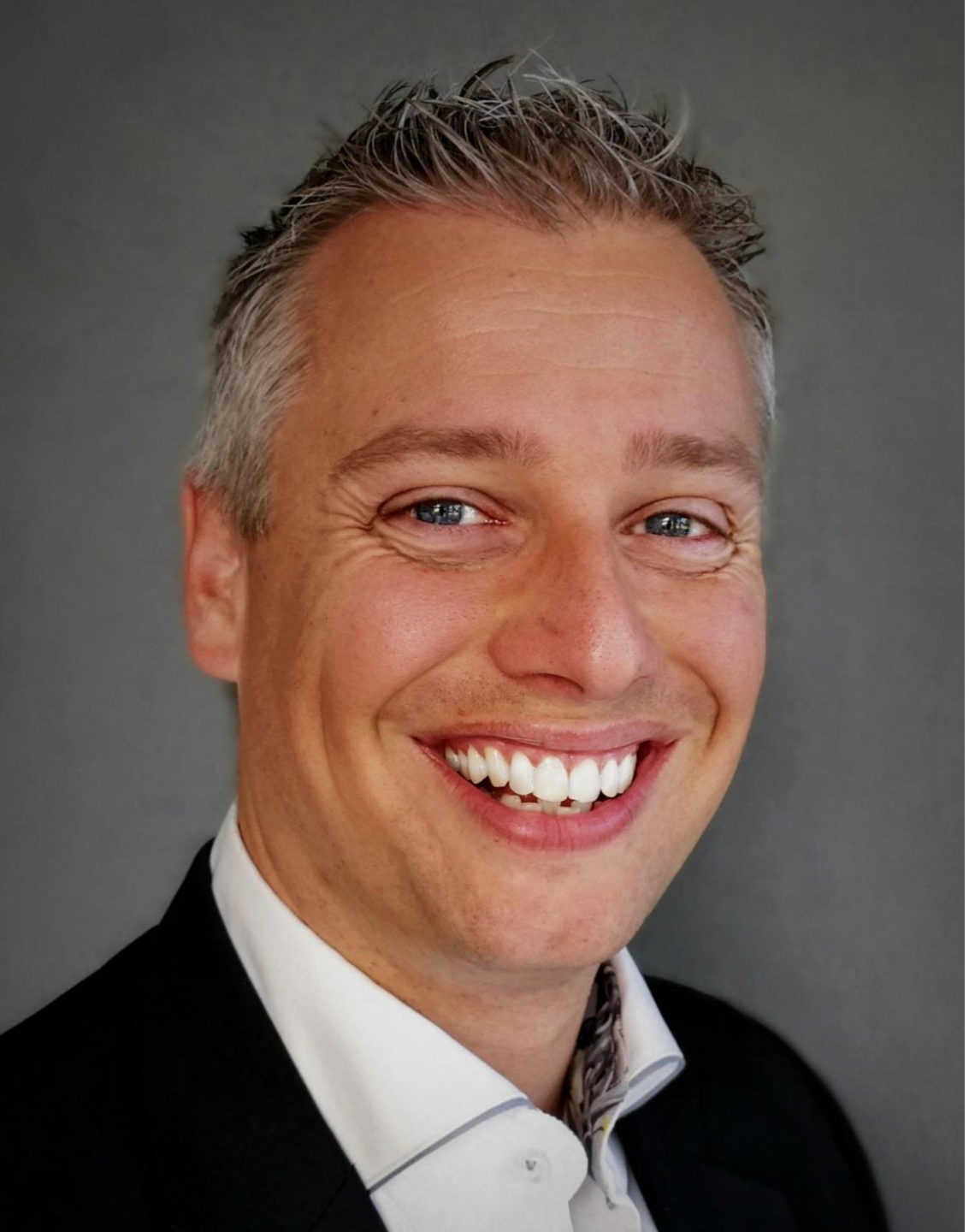
Welcome

Post-Quantum Cryptography Conference

Friday March 3, 2023 - Ottawa, Canada - Hybrid

PKI Consortium



Paul van Brouwershaven

Chair PKI Consortium

- Director Technology Compliance at **Entrust**
- Vice chair at **CA/Browser Forum**
- CEO at **Digitorus**

PKI Consortium

ENTRUST

KEYFACTOR

ascertia

NOREG

亞洲誠信 TRUSTAsia

PKI Consortium

PKI Consortium

History

- Created in 2013 as the **CA Security Council**
- **Restructured and renamed** to the PKI Consortium in **July 2021** and started to deversify our members
- Today we have **more than 70 members** with different backgrounds and are honored to keep welcoming new members
  - No membership fees
  - We rely on sponsors and donations (voluntary)

PKI Consortium

PKI Consortium

Public Key Infrastructure Consortium

- Registered as a 501(c)(6) **non-profit entity** (“business league”) under Utah law (10462204-0140).
- We have a **diverse member base**, including governments, auditors, consultants, trust service providers, software and hardware vendors.
- There are multiple workings groups, new ones can be created.
  - Each working group has a **private mailing list**
  - **Public discussions** can take place in the community discussions.
- The community discussions are used to collect topics (including interest using votes) and to have discussions with non-members.

PKI Consortium

“Trusted digital **assets** and **communication** for **everyone** and **everything**”

PKI Consortium

“**Advance Trust** in assets and communication for everyone and everything using Public Key Infrastructure (PKI) as well as the **security of the internet** in general, by **engaging** with users, regulators, supervisory bodies and other interested or relying parties”

PKI Consortium

What are we working on?

PKI
Consortium

List of trust lists

pkic.org/ltl

List of Trust Lists

A global list of CA certificates trusted by public, private, industry, or solution-specific PKI

Help the PKI Consortium to manage this list of Trust Lists

360 Browser

https://caprogram.360.cn/

360 is a security company in China and has always been working on the secure development of the Internet.

- **TLS**
  - View or download list: HTML
  - Audit scheme: WebTrust

Adobe

https://helpx.adobe.com/acrobat/kb/approved-trust-list2.html

The Adobe Approved Trust List is a program that allows millions of users around the world to create digital signatures that are trusted whenever the signed document is opened in Adobe® Acrobat® or Reader® software. Essentially, both Acrobat and Reader have been programmed to reach out to a web page to periodically download a list of trusted "root" digital certificates. Any digital signature created with a credential that can trace a relationship ("chain") back to the high-assurance, trustworthy certificates on this list is trusted by Acrobat and Reader.

PKI Consortium

Remote Key Attestation

github.com/pkic/remote-key-attestation

Remote Key Attestation is intended to prove to a remote party that a private key was generated, managed inside, and not exportable from, a hardware cryptographic module.

Common use cases for key attestation:

- Verifying that the subscribers private signature key is generated and managed in an approved cryptographic device.
  - Code signing certificates (CA/Browser Forum)
  - eIDAS qualified certificates

We are collecting information and looking for contributions from vendors on how or if solutions provide a method for Remote Key Attestation.

PKI Consortium

Remote Key Attestation

https://github.com/pkic/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	✘🕐		#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.htm https://thalesdocs.com/gphsm/luna/7/docs/network/Content/Utilities/cmu/cmu_getpkc.htm	
Marvell HSM	✔	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				

PKI Consortium

PKI Maturity Model

github.com/pkic/pkimm

Mission:

To build a PKI maturity model that will be recognized around the globe as a standard for evaluation, planning, and comparison between different PKI implementations

The PKI maturity model should provide 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

Resource	Description
Charter	PKI Maturity Model Working Group Charter describing our objectives and activities.
GitHub	Primary repository for the model. You can find here the current documentation of the model, assessment methodology, and other.
Discussions	Discussion forum for the PKI maturity model, open to anyone, if you would like to start a discussion or just ask a question related to the model.

PKI Consortium

PQC Capabilities Matrix (PQCCM)

github.com/pkic/pqccm

The PKI Consortium is managing a PQC Capabilities Matrix (PQCCM) of **software applications, libraries and hardware that includes support for Post Quantum Cryptography**, without endorsing their implementation or quality.

The list includes a wide variety of software applications, libraries, and hardware from different vendors. The list should be considered a living document and a starting point. Considering the rapid change in the area such things can vary from day to day and complete freshness of information can only be gathered from vendors directly.

The PKI Consortium is actively working to promote the adoption of Post-Quantum Cryptography, and the capabilities matrix is a key part of that effort.

PKI Consortium

PQC Capabilities Matrix (PQCCM)

github.com/pkic/pqccm

What the PQCCM do:

- collect and aggregate information on PQC capabilities across the cybersecurity landspace (vendors, software, hardware, etc..)
- list entries must be product the provide PQC functionality to the end user, not merely for example PQC enabled TLS access to a non PQC enabled service

What the PQCCM doesn't do:

- review, vet, verify or test implementations or interoperability
- source code review, formal review of algorithms, etc.
- provide information, documentation or any recommended usage of Post Quantum Cryptography
- No other activity besides what is listed under PQCCM DOs is under the purview of PKI Consortium (unless explicitly stated otherwise)".

PKI Consortium

Post-Quantum Cryptography Capabilities Matrix

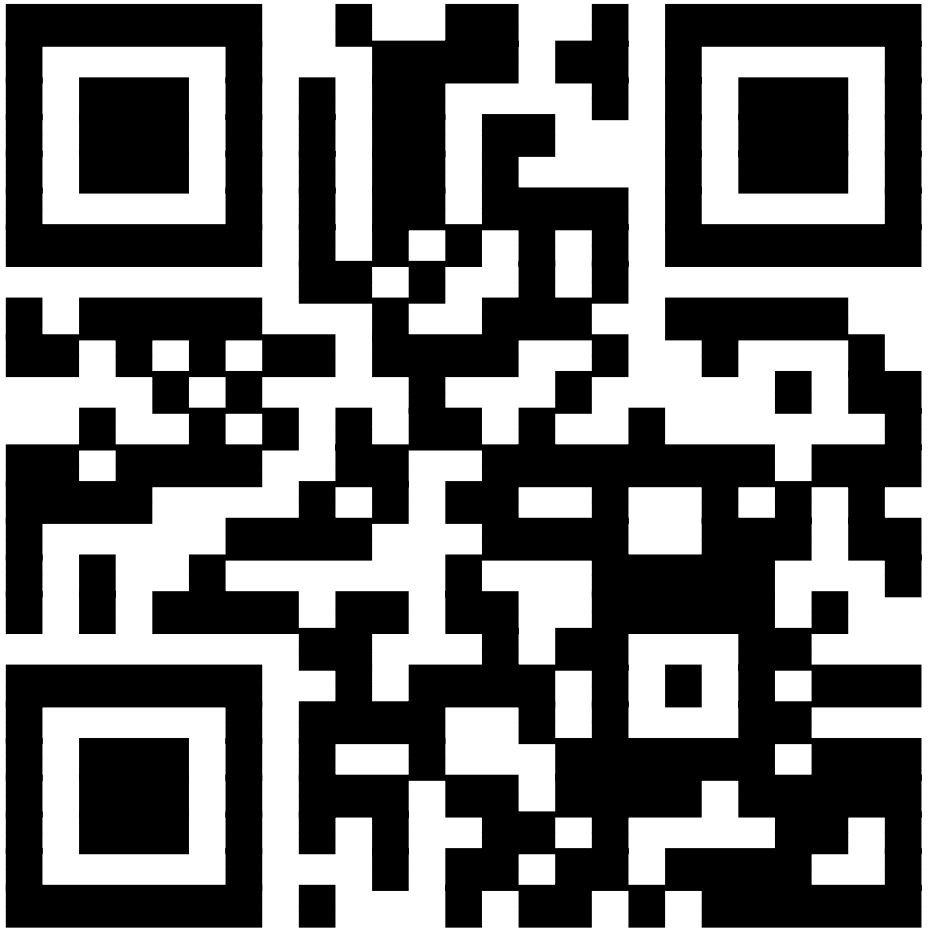
https://github.com/pkic/pqccm

Vendor	Product	Category	Last updated	Composite certificates	Hybrid certificates	LMS	XMSS	Falcon	Dilithium	SPHINCS+	Kyber	BIKE	McEliece	HQC
Crypto4A	QxEDGE	HSP	2022-12-04	🕐	✔	✔	✔	🕐	✔	✔	✔	✘	✔	✘
Crypto4A	QxHSM	HSM	2022-12-04	🕐	✔	✔	✔	🕐	✔	✔	✔	✘	✔	✘
Securosys	Primus	HSM	2022-11-28	🕐	🕐	✘	✘	✘	🕐	🕐	🕐	✘	✘	✘
Utimaco	Q-Safe	HSM	2022-11-28	✘	✘	✔	✔	✘	✔	✘	✔	✘	✘	✘
Utimaco	u.trust Identify	PKI	2022-11-28	✔	✘	✘	✘	✔	✔	✔	✘	✘	✘	✘
Thales	Luna	HSM	2022-11-22	✘	✘	✔	✔	✘	✔	✘	✔	✘	✘	✘
Entrust	nShield	HSM	2022-11-22	✘	✘	✘	✘	✔	✔	✔	✘	✘	✘	✘
Entrust	PKIaaS	PKI	2022-11-22	✔	✘	✘	✘	✔	✔	✔	✘	✘	✘	✘
Bouncy Castle	BC	Software library	2022-11-22	✔	✘	✔	✔	✔	✔	✔	✔	✔	✔	✔
Keyfactor	SignServer	Signing Software	2022-12-19	✘	✘	✘	✘	✘	🕐	✔	✘	✘	✘	✘
Keyfactor	EJBCA	PKI	2022-12-19	✘	✘	✘	✘	✔	✔	✘	✘	✘	✘	✘
Fortanix	FX2200	HSM	2022-11-29	✘	✘	✔	✘	🕐	🕐	🕐	✘	✘	✘	✘
Open Quantum Safe	liboqs	Software library	2022-11-30	✘	✘	✘	✘	✔	✔	✔	✔	✔	✔	✔
I4P	Trident	HSM	2022-12-01	✘	✘	✘	🕐	✘	✘	✔	✔	✘	✘	✘
3Key Company	CZERTAINLY	Software	2022-12-03	✘	✘	✘	✘	🕐	🕐	🕐	✘	✘	✘	✘
IBM	4769/CCA/EP11	HSM	2023-01-11	✘	✘	✘	✘	✘	✔	✘	✘	✘	✘	✘

PKI Consortium

Join the PKI Consortium

pkic.org/join



pkic.org/join

PKI Consortium

Post-Quantum Cryptography Conference

PKI Consortium