Post-Quantum

Cryptography Conference

Opening

Paul van Brouwershaven
Chair PKI Consortium

Albert de Ruiter
Logius

Post-Quantum Cryptography Conference

Paul van Brouwershaven

- Chair PKI Consortium
- Director Technology Compliance at Entrust
- Vice-chair CA/Browser Forum

Albert de Ruiter

- Policy Authority PKI Dutch Government (Logius)
- Board member HAPKIDO
- Member of the QVC WG Dutch Government

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 **110+ members** 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

CRYPTO4A
I4P
utimaco
ENCRYPTION CONSULTING
CREAPLUS
codegic
DirectTrust
sefira
ENTRUST
firmaprofesional
Information Security
dátil
NOREG
keytalk
DIGITALTRUST
QRL
ascertia
Garantir
3KEYCOMPANY
KIR
microsec
LEX persona
firma.digital
TÜV TRUST IT
ANF AUTORIDAD DE CERTIFICACIÓN
CALM
NGSIGN
BOSCH
Viasat
Trust SEC
EVERTRUST
AIRBUS
KEYFACTOR
buypass
CREDIT SUISSE
d-trust.
FPKI
Federal Public Key Infrastructure
zeva
NIMBUS
THALES
cleverbase
Trans Sped TSP
HID
DB
WELLS FARGO
INDEED ID
亞洲誠信 TRUSTASIA
Etugra
TRUSTZONE
SSL.com
TrustWrx
DELL Technologies
bakertilly
camerfirma
AN INFOCERT COMPANY
ZoTrus
QCee
Fidelity INTERNATIONAL
TD
comsign
HARICA
DavidGroup
real random
Sixscape
SEALWeb
SECTIGO

PKI Consortium

What are we working on?

PKI Consortium

Remote Key Attestation

pkic.org/remote-key-attestation

Vendor/Model	Capability	Format	Documentation	Notes
Cloud HSMs				
Google CloudHSM	✔	JSON	https://cloud.google.com/kms/docs/attest-key	
AWS CloudHSM	✘			
AWS KMS	✘			
Azure Key Vault	✘			
Azure Managed HSM	✘ ⏲			Claimed to be on the roadmap
HSMs				
Entrust nShield	✘ ⏲		https://github.com/pkic/remote-key-attestation/issues/3	Claimed to be on the roadmap
Utimaco CryptoServer	✘			
Thales Luna	✔	CMS/PKCS#7	https://thalesdocs.com/gphsm/luna/7/docs/network/Content/admin_partition/confirm/confirm_hsm.htmhttps://thalesdocs.com/gphsm/luna/7/docs/network/Content/Utilities/cmu/cmu_getpkc.htm	
Marvell HSMCMS/PKCS#7	✔	Proprietary/Binary	https://www.marvell.com/products/security-solutions/nitrox-hs-adapters/software-key-attestation.html	GCP Cloud HSM, AWS CloudHSM and MS Managed HSM are using Marvell hardware in the background
Securosys Primus HSM	✔	XML with external sig	https://www.securosys.com/hubfs/Securosys_PrimusHSM_KeyAttestation_SB-E01.pdf (Documentation in HSM User Guide)	
I4P Trident HSM	✔	CMS/PKCS#7	https://www.i4p.com/documents/Trident_RSS_summary_sheet_200929.pdf	No detailed documentation about using key attestation available publicly.
Fortanix	✘ ⏲			Claimed roadmap item for H1 2023
Tokens				
Yubico	✔	X.509	https://developers.yubico.com/YubiHSM2/Concepts/Attestation.htmlhttps://developers.yubico.com/yubico-piv-tool/Attestation.htmlhttps://developers.yubico.com/PIV/Introduction/PIV_attestation.html	
Trusted Platform Module	✔	TPMS_ATTEST/PKCS#10	https://www.cs.unh.edu/~it666/reading_list/Hardware/tpm_fundamentals.pdfhttps://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/component-updates/tpm-key-attestationhttps://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-wcce/f596c7df-a72c-4323-	

PKI Consortium

PKI Maturity Model

pkic.org/pkimm

The PKI maturity model and assessment methodology will be used as an entry point for anyone evaluating PKI environment by itself or using an independent third party.

The model provides the following benefits:

- Quickly understand the current level of capabilities and performance of the PKI
- Support comparison of PKI maturity with similar organizations based on size or industry
- Improvement strategy for the current PKI state
- Improve overall PKI performance and ability to meet the requirements of the industry

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
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	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗
Fortanix	FX2200	HSM	2022-11-29	✗	✗	✓	✗	⏲	⏲	⏲	✗	✗	✗	✗
I4P	Trident	HSM	2022-12-01	✗	✗	✗	⏲	✗	✗	✓	✓	✗	✗	✗
IBM	4769/CCA/EP11	HSM	2023-01-11	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗
ISC	CDK	Software library	2023-03-04	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✗
ISC	CertAgent	PKI	2023-03-04	✗	✗	⏲	✗	✓	✓	✓	✓	✗	✓	✗
Keyfactor	SignServer	Signing Software	2022-12-19	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗
Keyfactor	EJBCA	PKI	2022-12-19	✗	✗	✗	✗	✓	✓	✗	✗	✗	✗	✗
MTG AG	Corporate PKI	PKI	2023-09-25	✗	✗	✗	✗	✓	✓	✓	⏲	✗	✓	✗
Open Quantum Safe	liboqs	Software library	2022-11-30	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓
Securosys	Primus	HSM	2022-11-28	⏲	⏲	✗	✗	✗	⏲	⏲	⏲	✗	✗	✗
Thales	Luna	HSM	2022-11-22	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✗
Utimaco	Q-Safe	HSM	2022-11-28	✗	✗	✓	✓	✗	✓	✗	✓	✗	✗	✗
Utimaco	u.trust Identify	PKI	2022-11-28	✓	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗

PKI Consortium

Why do we organize this PQC Conference?

PKI Consortium

Key take aways from Ottawa

- Quantum computers will be able to break current public key encryption
- Long term data needs to be protected now
- Failure to migrate leaves applications and data at risk of compromise
- Accurate crypto inventory & mitigation strategies are required
- This crypto migration will be the hardest we've ever done

PKI Consortium

What is on the agenda?

PKI Consortium

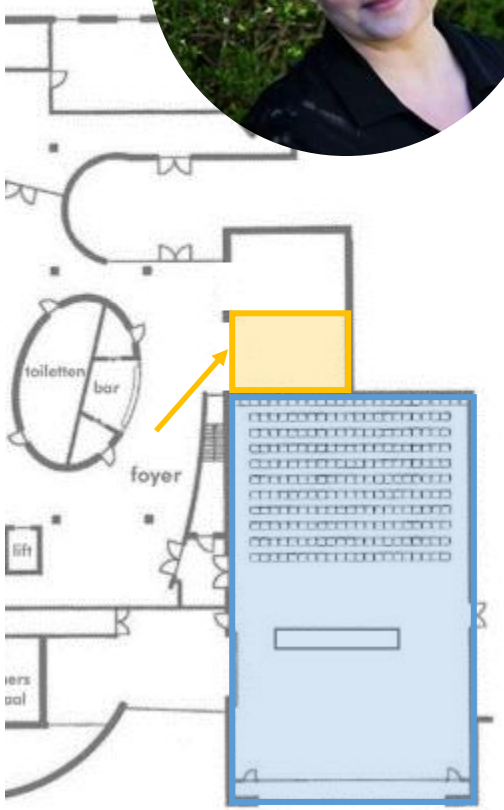
	Tuesday (7 November)	
	Plenary (Blue Hall)	
09:00	Opening	
09:30	Status update from NIST	
10:00		**Breakout (6 & 7)**
10:30	**Break**	
11:00	Preparing the United States for Post-Quantum Cryptography	Lattice-based Cryptography
11:20	A Quantum Cybersecurity Agenda for Europe	
11:40	Post-Quantum Policy and Roadmap of the BSI	Stateful Hash-Based Signature Schemes
12:00	ANSSI plan for post-quantum transition	
12:20	Unlocking the Quantum-Resilient Cryptography Strategy for the Dutch central government	Code-based Cryptography
12:40	Ask the Experts: Global Perspectives on Post-Quantum Cryptography Governance	
13:00	**Lunch**	
14:00	What is it going to take to break cryptography with a quantum computer?	LMS: Lighter, faster key generation
14:30	Crunching the Numbers: Post Quantum Algorithm Performance	Machine-checking post-quantum cryptography
15:00	Comparing Strategies for Quantum-Safe Cryptography Adoption in Organizations	Leading the Quantum-safe Transition: A Growth Stages Approach
15:30	**Break**	
16:00	Birth of the Post-Quantum Internet	Update from the GSMA Post Quantum Telco Network Task Force
16:30	Post-quantum crypto integration for enterprise applications	Building Your PQC Lab: Trust But Verify Your PQC Ecosystem
17:00	Closing remarks for day 1	
17:05	**Networking**	

	Wednesday (8 November)	
	Plenary (Blue Hall)	**Breakout (6 & 7)**
09:00	Post-Quantum Crypto: Challenges for Embedded Applications	A testbed for evaluating post-quantum algorithms for the DNS
09:30	Challenges for the Post-Quantum Transition of Mobile Ecosystems	Coping with post-quantum signatures in the WebPKI
10:00	Hardware Cryptographic Modules (panel discussion)	Your cryptography will be broken, prepare yourself now! (discussion)
10:30	**Break**	
11:00	How to Sell Post-Quantum Readiness by Combining it with a Zero Trust Journey	A Sign of the Times: The Transition to Quantum Secure Authentication
11:30	Quantum-safe PKI for the German administration	Quantum Resistance through Symmetric Key Cryptography
12:00	PKI and PQC Strategy for Payment Card Industry	Symmetric Key Exchange: Lightweight Alternatives for a Post-Quantum IoT
12:30	Post-Quantum Cryptography & Trust Services	Vulnerabilities of Blockchain Security in the World of Quantum Computing
13:00	**Lunch**	
14:00	NIST standardization of additional signature schemes	Investigating Post-Quantum Cryptography: building a PQC decision tree for developers
14:30	Moving toward a Quantum Security Maturity Index	Using quantum-safe hybrid certificates for signing documents
15:00	PKI deployments are as unique as any snowflake; how to build equally flexible PQ migration strategies	CRQC and Signatures – no Problem?
15:30	**Break**	
16:00	Final Q&A	
16:30	Recap: Unveiling Insights A Two-Day Conference Retrospective	
17:00	Closing remarks	
17:05	**Networking**	

ENTRUST HID PKI Consortium

The Leap to Quantum-Safety:
A game for the transition to QS PKI

Lærke Vinther Christiansen



In this workshop you will play the first prototype of a serious game meant to aid in the transition to QS PKI as a part of the HAPKIDO Project.

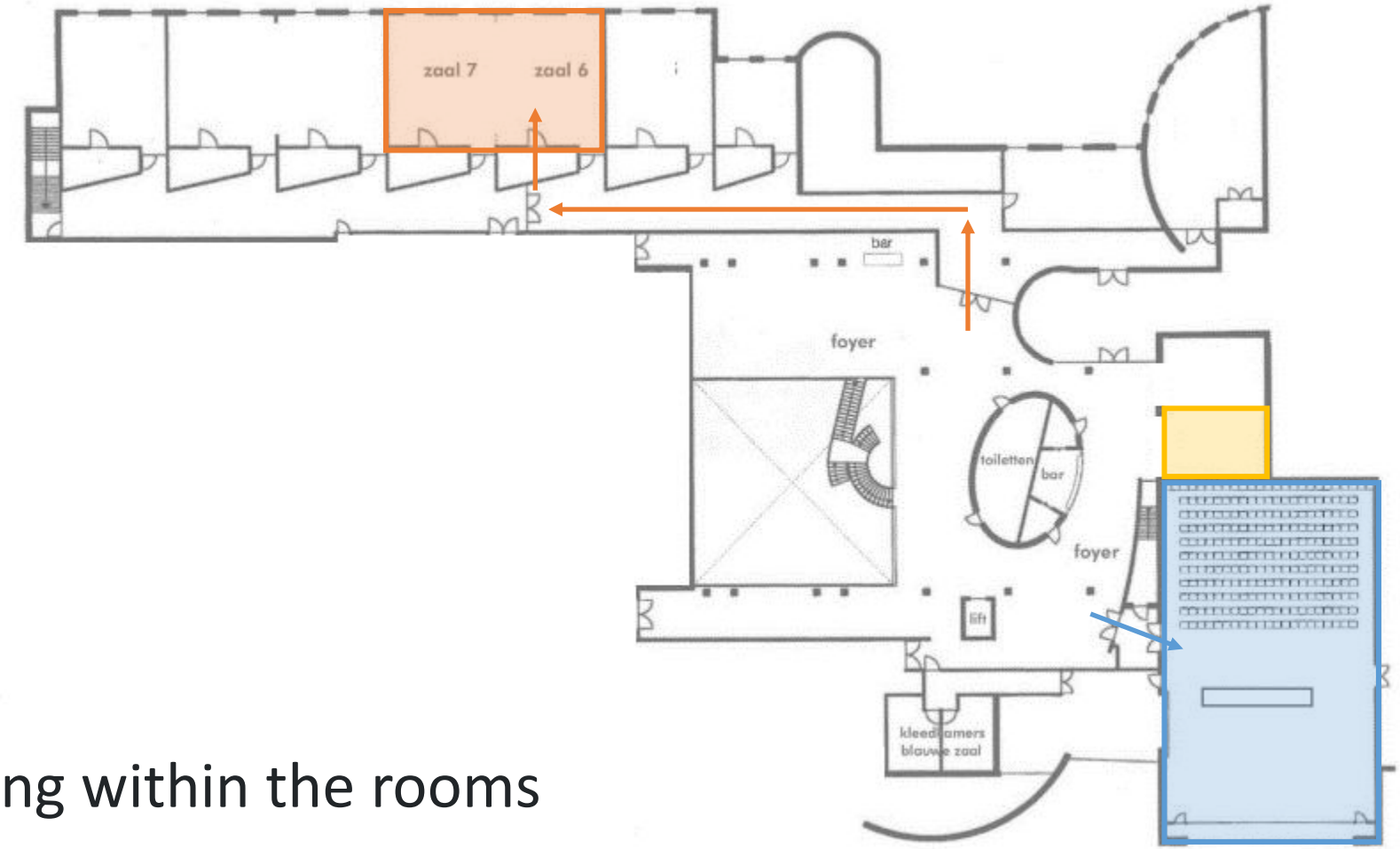
The game is played with two groups of 4-6 participants. You can register in the lobby (directly right outside the plenary/blue hall).

The purpose of the game is to give the player an actionable understanding of the interdependencies of the QS PKI transition, their role in the transition, and to provide them with a comprehensive understanding of the necessary next steps for the transition in general and for themselves specifically.

PKI Consortium

Housekeeping

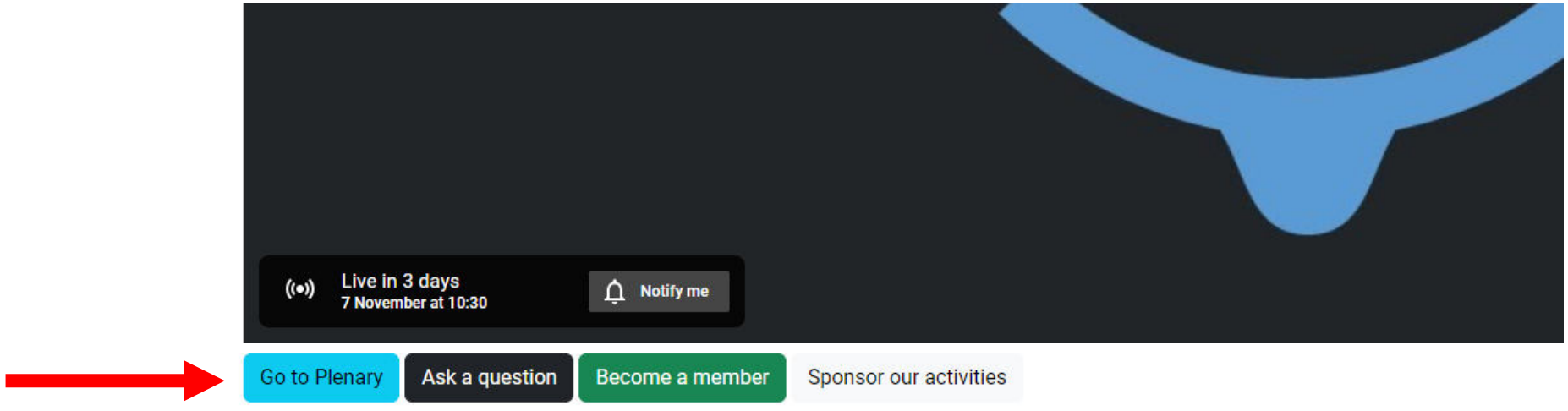
PKI Consortium

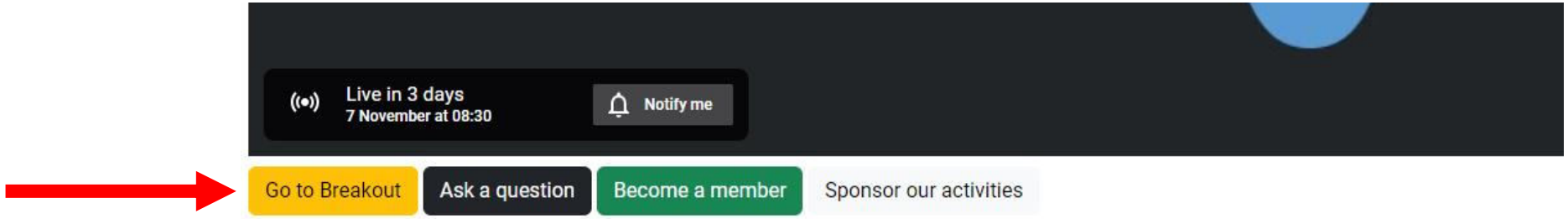


- No smoking
- No drinks or eating within the rooms

PKI Consortium

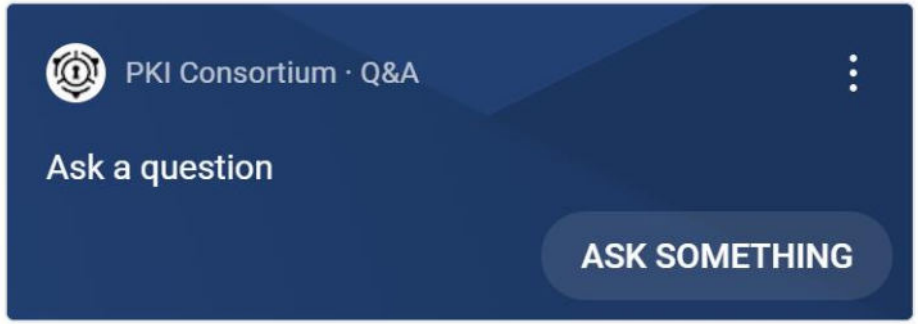
Switch between **Plenary** and **Breakout**

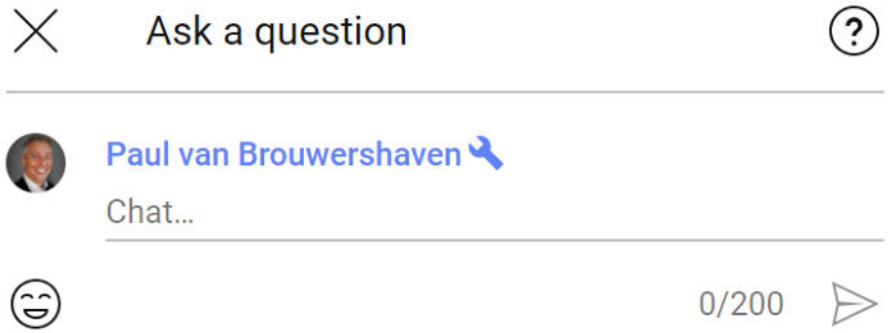


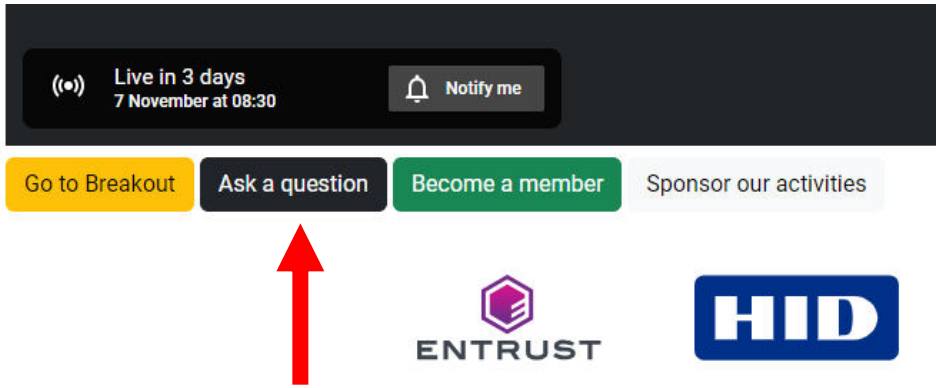


PKI Consortium

Questions







PKI Consortium

Thanks to the key contributors of this conference

PKI Consortium

PKI Consortium

ENTRUST

Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

TNO

CWI

This event would not have been possible without our sponsors

PKI Consortium

ENTRUST

HID

PQ SHIELD

QRL

d-trust.

THALES

NOREG

KEYFACTOR

Fortanix

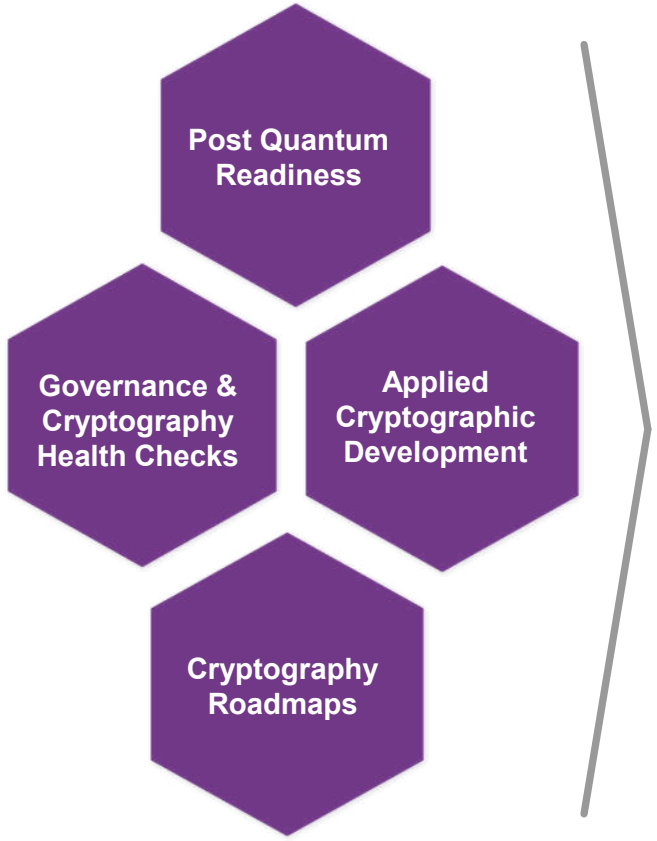
amsterdam convention bureau

ascertia

亞洲誠信 TRUSTASIA

PKI Consortium

Entrust Solutions for Today, and a PQ Future



PKI for Machines and People	Virtual Infrastructure compliance	Digital/Code Signing & Time Stamping	Crypto Discovery, Control & Automation	Trust Anchors
SSL, Verified Mark & Email Encryption	Digital onboarding	Identity (Smart, Risk Engine, Decentralized)	Key/Secrets Management	Hardware Key protection
Blockchain & MPC security	Instant & Bureau Card & Passport Issuance	Digital Payment Cards	Data Encryption Services	Custom Solutions

ENTRUST

PQ SHIELD

think openly, build securely

Hardware IP

Modular hardware IP delivering quantum-resistant security, co-processing and side channel protection.

Software IP

FIPS 140-3 ready modular cryptographic libraries, APIs and SDKs for quantum-safe and hybrid transition.

Research IP

Setting the standards at NIST, RISC-V, IETF, World Economic Forum and many more platforms beyond. 10+ Patents.

The Challenge

HSMs are out-dated

Fortanix®

Security, *wherever* your data is

The Solution

Fortanix re-invented the HSM

- DSM unifies HSM, KMS & more
- PQ-ready
- Written in Rust
- Native clustering
- Multi-tenancy
- User friendly & cloud friendly
- 100% remotely manageable
- 100% API driven

FIPS VALIDATED 140-2

PCI DSS COMPLIANT

SOC 2 TYPE 2

Deployment flexibility

- Physical appliance - for on-prem
- Virtual appliance - for public/private cloud
- SaaS - for simplicity (6 regions available)

Gartner

Fortanix.com

QUESTIONS?

Have any questions or would like to learn more?
We would love to hear from you.

Let's talk!

Press Inquiries

press@theqrl.org

Support Requests

support@theqrl.org

General Inquiries

info@theqrl.org

Social

Discord: https://www.discord.gg/qrl

Reddit: https://www.reddit.com/r/qrl

Twitter: https://twitter.com/QRLedger

YouTube: https://youtube.com/c/QRLedger

QRL Blog: https://www.theqrl.org/blog/

QRL

PKI Consortium

THALES

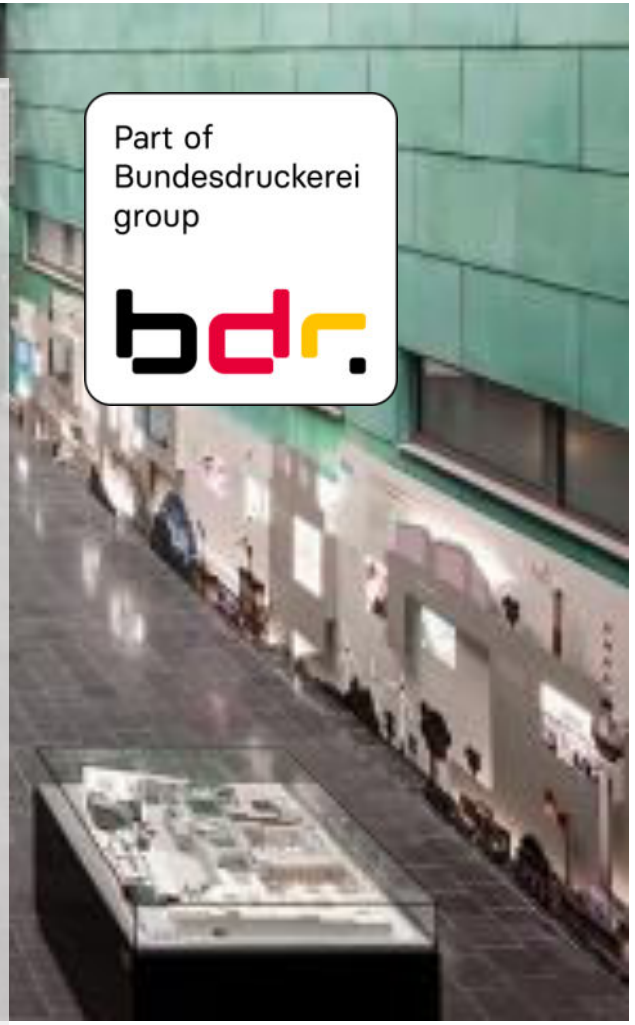
Building Your PQC Lab – Trust but Verify Your PQC Ecosystem

- What's the Problem We're Solving
- Getting Started
- Staffing, Budgeting and Planning Ahead
- Case Study: Major US Bank
- Ecosystem Support
- Q&A

Blair Canavan, Thales

Session: November 8, 14:30

- D-Trust, **a company of** the **Bundesdruckerei Group**
- **pioneer** in **secure digital identities**
- **independent** and **qualified trust service provider**
- **listed with the Federal Network Agency** since 2016 within the framework of the **eIDAS** regulation
- translates trust into concrete **products such as digital certificates and electronic signatures**
- enable secure digital identities for **companies, public authorities** and for **private use.**
- **workforce** of currently around **240,**
- generating **revenue of EUR 79.9 million in 2021**



Join the PKI Consortium

pkic.org/join

pkic.org/join

PKI Consortium

Post-Quantum Cryptography Conference

PKI Consortium

ENTRUST

HID

PQ SHIELD

Fortanix

KEYFACTOR

NOREG

QRL

THALES

d-trust.

amsterdam convention bureau

ascertia

亞洲誠信 TRUSTASIA