Demystifying the Quantum Threat for Network Operators

Rakesh Kandula, Technical Marketing Engineer (Cisco)

October 23rd, 2024

Agenda

1. Quantum threat to cryptography
2. Various areas of impact
3. Solutions for Quantum Readiness

Famous Quotes

Some say quantum computers are a fantasy

- "This 'telephone' has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us." --Western Union internal memo, 1876.
- "Heavier-than-air flying machines are impossible." --Lord Kelvin, president, Royal Society, 1895.
- "I think there is a world market for maybe five computers." --Thomas Watson, chairman of IBM, 1943
- "Computers in the future may weigh no more than 1.5 tons." --Popular Mechanics, forecasting the relentless march of science, 1949
- "I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a fad that won't last out the year." --The editor in charge of business books for Prentice Hall, 1957
- "But what ... is it good for?" --Engineer at the Advanced Computing Systems Division of IBM, 1968, commenting on the microchip.
- "There is no reason anyone would want a computer in their home." --Ken Olson, president, chairman and founder of Digital Equipment Corp., 1977

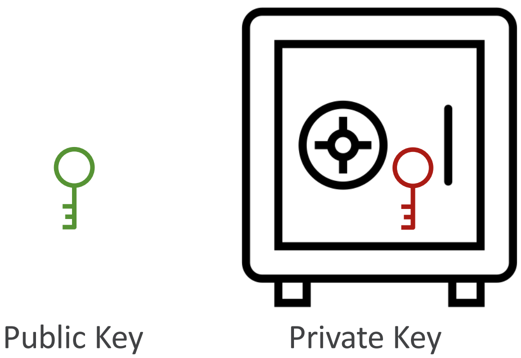
Source: https://www.ittc.ku.edu/~evans/stuff/famous.html

Quantum threat to cryptography

People are making incremental efforts
in developing a quantum computer.

Once they have one sufficiently
large and reliable, they could use it to
break current encryption (public key algorithms).

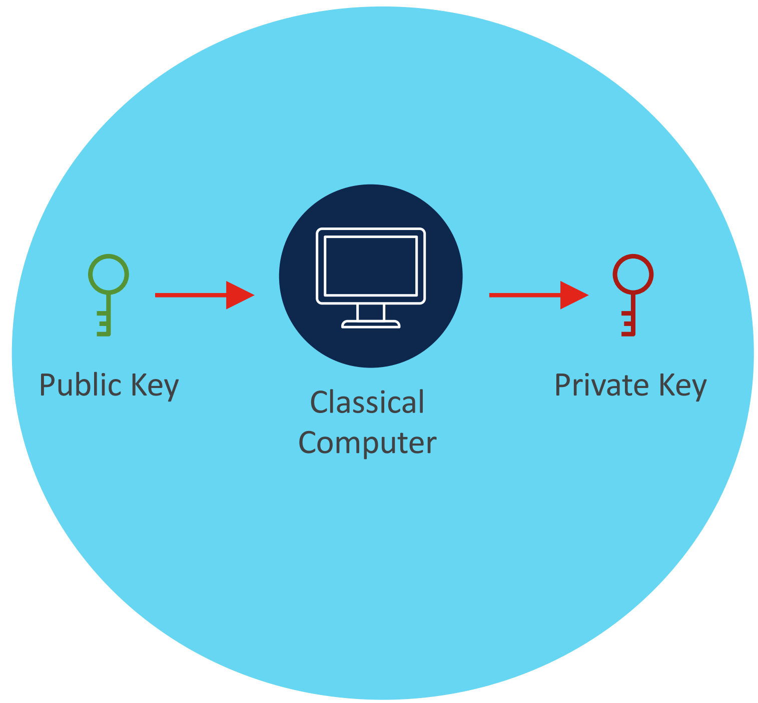
Public Key Cryptography – With Classical Computers



Digital Signatures → Encrypt with private key

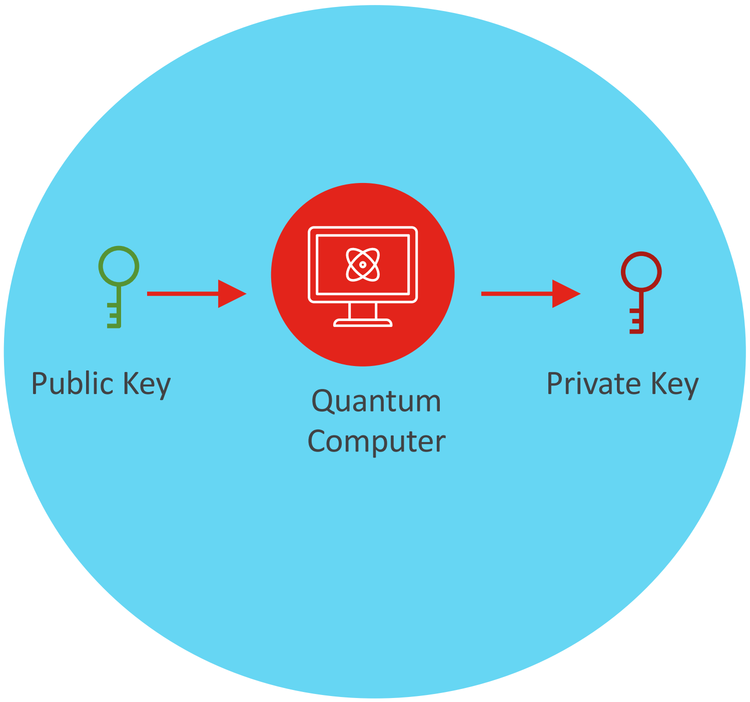
Identity → Encrypt with private key

Key Negotiation → Encrypt with peer's public key



Takes few years for the computation

Quantum Threat to Public Key Cryptography



This needs a **C**ryptographically **R**elevant **Q**uantum **C**omputer (CRQC) that is commercially feasible.

Might take just few hours for the computation

Areas of impact

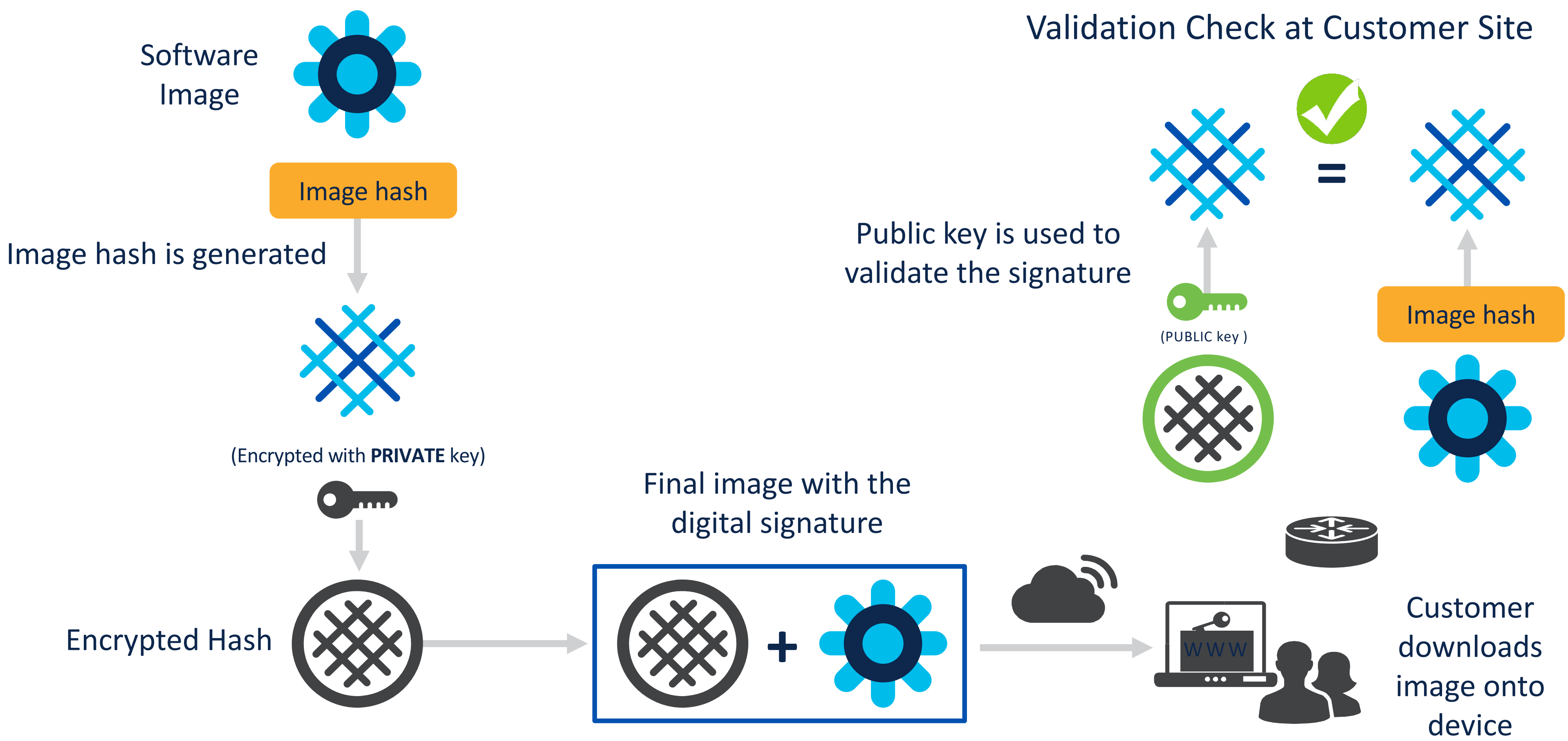
Scope of post-quantum threat

Firmware/software integrity	Identity	Transport security
• Firmware and NOS image signing • Secure Boot • IMA* keys, software image posting, etc.	• Device identity (like SUDI**) • Server certificates • Individual identities	• MACsec • IPsec • TLS • SSH

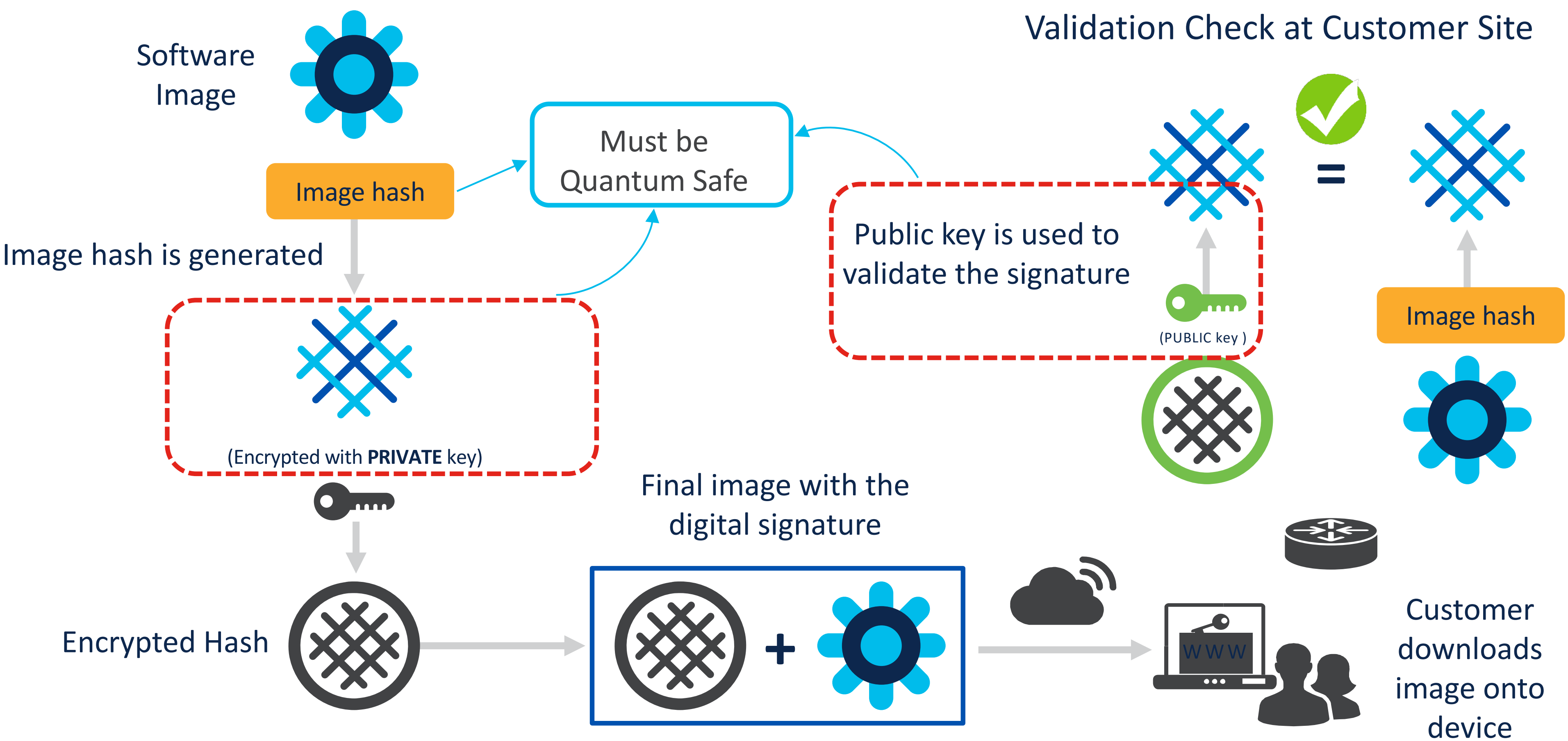
*IMA – Integrity Measurement Architecture

**SUDI – Secure Unique Device Identifier

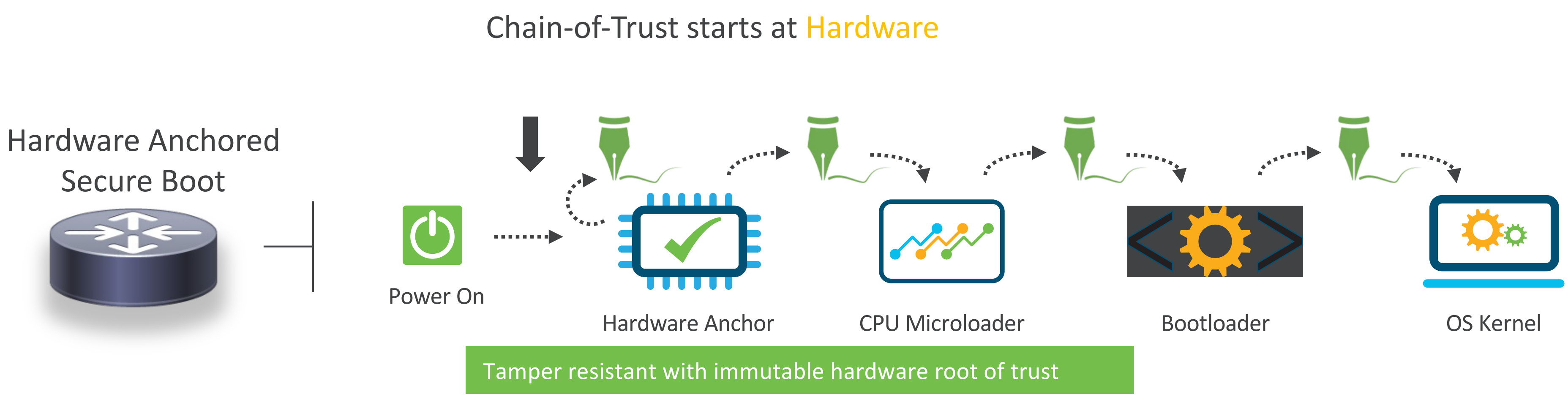
Firmware/Software Integrity – Generic Workflow



Firmware/Software Integrity – Quantum Threat



Quantum Threat To Secure Boot Workflow

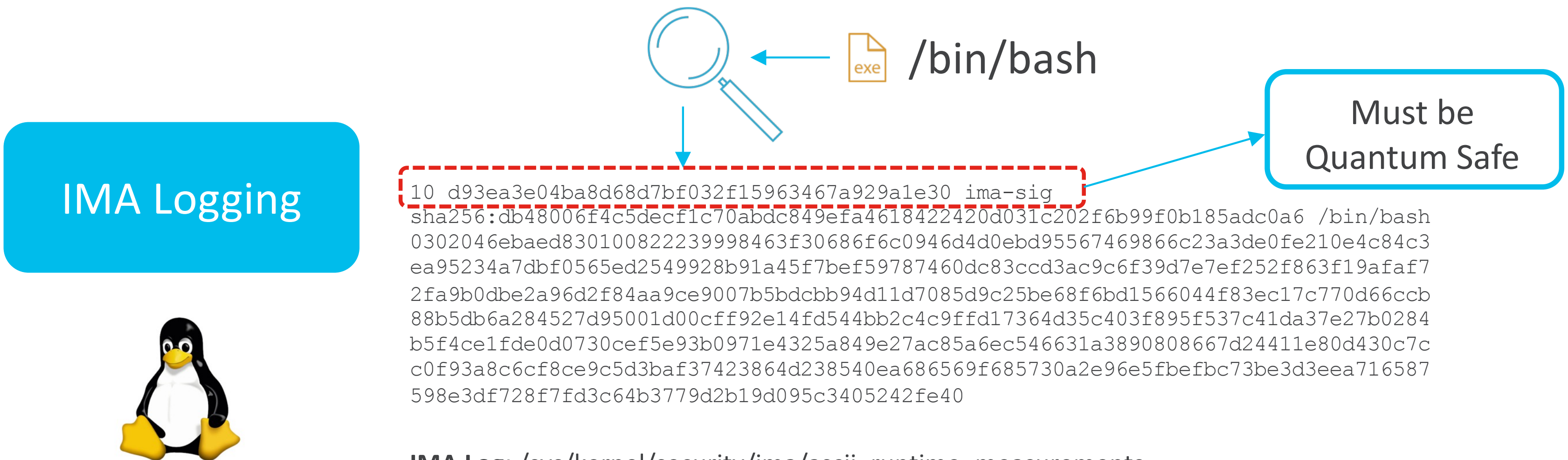


The Quantum threat

1. Signing of any of the secure boot artefacts could be impacted
2. Compromised images could be signed by bad actors if they can compute the private key used for signing

Tampering of any boot stage would imply the device cannot be trusted anymore.

Quantum Threat To Runtime Integrity – IMA*




```
10 d93ea3e04ba8d68d7bf032f15963467a929a1e30 ima-sig
sha256:db48006f4c5decf1c70abdc849efa4618422420d031c202f6b99f0b185adc0a6 /bin/bash
0302046ebaed830100822239998463f30686f6c0946d4d0ebd95567469866c23a3de0fe210e4c84c3
ea95234a7dbf0565ed2549928b91a45f7bef59787460dc83ccd3ac9c6f39d7e7ef252f863f19afaf7
2fa9b0dbe2a96d2f84aa9ce9007b5bdcbb94d11d7085d9c25be68f6bd1566044f83ec17c770d66ccb
88b5db6a284527d95001d00cff92e14fd544bb2c4c9ffd17364d35c403f895f537c41da37e27b0284
b5f4ce1fde0d0730cef5e93b0971e4325a849e27ac85a6ec546631a3890808667d24411e80d430c7c
c0f93a8c6cf8ce9c5d3baf37423864d238540ea686569f685730a2e96e5fbefbc73be3d3eea716587
598e3df728f7fd3c64b3779d2b19d095c3405242fe40
```

IMA Log: /sys/kernel/security/ima/ascii_runtime_measurements

1. IMA which ensures every file loaded during runtime goes through a measurement / appraisal
2. Kernel must have the ability to measure and verify the signature and extend the PCRs in TPM chip
3. IMA violations will be logged in audit.log

*IMA – Integrity Measurement Architecture

Firmware/Software Integrity – The Path Forward

PQ Hashing

1. The effort to find pre-image hash by a quantum computer is n/2 or n/3 (with Grover's algorithm) where n is the output size of the hash.

2. This would mean we need at least 384-bit hashes to be used to get the 128-bit equivalent security in a post quantum world.

3. Recommendation would be to use SHA-512 hashes wherever possible.

PQ Signatures

1. NIST approved PQ safe algorithms to be adopted.

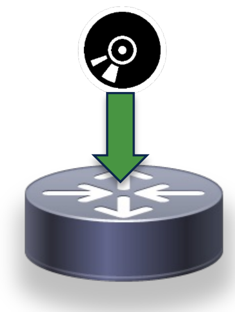
2. Multiple Hash-based Signatures (HBS) have been adopted by vendors already. They can be efficiently implemented in Hardware & FPGAs.

3. LDWM for firmware signing and LMS algorithms in use already by some vendors.

Impact to Hardware Identity

Need for Cryptographic Unique Hardware/Device Identity

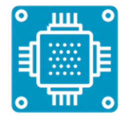
1. Counterfeit hardware from illegal markets.
2. Tampered hardware sold in resale markets.



1. Ability to cryptographically identify a device uniquely before booting.
2. Need to enroll and boot remote devices securely and in a scalable manner.

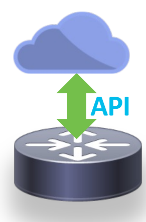
Requirements for Hardware Integrity

A tamper-proof, cryptographic unique identity to establish hardware identity remotely



Ability to validate integrity of critical hardware components

Ability to detect tampering, built-in crypto functions, providing entropy for RNGs, etc.



Ability to support remote attestation (identity challenge-response, boot measurements, etc.)

Role of TPMs & other security chips

TPM is a standard way to enable trust in computing platforms in general and is used for operations like measured boot, key storage for encryption, providing device identity, onboarding customer identity, etc.

- Boot Integrity Measurements (with PCRs*)
- Key Storage For Disk encryption
- Remote attestation for measured boot
- Device Identification, Device Enrollment, etc.

TPMs are present in Desktops/Laptops/Servers from most of the vendors.

*Platform Configuration Registers

Some Open & Proprietary Security Chips

Open Titan	Calliptra	Apple T2 Chip & Secure Enclave	Cisco TAm Chip
Opensource project for silicon root of trust (RoT) chips. Reference Link	OCP project defining RoT capabilities, etc. Reference Link	SoC providing hardware root of trust and other security features. Reference Link	Tamper-resistant chip providing hardware RoT, Secure Unique Device Identity, etc. Reference Link

Quantum Threat To Hardware Integrity/Identity

1. The algorithms/ciphers to provide the unique cryptographic identity need to be quantum safe.

2. The mechanisms to enroll end owner’s identity and the keys used must be quantum safe.

3. For other hardware tampering detection, the CPUs & ASICs must adopt quantum safe mechanisms to use the cryptographic identities.

4. Any boot stage artefacts that are signed/encrypted and used by the security chips must be signed/encrypted using algorithms that are quantum safe.

5. The methods used to update a device’s firmware must be quantum safe.

Quantum Safe Hardware Considerations

NIST PQC Algorithms to be finalized+ → TCG* to adopt PQ algorithms → TPM vendors and custom Silicon to adopt the new standards → OS Vendors and other Software integration

Various aspects to be considered are

1. Using PQ signatures for the firmware, etc.
2. Using PQ cryptographic identity for the chips.
3. Usage of at least 384-bit or longer hashes for PCR measurements, etc.
4. Key Enrollment mechanisms to support PQ signatures, workflows and keys/certificates.
5. Remote attestation procedures must be Quantum safe.

[+]Three algorithms are finalized

*TCG – Trusted Computing Group

Path to Post Quantum Cryptography

PQC Algorithms & Standards

LMS – RFC8554 – approved

XMSS – RFC8391 – approved

NIST SP.800-208 – approved (implementation requirements for LMS & XMSS)

FIPS-203 ML-KEM

- Module-Lattice-Based Key-Encapsulation Mechanism Standard

FIPS-204 ML-DSA

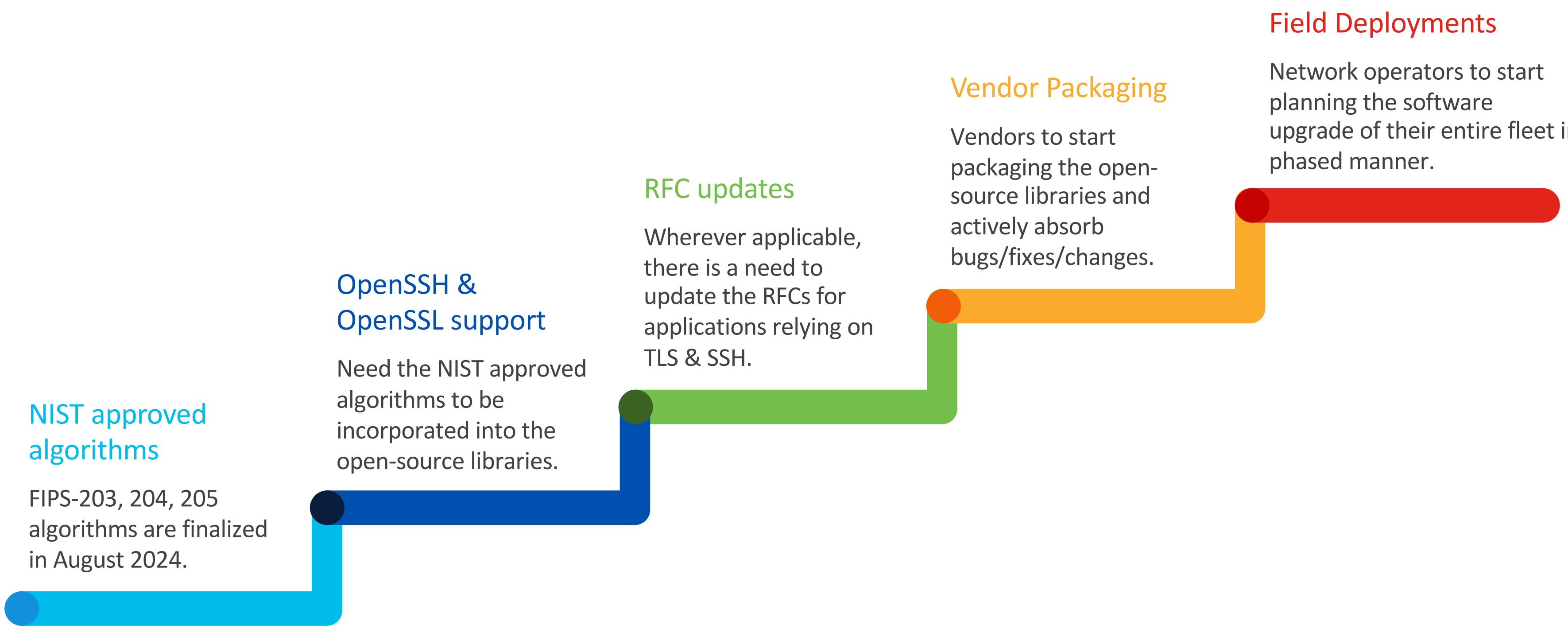
- Module-Lattice-Based Digital Signature Standard

FIPS-205 SLH-DSA

- Stateless Hash-Based Digital Signature Standard

CNSA 2.0 Quantum Computing FAQs can be found here.

Path To PQC Software Support



PQC Software Support – Other Considerations

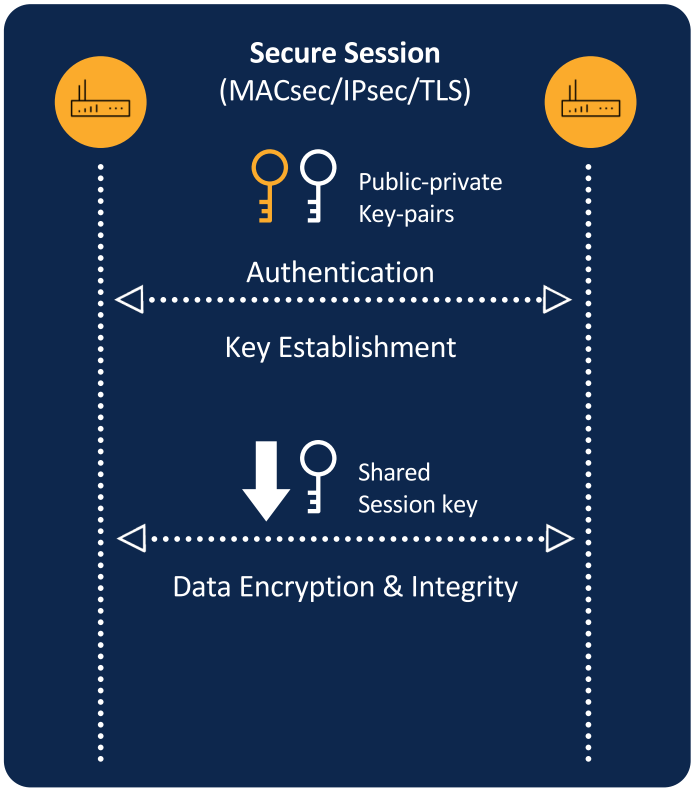
1. FIPS and other certifications for the new algorithms.
2. Stability of the implementations and absorbing the fixes.
3. Mechanism to let users pick PQC vs. classical ciphers. Keeping it as a global option or application-level option, etc.
4. Availability of servers capable of handling PQC algorithms for testing & deployment.
5. Consider crypto agility in the implementations to absorb future changes in algorithms quickly.

CNSA Recommended Algorithms and Use cases

<table>
<tr><th rowspan="2">Function/Use Case</th><th colspan="2">Algorithms</th></tr>
<tr><th>CNSA 1.0</th><th>CNSA 2.0</th></tr>
<tr><td>General system-wide, secret-based encryption and decryption</td><td colspan="2">AES-256
FIPS PUB 197</td></tr>
<tr><td rowspan="3">General system-wide secure key exchange protocol</td><td>ECDH-384</td><td rowspan="3">ML-KEM-1024 (CRYSTAL-Kyber 1024)
FIPS-203</td></tr>
<tr><td>DH-3072</td></tr>
<tr><td>RSA-3072</td></tr>
<tr><td rowspan="2">Device Identity and attestation certificates signature signing and verification</td><td>ECC P-384
FIPS PUB 186-4 (superseded by 186-5 in Feb 2024)</td><td rowspan="2">ML-DSA-87 (CRYSTAL-Dilithium)
FIPS-204</td></tr>
<tr><td>RSA-3072
FIPS PUB 186-4 (superseded by 186-5 in Feb 2024)</td></tr>
<tr><td>General system-wide hashing usage</td><td>SHA
FIPS 180-4
Use SHA-384 for all classification levels</td><td>SHA
FIPS 180-4
Use SHA-384 or SHA-512 for all classification levels</td></tr>
<tr><td rowspan="3">Image signing</td><td>RSA-3072
FIPS PUB 186-4 (superseded by 186-5 in Feb 2024)</td><td>LMS
FIPS SP 800-208
RFC 8554</td></tr>
<tr><td rowspan="2">ECC P-384
FIPS PUB-186-4 (superseded by 186-5 in Feb 2024)</td><td>XMSS
FIPS SP 800-208
RFC 8391</td></tr>
<tr><td>ML-DSA-87 (CRYSTAL-Dilithium)
FIPS-204</td></tr>
</table>

Transport security impact

Quantum computing impact on cryptography



Quantum-resistant?

Asymmetric cryptography

- Based on **mathematically related** public-private key-pairs
- Used for control plane operations
  - Authentication, key establishment
- Examples: RSA, DH, ECC

Large, reliable quantum computers can break RSA, DH, ECC

Symmetric cryptography

- Based on shared key
- Used for bulk data encryption and integrity
- Protection level based on key strength
  - Key size and entropy
- Example: AES-GCM

Symmetric crypto with large and high-entropy keys is resistant to quantum computer attacks

Why care about quantum threats now?

1. Attackers can tap flows today and store them to be decrypted in the future.

2. Any sensitive deployments that need forward secrecy for 5+ years must act now.

   - Military or other defense networks
   - Federal or other government agencies
   - Financial institutions and banks
   - Service provider networks catering to enterprises with sensitive data

3. Less critical or short-lived sessions without long-term significance can wait.

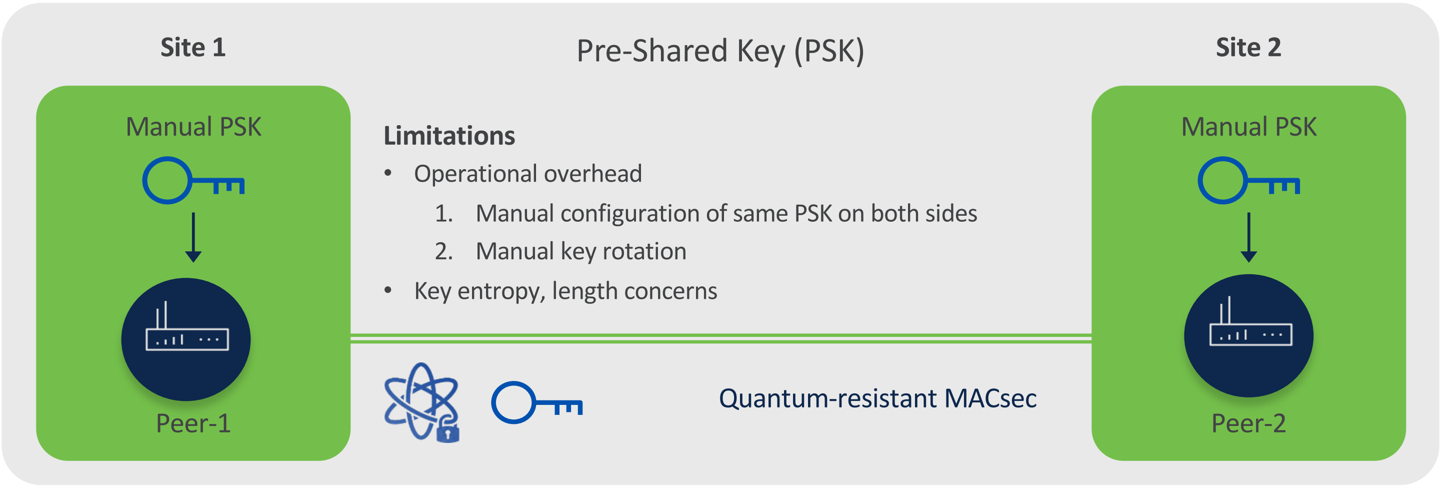
Transport security solutions

Available options

Symmetric cryptography	Quantum key distribution	Post-quantum cryptography
✓ Long symmetric keys are quantum-safe	✓ Use quantum mechanics to protect the data	✓ Replace current public key algorithms with new ones
⚠ Issues with distributing keys and trust	⚠ Technology limitations	⚠ Still evolving and needs vendor adoption, certification, etc.
IEEE 802.1AE standard from 2006 (MACsec PSK)	2015 – 2024 (Cisco SKS, SKIP, ETSI, etc.)	1H CY'24 → 2H CY'24 & Beyond

Quantum-safe MACsec

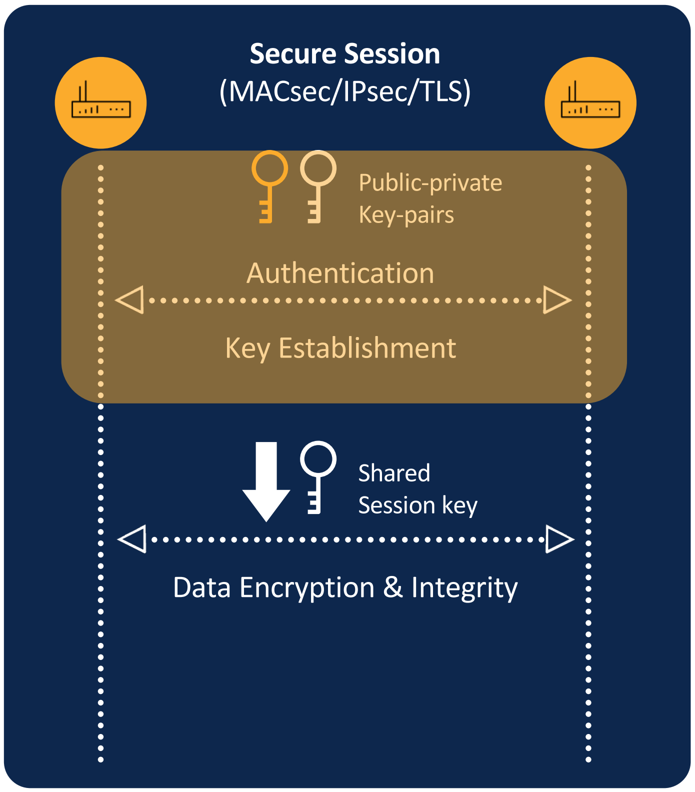
Pre-shared key (PSK) option

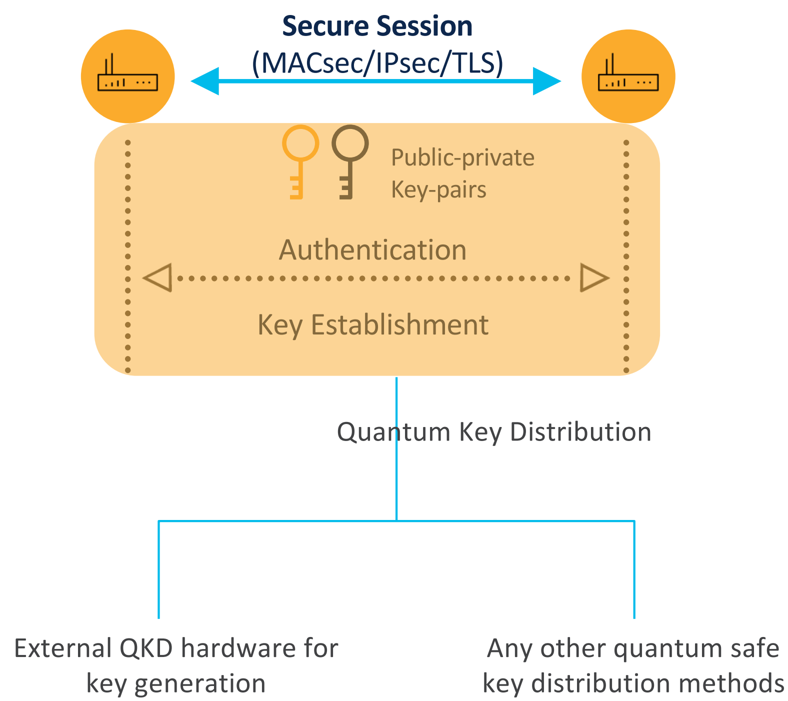


1. MACsec with PSK option is already supported and used by customers.
2. There is no need for additional hardware (like QKD*) or software upgrade.
3. Quantum-safe as this is based on symmetric cryptography (which is quantum-resistant).

*Quantum Key Distribution

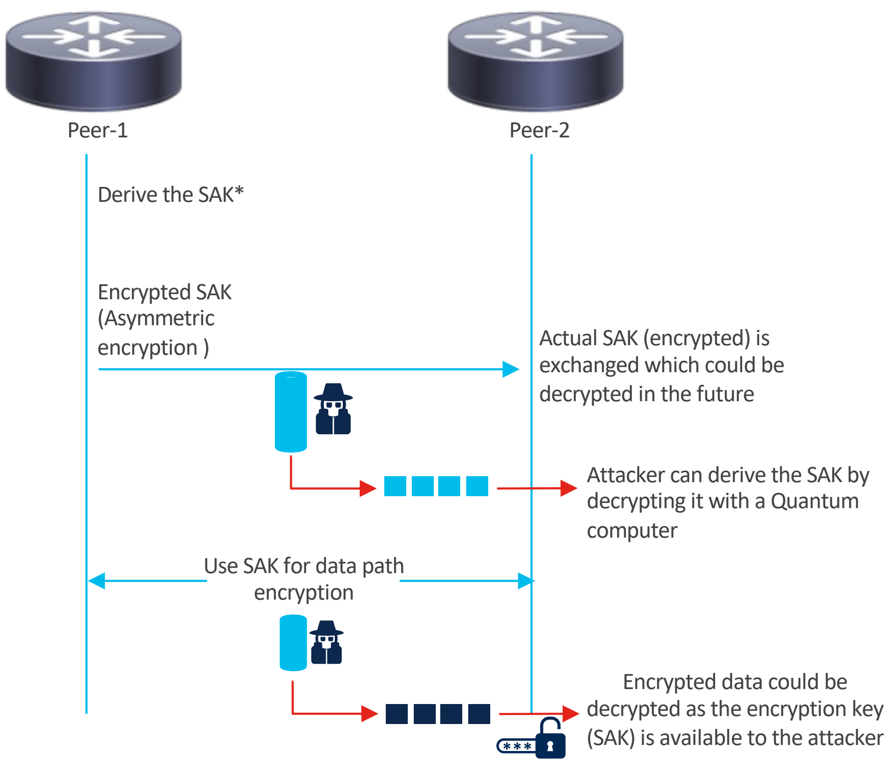
Quantum key distribution option



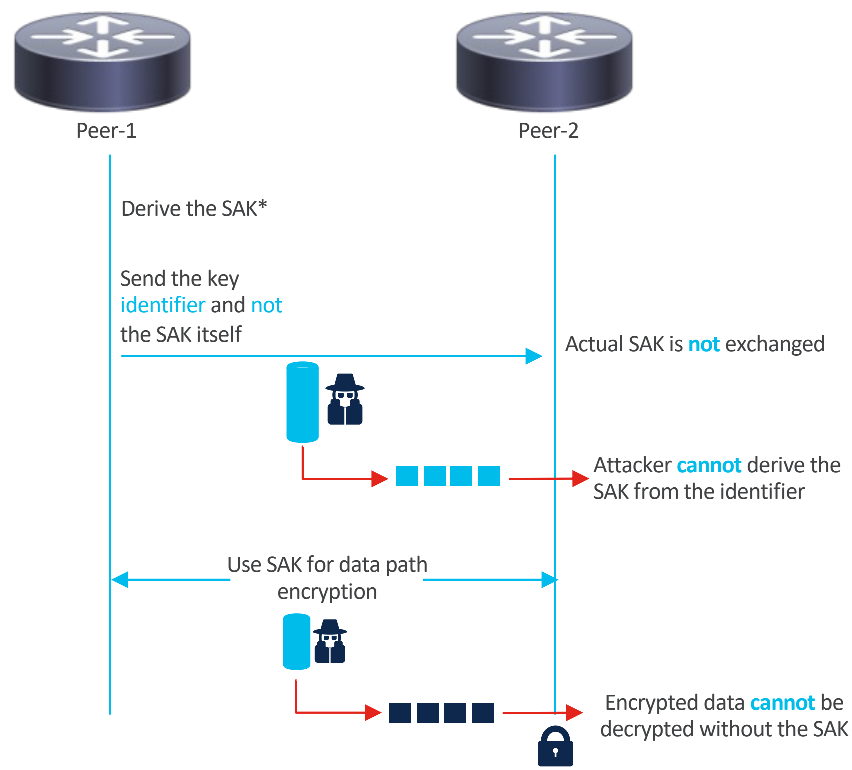


Quantum key distribution – Basic principle

Existing method



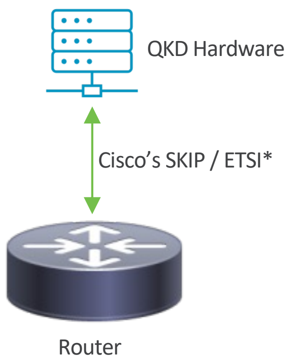
QKD method

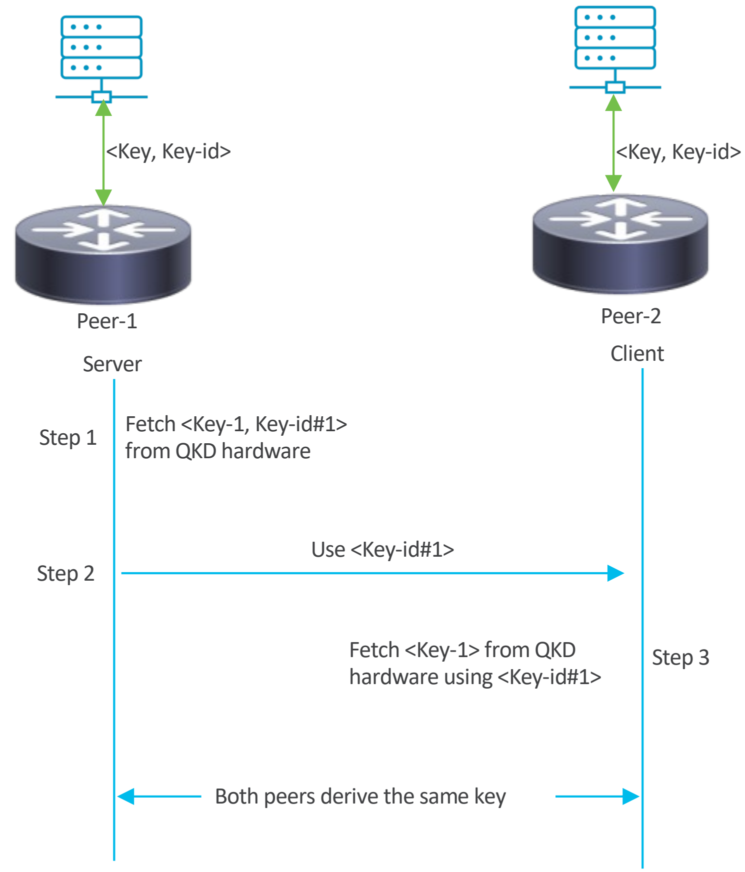


*SAK – Security Association Key

Quantum key distribution options

External QKD hardware option





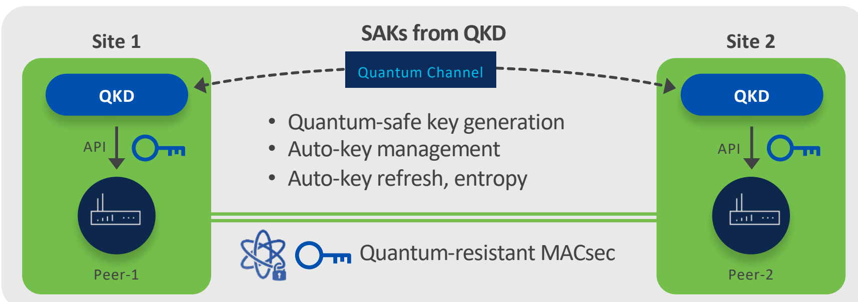
1. Dedicated hardware to generate the session keys and key-id’s
2. The QKD hardware for a given pair of devices would be in sync
3. Each peer fetches the key and key-id from the QKD hardware over a TLS connection
4. Only key-id is sent on the wire, and the peer fetches the key from the QKD hardware

*Links to Cisco SKIP & ETSI

Quantum-safe MACsec

Quantum key distribution options

External QKD hardware



1. Hardware-based key source
2. Dedicated optical fiber (up to 100 km)
3. QKD hardware per-site/peer
4. Expensive (cost of QKD hardware, etc.)

Path to Post Quantum Cryptography

PQC Algorithms & Standards

LMS – RFC8554 – approved

XMSS – RFC8391 – approved

NIST SP.800-208 – approved
(implementation requirements for LMS & XMSS)

FIPS-203 ML-KEM
- Module-Lattice-Based Key-Encapsulation Mechanism Standard

FIPS-204 ML-DSA
- Module-Lattice-Based Digital Signature Standard

FIPS-205 SLH-DSA
- Stateless Hash-Based Digital Signature Standard

Protocol standards (the most urgent set)

IKEv2:

RFC 9370 – Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved

RFC 9242 – Intermediate Exchange in the Internet Key Exchange Protocol Version 2 (IKEv2) – approved

Post-quantum Hybrid Key Exchange with ML-KEM in the Internet Key Exchange Protocol Version 2 (IKEv2) – draft

TLS:

Hybrid key exchange in TLS 1.3 – draft

SSH:

Post-quantum Hybrid Key Exchange in SSH - draft

Crypto Services:

Composite Signatures For Use In Internet PKI - draft

Internet X.509 Public Key Infrastructure: Algorithm Identifiers for ML-DSA - draft

Internet X.509 Public Key Infrastructure - Algorithm Identifiers for Kyber – draft

CNSA 2.0 Quantum Computing FAQs can be found here.

Q&A