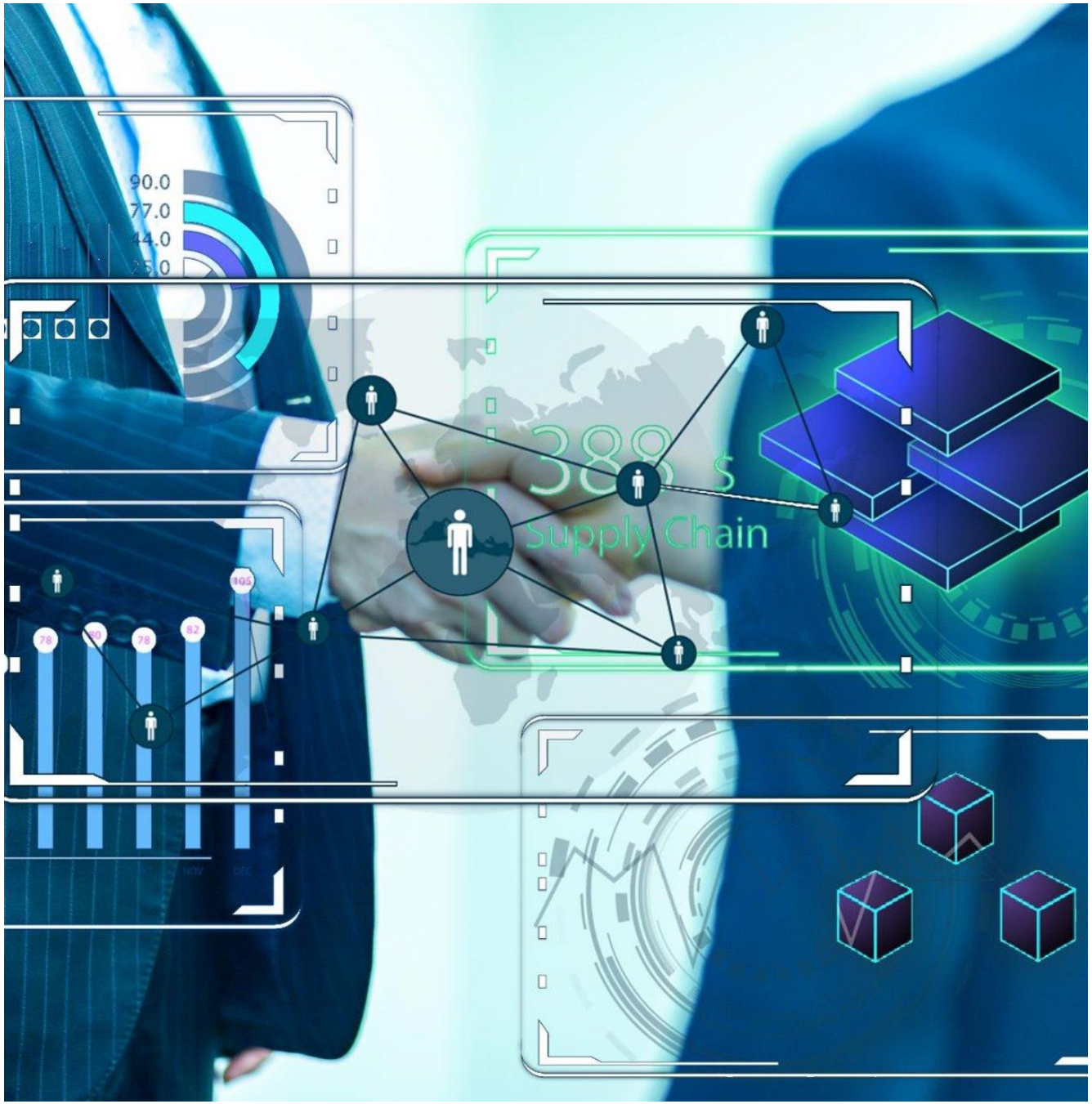
A game-changer for humanity

- **Cure Diseases Faster**
  - Discover life-saving drugs in months, not years.
  - Create medicine personalized for your unique DNA.
- **Solve the Climate Crisis**
  - Engineer super-efficient batteries for electric cars and power grids.
  - Design materials that capture carbon and generate clean energy better than ever before.
- **Unleash True AI**
  - Power machine learning to its ultimate potential, leading to revolutionary insights across science and industry.

PKI Consortium

Break the communication and encryption **we use today**

PKI Consortium



The time to act is NOW!

Prepare for large scale migration

PKI Consortium

Quantum Computers are already a Reality

They are just not yet powerful enough and there are still a lot of developments ongoing

- Quantum computers will be able to break **current** public key encryption; long term data needs to be protected now!
- It is important to view the migration as an **evolution of security**, rather than waiting for quantum computers to become a reality before doing anything
- Organizations should begin their **cryptographic inventory** and determine what data needs protection.
- **Technology is already available**, and organizations should start experimenting with it. It is important to start putting this technology in labs to learn.
- **Side-channel resistance** in PQC implementations remains a significant challenge.
- This crypto migration will be the hardest we've ever done!

PKI Consortium

Who is the PKI Consortium?

PKI
Consortium

PKI Consortium

Registered as a 501(c)(6) **non-profit entity** ("business league") under Utah law (10462204-0140)

- A diverse group of **300+ organizations** such as governments, auditors, consultants, trust service providers, software and hardware vendors
- We are a **non-profit entity**, we have no membership fees
- Our vision is "Trusted digital **assets** and **communication** for **everyone** and **everything**"
- We are committed to improve, create and **collaborate** on generic, industry or use-case specific policies, procedures, best practices, standards and tools that **advance trust** in assets and communication

PKI Consortium

INFOSEC GLOBAL
BANK OF AMERICA
d-trust.
Etugra
DB
SECTIGO
cleverbase
PKI partners
ANKA TECH
CHUNK WORKS
emudhra
gellum
HID
izenpe
Qrypt
KEYSIGHT
University of York
IBM
TRUSTGATE
digitorus
Aprio
cognizant
GlobalSign by GMO
tcs TATA CONSULTANCY SERVICES
SSL.com
firma.digital
vikingcloud
keytalk
codegic
PQSecure
CertiPath
ZoTrus
Capgemini
DIGITALTRUST
Quantum Bridge
utimaco
Camerfirma AN INFOCERT COMPANY
Ministry of Defence
EVERTRUST
THALES
firmaprofesional
nowquantum
QuSecure
BLOOMBASE
CRYPTO4A
DECENT CYBERSECURITY
TNO
I4P
ENCRYPTION CONSULTING
DavidGroup
TWCA 臺灣網路認證
Fidelity INTERNATIONAL
SEALWeb
VISA
TrustWrx
NGSIGN
ACCUTIVE SECURITY
TURKCELL
Landis+Gyr manage energy better
VIAVI Solutions
Digidentity
LEX persona
eval
QUANTINUUM
ANF AUTORIDAD DE CERTIFICACIÓN
SIBS Multicert
Yōkai
Easy - PKI Encryption, Certificates, PKI Simplified
acubed.it
DELL Technologies
Viasat
QTrin
PQC
Trust SEC
QUANTAG IT SOLUTIONS
NAVY FEDERAL CREDIT UNION
MAGICARD
NOREG
Data-Warehouse GmbH
Q→NU
versasec
SUNNIC
GSE GESTIÓN DE SEGURIDAD ELECTRÓNICA
M&T Bank
ALTRON SECURITY
EVIDEN
Information Security CORPORATION
TRUSTZONE
ENTRUST
bakertilly
digisign
B.EST SOLUTIONS
appviewx
smart.crypto
Fortanix
dátil
TD
CYBERARK THE IDENTITY SECURITY COMPANY
SafeCipher
nexus INGROUPE
CRYPTONEXT SECURITY
TÜV TRUST IT
FPKI Federal Public Key Infrastructure
AIRBUS
microsec
WISeKey
WELLS FARGO
HARICA
QRL
Uber
ascertia
Trans Speed TSP
citi
PKI SOLUTIONS
comsign
CREDIT SUISSE
CRYPTOMATHIC
Microsoft
buypass
POS Digicert
BOSCH
CALM
INDEED ID
KEYFACTOR
zeva
RELIEF VALIDATION
real random
DirectTrust
sefira
digicert
NIMBUS
BILGEM
cryptas
亞洲誠信 TRUSTASIA
Unsung All Things PKI Ltd.
Garantir
essendi it
CREAPLUS
KIR
SIXSCAPE
3KEYCOMPANY

PKI Consortium

What are we working on?

PKI Consortium

PKI Maturity Model

pkic.org/pkimm

Overview | Governance | Management | Operations | **Resources** | Report

PKI Consortium

Ensures that the activities related to the PKI are performed with a proper knowledge and experience, with enough capacities, and that it provides complete and accurate information to relying parties

R.10 Sourcing

PKI is a complex system that requires a lot of resources to be managed and maintained. Proper sourcing of the resources is one of the key factors of a mature infrastructure that can maintain and improve trust over the time. The resources can be:

- Financial resources needed to maintain the PKI
- Computing resources like hardware, software, tools, technologies
- Human resources (personnel)
- Management resources like processes and procedures

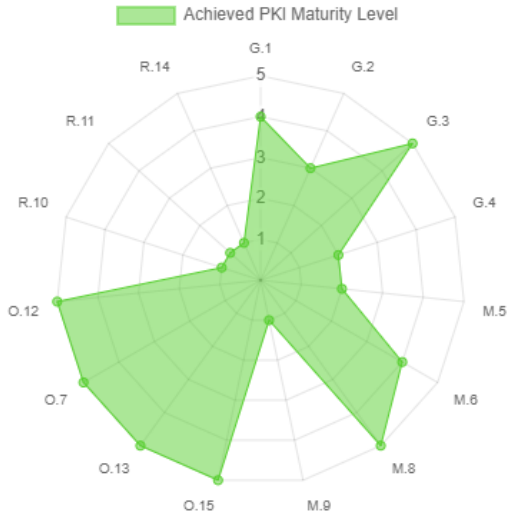
Sourcing is a process of defining the required resources and their specification, availability, and management. Sourcing requires monitoring and periodic review of the resources needed and alignment with the overall strategy of the organization and scope of the PKI.

1 - Initial:
The resources needed for the PKI are not defined and documented. There is a risk of unavailable resources causing the PKI to be unavailable.

2 - Basic:
Resource are identified and documented. The resources and their specification are not clearly defined, which can lead to misuse of resources.

Version: 1.0.2

3 - Advanced



This radar chart represents the maturity level of categories. The data is derived from user inputs and reflects the current status of the development.

Governance	3 - Advanced
Management	2 - Basic
Operations	5 - Optimized
Resources	1 - Initial

PKI Consortium

PKI Maturity Model

- Maturity models assess organizational capabilities and readiness.
- They provide a structured framework for continuous improvement.
- Help identify gaps in processes and technologies.
- Support strategic planning and resource allocation.
- Enable benchmarking against industry standards.

PKI Consortium

PQC Maturity Model

- Not for the **PQC Maturity** of your organization, but the maturity of a **product** or **service**.
- Intended to support your PQC readiness assessments from the perspective of **procurement** and **supply chain**.

Training & Certification

for Public Key Infrastructures

PKI Consortium

PQC Capabilities Matrix (PQCCM)

pkic.org/pqccm

Vendor	Product	Category	Last updated	Composite certificates	Hybrid certificates	LMS	XMSS	Falcon	Dilithium	SPHINCS+	Kyber	BIKE	McEliece	HQC
Ascertia	ADSS Server	PKI	2024-09-03	✗	✗	✗	✗	✗	✓	✗	✓	✗	⏲	✗
Botan	Botan	Software library	2023-10-04	✗	✗	⏲	✓	✗	✓	✓	✓	✗	⏲	✗
Bouncy Castle	BC	Software library	2022-11-22	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Crypto4A	QxEDGE	HSP	2022-12-04	⏲	✓	✓	✓	⏲	✓	✓	✓	✗	✓	✗
Crypto4A	QxHSM	HSM	2022-12-04	⏲	✓	✓	✓	⏲	✓	✓	✓	✗	✓	✗
CZERTAINLY	CZERTAINLY	Software	2023-02-19	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Entrust	nShield	HSM	2022-11-22	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Entrust	PKIaaS	PKI	2022-11-22	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
EVERTRUST	STREAM/HORIZON	PKI	2024-12-10	✗	✓	✗	✗	⏲	✓	⏲	✗	✗	✗	✗
Eviden	Trustway Proteccio™ NetHSM	HSM	2024-12-09	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗
Fortanix	FX2200	HSM	2024-06-21	✗	✗	✓	⏲	⏲	✓	⏲	✓	✗	✗	✗
I4P	Trident	HSM	2022-12-01	✗	✗	✗	⏲	✗	✗	✓	✓	✗	✗	✗
IBM	4769/CCA	HSM	2023-01-11	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
IBM	Crypto Express 7S (CEX7S) / CCA/EP11	HSM	2023-01-22	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
IBM	Crypto Express 8S (CEX8S) / CCA/EP11	HSM	2023-01-22	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗
InfoSec Global	AgileSec Analytics	Software	2024-04-24	✗	✗	✓	✓	⏲	✓	✓	✓	⏲	⏲	⏲
Infrasoft Pty Ltd	uLinga Suite	Software	2024-05-24	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗
ISC	CDK	Software library	2023-03-04	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✗
ISC	CertAgent	PKI	2023-03-04	✗	✗	⏲	✗	✓	✓	✓	✓	✗	✓	✗

And more…

- **Post-Quantum Cryptography**
  - PQC Maturity Model
  - PQC Capability Matrix
  - PQC Conference
- **PKI Maturity Model**
  - Incorporating feedback
- **PKI Training & Certification**
  - Chapter one open for public feedback
- **Cryptographic Module**
  - Remote Key Attestation
  - Vendor-Independent Key Backup

What is on the agenda?

https://pkic.org/pqcc

PKI Consortium

Yesterday, we had Workshops and Roundtables

Tuesday | Wednesday | Thursday | Speakers

All Locations | Room 1 | Room 2 | Room 3 | Room 4 | Room 5 | Room 6 | Room 7 | Room 8

8:30 01:30 CET — **Registration**

9:00 02:00 CET

Advancing CBOM: Hands-On with CycloneDX v1.7 and PKI Extensions

Michael Osborne
CTO IBM Quantum Safe at IBM Research

The Linux Foundation CBOM with CycloneDX

The CBOM workshop will help participants understand and become familiar with the upcoming extensions to the CycloneDX CBOM standard v1.7. In particular new extensions targeted at reporting PKI certificates. We are actively talking to industry vendors who have expressed interest in collaborating on this workshop.

We will explore:

Securing the Healthcare Sector in the Quantum Era: a PQC Readiness Roundtable

Scott Rea
Emeritus Board Member at DirectTrust and Global Strategic Advisor at eMudhra

This session is held under Chatham House Rules.

Draft Agenda

Welcome (20 min)

- Setting the stage: Why PQC matters for healthcare
- Objectives of the discussion

Enabling Quantum-Safe, Crypto-Agile Security with Crypto4A's QxHSM™: Business & Technical Insights

Bruno Couillard
Co-Founder & CEO at Crypto4A

Olivier Couillard
Technical Product Manager at Crypto4A Technologies, Inc.

As quantum computing threatens modern cryptography, organizations must prepare their infrastructure for a post-quantum world. Hardware security modules (HSMs) — key to digital trust — must evolve. This workshop covers the strategic and technical foundations of

Securing the future Internet of Things with ML-KEM and ML-DSA

Kevin Hilscher
Sr. Director, Product Management at DigiCert

Today's Internet of Things (IoT) relies on a variety of protocols and communications technologies… CoAP, LwM2M, LoRaWAN, NB-IoT, Wi-Fi, Thread … many of which are not quantum-safe.

While large-scale quantum computers capable of breaking current encryption aren't yet available, the concept of ""harvest now, decrypt later"" is a significant concern. Now that NIST has released final versions of its first three Post-Quantum Cryptography (PQC) standards the race is on to make IoT quantum-safe.

Create your own quantum-safe signed PDF documents with hybrid cryptography

Alessandro Amadori
Cryptographer at TNO

Sven Konings
Software Developer at ZYNYO

Stefan van den Berg
Researcher Cryptography and Cyber Security at TNO

This workshop is from a collaborative effort between TNO and Zynyo. Standards are now established and libraries are being released, the integration of Post-Quantum Cryptography into products is increasing. However, the adoption of

A Practical Guide to PQC Migration: Securing Digital Identities for the Quantum Era

Steven Gan
General Manager at Blue Fortress

Maeson Maherry
Chief Operating Officer at Ascertia

Wilson Yan
Channel Solution Engineer Lead at CyberArk APJ

Ivan Tan
Principal Presales Consultant at Thales

Module 1: Verifiable everything - Trust solutions built on trustworthy crypto

Government & Regulatory Approaches to PQC: From Policy to Implementation

Zygmunt Lozinski
Senior Technical Staff Member and Quantum Ambassador at IBM Research

This session is held under Chatham House Rules.

Draft Agenda

Welcome (20 min)

- What problem are we solving? Why PQC policy and regulation matter now
- Objectives and expected outcomes (cross-sector takeaways, commitments)

Hands-On Cryptograp PQC Crypt

Tomas Chief Pk

Chris H Chief Se

Tony C Solution

With NIST setti deprecation of safe algorithm need to assess landscape. Thi to and speaking

11:00 04:00 CET — **Break**

11:30 04:30 CET

Continuation of the morning workshop

The morning workshop continues until lunch.

Continuation of the morning workshop

The morning workshop continues until lunch.

Continuation of the morning workshop

The morning workshop continues until lunch.

Continuation of the morning workshop

The morning workshop continues until lunch.

Continuation of the morning workshop

The morning workshop continues until lunch.

Continuation of the morning workshop

The morning workshop continues until lunch.

Continuati workshop

The morning w

13:00 06:00 CET — **Lunch**

14:00 07:00 CET

PKI and Crypto Agility: Know Your Infrastructure

Alexander Löw
CEO at Data-Warehouse

Building and Monitoring Your Cryptographic Inventory with PCert

This workshop offers a deep dive into cryptographic discovery and inventory practices essential for organizations aiming to establish robust CBOM (Cryptographic Bill of Materials) and SBOM (Software Bill of Materials). Participants will learn how to identify and catalog all cryptographic assets across complex

Securing the Telecommunication Sector in the Quantum Era: a PQC Readiness Roundtable

Lory Thorpe
Quantum Safe Industry Lead at IBM

Luke Ibbetson
Group Research and Development Director at Vodafone Group

This session is held under Chatham House Rules.

Welcome (20 min)

- Frame the discussion (Aligning standards, strategy, and compliance)

Enabling Quantum-Safe, Crypto-Agile Security with Crypto4A's QxHSM™: Business & Technical Insights

Bruno Couillard
Co-Founder & CEO at Crypto4A

Olivier Couillard
Technical Product Manager at Crypto4A Technologies, Inc.

As quantum computing threatens modern cryptography, organizations must prepare their infrastructure for a post-quantum world. Hardware security modules (HSMs) — key to

Crypto-Agile PKI in the Quantum Era: Building Trust with Utimaco's Quantum Protect

Nils Gerhardt
Chief Technology Officer at Utimaco

Lai Seow Yong
Technical Head, Asia Pacific at Utimaco

As organizations worldwide prepare for the quantum threat anticipated by 2030, the resilience of Public Key Infrastructure (PKI) will depend on a critical capability: crypto agility. This workshop presents Utimaco's comprehensive strategy for quantum-safe PKI deployment, anchored around

Implementing Post-Quantum Cryptography with HSMs: Show & Tell

Shaun Chen
VP APJ Strategic Account Sales Engineering at Thales

Chris Hickman
Chief Security Officer at Keyfactor

Implementing post-quantum cryptography shouldn't feel like a leap into the unknown. In this workshop, you'll see how Luna HSM enables a smooth transition to PQC through hands-on exercises and real-world scenarios. Together, we'll

Building Quantum-Safe Trust: A Hands-On Workshop with Entrust

Giuseppe Damiano
Vice President of Product Management for the HSM product offering at Entrust

Matt Rose
Manager Sales Engineer North America at Entrust

Moving to post-quantum cryptography isn't just about swapping algorithms - it's about evolving the entire trust infrastructure. In this interactive workshop, you'll learn how to build a quantum-ready environment from the ground up using Entrust's PQ Secure Solutions. From Strategy

Securing the Financial Sector in the Quantum Era: a PQC Readiness Roundtable

Jaime Gómez García
Global Head of the Santander Quantum Threat Program, Chair of the Europol Quantum Safe Financial Forum

Sudha Iyer
Chief/Principal Engineer-PKI & Cryptography at Citi

Sarah McCarthy
Quantum Readiness Program Lead at Citi

This session is held under Chatham House Rules.

A Deep Div EJBCA, an

Tomas Chief Pk

Tony C Solution

David H VP Soft

Sven R Internati

The world of cr with the adven (PQC). This is

Today, we have Strategic and Technical track

For the complete agenda got to: https://pkic.org/pqccc

Tuesday | **Wednesday** | Thursday | Speakers

All Locations | Plenary | Breakout

8:30 01:30 CET — **Registration**

9:00 02:00 CET

Opening

Paul van Brouwershaven
Chair PKI Consortium

Albert de Ruiter
Vice Chair PKI Consortium and Policy Authority PKI Dutch Government (Logius)

9:30 02:30 CET

Malaysia's PQC Vision for the Region

Tuan Fabian Bigar
Secretary General of the Ministry of Digital, Malaysia

Digital trust is the foundation of modern economies and societies, and the arrival of quantum computing will test how ready we are to safeguard it. Post-quantum cryptography (PQC) is more than a technical response, it is a catalyst for rethinking how nations, industries, and communities build resilience and foster innovation in a rapidly changing world. In his opening keynote, Tuan Fabian Bigar, Secretary General of the Ministry of Digital, Malaysia, will welcome participants to the PKI Consortium's PQC Conference in Kuala Lumpur and share Malaysia's broader vision for a secure, inclusive, and sustainable digital future.

He will highlight the role of digital trust as a driver of economic growth, the importance of regional leadership within ASEAN to advance quantum readiness, and the need for global cooperation to ensure that no nation is left behind in this transition. By framing PQC as a shared opportunity rather than just a challenge, his address will set the stage for the conference, inviting all participants, governments, industry, academia, and civil society, to engage in shaping a quantum-secure world.

10:00 03:00 CET

Navigating National Cyber Resilience in the Quantum Era

Megat Zuhairy Bin Megat Tajuddin
Chief Executive at National Cyber Security Agency (NACSA), Malaysia

As the quantum computing horizon draws nearer, the imperative to secure national critical information infrastructure (NCII) against quantum threats becomes a matter of strategic urgency. In this keynote, Ir. Dr. Megat Zuhairy Bin Megat Tajuddin, Chief Executive of Malaysia's National Cyber Security Agency (NACSA), will explore the evolving landscape of Post-Quantum Cryptography (PQC) through the lens of national security, policy, and technological leadership.

Drawing from over two decades of experience in ICT, telecommunications, and strategic innovation, including pioneering work in large-scale digital transformation projects and international policy development. Dr. Megat will outline Malaysia's roadmap for quantum resilience. His address will highlight:

- National strategies for PQC adoption across critical infrastructure and government systems.
- Public-private collaboration models to accelerate cryptographic agility and secure transitions.
- Regulatory and compliance frameworks aligned with global standards and regional priorities.
- The role of ASEAN leadership in shaping the future of quantum-safe digital ecosystems.

This keynote will frame Malaysia's strategic approach to PQC not only as a national imperative but also as a collaborative opportunity, bridging policy, standards, and implementation. Dr. Megat will

10:30 03:30 CET — **Break** | Unsung All Things PKI Ltd. | **Break**

11:00 04:00 CET

PQC Across Verticals: What We've Learned, Where We're Headed

Paul van Brouwershaven Moderator
Chair PKI Consortium

Jaime Gómez García
Global Head of the Santander Quantum Threat Program, Chair of the Europol Quantum Safe Financial Forum

Performance Metric Evaluation of MLWE in Web and other TLS Use-cases

Mila Anastasova
Applied Scientist at Amazon Web Services (AWS)

The cryptographic community is actively debating the shift to Post-Quantum PKI as quantum computing progresses and NIST advances standardization. While larger certificate sizes (15–22KB extra) raise

:ium

Tomorrow, we continue with more sessions

For the complete agenda got to: https://pkic.org/pqccc

Tuesday | Wednesday | **Thursday** | Speakers

All Locations | Plenary | Breakout

8:30 01:30 CET — **Registration**

9:00 02:00 CET

PQC Integration in HSMs: From Standards to Strategy

- **Bruno Couillard** — Co-Founder & CEO at Crypto4A
- **Giuseppe Damiano** — Vice President of Product Management for the HSM product offering at Entrust
- **Blair Canavan** — Director, Alliances at Thales
- **Nils Gerhardt** — Chief Technology Officer at Utimaco
- **Zsolt Rózsahegyi** — CEO at i4p informatics
- **John Buselli** Moderator — Offering Manager at IBM Quantum

With the release of NIST's first set of post-quantum cryptographic standards, the conversation around quantum readiness has moved from research into execution. For organizations relying on hardware-

Advancing Cryptographic Transparency: CBOM Standardization in CycloneDX

Basil Hess — Senior Research Engineer at IBM Research

As quantum-safe migration and supply chain security become critical priorities, the Cryptography Bill of Materials (CBOM) is emerging as a foundational concept and standard for cryptographic visibility and assurance. This session explores the standardization of CBOM within OWASP's CycloneDX 1.6, highlighting its role in cataloging cryptographic assets and their dependencies, including PQC primitives and hybrids. It will also preview upcoming enhancements in CycloneDX 1.7, including standardized algorithm naming and improved interoperability for certificates and keys, both essential for quantum readiness and cryptographic agility. The talk will show how CBOM integrates into the broader xBOM ecosystem - spanning Software, Hardware, SaaS, AI, and Operations - to support unified cryptographic governance across complex environments.

9:30 02:30 CET

Continuation: PQC Integration in HSMs: From Standards to Strategy

This session continues the panel discussion on PQC integration in HSMs, focusing on the evolving landscape from standardization efforts to real-world deployment strategies.

Transitioning to Post-Quantum Cryptography in IAM

Udara Pathum — Senior Software Engineer at WSO2

The quantum threat demands urgent upgrades to IAM systems, spanning TLS, PKI (encryption and digital signatures), and SSO protocols like SAML and OIDC. This session outlines practical strategies for transitioning to post-quantum cryptography, emphasizing post-quantum TLS (e.g., ML-KEM) and quantum-safe PKI. We highlight hybrid encryption and hybrid digital signatures to enable smooth migration with backward compatibility. Additionally, we provide actionable post-quantum recommendations for organizations to ensure crypto agility and resilience in identity management.

10:00 03:00 CET

Cryptographic Discovery and Inventory: The Hidden Foundation for Enterprise Security

Alexander Löw — CEO at Data-Warehouse

Most enterprises are preparing for tighter regulations, certificate renewal challenges, and post-quantum threats — yet few have a complete picture of their cryptographic landscape. Without visibility, automation and resilience remain out of reach.

This session will reveal how organizations can build a robust cryptographic inventory and discovery process, comparing three leading approaches: targeted scanning of cryptographic material, leveraging existing databases, and full enterprise assessments. We'll map these strategies to US-NIST and CISA use cases, explore their advantages and limitations, and show how they form the foundation for PKI automation and post-quantum readiness.

Attendees will leave with actionable steps to uncover, document, and manage cryptographic assets, tackle the 47-day certificate renewal challenge, and build a scalable, future-ready security posture.

PQC Formal Verification: Challenges and Tools for Formal Verification of Post-Quantum Cryptography

Reza Azarderakhsh — CTO at PQSecure and FAU

As post-quantum cryptography advances toward deployment, formal verification becomes essential for ensuring trust in both hardware and software implementations. Each PQC algorithm—such as ML-KEM, ML-DSA, and SLH-DSA—presents unique challenges, and while tools like Cryptol, SAW, and Coq offer valuable support, no single framework offers a complete solution. In this talk, we introduce an effort focused on practical formal assurance for PQC. We will demonstrate how Cryptol and SAW can verify key properties of ML-KEM and ML-DSA components. We also highlight the growing role of Rust in cryptographic implementations and discuss the importance of verifying PQC libraries in memory-safe languages. Our goal is to promote scalable, implementation-aware formal methods to ensure secure and verifiable PQC adoption.

10:30 03:30 CET — **Break**

11:00 04:00 CET

The ABCs (Accelerated, Better and Cheaper) to Cryptographic Resilience

Sudha Iyer — Chief/Principal Engineer-PKI & Cryptography at Citi

The session covers practical priorities in the quantum readiness Journey for financial industry. This session provides a focused update for C-level leaders on the financial sector's preparedness for post-quantum cryptography. It covers recent developments across NIST, IETF, PCI DSS, and other regulatory bodies, highlighting their impact on existing architectures and risk postures. We will examine sector-specific challenges, current sandbox and testing efforts, and practical collaboration options available to institutions. The session concludes with a tactical roadmap that CISOs and senior executives can

Hybrid Quantum-Safe Cryptography for Electric Vehicle Charging Infrastructure

Alessandro Amadori — Cryptographer at TNO

Europe is advancing in EV adoption to combat climate change and support renewable energy. This shift requires redesigning the energy infrastructure for charging demands. The DITM project aims to create a digital infrastructure for automated transport, enhancing safety, efficiency, and sustainability. The EnergyPod, part of DITM, optimizes EV charging and manages grid interaction. To secure against future quantum threats, TNO, NXP, and Infiniot upgraded OCPP with hybrid quantum-safe cryptography (TLS handshake and X.509 certificates). This protocol was tested on the NXP "i.MX 8" board, similar

:ium

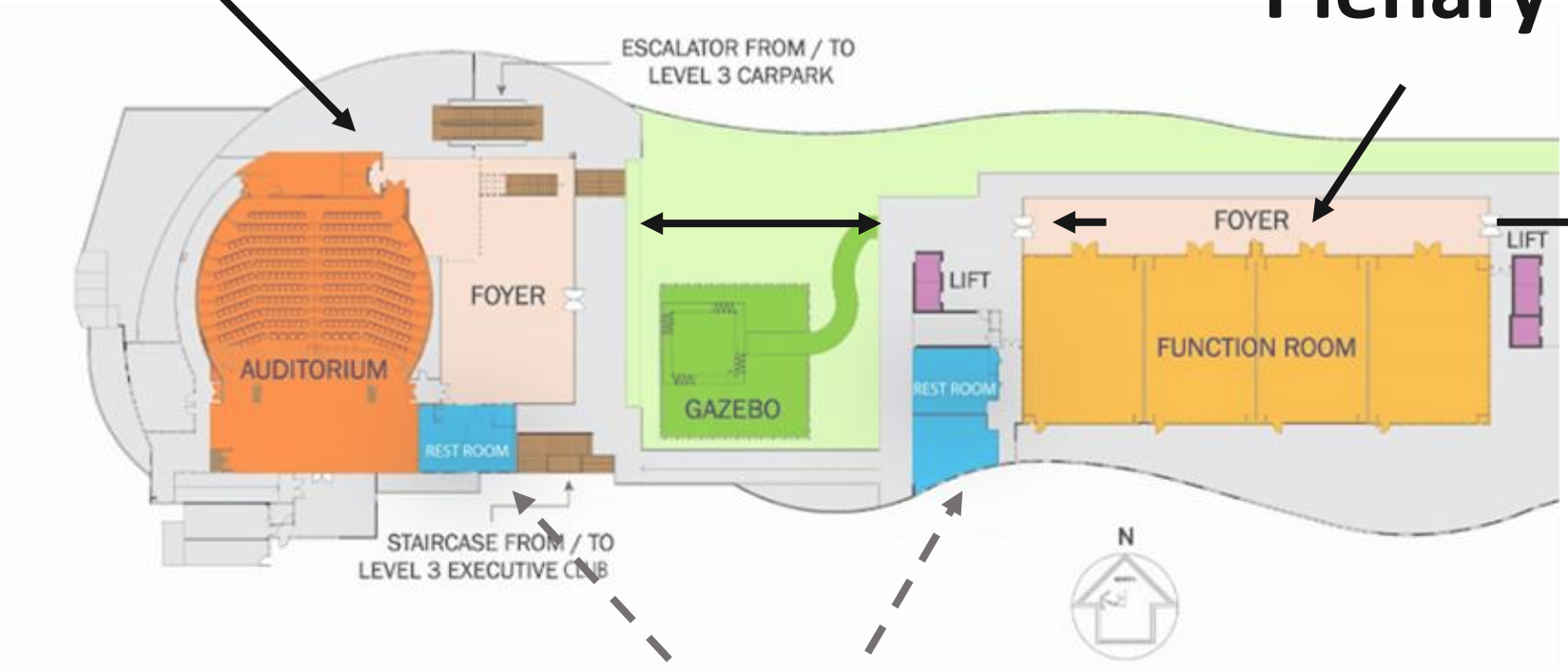
Housekeeping

PKI Consortium

Breakout

Plenary

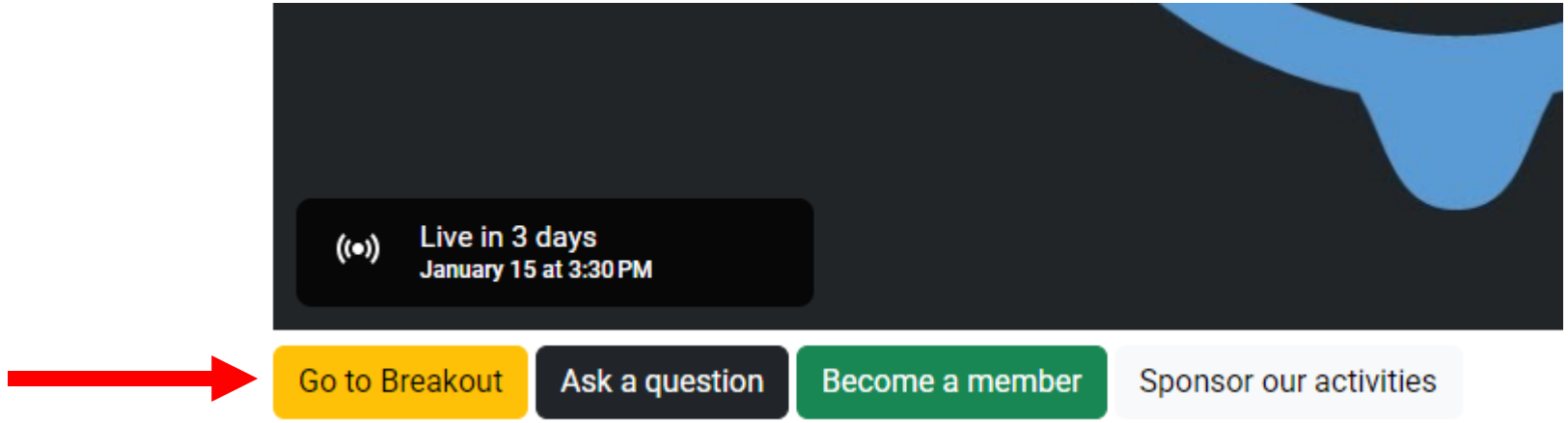
Lunch

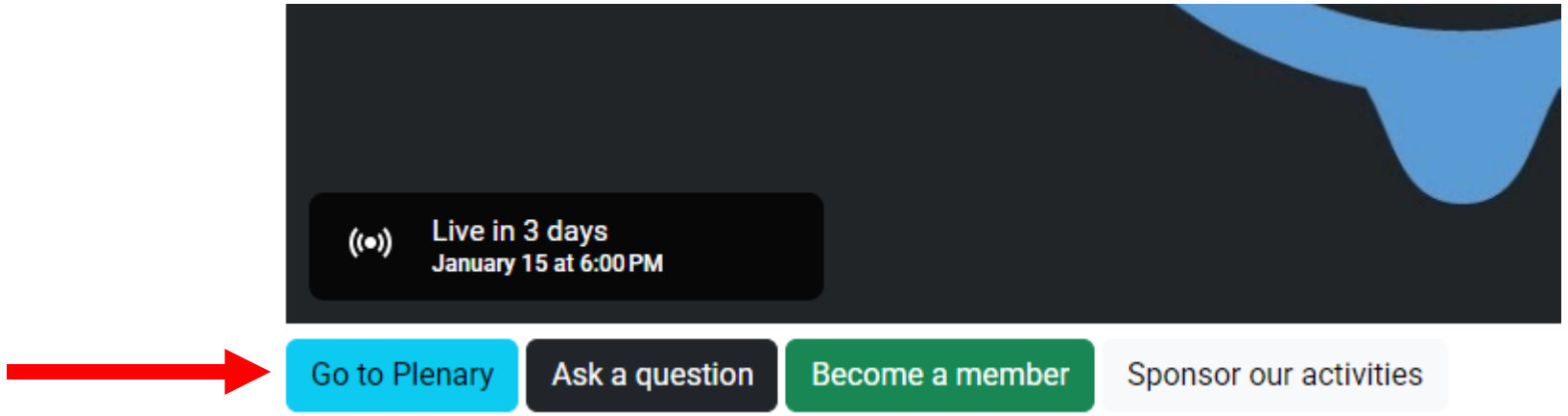


Restrooms

PKI Consortium

Switch between **Plenary** and **Breakout**

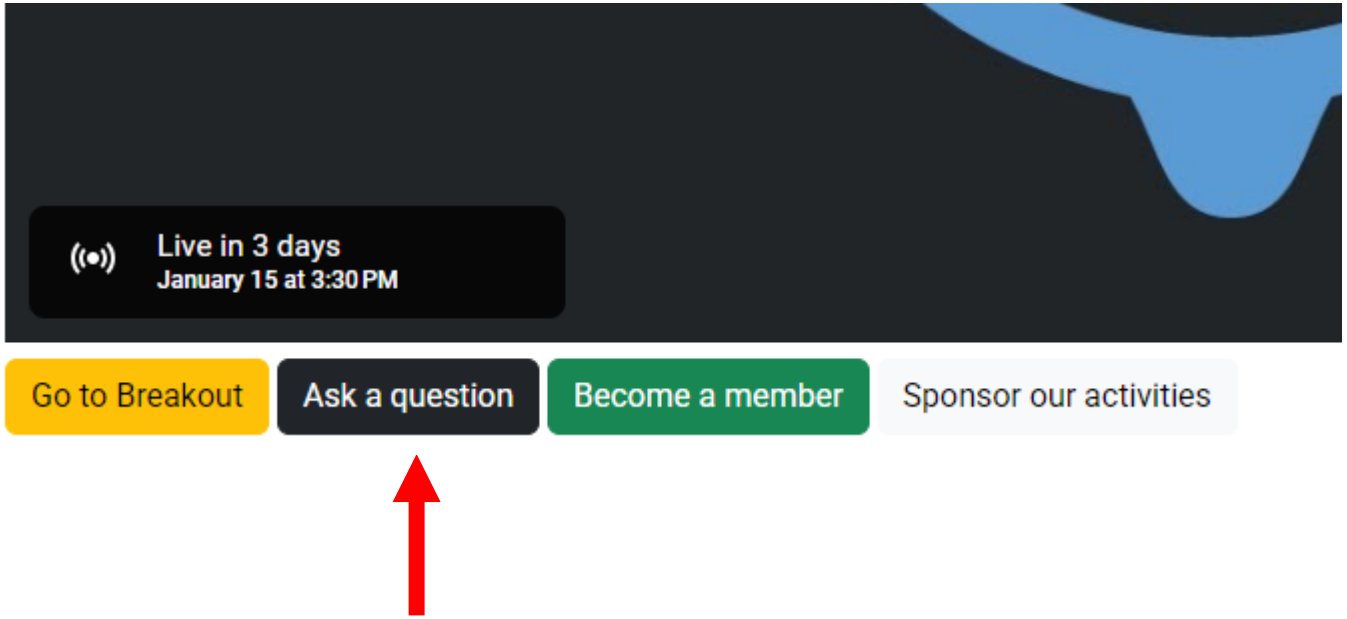




PKI Consortium

Questions

pkic.org/ask



PKI Consortium

Thanks to the **key contributors** of this conference

PKI Consortium

PKI Consortium

SSL.com

KEYFACTOR

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

POS Digicert

bakertilly

TRUSTGATE

digitorus

- Adib
- Aina Hafieza Binti Fauzahar
- **Albert de Ruiter**
- Amir Suhaimi Hassan
- Aniza Binti Roslan
- Anuarul Datoabhalim
- Anuarul Halim
- Blair Canavan
- **Chris Bailey**
- Chris Hickman
- Effy Shafinaz Binti Zainodin
- Ezfar Afham Bin Azni
- Ganesh Mallaya
- Harald Kaiblinger
- Hazhar Ismail
- HuckHai Lim
- Iylia Afiqah Binti. Ismail
- John Buselli
- Jonathan Jackson
- **Leigh Bailey**
- Lois Teh
- Marcus Teh
- Mohd Afiq bin Mohd Izham
- Mohd Hafiz Bin Bahrin
- Muhammad Ikhwan Roslan
- Muhammad Rusydi Bin Adnan
- Muhammad Zahier Bin Idris
- Muhammad Zulfadhli bin Ibrahim
- Nazril Mohd Ghani
- Noor Afiqa Farhah binti Mohd Faris
- Nor Aziana binti Mohamad
- Nor Hakimie Bin Sabri
- Nor Idayu binti Abd Rahim
- Noraishah Bt Yahaya
- Norhashima Binti Bashah
- Norsolehah Binti Mohamad Hashim
- Nur Majdina Binti Mohd Nizam
- Nurul Syakirah binti Ismail
- Nurzilah Farhana
- **Paul van Brouwershaven**
- Razzuwan Bin Mat Razali
- Rohaizan Mohammad Aseri B. Md. Said
- Rohani Binti Ismail
- Samantha Mabey
- Scott Rea
- Shahira Zulaikha Binti Mohd Sharif
- Sharifuzan Noh
- Siti Sarah Binti Ishak
- **Sven Rajala**
- Thanen Thiran
- Tony Chen

PKI Consortium

This event would not have been possible without our **sponsors**

PKI Consortium

Titanium

CRYPTO4A

KEYFACTOR

Leader

SSL.com

Platinum

ENTRUST

HID

Gold

Data-Warehouse GmbH

THALES

Inspirator

POS Digicert

Innovator

PQ SHIELD

Silver

ANKA TECH

appviewx

digicert

NOREG

SECTIGO

亞洲誠信 TRUSTASIA

Ambassador

Unsung

PKI Consortium

Speakers are **not permitted** to promote products or services during their presentations

A few sponsor Pitches

PKI Consortium

The Answer

A quantum-ready platform to manage digital trust at scale

Visibility Discover, inventory, and assess cryptographic assets that underpin your infrastructure.

Trust Issue trusted non-human identities for devices, workloads, and code.

Lifecycle Automate the lifecycle of keys and digital certificates across hybrid and multi-cloud.

Find and inventory all cryptographic assets

Identify, prioritize, and remediate vulnerabilities

Issue identities to devices, workloads, and code

Sign code and software to ensure trust and integrity

Manage the lifecycle of keys and certificates

Automate rotation and provisioning at scale

Cryptographic Discovery & Inventory

Private PKI, Signing Solutions, & Cryptography

Certificate Lifecycle Automation

CipherInsights from Keyfactor

INFOSEC GLOBAL a Keyfactor company

Keyfactor EJBCA

Keyfactor SignServer

Bouncy Castle with Keyfactor

Keyfactor Command

KEYFACTOR

CRYPTO4A | Securing the World’s Digital Future

Quantum-Safe Hardware Security Modules (QxHSM™)

Future-proof cryptography designed for post-quantum resilience.

Secrets. Simplified. (QxVault™)

Fully integrated secrets management vault with built-in HSM.

Proven Innovation, Global Recognition

Titanium Sponsor • Recognized in 11 Gartner® Hype Cycles • Trusted by governments & enterprises.

Delivering innovative, quantum-safe hardware security solutions with uncompromising integrity.

Quantum Safe. Crypto-Agile. Designed, engineered and manufactured in Canada.

PKI Consortium

SSL

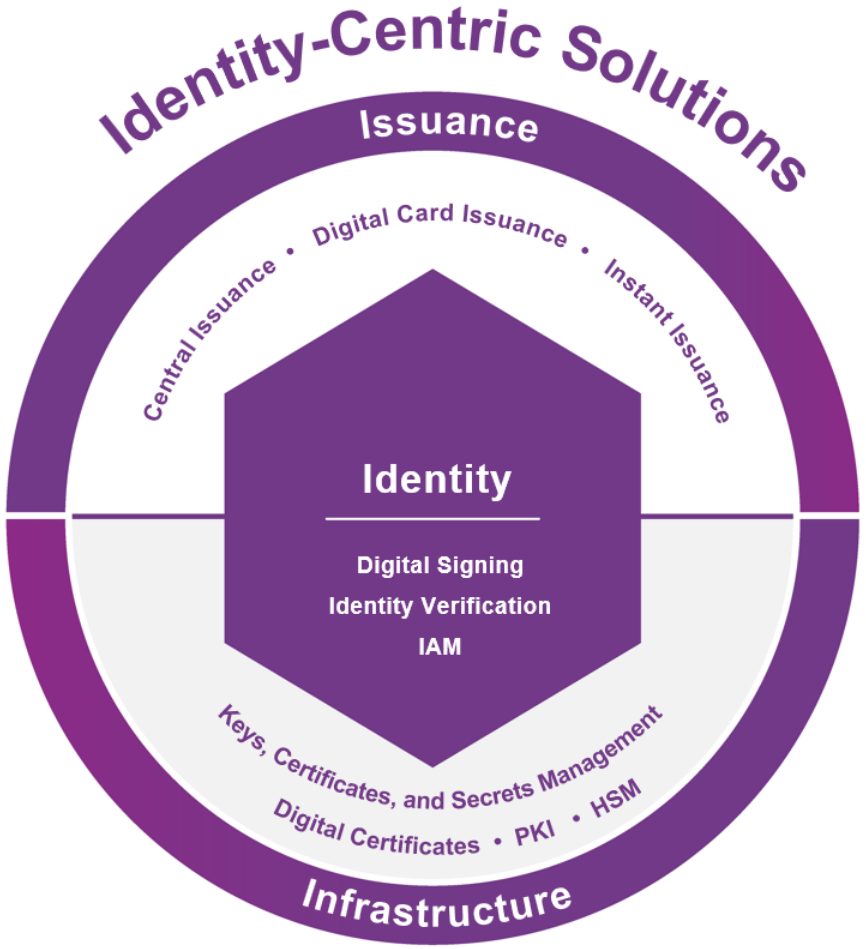
Powering Trust in Business

ENTRUST

SECURING A WORLD IN MOTION

Identity-Centric Solutions Powered by AI

Founding member of the PKI Consortium



$1B+ in revenue	**3,400+** colleagues	**50+** years of innovation
2k+ partners	**150+** countries served	**65%** Fortune 500 served

On-prem PKI
mPKI
PKIaaS PQ Ready

CCoE
PQC Readiness assessment
PQ Lab

nShield HSM
PQ SDK

HID PKI-as-a-Service Overview

Dedicated Issuing CA Service

- ✓ Provides a branded trust anchor at the issuing CA level.
- ✓ Works well for organizations that don't need their own fully off-line root CA.

Private Root PKI Service

- ✓ Provides full turnkey service including private root key gen ceremony and management of all off-line key material and online issuing CA's.
- ✓ Perfect for large organizations with unique trust models and PKI hierarches.

Trusted TLS/SSL Service

- ✓ Subscription-based SSL means no per-certificate or certificate-type pricing– one fixed fee.
- ✓ You can get all the certs you need, on-demand for one fixed subscription fee.
- ✓ Third-party certificate authority integration

HID PKIaaS

Automation Protocols

ACME
SCEP
EST
REST API

Full Certificate Lifecycle Management

Centralize Management
Certificate Discovery
Reporting & Alerting
Approval Workflow
Delegated Administration

Automation Integrations

Webservers & Network Devices
Mobile Device Management
Key Vaults
DevOps Tools
Crypto Agility Public CA

Data Warehouse GmbH

Our portfolio		Our products Made in Germany	Our customers
Software development	•Cybersecurity •Individual & SME multiple branch and production solutions •Networking implementation and Communication solutions •Low Code Universal Software development platform (EBUS –J) •Consulting, Support, GDPR Consulting (GDPR) •Project management	Ebus-J	DER PARITÄTISCHE BAYERN, Bäreurserei Ilicke Zuckerwatt, Audi, SIEMENS, handicap international humanité & inclusion, KINDER SCHUTZ MÜNCHEN
+ Information management	•Enterprise Solutions, Data Center solutions •Central information mangement systems, Logistics optimisation, PLM/PDM, Supply chain optimisation •Distributed database systems •Social collaboration, messaging (tixxle) •Master data management & logistics (IQIMS) •(High) secure software development •Mobile, Cloud and web solutions	IQIMS SPOT Platform Interface Plan Act IQ IMS Do Check	Deutsche Post, Bundeswehr, AIRBUS DEFENCE & SPACE, Eurofighter Typhoon, O2, DEUTSCHE BÖRSE GROUP, BUNDESHEER, ESG, EnBW, DB BAHN
+ (IT & ID) Security	•Implementation strategy of complex products •I(T-)Security concepts for high secure areas •Cyber security strategies, security research •Development of national standards •Online trainings, awareness, pentesting •Implementation of (national) CA and PKI •Identity Management und Privileged Identities •P-Cert		BMW, Eurofighter Typhoon, BNotK BUNDESNOTARKAMMER, secunet, TMS, AIRBUS DEFENCE & SPACE, EVG, HUK-COBURG

ISO 9001 | ISO 27001 | Aero Excellence Certified

PKI Consortium

THALES
Building a future we can all trust

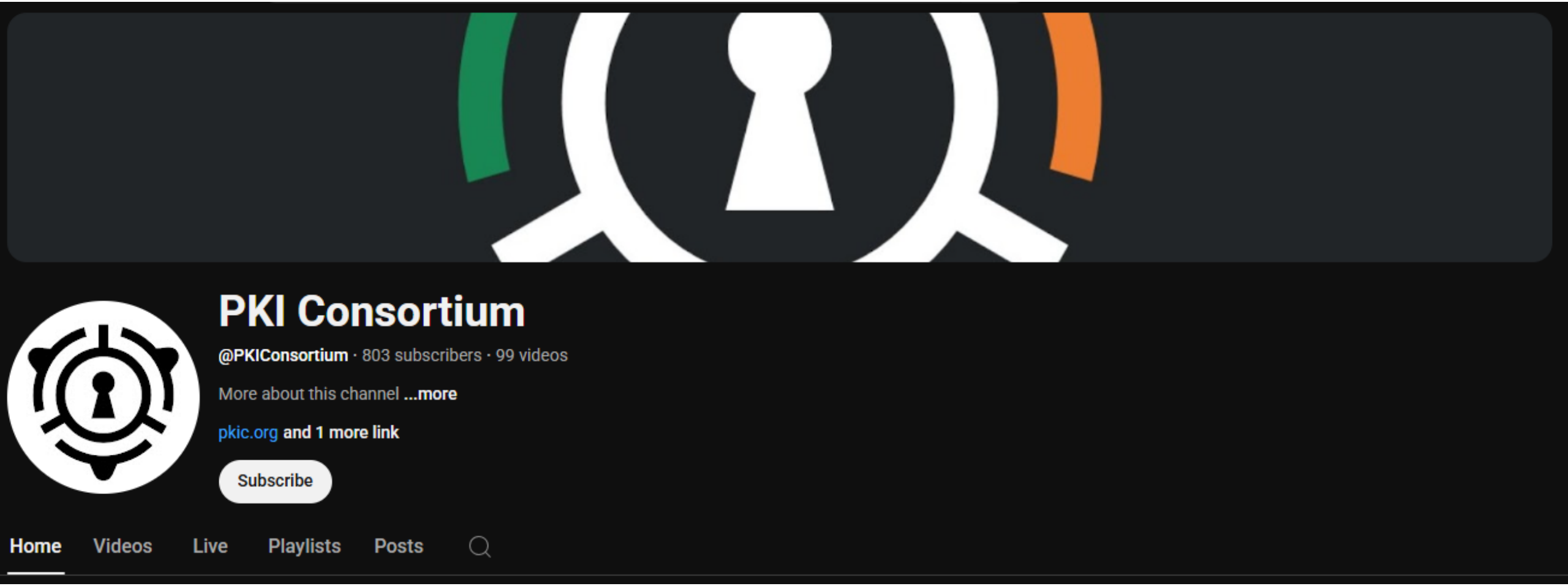
Security for What Matters Most

Applications | Data | Identities

cpl.thalesgroup.com

Subscribe to our YouTube channel for the recordings

https://youtube.com/@PKIConsortium



Join the PKI Consortium

pkic.org/join

pkic.org/join

PKI Consortium

Enjoy your day!

PKI Consortium