Post-Quantum

Cryptography Conference

Quantum-Safe Secure Boot: How hard can it be?

Secure boot is hard. Quantum-safe secure boot is even harder. It starts with the choice of a suitable algorithm. On the signature verification side, conflicting regulatory requirements on Post-Quantum/Traditional (PQ/T) hybrid mean there is no silver-bullet, while on the signature generation side, key management challenges and the lack of available end-to-end quantum-safe solutions further complicate the decision process. In this talk we highlight open issues at various stages of the secure boot lifecycle.

Axel York Poschmann
VP of Product at PQShield

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

PKI Consortium
PQC Conference

PQSHIELD

Quantum-Safe Secure Boot

How hard can it be?

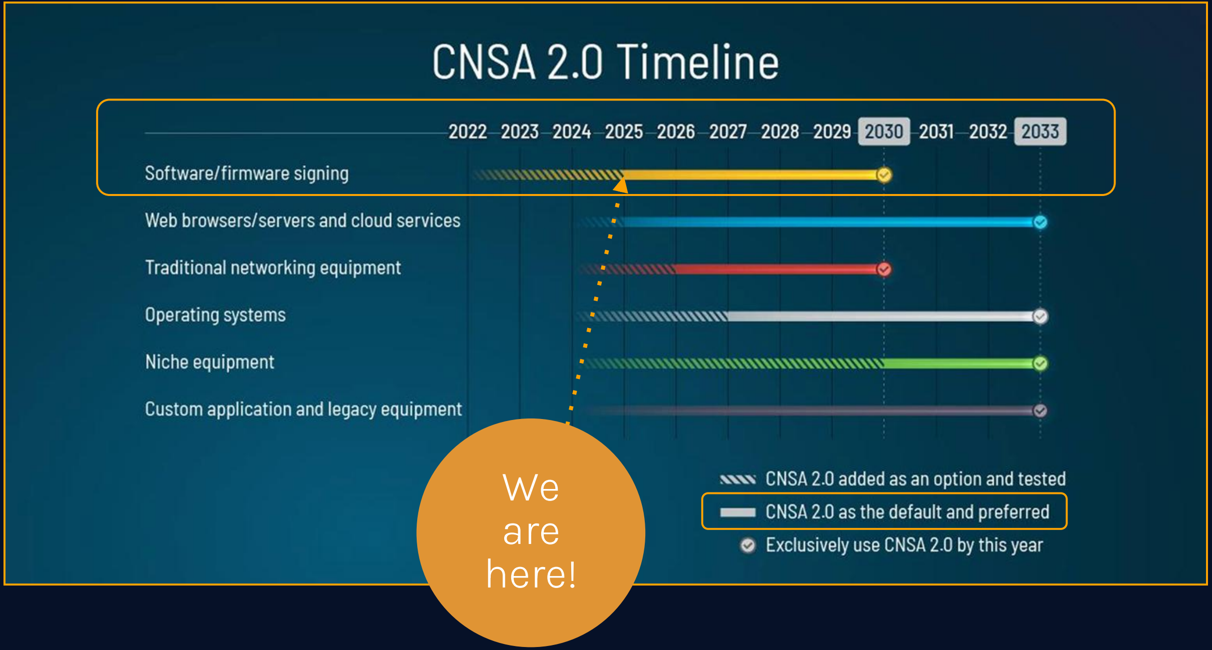
Dr. Axel Y. Poschman

Speaker: about me

Dr. Axel Y. Poschmann
axel.poschmann@pqshield.com
Linkedin

- 2006-2009 U Bochum:
  PhD in Lightweight Cryptography
- 2009-2014 NTU:
  Asst Prof in Cryptographic Engineering
- 2014-2017 NXP Semiconductors:
  Leading internal hardware hacking team
- 2017-2023 xen1thLabs:
  General Manager of the NTVL of the UAE
- 2022 INSEAD:
  Executive MBA
- 2023 PQShield:
  VP of Product

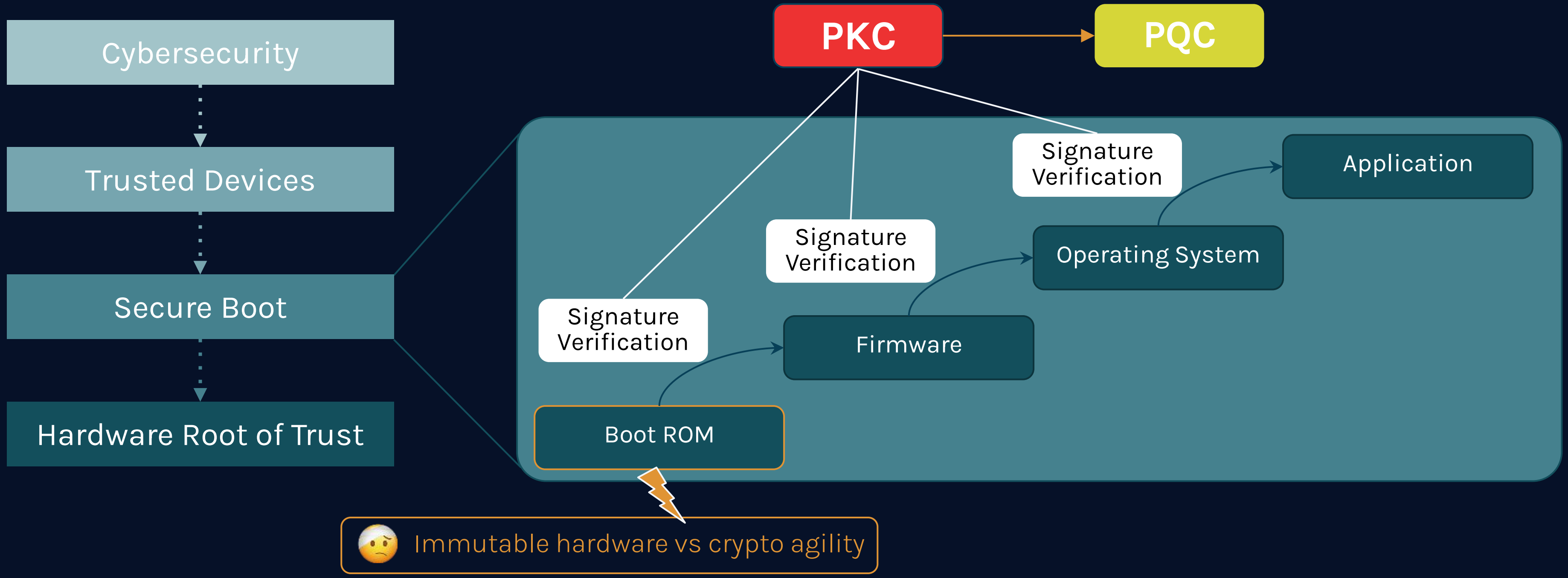
Secure Boot: why act now?



All markets with long product life cycles have to act now:

- Semiconductors
- Automotive
- Defense
- …

Secure Boot: the bedrock of cybersecurity



Secure Boot: full PQC or PQ/T Hybrid?

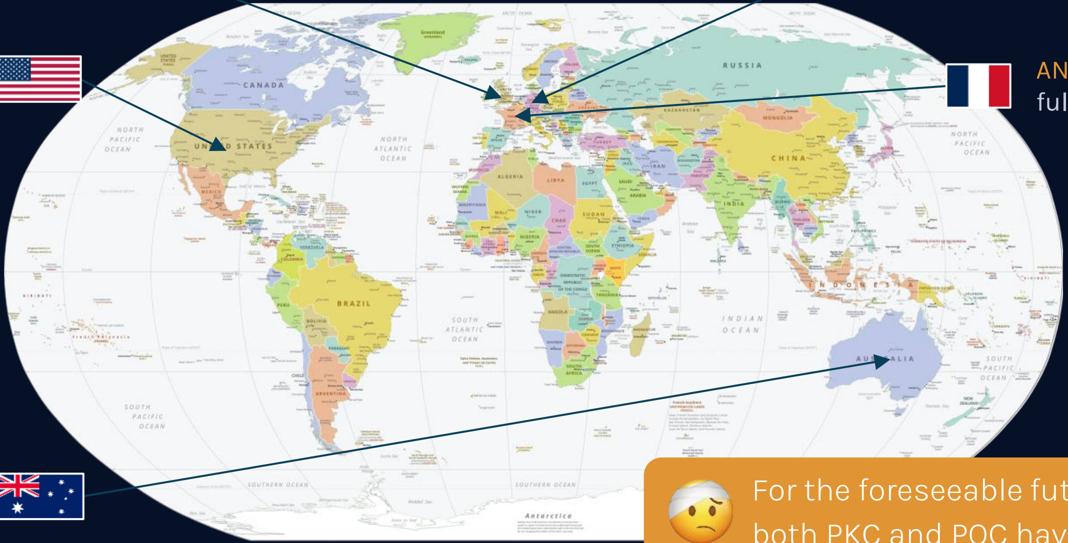
NCSC: Transition to full PQC
PQ/T hybrid should be carefully evaluated

NSA: Transition to full PQC
PQ/T hybrid not recommended (CNSA1.0 for IKEv2 indefinitely)

ASD: Transition to full PQC
PQ/T hybrid not recommended, but not prohibited

BSI: Transition to PQ/T hybrid
optional full PQC at a later stage

ANSSI: Transition to PQ/T hybrid
full PQC after 2030



For the foreseeable future (2030/2035) both PKC and PQC have to be supported

Secure Boot: deprecated and disallowed algorithms

	2025	2026	2027	2028	2029	2030	2031	2032	2033	2034	2035
USA	Fully PQC										
UK	Fully PQC										
AUS	Fully PQC										
FR	PQ/ T Hybrid					Fully PQC					
DE	PQ/ T Hybrid					Fully PQC Optional					

Conflicting regulatory requirements regarding use of RSA and ECDSA

Not to mention additional regional algorithms…

Painpoints: PQ/T Hybrid = 2x complexity

PQ/T Hybrid doubles number of algorithms to support

Increases cost due to increased
- Memory
- Area

Greater computational overhead
- Latency
- Energy consumption

Greater bandwidth overhead
- Latency
- Throughput

Increased complexity results in more difficult:

- Maintenance
- Analysis
- Secure implementation

Protectability: Side-Channel

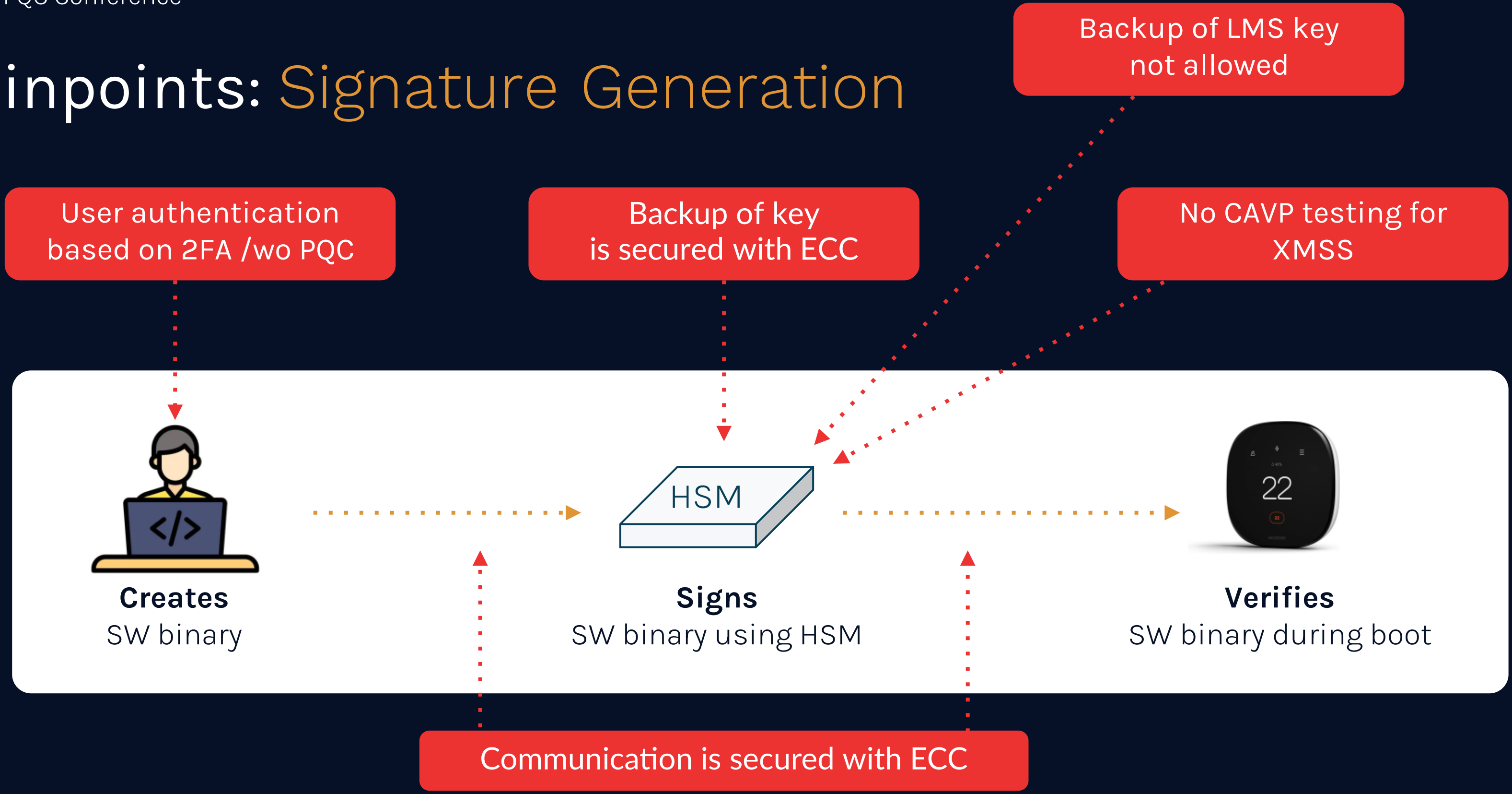
Algorithm	Grade (5= best)	Argument
ML-DSA	3	Operations computing directly on the long term secrets are easy to protect, while ephemeral secrets involve more complicated operations.
FN-DSA	1	Contains floating point operations vulnerable to SCA.
SLH-DSA	5	Due to the structure of HBS, very few SCA attack paths exist.
LMS	5	Similar to SLH-DSA, but with a limited number of traces available.
XMSS	5	Similar to SLH-DSA, but with a limited number of traces available.

PKI Consortium
PQC Conference

Protectability: Fault Attack

Algorithm	Grade (5= best)	Argument
ML-DSA	3	Protection against loop-abort attacks required. Full signature recomputation has relatively low performance cost due to rejection sampling.
FN-DSA	2	Recomputation countermeasure against FA using faulty valid signatures, is more costly than for ML-DSA.
SLH-DSA	1	FA forcing multiple uses of one time signature (WOTS) scheme.
LMS	1	Similar to SLH-DSA but with a limited number of faults.
XMSS	1	Similar to SLH-DSA but with a limited number of faults.

Painpoints: Signature Generation



PKI Consortium
PQC Conference

PQSHIELD

Secure Boot Challenges: no silver bullet in sight

Cybersecurity

Trusted Devices

Secure Boot

Hardware Root of Trust

Painpoint Crypto Agility:
- ROM code cannot be changed once manufactu
- Favours more mature algorithms like LMS

Painpoint Government Compliance:
- SLH-DSA and FN-DSA not all ment use
- XMSS not FIPS certifia

Painpoint PQ/T Hybri
- France ers mandate PQ/T hybrid
- Do e for ML-DSA and FN-DSA

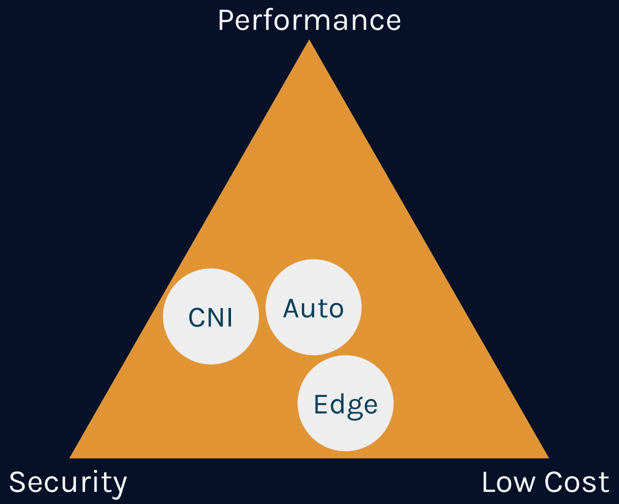
ure Generation:
- ware signature generation requires using an HSM
- No practical HSM for LMS and XMSS available

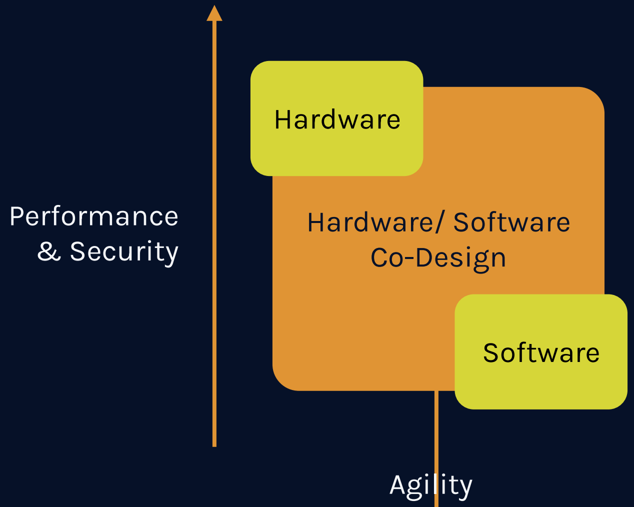
There is no one-size-fits-all solution

Algorithmic choice: no silver bullet in sight

Algorithm	CNSA2.0	PQ/T Hybrid	SCA	Fault	CAVP/ACVP	Key Backup
ML-DSA	V	V	3	3	V	V
FN-DSA	X	V	1	2	X	V
SLH-DSA	X	X	5	1	V	V
LMS	V	X	5	1	V	X
XMSS	V	X	5	1	X	X

Secure Boot: trade-offs, hardware, and software





Use-case specific optimization goals

- Performance
- Security
- Cost

Optimized integrated solution

- Hardware for performance and security
- Software for agility

Take away: optimized, flexible HW/SW solutions required

- CNSA2.0 already mandates quantum-safe secure boot today
- Secure boot is the bedrock of cybersecurity
- Different regulatory timelines -transition and deprecation- require configurability
- For the foreseeable future a zoo of algorithms -PKC and PQC- need to be supported
- No silver bullet available

Flexible HW/SW co-design solutions optimized for specific use cases required

PQShield

think openly, build securely