

From Shadow Crypto to Crypto Agility

How PQC migration can become an opportunity

Reto Stäubli | Executive Vice President Solutions & Services | Securosys SA



Shadow IT and Crypto Sprawl

Shadow IT

What: IT tools or services used without the knowledge or approval of IT

Why: Teams look for quick solutions to their needs

Result: IT may not know what is in use

Crypto sprawl

What: Keys and certificates created and used across many applications, systems and teams

Why: The number of cryptographic assets grows over time

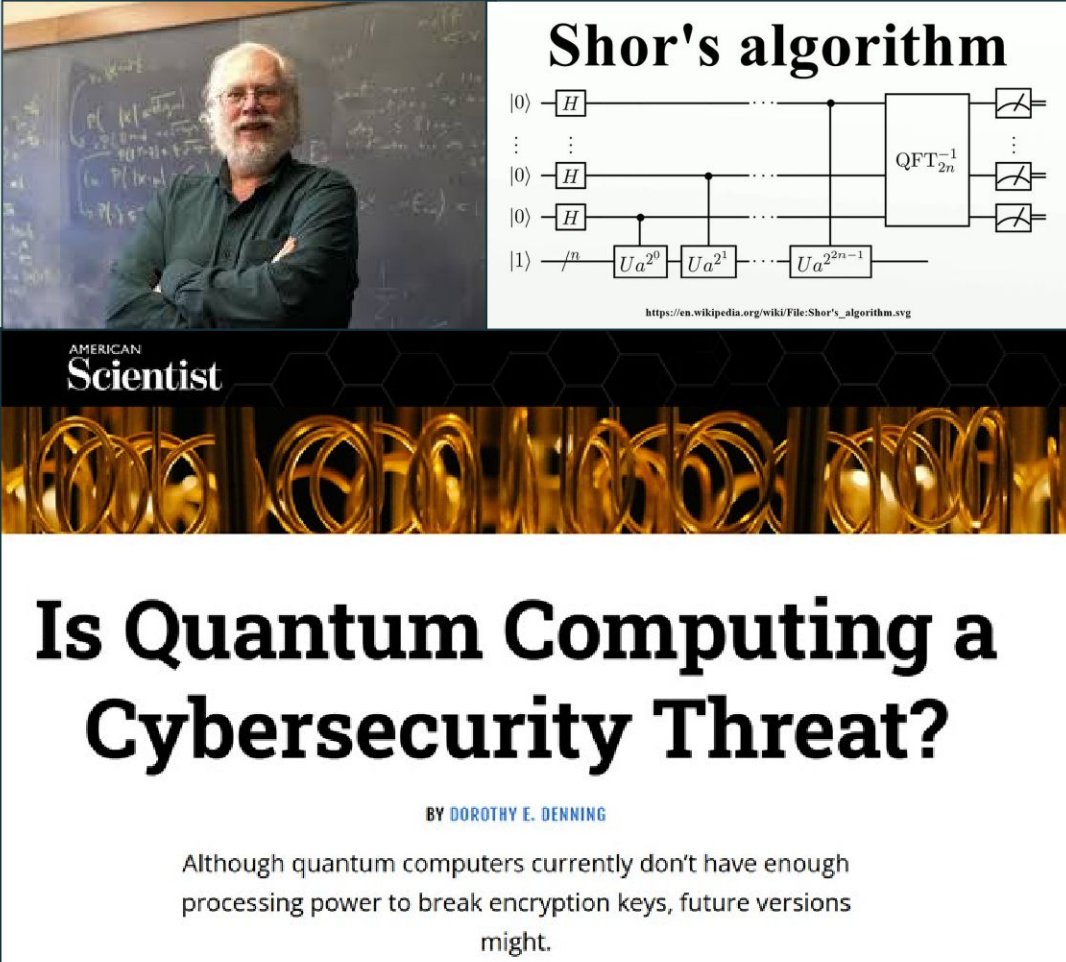
Result: No complete overview of cryptographic assets

With the upcoming Post Quantum Cryptography migration, this becomes an important challenge.

Should You Be Worried?

- / Existing signing algorithms can be broken with Quantum Computers
 - Shor's algorithm (1994) allows quantum computers to efficiently factor large prime numbers
 - Today's cryptography will need to be replaced
 - Algorithms **remain secure and have not yet been broken**

- / No consensus for when we might reach "Q-Day"
 - "Early 2030s" – BSI, Germany
 - Guidance for transition plans to follow



Shor's algorithm

$|0\rangle$ $|0\rangle$ $|0\rangle$ $|1\rangle$

H H H Ua^{2^0} Ua^{2^1} $Ua^{2^{2n-1}}$ QFT_{2n}^{-1}

https://en.wikipedia.org/wiki/File:Shor's_algorithm.svg

AMERICAN
Scientist

Is Quantum Computing a Cybersecurity Threat?

BY DOROTHY E. DENNING

Although quantum computers currently don't have enough processing power to break encryption keys, future versions might.

NIST Guidance

/ Guidance for the digital signature standards commonly in use today:

Algorithm	Parameters	Transition Guidance
RSA (PKCS #1 v1.5 & PSS)	112 bits of security (2048-bit)	Deprecated end Dec 2030 Disallowed end Dec 2035
	128 bits of security (3072-bit) and above	Disallowed end Dec 2035

/ Similar guidance recently from the BSI in Germany:

Scheme	RSA	DLIES	ECIES	DH	ECDH
Key Length l in bits	3000	3000	250	3000	250
Reference	[91]	[2]	[2, 67]	[2, 118]	[2, 118]
More detailed information in	Section 2.3.2	Section 2.3.3	Section 2.3.4	Section 2.3.5	Section 2.3.6
Recommended until	2031	2031	2031	2031	2031

Table 2.2: Recommended classical asymmetric encryption and key derivation schemes as well as key lengths and normative references.

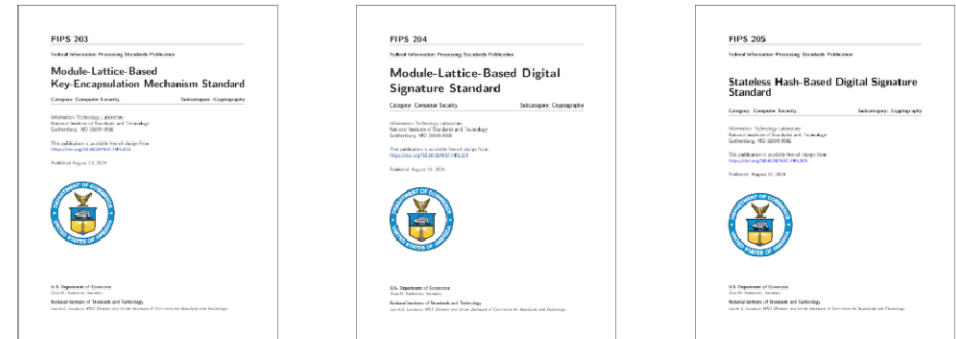
Deprecated end Dec 2030
Disallowed end Dec 2035

Disallowed end Dec 2035

Disallowed end Dec 2035

What Should We Use Instead?

- / The 'Post-Quantum Cryptography Standardization' competition announced by NIST in 2016
- / From 69 submissions, 3 'QC safe' algorithms selected in 2024
 - **FIPS 203:** ML-KEM (*CRYSTALS-Kyber*)
 - **FIPS 204:** ML-DSA (*CRYSTALS-Dilithium*)
 - **FIPS 205:** SLH-DSA (*SPHINCS+*)
 - More algorithms arriving, including FALCON (FN-DSA) and HQC
- / Migration will not be a trivial project and requires careful planning
 - Could take as long as 5-10 years



- / NOTE:
"the existing algorithm standards for symmetric cryptography are less vulnerable to attacks by quantum computers. NIST does not expect to need to transition away from these standards as part of the PQC migration"

Anything Else I Should Worry About?

“Harvest Now, Decrypt Later”

1 Capture

2 Store

3 Wait

4 Decrypt

5 Exploit



The signals are converging fast

Regulatory Direction

United States

- [NIST IR 8547](#) (draft, Nov 2024): quantum-vulnerable algorithms deprecated after 2030, disallowed after 2035
- [Executive Order 14412](#) (22 Jun 2026) »Securing the Nation Against Advanced Cryptographic Attacks"
mandates: key establishment by **31 Dec 2030**, digital signatures by **31 Dec 2031** (high-value and high-impact federal systems)

Europe and Germany

- [EU PQC roadmap](#): national roadmaps by end 2026, high-risk use cases by 2030, full transition by 2035
- [EU Cyber Resilience Act](#): essential requirements apply from 11 Dec 2027
- [France \(ANSSI\)](#): plans to stop certifying security products without quantum-safe cryptography from 2027
- [Germany \(BSI TR-02102\)](#): RSA-2048 and ECC-224 not recommended after 2031

United Kingdom

- [NCSC](#): **discovery and an initial plan by 2028**
- Early, highest-priority migration by 2031
- Complete migration by 2035

Switzerland

- [NCSC technology brief](#) (8 Dec 2025): harvest-now-decrypt-later “argues strongly in favour of implementing PQC”
- [Federal PKI](#) (BIT): migration in planning phase
- [FINMA](#) (9 Jul 2026): institutions need a clear PQC strategy and roadmap
- [SIX](#) (Apr 2026): “We absolutely have to get to grips with PQC... right away”

NIST IR 8547: <https://csrc.nist.gov/pubs/ir/8547/ipd>

PQC Readiness of Common Tools

Tool	Key exchange	Signatures	Status
OpenSSL	Hybrid X25519MLKEM768 default since 3.5	ML-DSA, SLH-DSA since 3.5	LTS until April 2030
OpenSSH	mlkem768x25519 default since 9.9	Experimental composite ML-DSA-44 + Ed25519 since 10.4; hybrid in 10.6 (Oct 2026)	Default since April 2025
IKEv2 (VPN)	ML-KEM hybrid still an IETF draft (v09, July 2026)	PQC authentication draft at version 12 (Aug 2026), in RFC Editor queue	Cisco IOS XR 26.1.1 and FortiOS 7.6.6+ interoperate with Cloudflare ML-KEM
Browsers (Chrome, Edge, Firefox, Safari)	Hybrid key exchange default	Not yet	Chrome plans Merkle Tree Certificates
TLS servers (NGINX, Traefik)	NGINX Default with OpenSSL 3.5+; Traefik with Go 1.24+	Blocked on Go support (Traefik)	Traefik since 3.4.2; NGINX with OpenSSL 3.5+
Code signing	Not applicable	ML-DSA (FIPS 204) and LMS/XMSS (NIST SP 800-208) standardized	Tool support to be confirmed

OpenSSL 3.5 release notes: <https://openssl-library.org/news/openssl-3.5-notes> ; OpenSSH 10.0 release notes: <https://www.openssh.org/txt/release-10.0> ; IETF draft-ietf-ipsecme-ikev2-mlkem: <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-mlkem> ; IKEv2 PQC signature authentication draft: <https://datatracker.ietf.org/doc/html/draft-ietf-ipsecme-ikev2-pqc-auth> ; Cloudflare IPsec ML-KEM changelog: <https://developers.cloudflare.com/changelog/post/2026-04-30-ipsec-post-quantum-third-party/> ; Cloudflare PQC support table: <https://developers.cloudflare.com/ssl/post-quantum-cryptography/pqc-support/> ; Cloudflare, “Post-Quantum Encryption”: <https://radar.cloudflare.com/post-quantum>

The Migration Challenge: Shadow Crypto

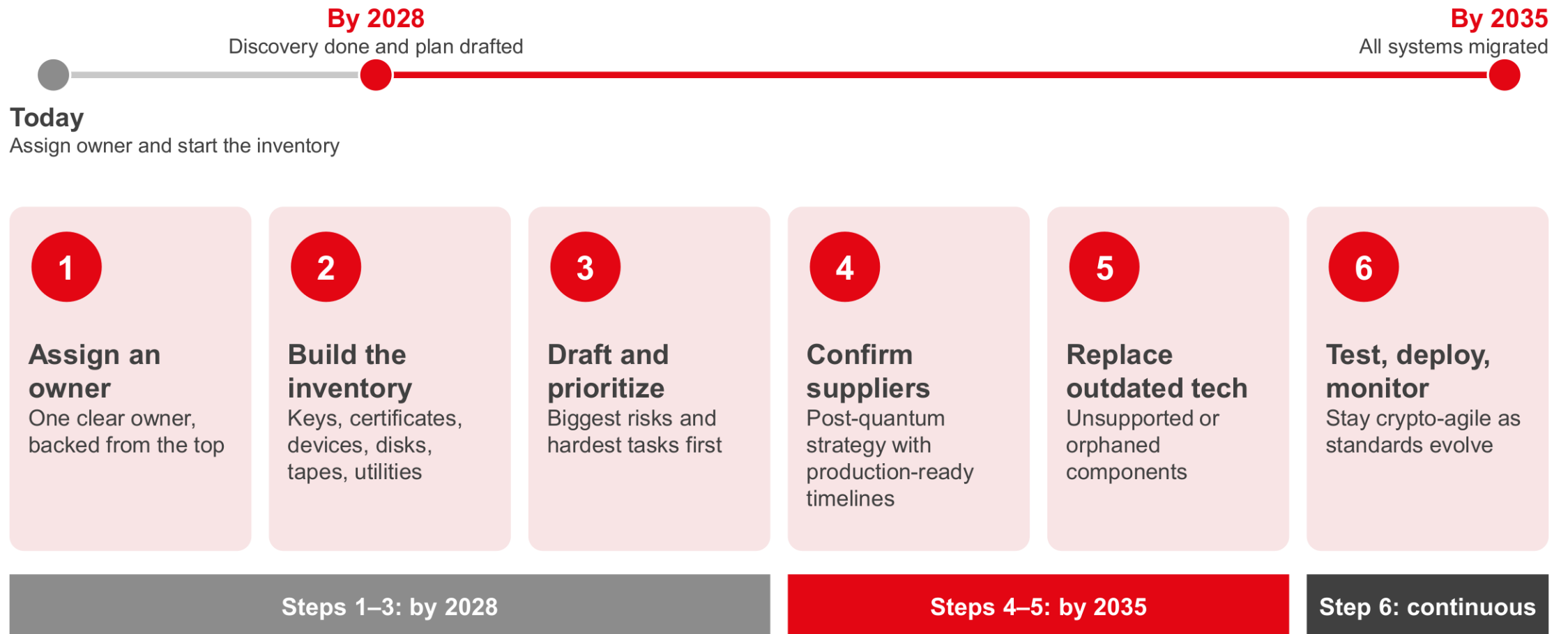
- / Keys and certificates outside central control
- / Found in applications, cloud services, certificates, HSMs and suppliers
- / You cannot migrate what you cannot see
- / You cannot protect what you do not know you have

Where keys and certificates live today



Central key management (KMS): missing at most organisations

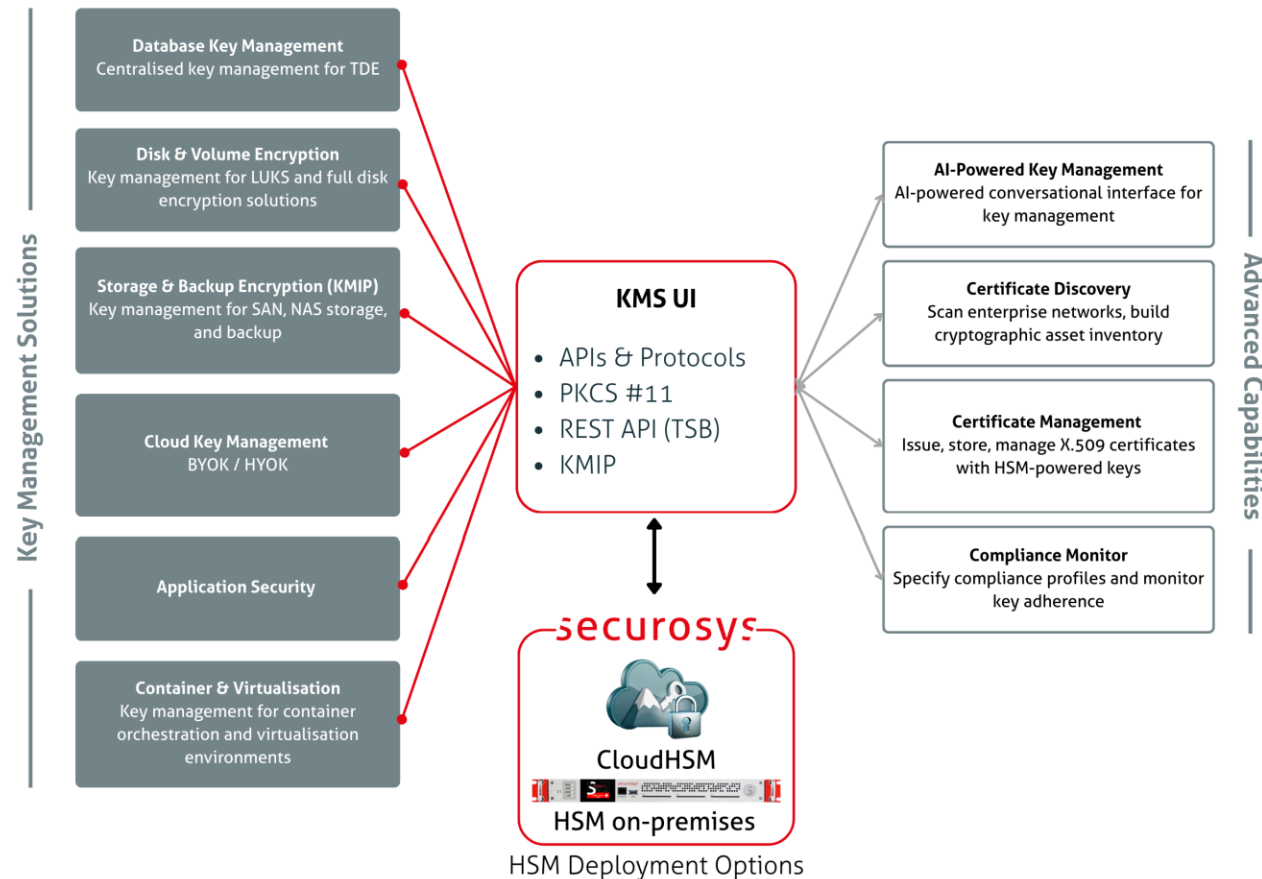
Developing Your Migration Plan



Medium Quantum Sundays 62: <https://medium.com/@adnanmasood/quantum-sundays-62-enterprise-blueprint-for-post-quantum-cryptography-migration-3e75e9d85136> ; The Applied Quantum PQC Migration Framework & Methodology: <https://pqcframework.org/>

One Central, Crypto-Agile Key Store

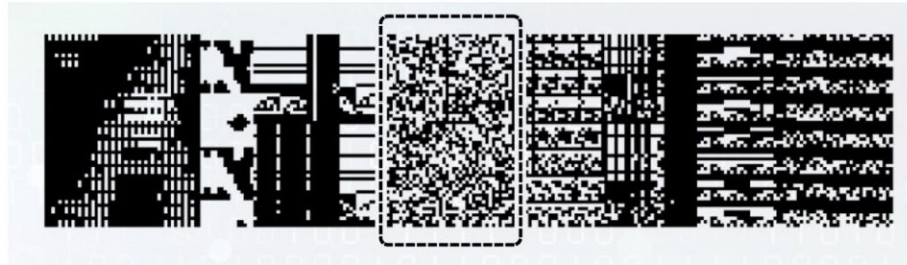
During the migration, build one central place for your keys, with crypto agility at its core.



Why Hardware Security?

/ Software keys = soft security

- Keys are exposed and vulnerable
- Easy to see with the naked eye, trivial for an algorithm or an AI Agent



“Playing “Hide and Seek” with Stored Keys” (1999)

Adi Shamir, Nicko van Someren

<https://www.digiater.nl/openvms/decus/vmslt99a/sec/keyhide2.pdf>

/ Hardware Security Modules: validated and certified

/ Important: Your chosen Key Management solution needs to support hardware-based key protection

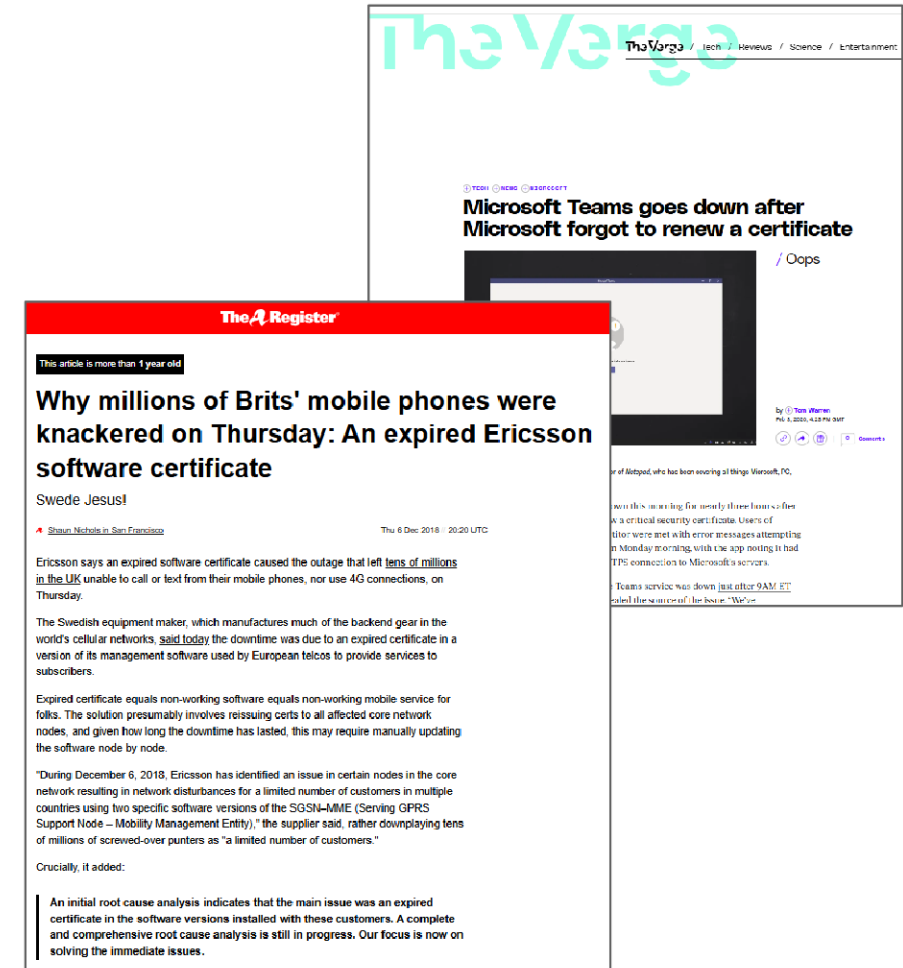


Certificate Management Matters

- / Digital Certificates (x509v3) add the identity
 - Also specify policies and **expiry dates!**
- / Certificates must be centrally monitored and managed to prevent outages.

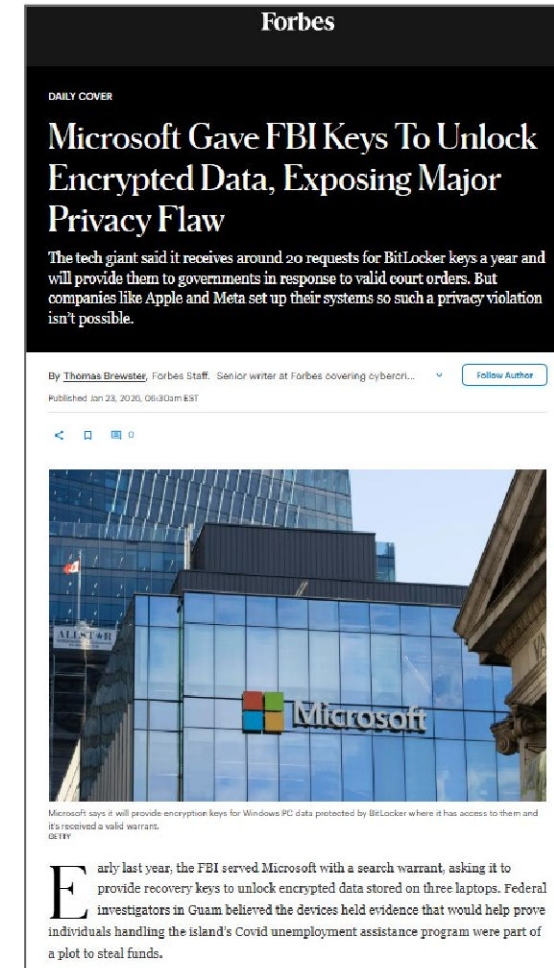
Real world examples:

- Microsoft Teams outage, 2020
- Ericsson UK mobile disruption, 2018
- Apple services issue, 2023
- / CA/Browser Forum changes
 - **March 15, 2026:** 200 days
 - **March 15, 2027:** 100 days
 - **March 15, 2029:** 47 days



Cloud & Digital Sovereignty

- / Ensure 'data sovereignty' - retain control over cloud-hosted data
- / **BYOK** and **HYOK** allow customers to:
 - Generate encryption keys in-house
 - Provide limited-time access to cloud providers
 - Withdraw access to prevent misuse or offshore disclosure
 - Reclaim, cancel or migrate data
- / **HYOK** (such as DKE, XKS or 'Cache Only Keys'):
 - Key held directly by you
 - Ability to cut off third-party access at any time



Summary

- / **Cryptographic keys are central to the security solutions deployed today**
- / **Find your keys and take control of them**
- / **Manage keys in a KMS, and keep the most important keys in hardware**
- / **Keep certificates under central control and automate renewal**
- / **Don't ignore your cloud deployments**
- / **Build crypto agility into every new system**
- / **And start the PQC migration now**

“Start while it's a project, before it's a crisis.»

Marin Ivezic, CEO, Applied Quantum

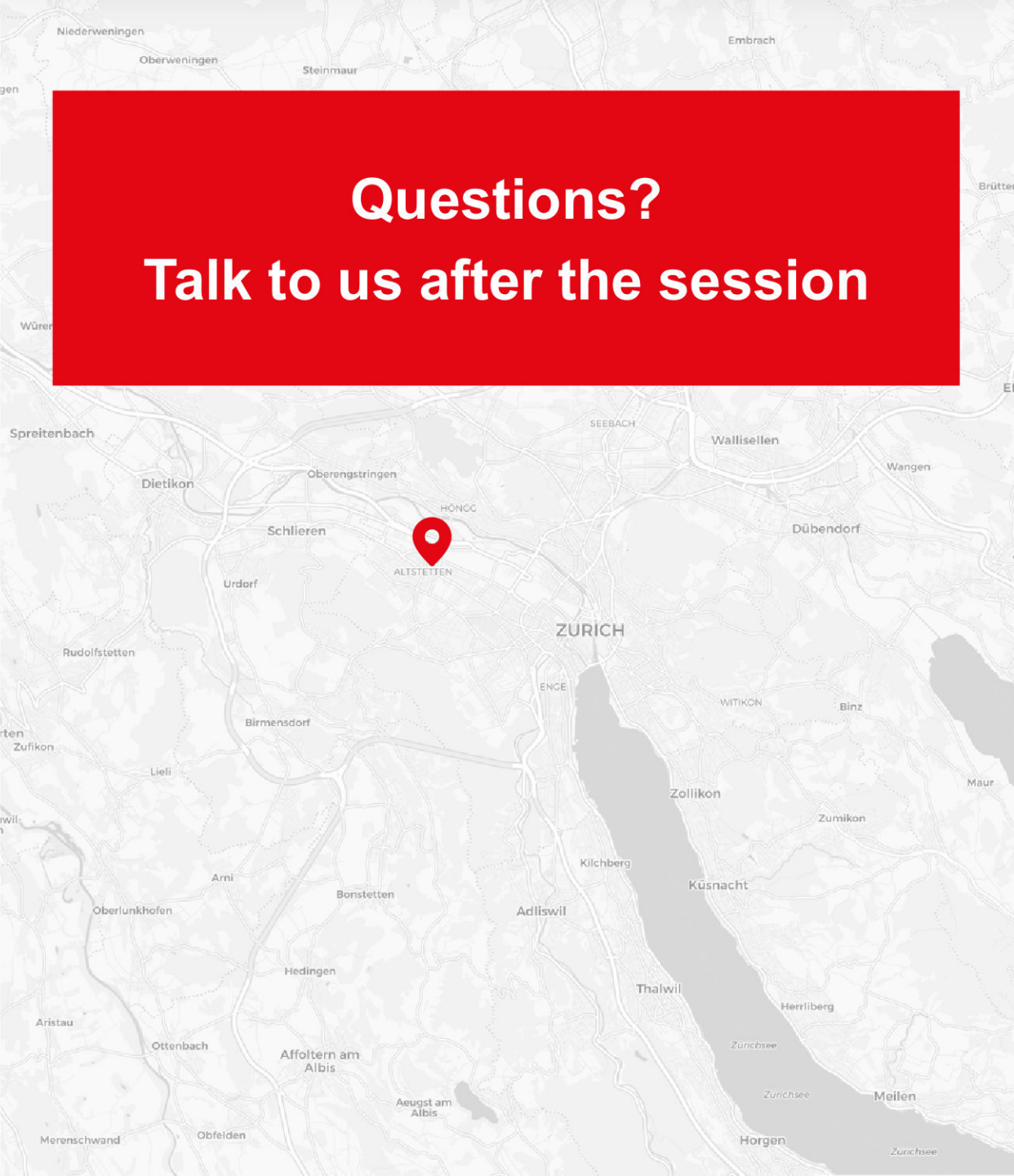
Thank You!

📍 Max-Högger-Strasse 2
8048 Zürich
Switzerland

☎ +41 44 552 31 00

✉ info@securosys.com

Some illustrations were created with AI tools. All content was reviewed by the speaker.



Questions?
Talk to us after the session

What Is a Key Management System?

- / Integrates with applications and secure devices
 - via **KMIP** protocol - Key Management Interoperability Protocol (OASIS)
- / A capable KMS provides:
 - Secure key **generation** and **backup**
 - Lifecycle management (**rotation & expiry**)
 - **Compliance**
 - **Discovery**
 - Secure **access controls**
 - **Logging** and **audit** functionality

A well-managed KMS is essential for PQC migration and long-term crypto agility.



Cryptography Key Drivers in IT

Compliance

- / GDPR
- / Industry regulation: Health, Finance, Payment
- / Qualified signature

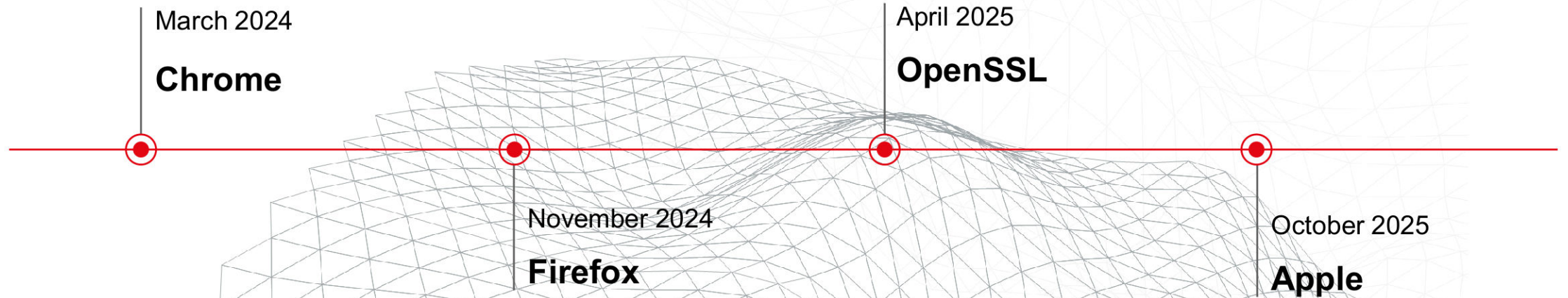
Privacy

- / Confidentiality
- / IP Protection
- / Network encryption (TLS, VPN)
- / Blockchain

Cyber Protection

- / Encryption to prevent data breaches and theft (data at rest, DB column & TDE, drive, cloud data, DKE)
- / Access control (Oauth, JWT)
- / Verifiable authenticity (sMIME, document signing)

Reality Check: You're Already Using PQC



“over 50% (and rising!) of human traffic is protected”

Cloudflare - <https://blog.cloudflare.com/pq-2025/>

“eight of the Top 10 websites now support X25519MLKEM768”

Prof Bill Buchanan OBE - <https://medium.com/asecuritysite-when-bob-met-alice/>

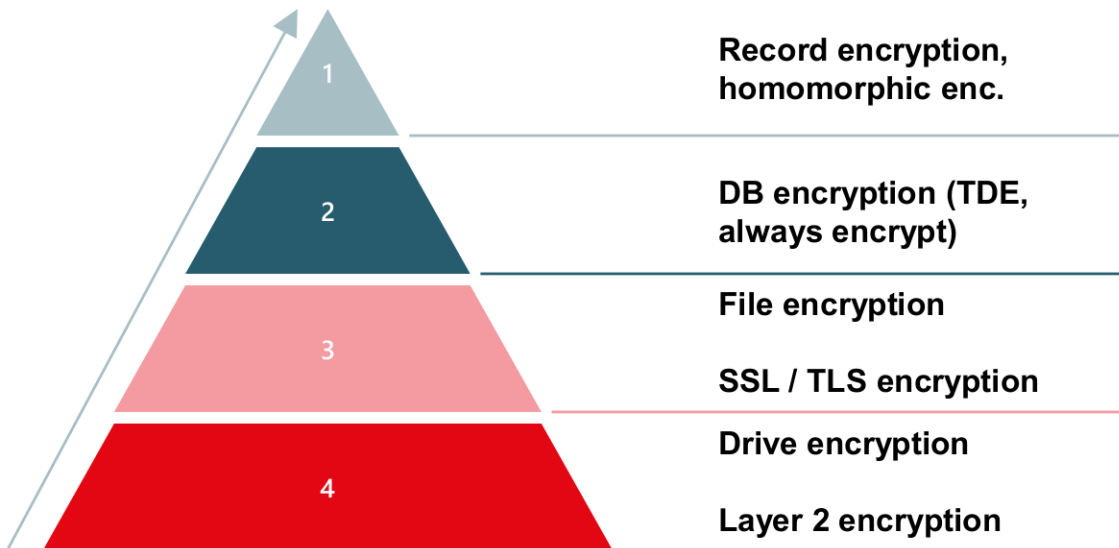


ChatGPT



Securing the Digital Space

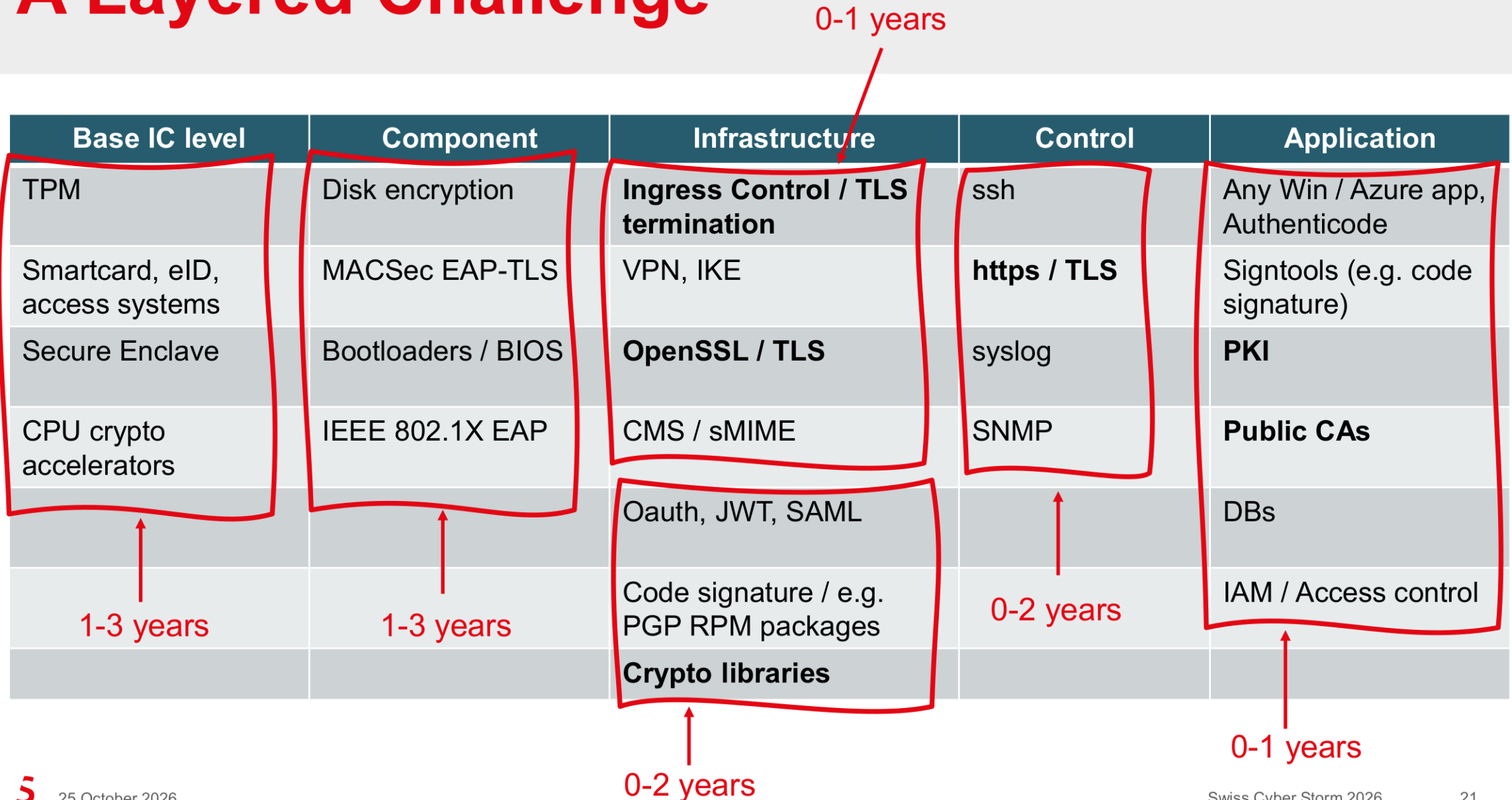
/ Encryption



/ Digital Signature



A Layered Challenge



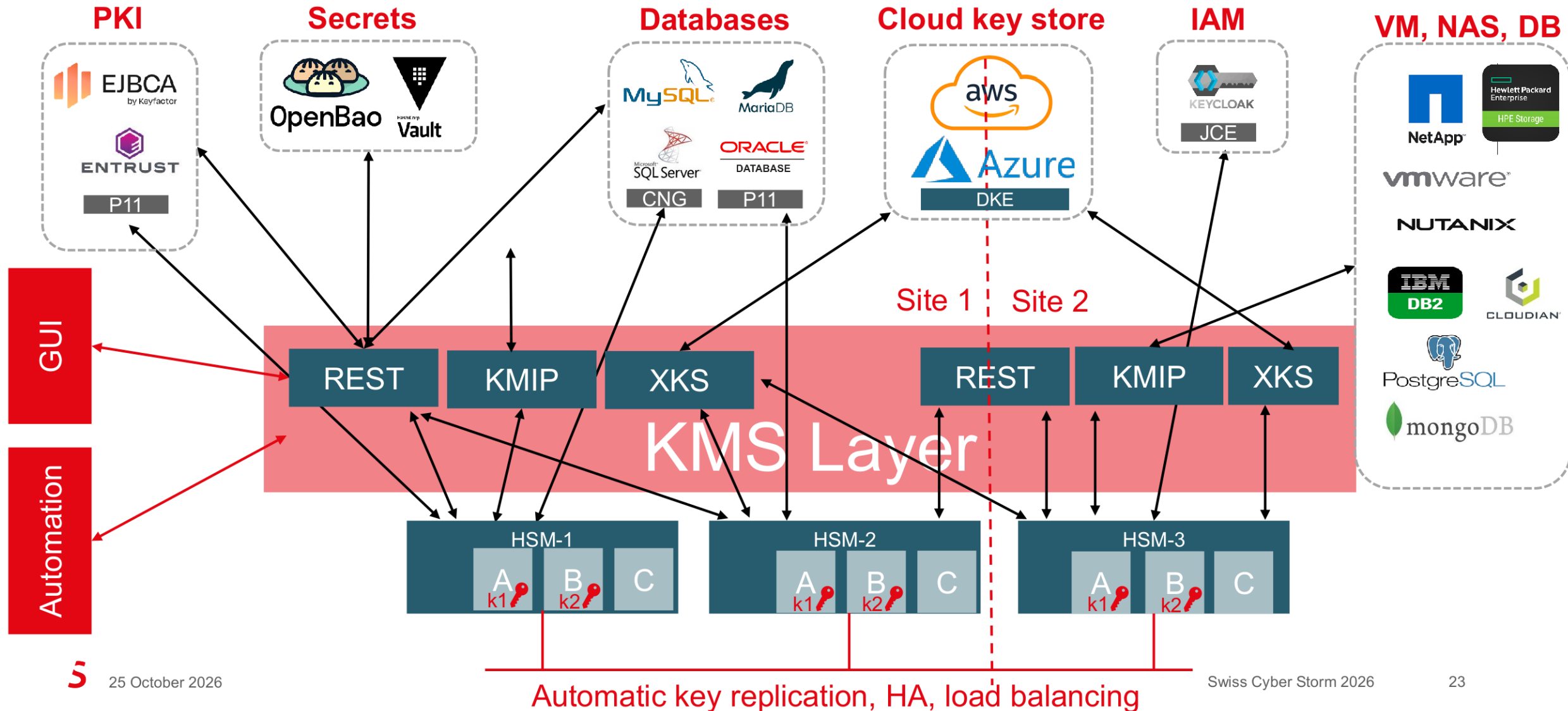
PQC sizes and performance

Algorithm	Security	Standards	Pub key (bytes)	Private key (bytes)	Signature size	Sig time O(ms)
RSA 3072	128b	FIPS 186-5	384	384	384	10
ECC (384)	192b	FIPS 186-5	96	48	256	.5
ML-DSA	L5	FIPS 204	2,6KB	4,8KB	4.6KB	.5
SLH-DSA (256)	L2-L5	FIPS 205	32- 64	$O(n*pk)$	50.0KB	100
LMS/XMSS	L2-L5	SP800-208	32-128	$O(n*pk)$	$\text{Log}_2(n)*32$	100
ML-KEM	L5	FIPS 203	2,6KB	4,8KB	4.6KB	.5
FN-DSA	L5	FIPS 206*	1,8KB	2KB	1.3KB	.5

Performance

Message size

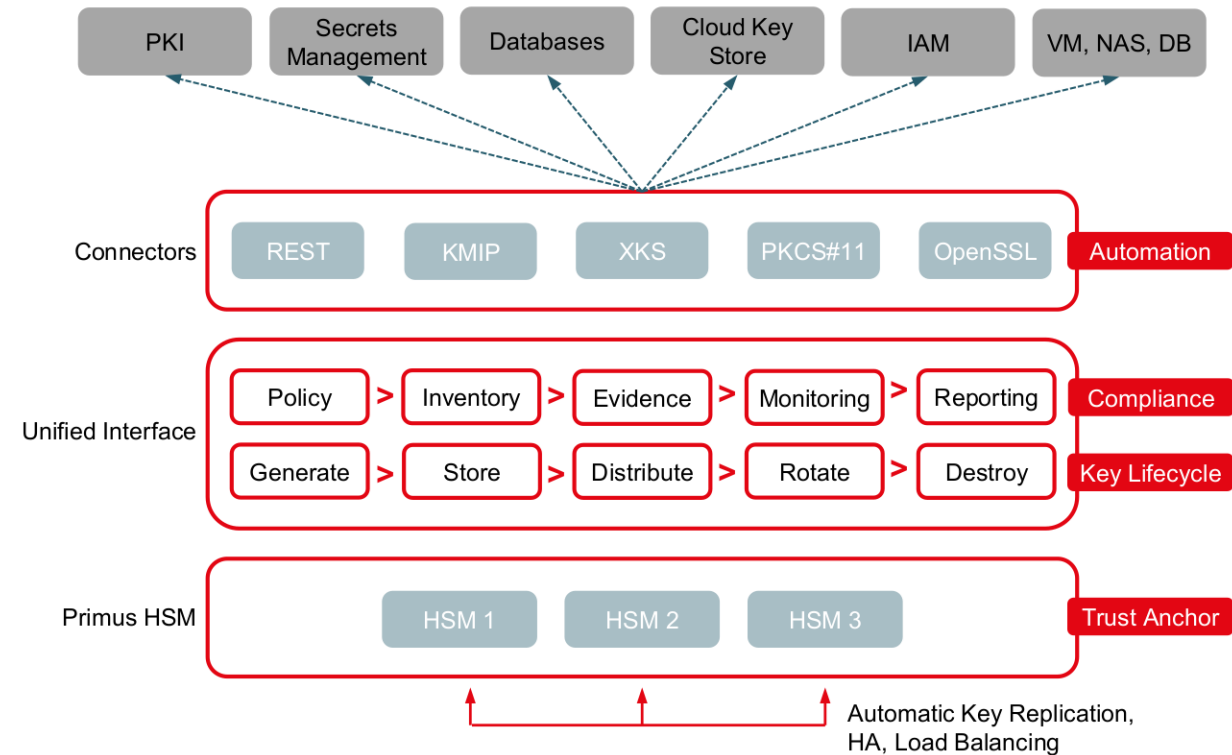
Unified Key Store, Many Access Protocols



Enterprise Integration

/ One KMS for many environments

- **PKI & certificates:** issuance, storage, templates, and expiration monitoring
- **Databases:** TDE master key management
- **Storage & backup:** KMIP-based integration
- **Disk & volume encryption:** LUKS and full-disk encryption
- **Cloud:** BYOK and HYOK scenarios
- **Containers & virtualization:** etcd, secrets, VM encryption, virtual SAN
- **Applications:** REST API, PKCS#11, JCE, MS-CNG



Step 1: Know What You Have

- / Inventory every key, certificate and algorithm
- / Record which systems and owners use them (CBOM)
- / Use discovery tools to scan the network
- / Keep the list maintained, not a one-time exercise
- / FINMA expects a comprehensive and maintained cryptographic inventory

More Security Means More Keys...

- / Organisations have faced increasing regulations around data security
 - **GDPR**: Article 32 requires "*appropriate technical and organisational measures*"
 - **Swiss FADP (revised)**: appropriate technical measures for personal data
 - **PCI DSS**: Mandates strong encryption for cardholder data
- / **‘Crypto Sprawl’** – a plethora of security solutions using cryptography, holding vital key material

