

Post-Quantum

Cryptography Conference

Opening



**Paul van Brouwershaven**

Chair PKI Consortium and Director of Technology Compliance at Entrust



**Albert de Ruiter**

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



KEYFACTOR



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

PKI Consortium Inc. is registered as a 501(c)(6) non-profit entity ("business league") under Utah law (10462204-0140) | [pkic.org](https://pkic.org)



**PKI**  
Consortium

# Welcome



**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 160+ 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



What are we working on?



**PKI**  
Consortium

# Remote Key Attestation

[pkic.org/remote-key-attestation](http://pkic.org/remote-key-attestation)

Vendor/Model	Capability	Format	Documentation	Notes
<b>Cloud HSMs</b>				
Google CloudHSM	✓	JSON	<a href="https://cloud.google.com/kms/docs/attest-key">https://cloud.google.com/kms/docs/attest-key</a>	
AWS CloudHSM	✗			
AWS KMS	✗			
Azure Key Vault	✗			
Azure Managed HSM	✗ ⓘ			Claimed to be on the roadmap
<b>HSMs</b>				
Crypto4A QASM	✓	Proprietary/PEM	<a href="https://support.crypto4a.com/public/documentation/C4A-302-0043-AttestationInQasm.html">https://support.crypto4a.com/public/documentation/C4A-302-0043-AttestationInQasm.html</a>	
Entrust nShield	✓	JSON	<a href="https://nshielddocs.entrust.com/key-attestation-docs/v1.0.2/intro.html">https://nshielddocs.entrust.com/key-attestation-docs/v1.0.2/intro.html</a>	
Utimaco CryptoServer	✗			
Thales Luna	✓	CMS/PKCS#7	<a href="#">Meeting CA/Browser Forum Standards with Luna and Luna Cloud HSMs / Public Key Confirmations</a>	
Marvell HSMCMS/PKCS#7	✓	Proprietary/Binary	<a href="https://www.marvell.com/products/security-solutions/nitrox-hs-adapters/software-key-attestation.html">https://www.marvell.com/products/security-solutions/nitrox-hs-adapters/software-key-attestation.html</a>	GCP Cloud HSM, AWS CloudHSM and MS Managed HSM are using Marvell hardware in the background
Securosys Primus HSM	✓	XML with external sig	<a href="#">HSM User Guide Docs</a>	
I4P Trident HSM	✓	CMS/PKCS#7	<a href="https://www.i4p.com/documents/Trident_RSS_summary_sheet_200929.pdf">https://www.i4p.com/documents/Trident_RSS_summary_sheet_200929.pdf</a>	No detailed documentation about using key attestation available publicly.
Fortanix	✓	JSON	<a href="#">Verifying Key Attestation Statements Doc</a>	
<b>Tokens</b>				
Yubico	✓	Y.509	<a href="#">Attestation Concept: DIM Attestation</a>	

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:**

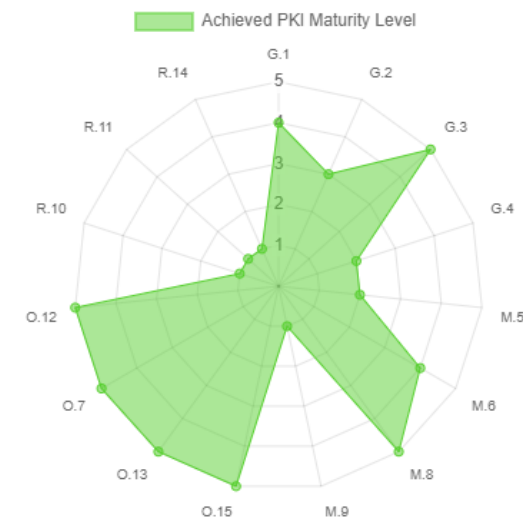
The resources needed for the PKI are not defined and documented. There is a risk of unavailable resources causing the PKI to be unavailable.

**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.



# PKI Maturity Model

[pkic.org/pkimm](http://pkic.org/pkimm)



# PQC Capabilities Matrix (PQCCM)

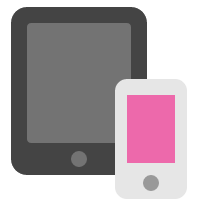
[pkic.org/pqccm](https://pkic.org/pqccm)

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

# Training & Certification



- Legislation
- Cryptography basics
- PKI building blocks
- PKI management and Security
- PKI Roles and Responsibilities
- Governance, Risk management & Compliance



# Post-Quantum Cryptography



**PKI**  
Consortium

# Quantum Computers are already a Reality

But 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!

What is on the agenda?



**PKI**  
Consortium

	Plenary	Breakout
<b>8:30</b>	<b>Registration</b>	<b>Registration</b>
<b>9:00</b>	Opening	
<b>9:30</b>	Quantum Computing: Between Hope and Hype	
<b>10:00</b>	NIST Post-Quantum Cryptography Update	
<b>11:00</b>	<b>Break</b>	<b>Break</b>
<b>11:30</b>	Transitioning National Security Systems to a Post Quantum Future	Migrating and benchmarking a banking application
<b>12:00</b>	ELI5: Implementing Digital Certificates for a Post-Quantum World	Architecting PKI Hierarchies for Graceful PQ Migration
<b>12:30</b>	Strategies for Transitioning to Future-Proof Cryptography	Update on end-to-end PKI and HSM integrations with ML-DSA
<b>13:00</b>	<b>Lunch</b>	<b>Lunch</b>
<b>14:00</b>	2025 is Here - How to get your PQC Readiness Plan Underway	Online Quantum-safe Readiness Tool
<b>14:30</b>	X9 Financial PKI: PQC Readiness and Crypto-Agility for Financial Services	Hybrid PQC E-Mail Communication: Easing Migration Pain
<b>15:00</b>	Why the Internet isn't ready for Post-Quantum Certificates	Quantum-Safe Secure Boot: How hard can it be?
<b>15:30</b>	<b>Break</b>	<b>Break</b>
<b>16:00</b>	Extending or Evolving: Choosing the Path to Quantum Readiness	Making PQ Signatures work in the WebPKI
<b>16:30</b>	To Hybrid or Not to Hybrid: Navigating the PQC Transition	
<b>16:55</b>	Closing remarks for day 1	
<b>17:00</b>	<b>Networking</b>	<b>Networking</b>
<b>19:00</b>	<b>End of Day One</b>	<b>End of Day One</b>

Wednesday

	Plenary	Breakout
<b>8:30</b>	<b>Registration</b>	<b>Registration</b>
<b>9:00</b>	Update on the NIST standardization of additional signature schemes	PQC Standardization at the Internet Engineering Task Force (IETF)
<b>9:30</b>	Is CBOM Enough?	PQC Interoperability Project
<b>10:00</b>	PQC in FIPS 140-3, status and roadmap	ETSI ESI and Quantum-Safe Cryptography
<b>10:30</b>	<b>Break</b>	<b>Break</b>
<b>11:00</b>	Hardware Cryptographic Modules	Lessons Learned from Testing Millions of Servers for Post-Quantum Compatibility
<b>11:30</b>	Crypto Asset Discovery Tooling – an Overview of Capabilities, Characteristics and Gaps	How much will ML-DSA Signatures affect Web Metrics after all?
<b>12:00</b>	NIST National Cybersecurity Center of Excellence’s Migration to Post-Quantum Cryptography Project	The impact of ML-KEM and ML-DSA on mTLS connection Time-to-Last-Byte
<b>12:30</b>	Practical Insights from Following NIST SP 1800-38B	X9.146 Quantum TLS
<b>13:00</b>	<b>Lunch</b>	<b>Lunch</b>
<b>14:00</b>	Communication among Financial Institutions: What are the available answers to the quantum threat?	Hybrid PQC Digital Signatures and SSI
<b>14:30</b>	Curriculum Development for Post-Quantum Workforce Development Programs	Quantum Key Distribution – What is done and what is to come
<b>15:00</b>	Perspectives on the transition to PQC in the financial sector	Is your HSM quantum-ready? Here’s what you need to know!
<b>15:30</b>	Accelerated Quantum Supercomputing and Post-Quantum Cryptography	Securing Data in the Quantum Era: From the Root of Trust to Protecting Ecosystems
<b>16:00</b>	Closing remarks	
<b>16:10</b>	<b>Networking</b>	<b>Networking</b>
<b>18:00</b>	<b>End of Day Two</b>	<b>End of Day Two</b>

# Thursday

Subscribe to our YouTube channel for the recordings

<https://youtube.com/@PKIConsortium>




## PKI Consortium

@PKIConsortium · 377 subscribers · 56 videos

More about this channel ...more

[pkic.org](https://pkic.org) and 1 more link

Subscribe

[Home](#) [Videos](#) [Live](#) [Playlists](#) [Community](#) 

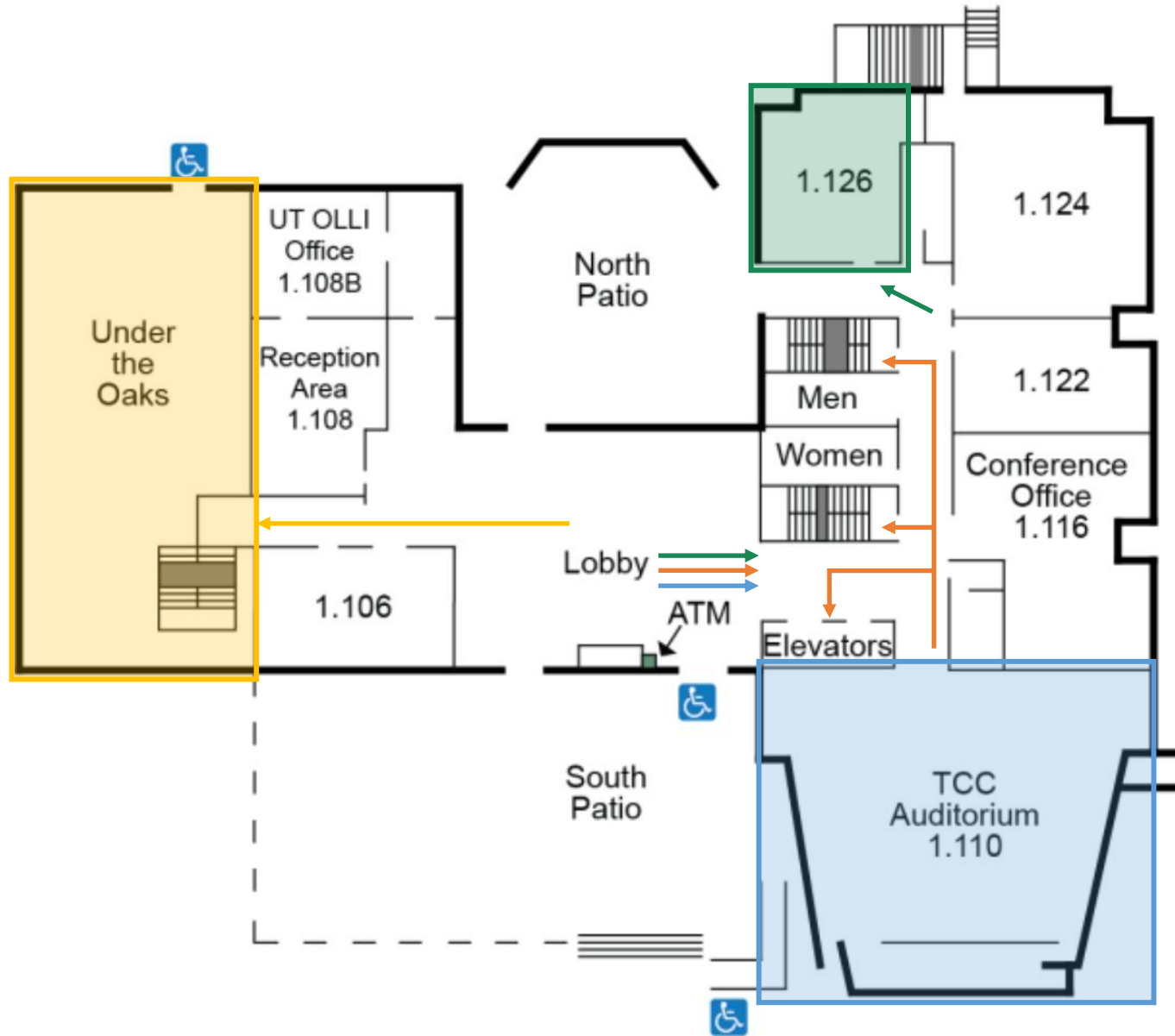


# Housekeeping

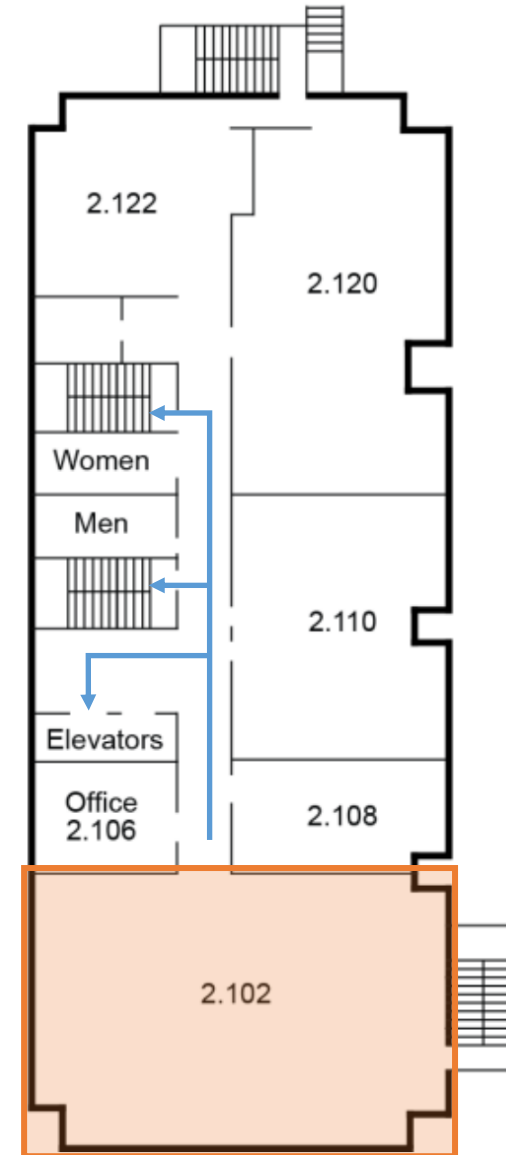


**PKI**  
Consortium

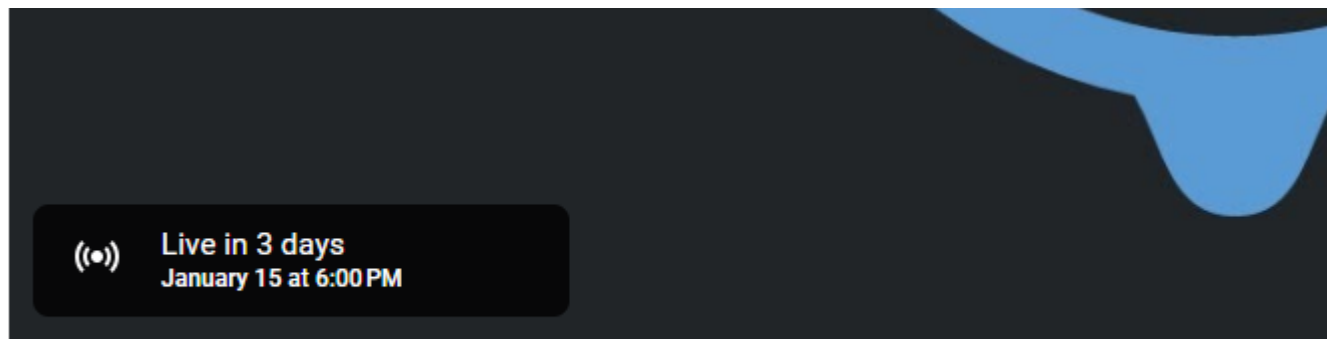
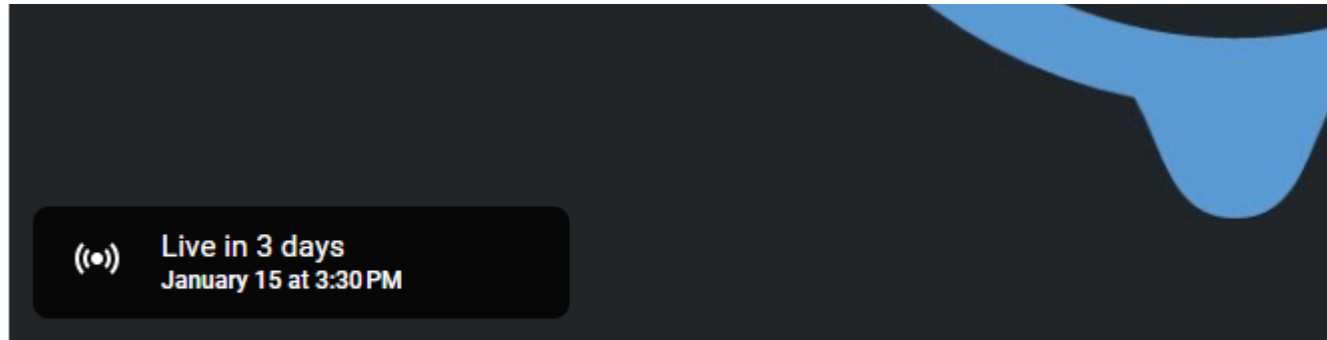
TCC Ground and First Floor



TCC Second Floor




# Switch between Plenary and Breakout



# Questions

[pkic.org/ask](https://pkic.org/ask)

 Live in 3 days  
January 15 at 3:30 PM

[Go to Breakout](#)

[Ask a question](#)

[Become a member](#)

[Sponsor our activities](#)



Thanks to the key contributors  
of this conference



**PKI**  
Consortium



# PKI Consortium



Logius  
Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties

KEYFACTOR



ENTRUST

- Albert de Ruiter
- Chris Bailey
- Chris Ghantous
- Chris Hickman
- Giuseppe Cimmino
- John Buselli
- Leigh Bailey
- Mariana Santiago Lerco
- Paul van Brouwershaven

- Phillip Zacharia
- Ralph Poore
- Rebecca Kelley
- Samantha Maybe
- Sven Rajala

This event would not have been possible without our sponsors

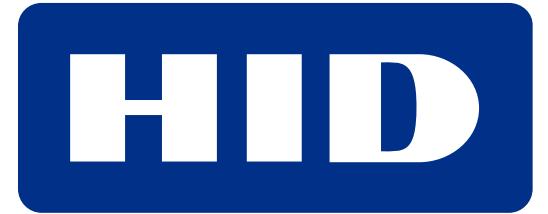


**PKI**  
Consortium





KEYFACTOR



digicert®



NOREG

SECTIGO®

CRYPTO4A

utimaco®

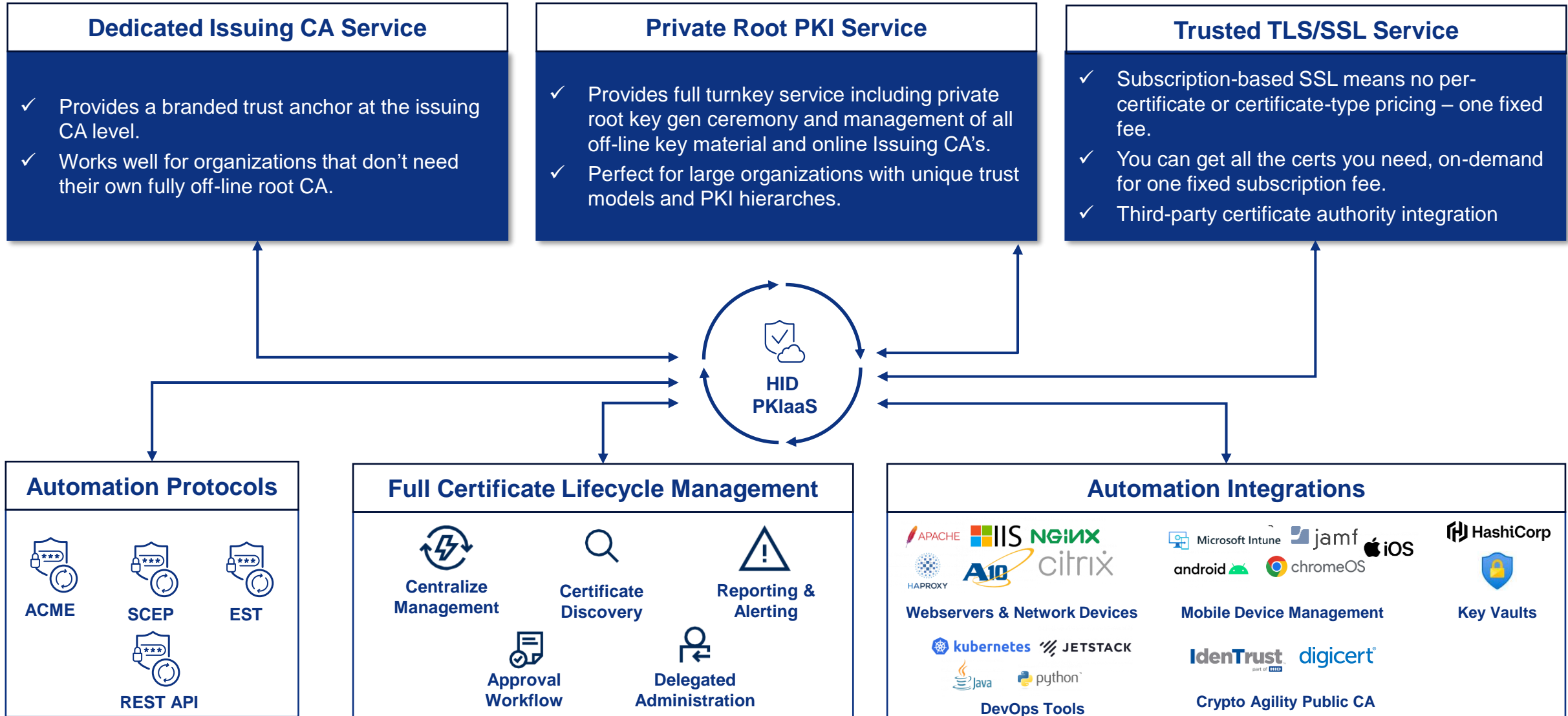


# A few sponsor Pitches



**PKI**  
Consortium

# HID PKI-as-a-Service Overview



Quick Intro.

# PQShield: mature PQC in Software, FPGA and ASIC

With an 80 strong global team and having helped set the the PQC standards, PQShield is delivering solutions to customers across **Semiconductor, Networking, Government & Defence, Automotive, Industrial IoT** and **many more...**

## SOFTWARE IP

From embedded systems to server class devices and beyond. FIPS 140-3 CMVP certified hybrid cryptography library at its core

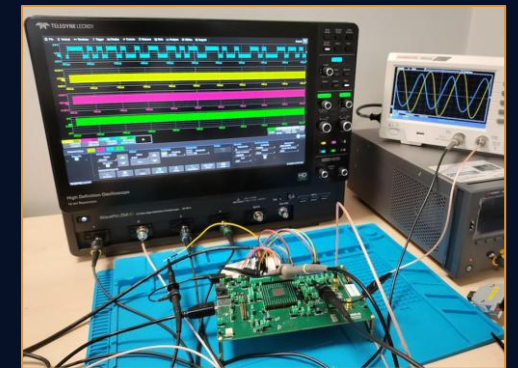
- 
- 
- 



## HARDWARE IP

From Platform Security to High-Throughput PQC accelerators. Extensive SCA and Fault Injection testing, including our very own NIST standards compliant silicon test chip

- 
- 
- 
- 



**PQShield has defined 3 security levels - Cloud, Edge and Government Grade**

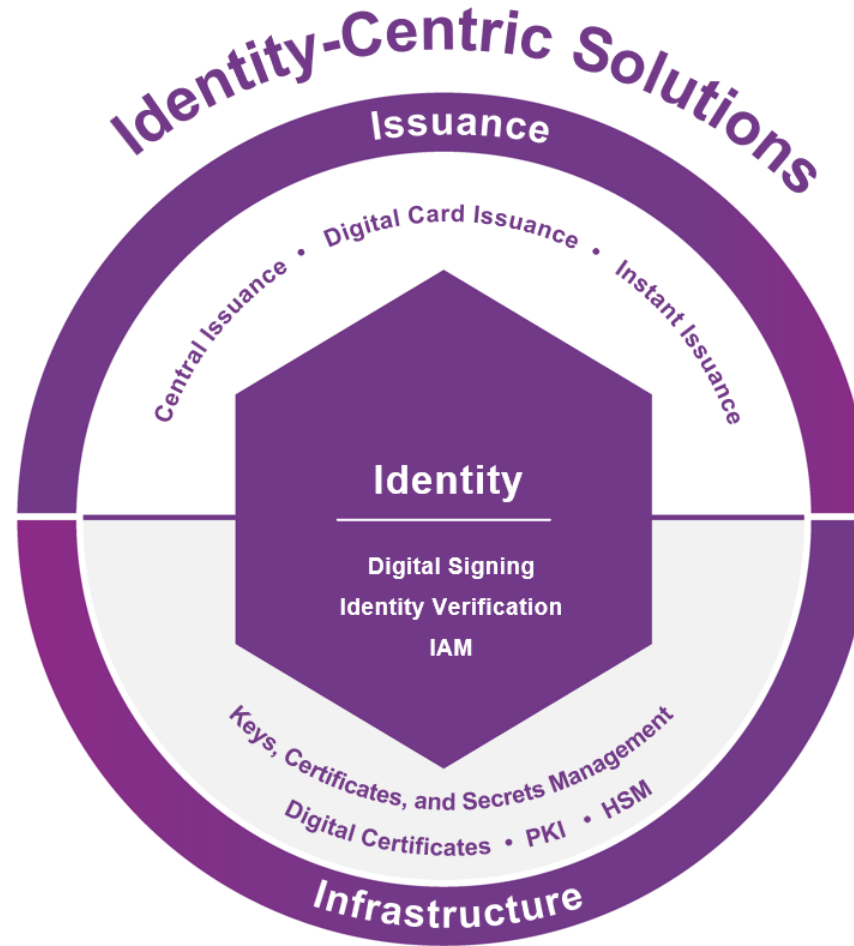
These align to various levels of standards like FIPS, Common Criteria, SESIP and PSA - helping PQC into the real world



# Identity-Centric Solutions Powered by AI

Founding member of the PKI Consortium

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



On-prem PKI  
mPKI  
PKIaaS PQ Ready



CCoE  
PQC Readiness assessment  
PQ Lab



nShield HSM  
PQ SDK



**SSL.com**

---

TRUST IS WHAT WE DO

# KEYFACTOR

## Do digital trust right

### Modernize your PKI

---



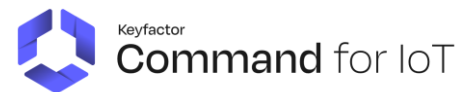
Simplify and scale PKI for enterprise, IoT, and DevOps

### Gain visibility and control

---



Discover, manage, and automate digital certificates



Manage IoT device identities from manufacturing to EOL

### Secure software and code

---



Sign code at scale for IoT and manufacturing



Enable fast and secure signing for DevOps

### Implement cryptography

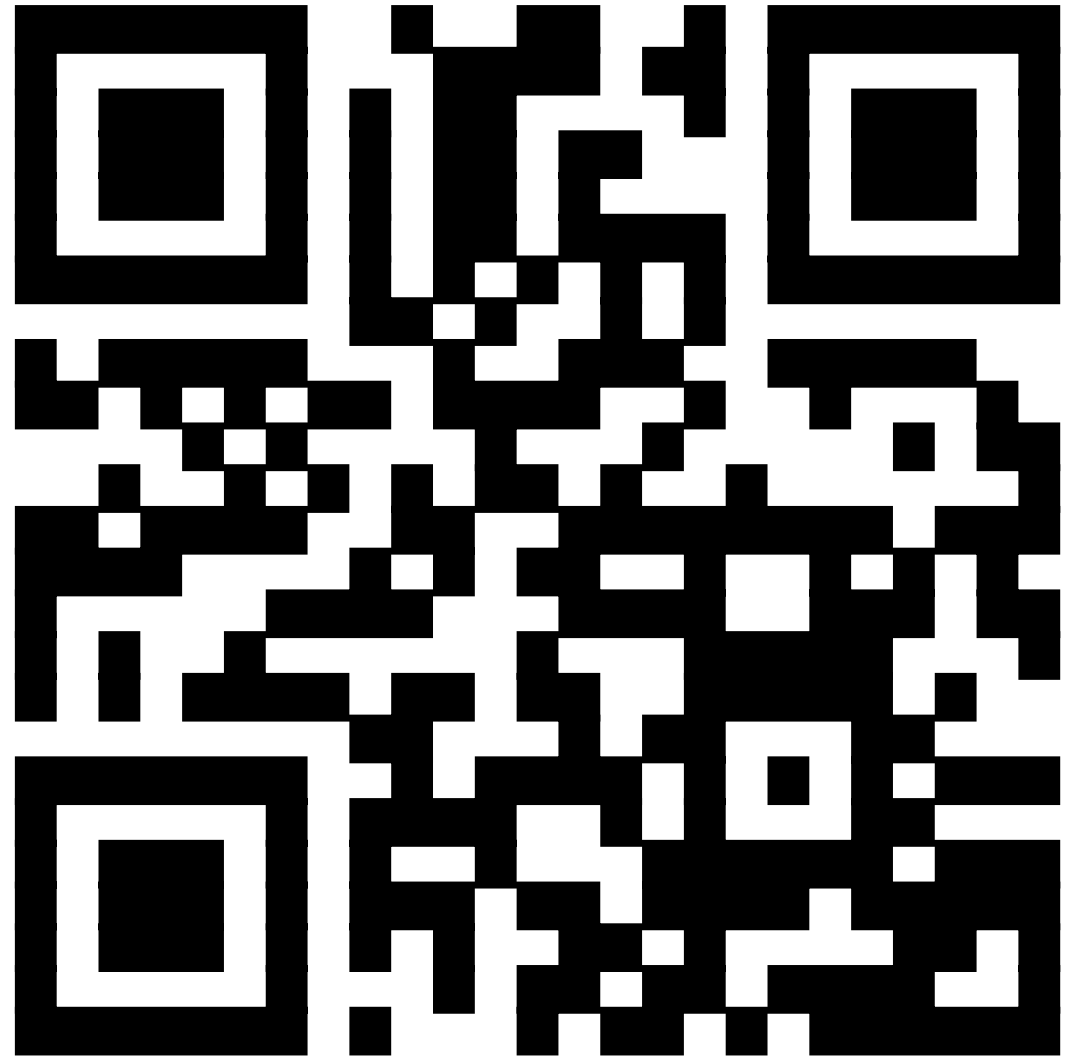
---



Implement quantum-ready, FIPS-certified crypto APIs

# Join the PKI Consortium

[pkic.org/join](https://pkic.org/join)



[pkic.org/join](https://pkic.org/join)



