Quantum-safe with Cisco & Wingmen

Søren Dulong Andreasen
Soren@cisco.com



Bo Urskov
bur@wingmen.dk



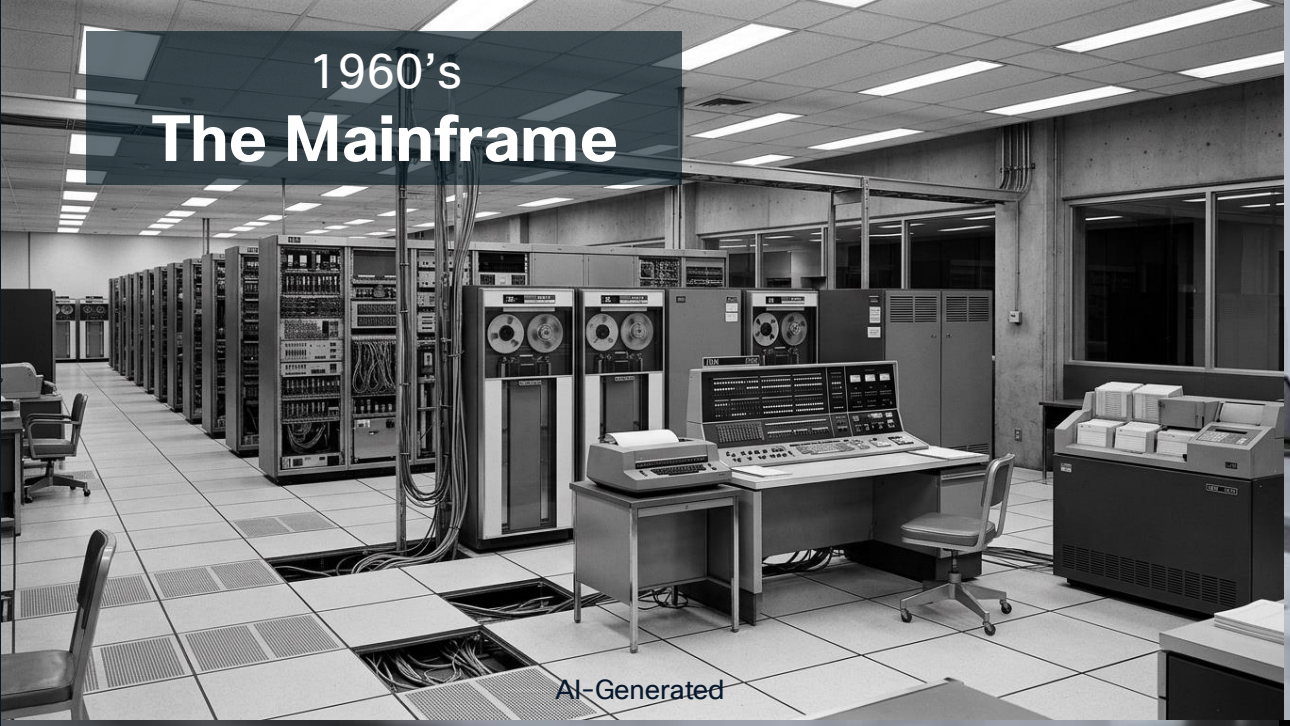
Maj 2026

Agenda

- Introduction
- Quantum, the next paradigm.
- What are use cases for Quantum
- Why are Quantum computers impressive
- The Impact of Quantum Computer on Cryptography
- QKD & PQC : Quantum-Safe Communications
- Conclusion and recommend next step

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential


1960’s
The Mainframe
AI-Generated


1980’s
The PC


2000’s
Mobile Computing


2010’s
Cloud Computing

The next computing paradigm
Quantum Computing

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Post-quantum cryptography (PQC)

Why it matters (now)

Threat Actors use ***Quantum*** computers to crack encrypted data



?

But bad guys don't have Quantum computers

and

The Quantum Computers are not fast enough



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Industry verticals













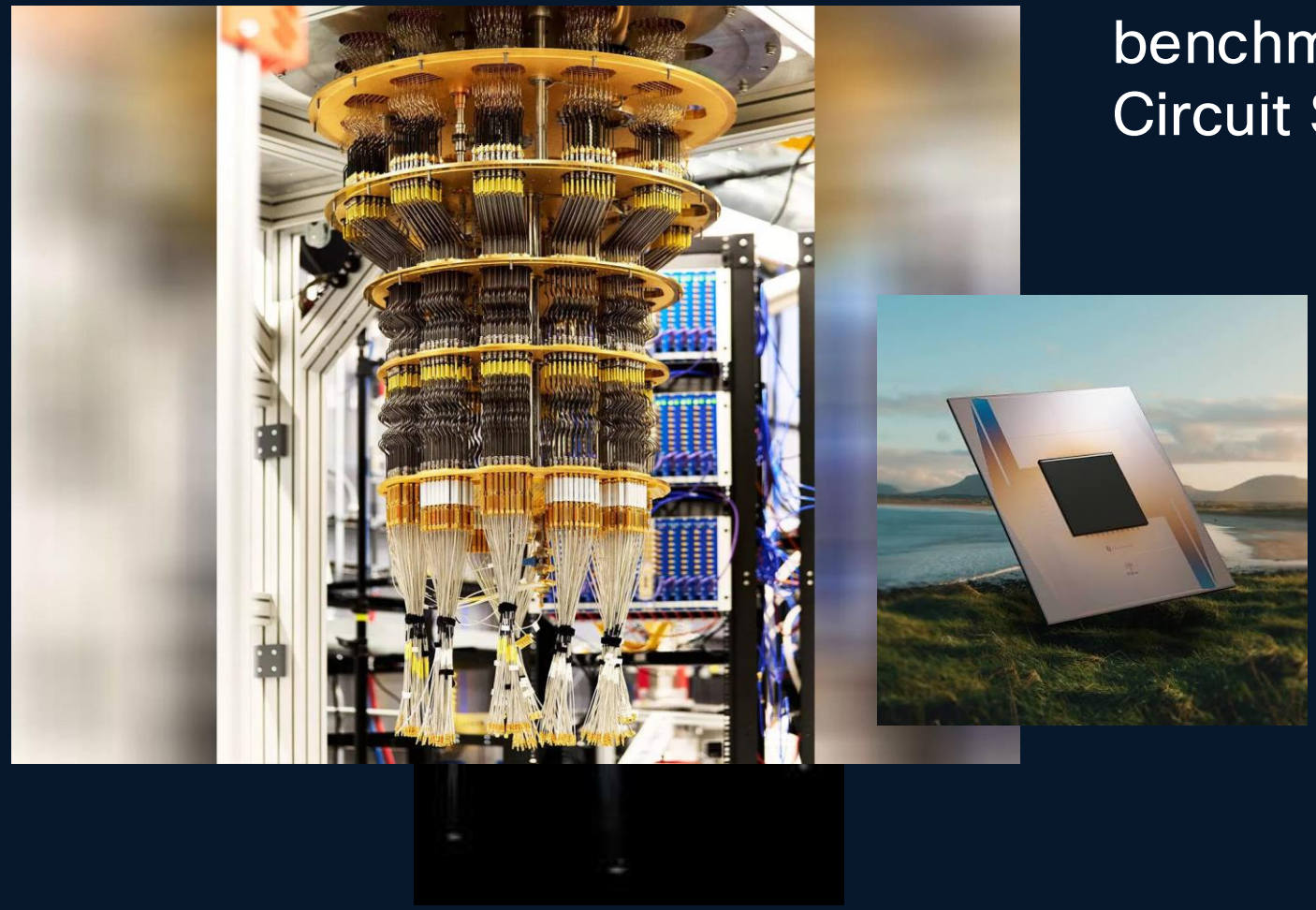




© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Google Willow- 2025



To demonstrate quantum supremacy, the Willow processor was tasked with a benchmark problem called Random Circuit Sampling

Task completion on Google Willow
5 Minutes

Task completion on Worlds fastest supercomputer (El Capitan)
10.000.000.000.000.000.000.000.000.000 Years

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential



The Risk of **Quantum**

© 2026 Cisco and/or its affiliates. All rights reserved.
© 2026 Cisco and/or its affiliates. All rights reserved.

Threat Actors using ***Quantum*** to crack encrypted data

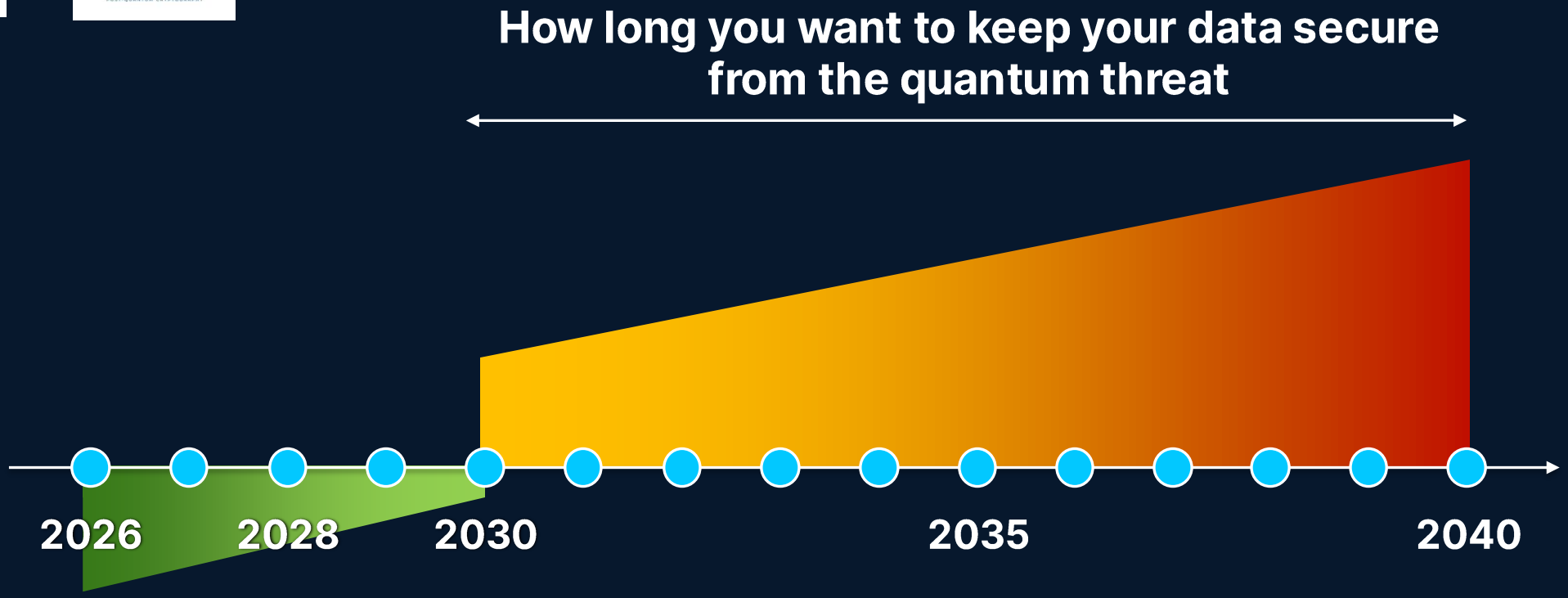
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The Quantum Threat Timeline



V



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Quantum Threat, 3 areas

Transport Security

- **MACSec**
- **IPSec**
- **TLS**

Firmware/Software Integrity

- **Firmware and OS image signing**
- **Secure Boot**
- Integrity Measurment Architecture (IMA) keys, software image posting, etc.

Identity

- Server certificates
- Individual identities
- Device identity (for ex. SUDI)
- **SSH**

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential



Harvest Now Decrypt Later (HNDL)

© 2026 Cisco and/or its affiliates. All rights reserved.

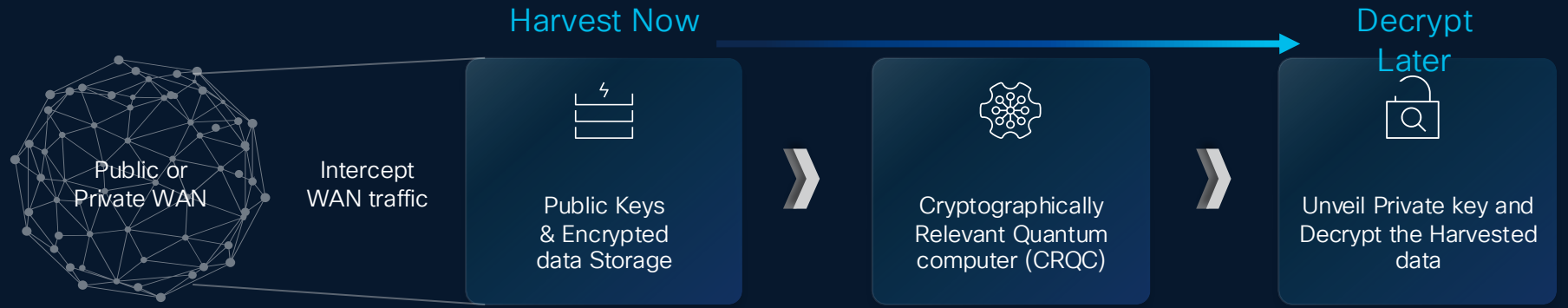
Cisco Confidential

Quantum Threat, Harvest Now, Decrypt Later

Transport Security

- MACSec
- IPSec
- TLS

Attacker captures the key exchange phase, encrypted data in-transit & uses Quantum calculated Private Key to get shared secret session Key and decrypt the harvested data!



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

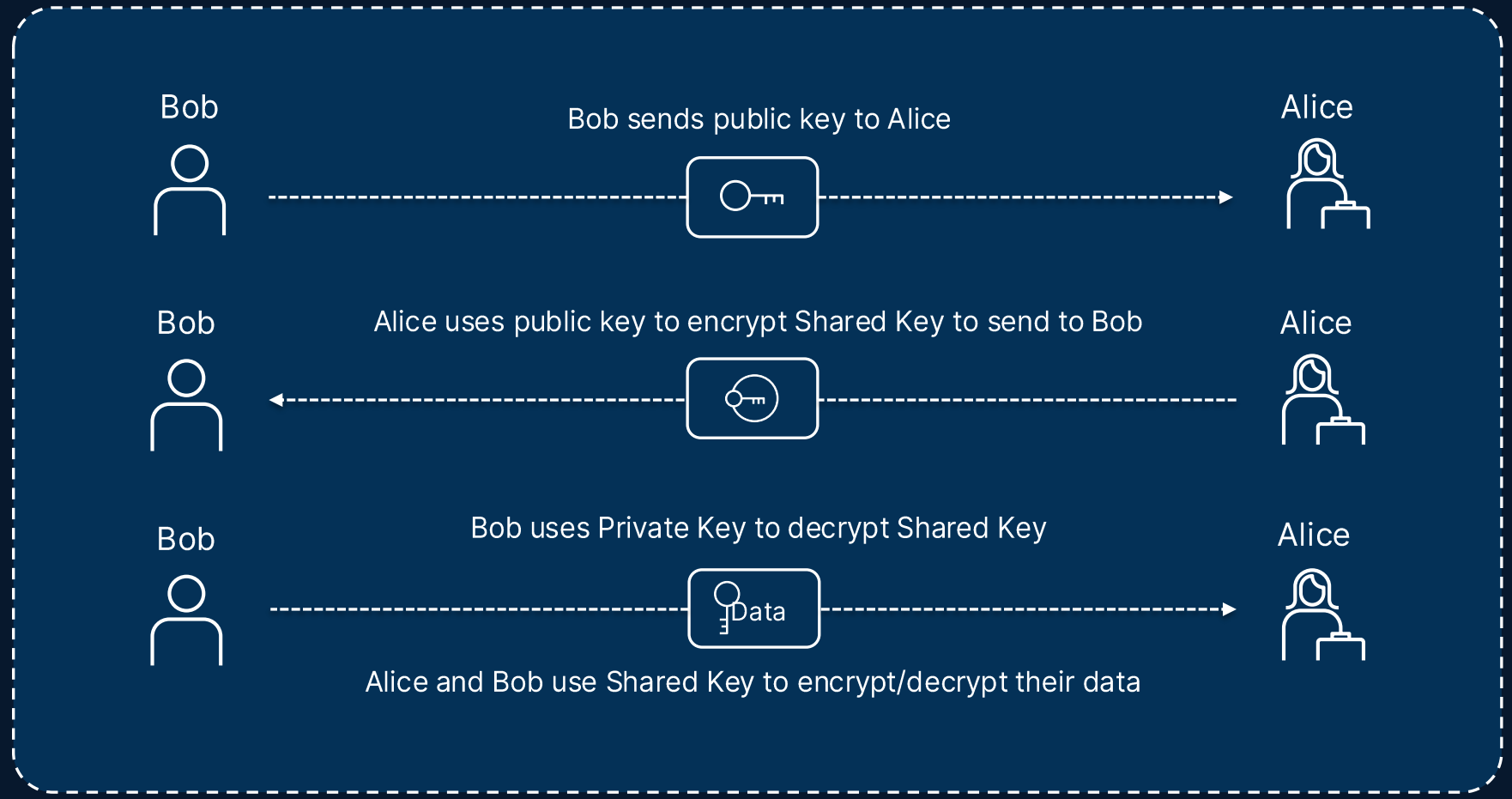
The **asymmetric** *cryptography* HNDL use case

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Harvest Now Decrypt Later explained

Threat actor *intercepts* and *copies* the **entire** data exchange

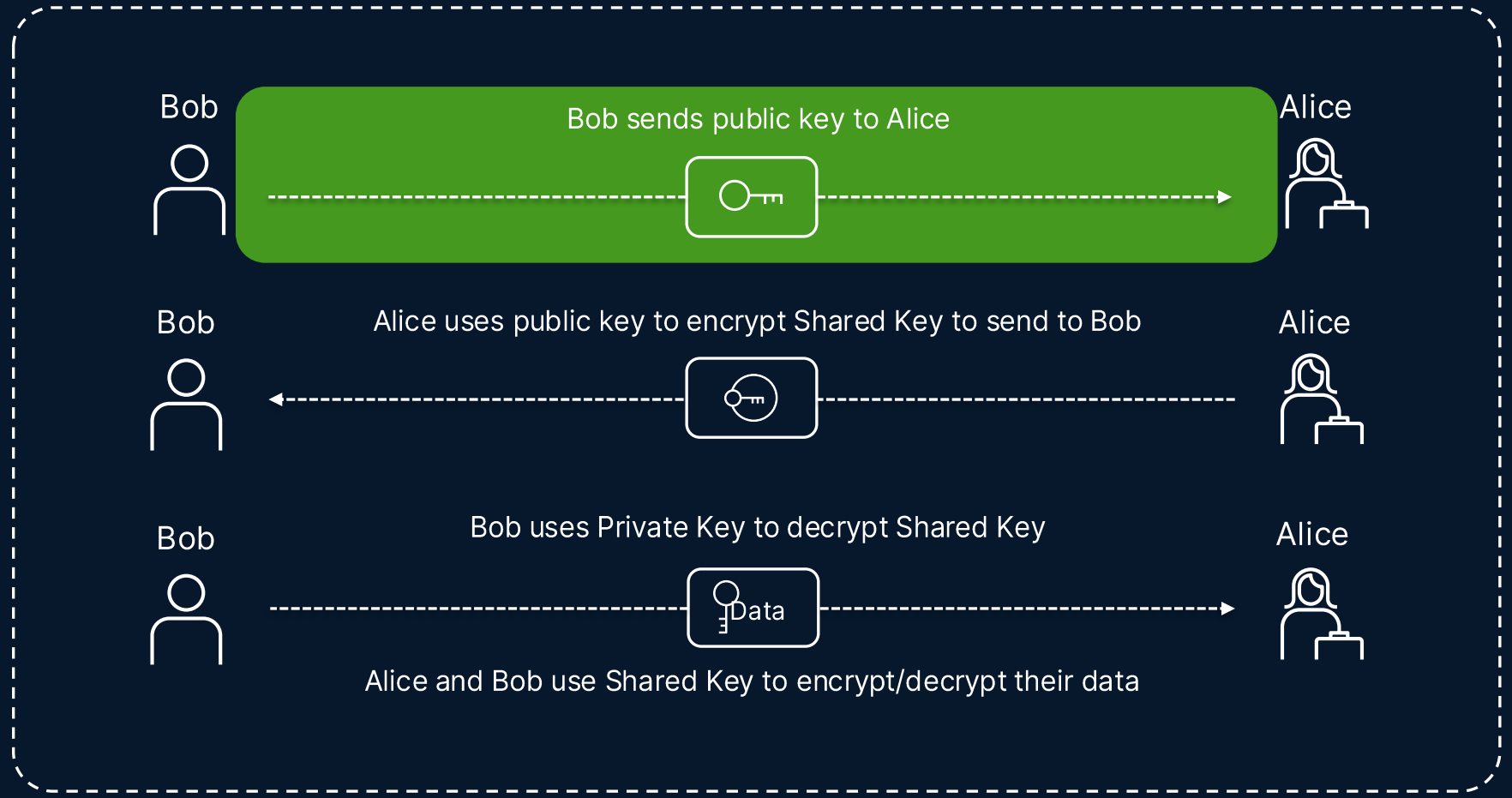


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Harvest Now Decrypt Later explained

Public key is inputted into the **Quantum** *Computer*

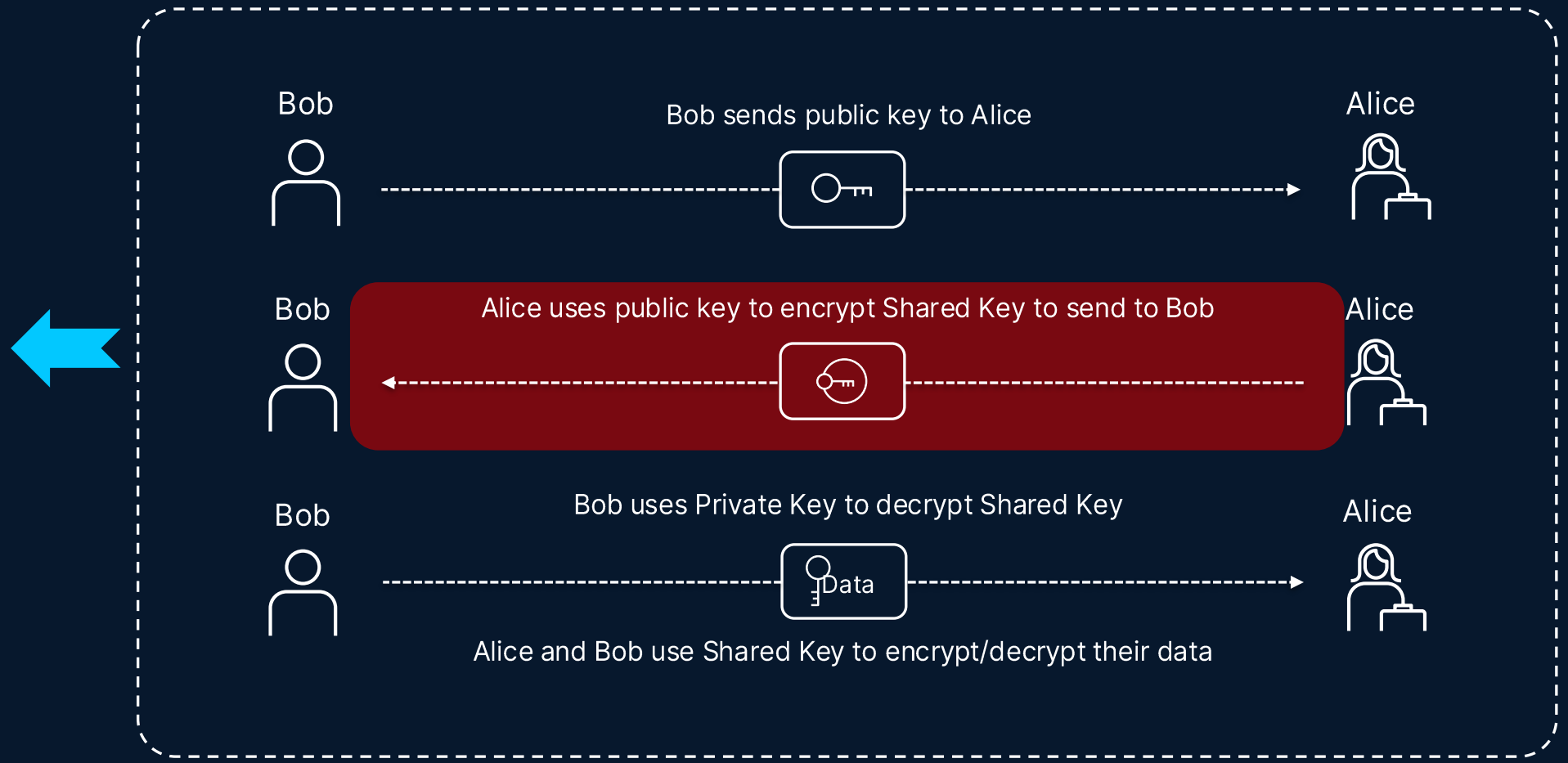


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Harvest Now Decrypt Later explained

Quantum *Computer* uses **Shor's** Algorithm to derive Private Key from the Public Key

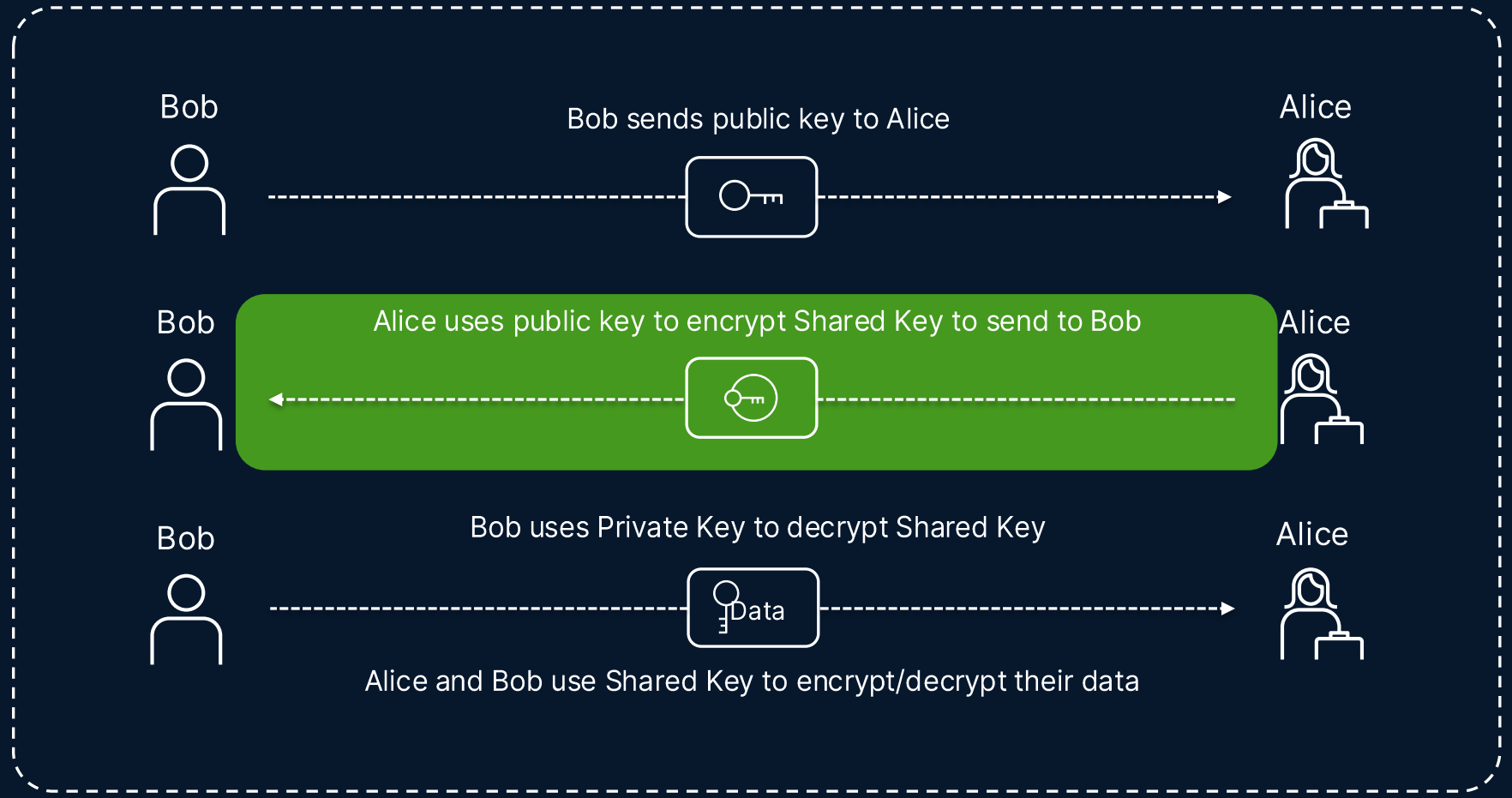


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Harvest Now Decrypt Later explained

Threat actor uses Private Key to decrypt data containing Shared Key

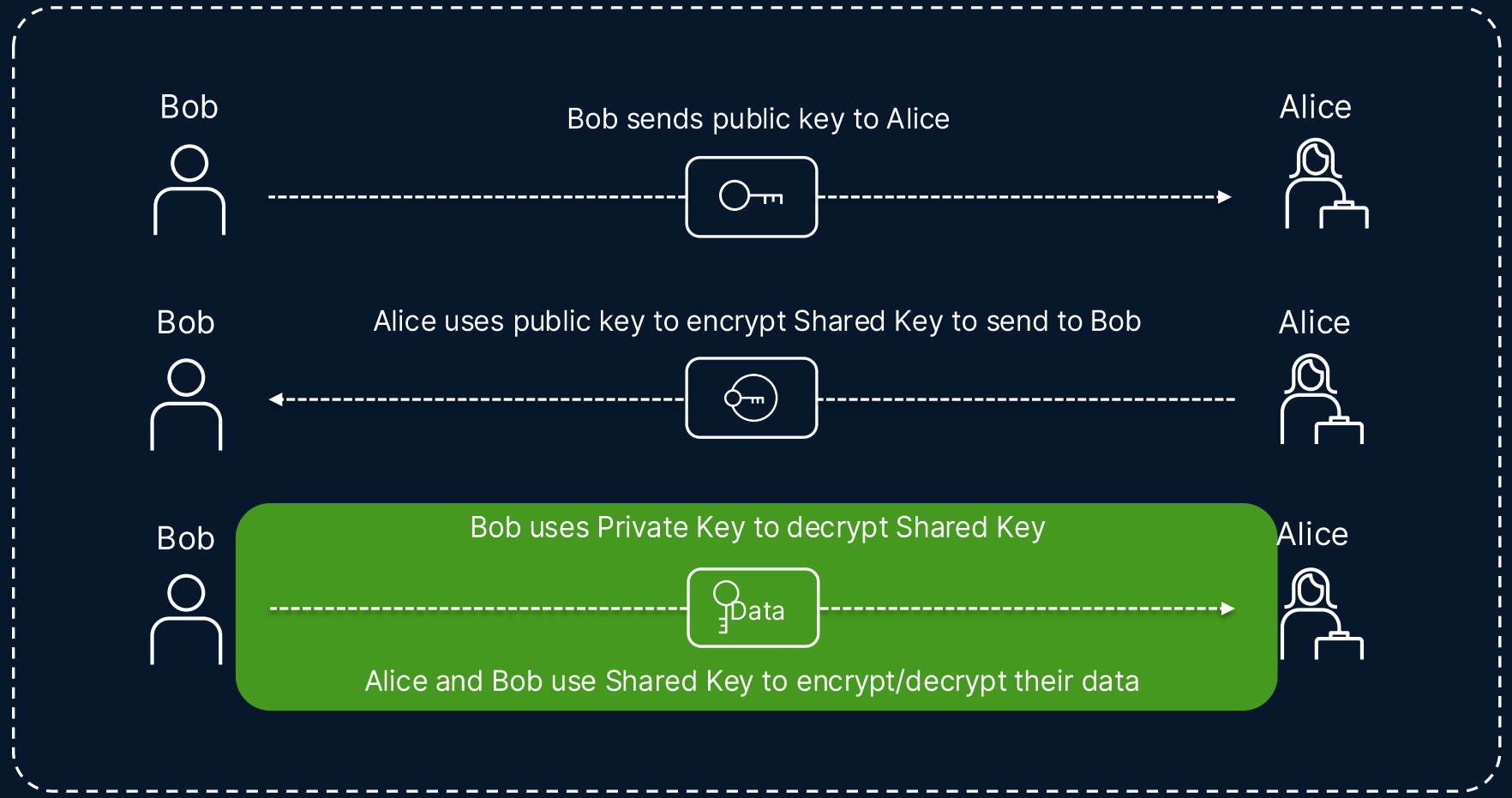


© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Harvest Now Decrypt Later explained

Threat actor uses Shared Key to decrypt data between Alice and Bob



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

At risk cryptography options
What you need to look for?

PQC ready protocols

Asymmetric Cryptography	RSA	ECC	DH	ML-KEM	ML-DSA	
	Vulnerable	Vulnerable	Vulnerable	Resistant	Resistant	
Symmetric Cryptography	3DES	AES128	AES256	SHA1	SHA256	SHA384	SHA512
	Vulnerable	At Risk	Resistant	Vulnerable	At Risk	Resistant	Resistant

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

How does this threat impact **Networking** devices?

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Securing data transport

MACSEC – Hop by Hop Encryption

1



IPSEC – End to End Encryption

2

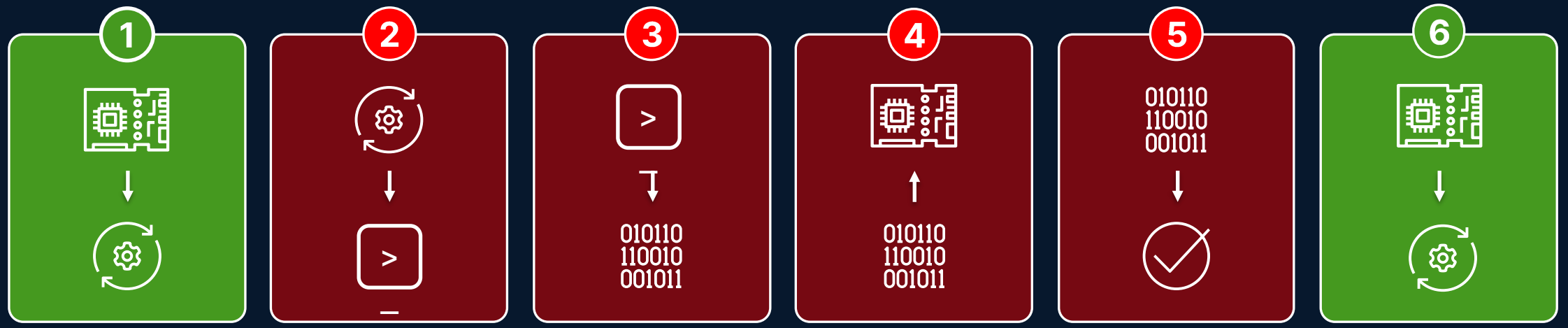


Encryption Type	Cryptography	Type	PQC Compliance
MACSEC	Symmetric	Pre Shared Key	Resistant
MACSEC	Asymmetric	Cert Based MKA-EAP-TLS	Vulnerable
IPSEC	Asymmetric	IKEv2 Key Exchange	Vulnerable

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The bootup process – the risks



Micro-loader Image in *Trust Anchor* Module

Micro-loader activates *Bootloader*

Bootloader checks IOS –XE code (*validates OS*)

Bootloader initiates CPU to load *IOS-XE code*

SUDI Certs authenticated by IOS-XE (*validates HW*)

Trust Anchor provides on going *secure storage* and *integrity checks*

TAM encrypted with AES-256

Bootloader signed with RSA

IOS-XE signed with RSA & ECC

IOS-XE signed with RSA & ECC

Sudi signed w/RSA

TAM encrypted with AES-256

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential



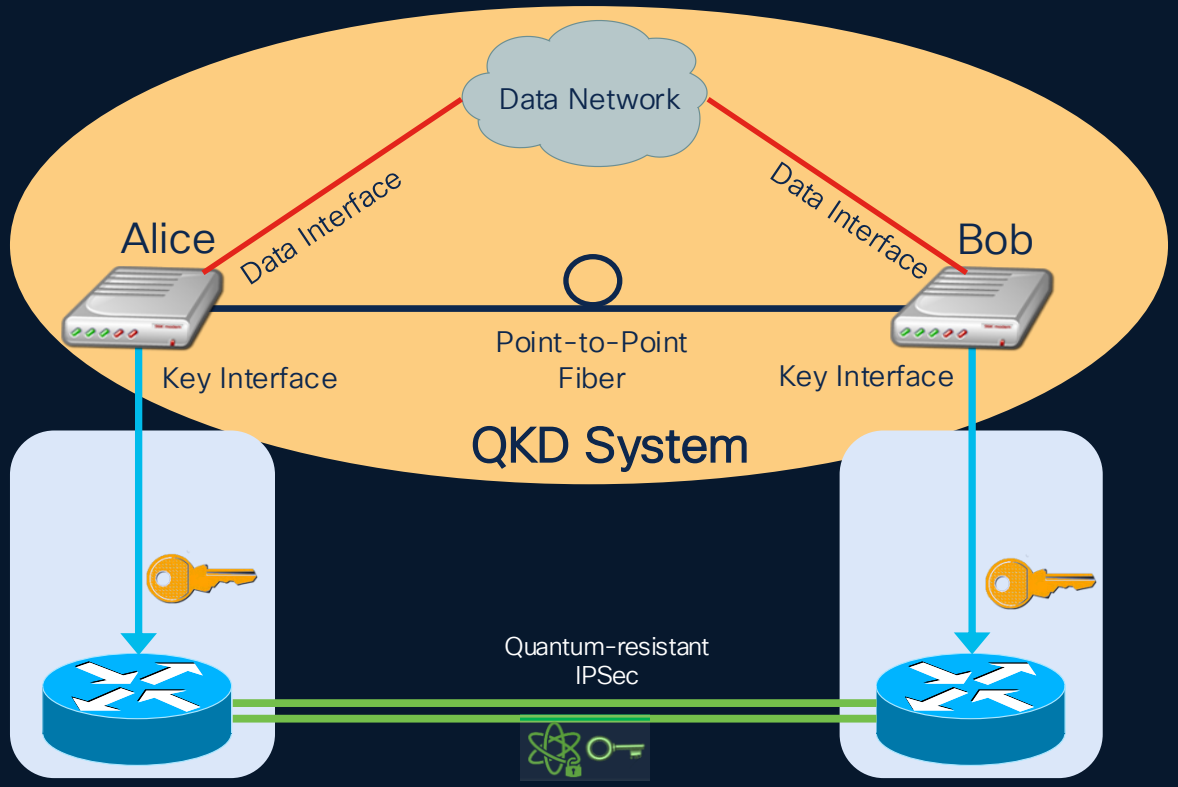
© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Quantum Key Distribution

QKD: How Does It Work?

- QKD system “Alice” generates a random key
- The key is sent to “Bob” as photon quantum states



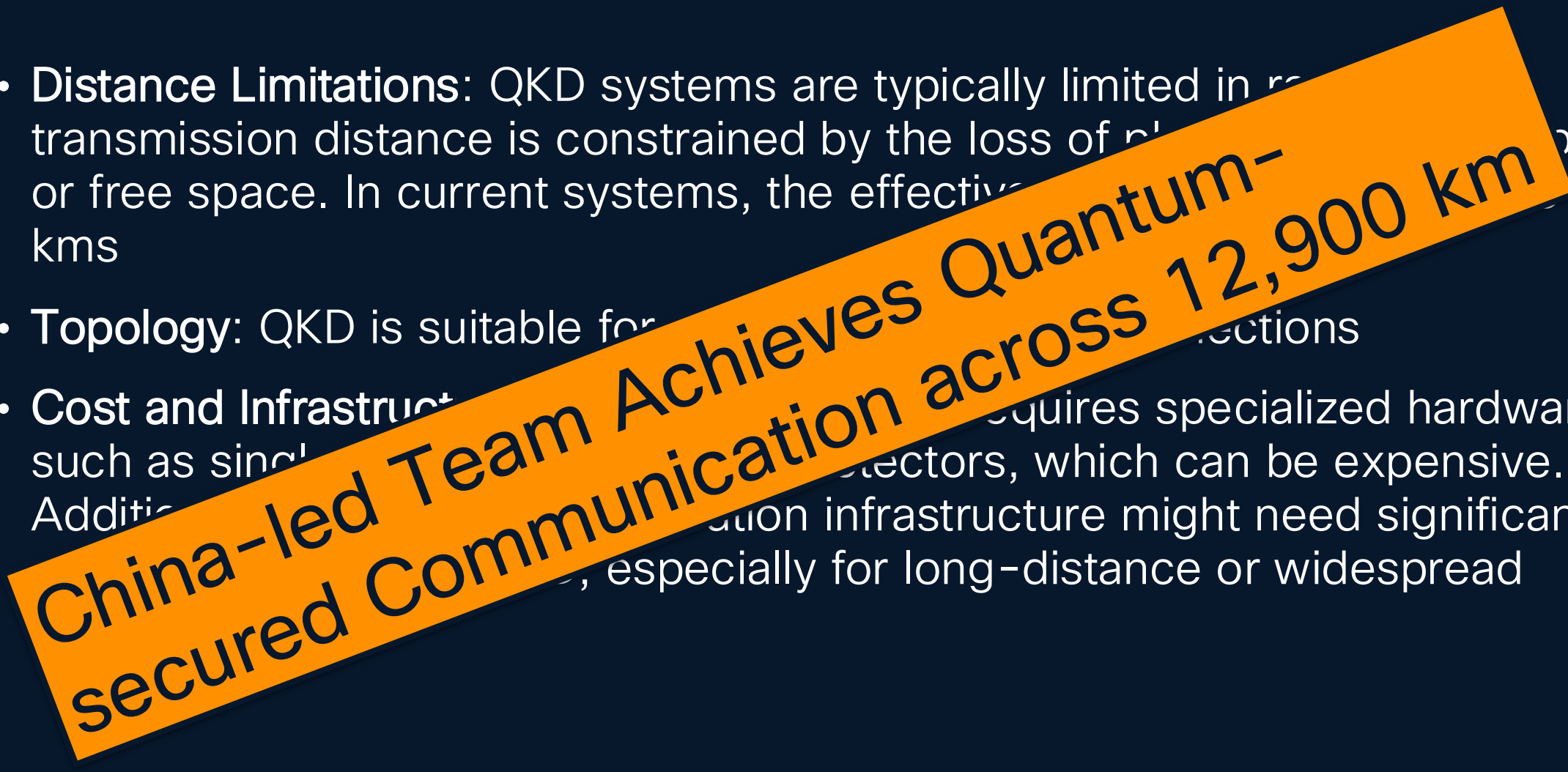
- Bob receives the photons and decodes the quantum states, recovering the key
- Once the key is securely distributed, “Alice” and “Bob” pass the key to the encryption systems

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

QKD Limitations

- **Distance Limitations**: QKD systems are typically limited in r
  transmission distance is constrained by the loss of p
  or free space. In current systems, the effecti
  kms
- **Topology**: QKD is suitable for
- **Cost and Infrastruct**
  such as sing
  Additi
  , especially for long-distance or widespread



© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential



Post-Quantum Cryptography (PQC)

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

THE NIST POST-QUANTUM CRYPTOGRAPHY STANDARDIZATION TIMELINE: FOUR KEY PHASES

PHASE 1

THE QUANTUM SHADOW (2015-2016)

2015: NIST officially recognized "Quantum Threat"



Quantum Computer or traditional encryption

2016: Issued a Global Call for Proposals



Start of "cryptographic tournament" for new math.



Global outreach

PHASE 2

THE GLOBAL TOURNAMENT (2017-2021)

2017 DEADLINE: 82 CANDIDATE ALGORITHMS SUBMITTED FROM 25 COUNTRIES

MATHEMATICAL FAMILIES



Lattices



Code-based Problems



Multivariate Equations

TRANSPARENT & ADVERSARIAL PROCESS

The community tries to break algorithms.

- Round 1 (2017): **69** Candidates ✕
- Round 2 (2019): **26** Narrowed ✕
- Round 3 (2020): **15** Finalists & Alternates after mathematical attacks



Clever peer attacks discover high-profile breaks

PHASE 3

THE WINNERS & STANDARDIZATION (2022-2024)

JULY 2022: FIRST FOUR WINNERS ANNOUNCED



Kyber encryption



Dilithium



Falcon



SPHINCS+ signatures

Selected for balance: Security, Speed, Key Size

AUGUST 2024: HISTORIC MILESTONE, FIRST THREE FINALIZED STANDARDS RELEASED



FIPS 203 (ML-KEM, based on Kyber)



FIPS 204 (ML-DSA, based on Dilithium)

FIPS 205 (SLH-DSA, based on SPHINCS+)

FIPS 205 (SLH-DSA, based on SPHINCS+)



PHASE 4

THE PATH FORWARD (2025-2026)

MARCH 2025: NIST INTRODUCED HQC AS A FIFTH BACKUP ALGORITHM



Code-based math to mitigate future breakthrough attacks

AUGUST 2025: FOURTH DRAFT FOR FALCON FALCON (FIPS 206) SUBMITTED FOR REVIEW



Quantum Threat, 3 areas

Transport Security

- **MACSec**
- **IPSec**
- **TLS**

Firmware/Software Integrity

- **Firmware and OS image signing**
- **Secure Boot**
- Integrity Measurment Architecture (IMA) keys, software image posting, etc.

Identity

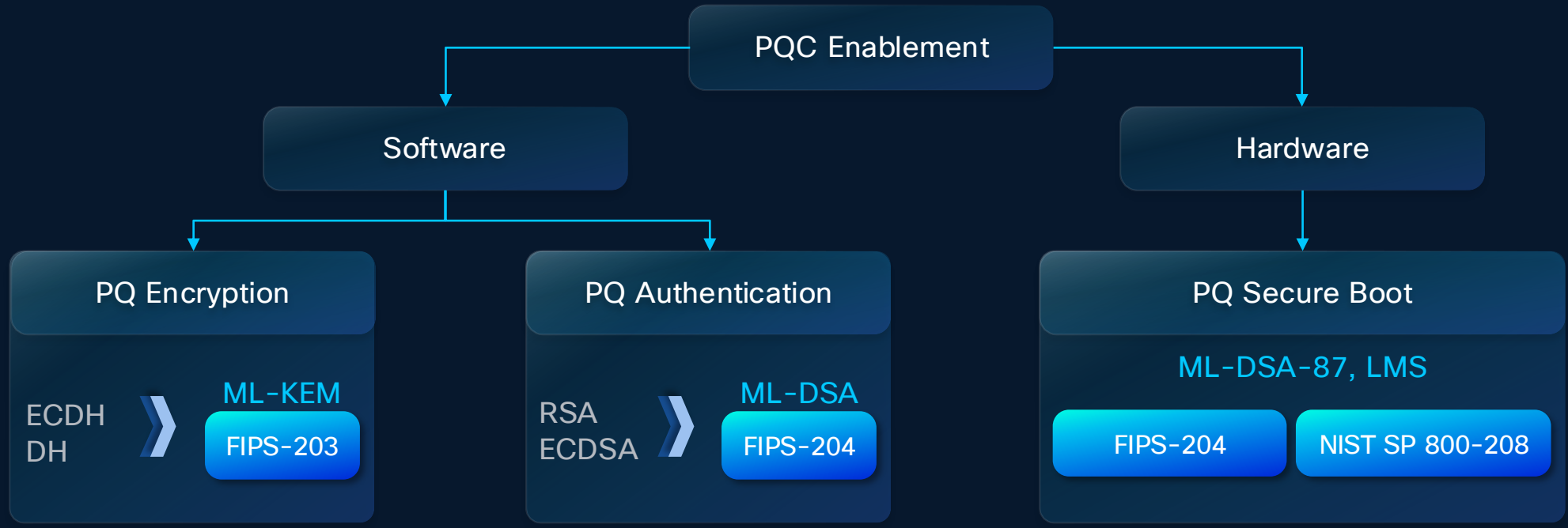
- Server certificates
- Individual identities
- Device identity (for ex. SUDI)
- **SSH**

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

PQC Algorithm & Protocol Standards

A Comprehensive list of Quantum-Safe Algorithms defined by NIST as a part of CNSA 2.0 suite



Transport Security

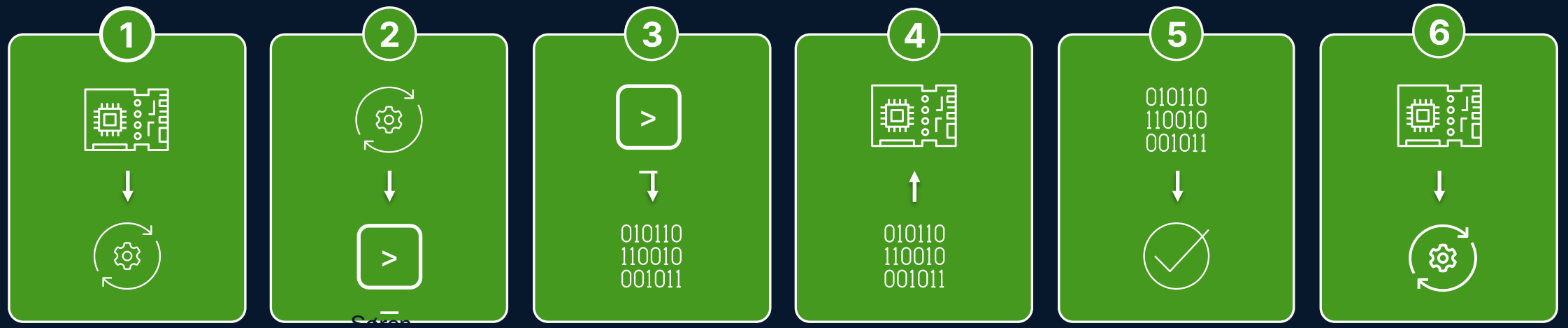
Identity

Firmware/Software Integrity

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

The bootup process in our new hardware



Micro-loader Image in *Trust Anchor* Module

Micro-loader activates *Bootloader*

Bootloader checks IOS –XE code (*validates OS*)

Bootloader initiates CPU to load *IOS-XE code*

SUDI Certs authenticated by IOS-XE (*validates HW*)

Trust Anchor provides on going *secure storage* and *integrity checks*

TAM encrypted with AES-256

Bootloader signed with LMS

IOS-XE signed with ML-DSA-87

IOS-XE signed with ML-DSA-87

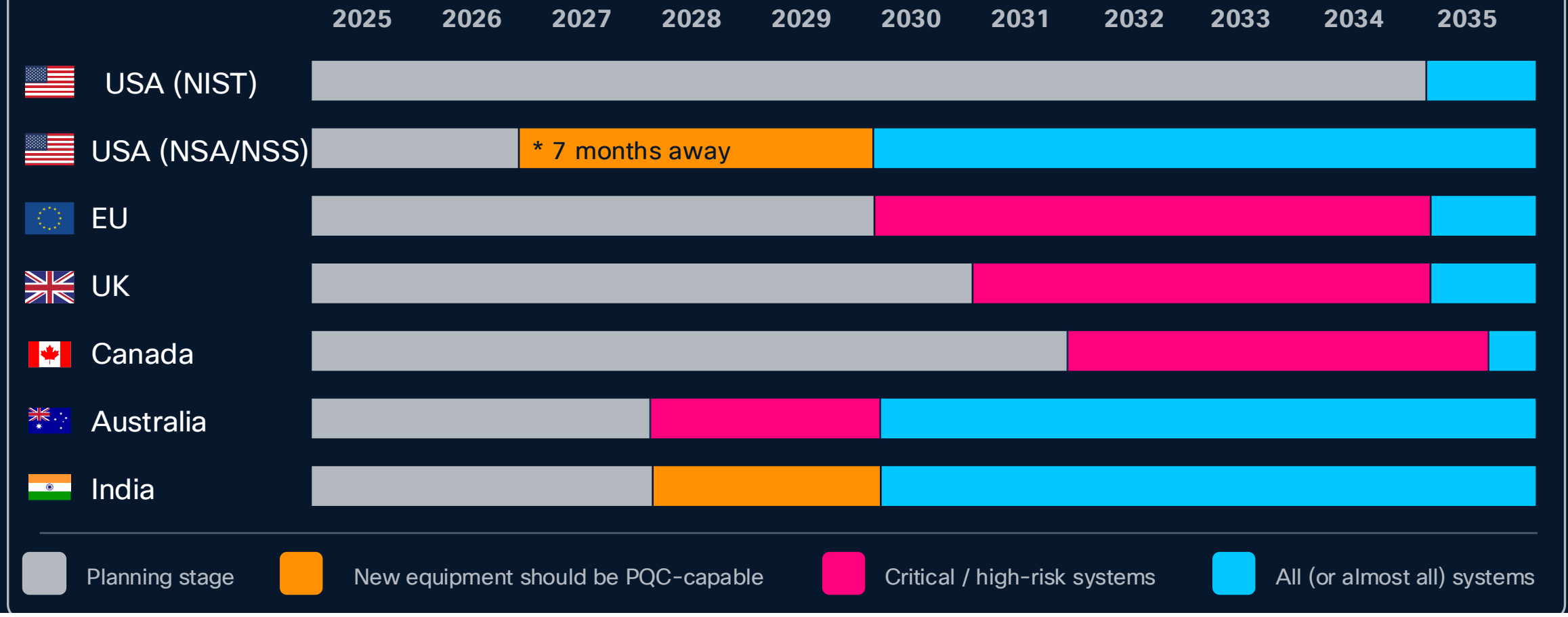
Sudi signed with ML-DSA-87

TAM encrypted with AES-256

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Regulator's PQC transition timelines



As mandated by the Committee on National Security Systems Policy 15, starting in 2027, all new commercial NSS must be capable of supporting quantum-resistant algorithms. Legacy systems that cannot support quantum-resilient algorithms are to be phased out by 2030.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

wingmen

part of springboardnetwork



Wingmen Security Assessments

- Clear picture of current security posture
- Identification of risks and exposures
- Best practices based on NIS2, CIS, IEC 62443
- PQC readiness
- Prioritized roadmap for next steps
- Features you may already own but don’t use



wingmen
part of springboardnetwork

PQC readiness

- Equipment
- WAN
- VPNs – remote access
- Campus networks
- Management
- Certificates

Cisco Confidential

Encryption is the *lock*, but **Quantum** can become the *universal key*.
It's time to **change** the locks before the door can be *opened*.

© 2026 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential


CISCO