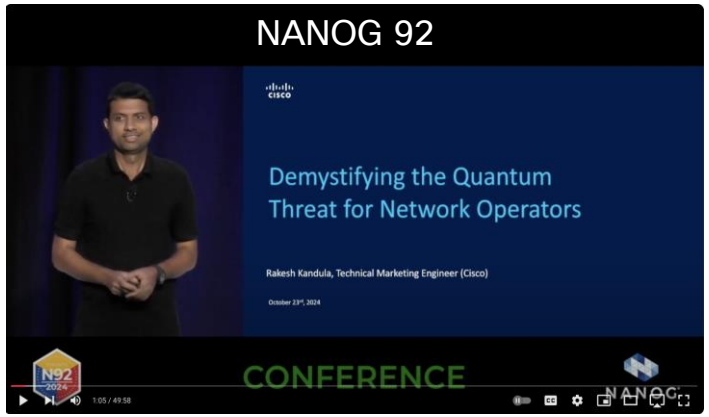
Security Journey of a Router: Design to Deployment & Beyond

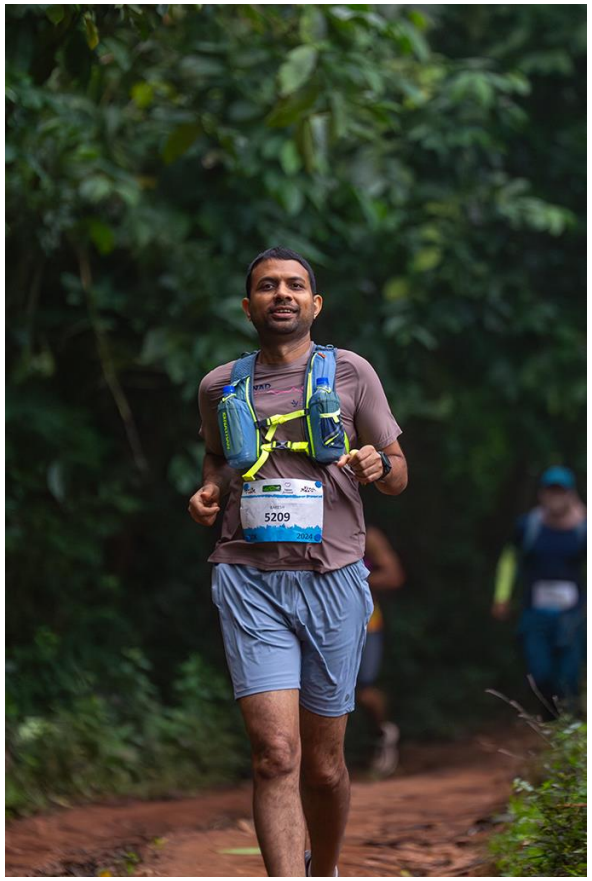
Rakesh Kandula
Technical Marketing Engineer

BRKSPG-2868

About Me

- Technical Marketing Engineer @ Cisco
- 17+ Years in Cisco
- Current Focus Areas
  - Trustworthy Systems
  - Platform Security Chips
  - Secure Boot
  - Quantum Safe Security
  - DDoS Solutions, etc.
- Outdoor enthusiast & marathoner who loves trail ultras





TRAIL ULTRA IN INDIA

Cisco Webex App

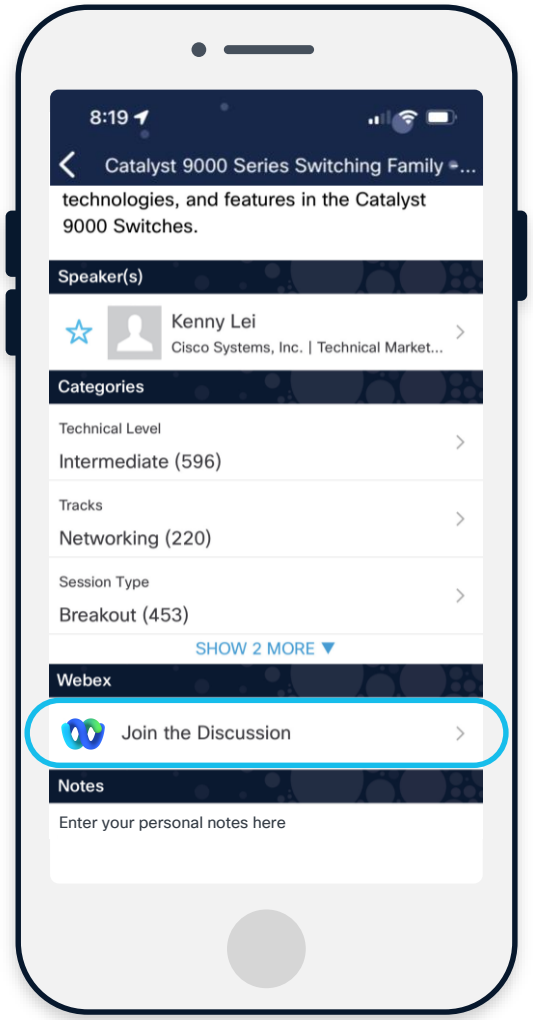
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

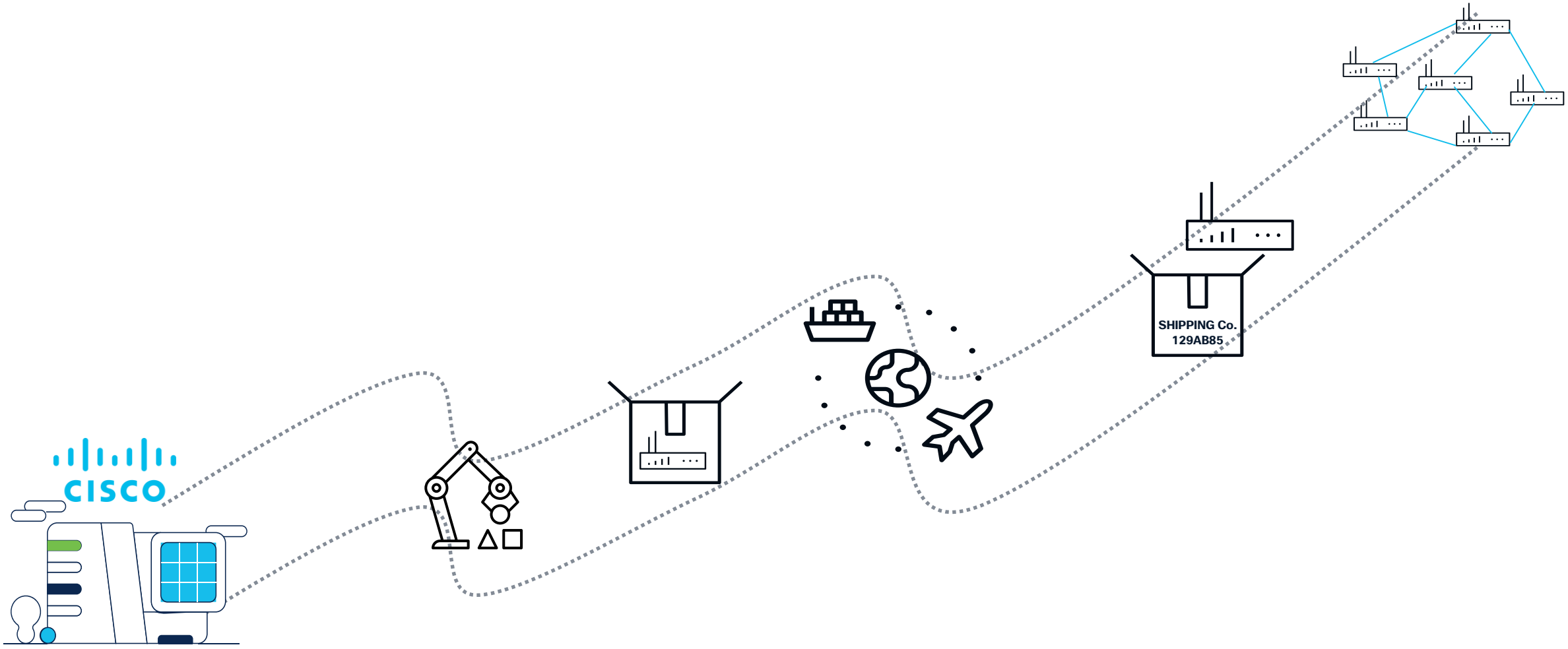
1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.

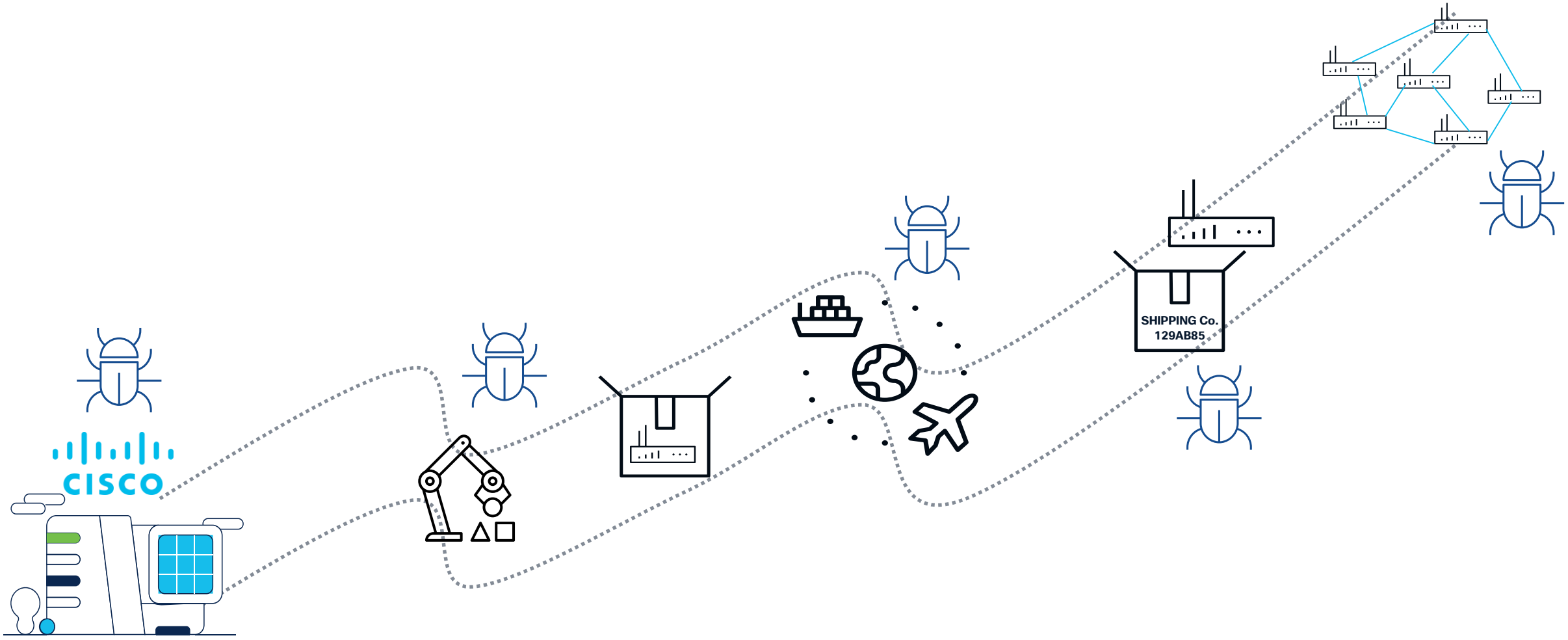


https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSPG-2868**

Journey of a Router: Design to Deployment



Threat Surface: Design to Deployment



Secure By Design At Every Stage

SECURE BY DESIGN AT EVERY STAGE

Agenda

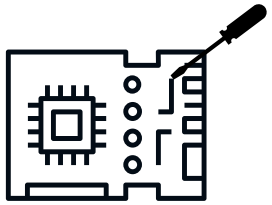
01 Secure Design & Development

02 Supply Chain Security

03 Secure Deployment

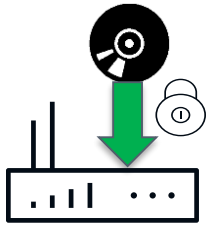
04 Beyond Deployment

Cisco’s Top Security Design Considerations

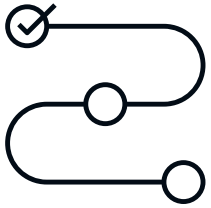


Hardware Tampering Detection

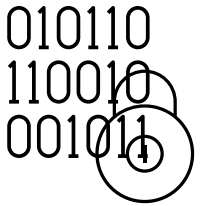
Counterfeit Hardware Detection



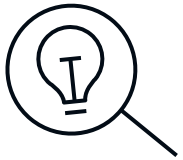
Secure Boot



Operational Security



Data Protection



Product Integrity Visibility

Legal / Certification Requirements

Internal Threats

Secure Design & Development

Building A Resilient & Trusted Infrastructure

Secure Development Lifecycle

Secure Coding Guidelines, Build Security, SSDF*, Threat modelling, etc.

Prevent Vulnerabilities in Our Offers

Designing Trustworthy Products

- Ensuring Hardware Integrity
- Providing Boot Integrity
- Providing Runtime Defenses
- Ensuring Data Protection
- Strengthening Operational Security

Ensure Hardware + Software Integrity

*Secure Software Development Framework – https://csrc.nist.gov/projects/ssdf

Cisco’s Trustworthy Platforms Overview

Trust Begins in Hardware

Trust Anchor Module with anti-counterfeit design

Enabling Trust in the Network OS

Hardware Anchored Cisco Secure Boot, Chip Guard

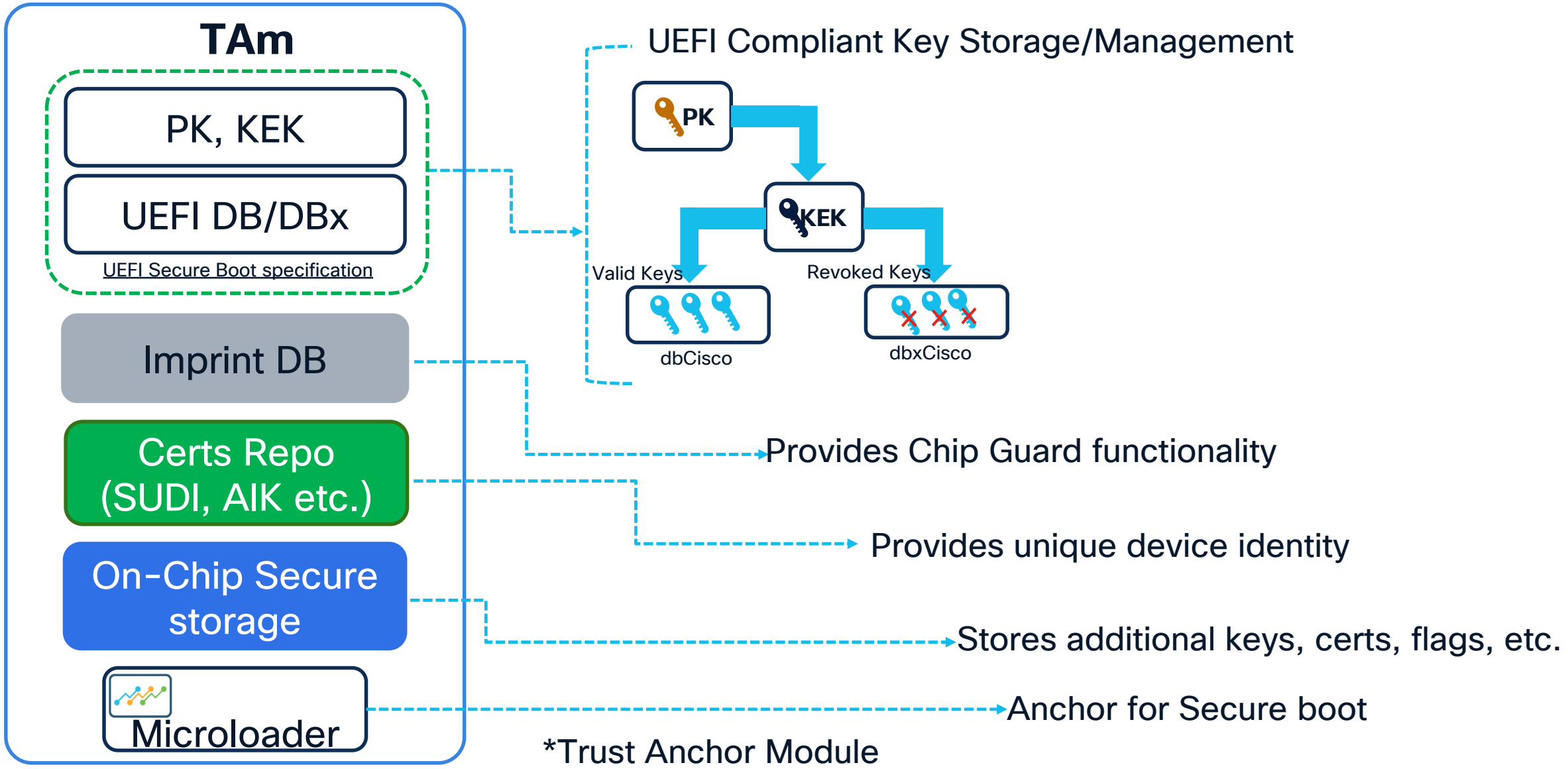
Maintaining Trust at Runtime

Run-time Defenses, Config Encryption, DDoS Protection

Visualize and Report on Trust

Trust Dossier & Crosswork Trust Insights

Enabling Trust in Hardware – Cisco's TAm* Chip



Supply Chain Security

Supply Chain Threat Surface

Increasing Supply Chain Attacks

1. Compromising CPU Integrity
2. Compromising ASIC Integrity
3. Compromising Boot Media

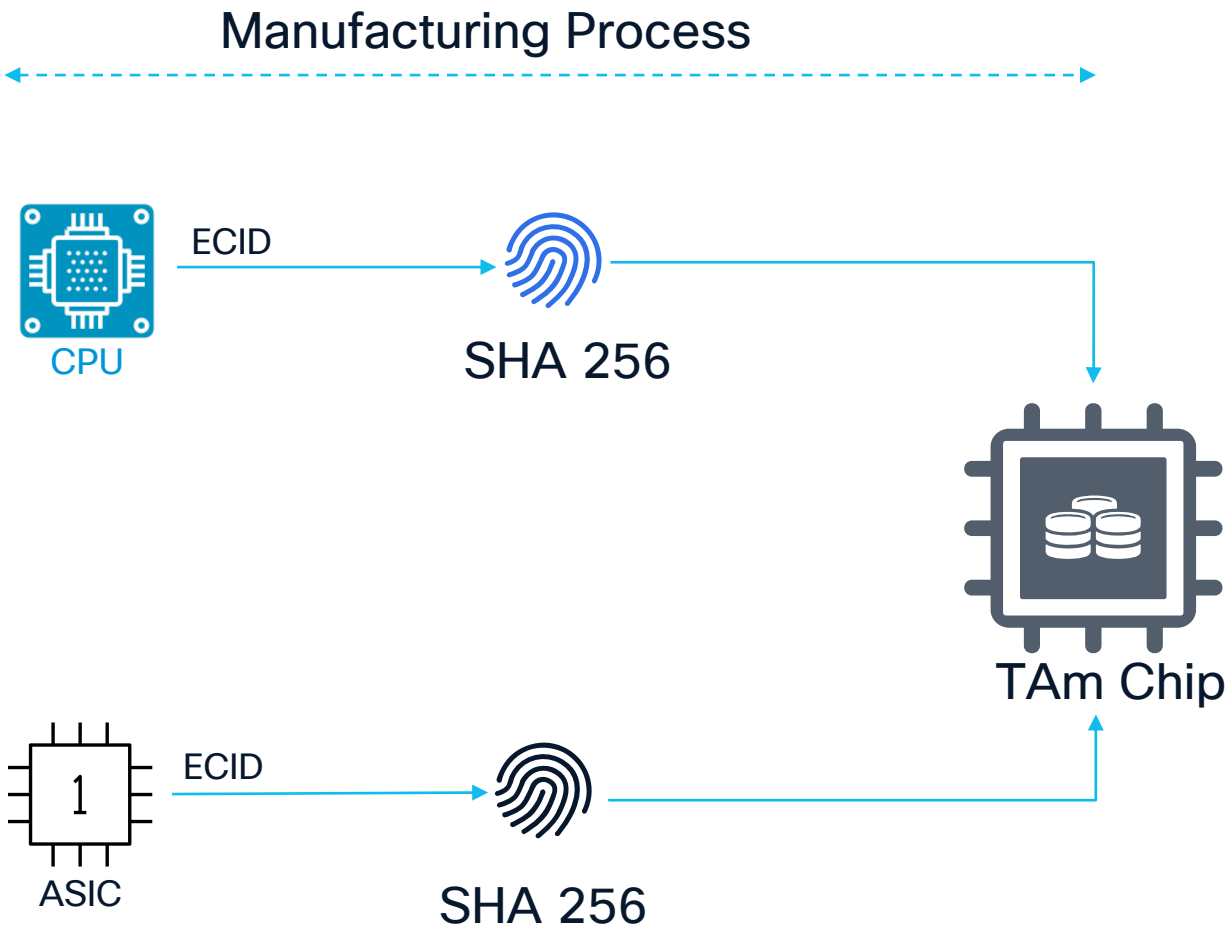
Increasing Counterfeit Hardware

1. Counterfeit hardware sold in resale markets
2. Swapping of genuine hardware during transit
3. Swapping of genuine hardware during deployment

Introducing Chip Guard

1. Detects counterfeit CPU/NPU on routers
2. Enabled by ImprintDB in TAm chip
3. Part of BIOS sequence during boot
4. Chip Guard verification failure halts the boot process

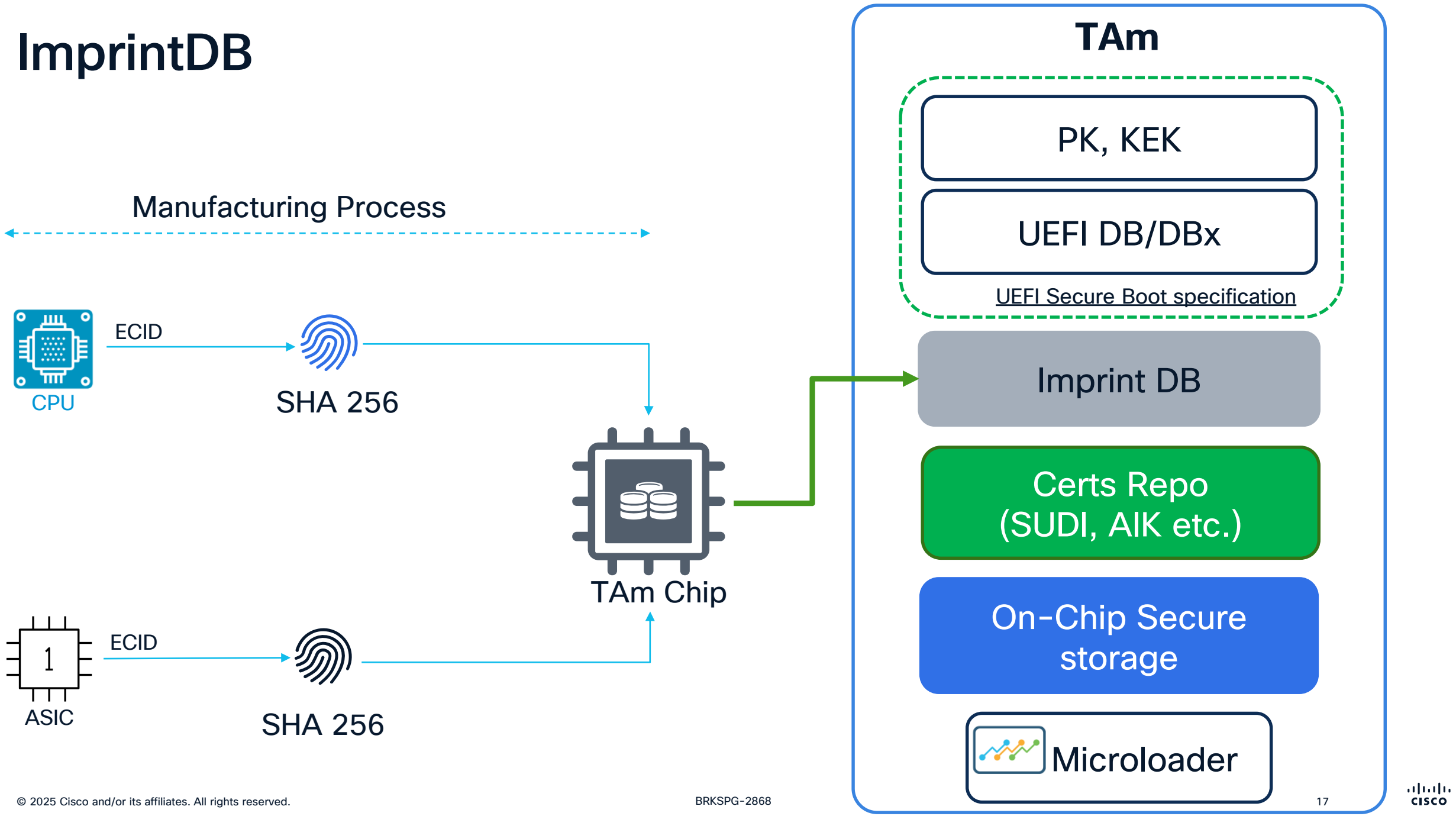
What is ImprintDB?



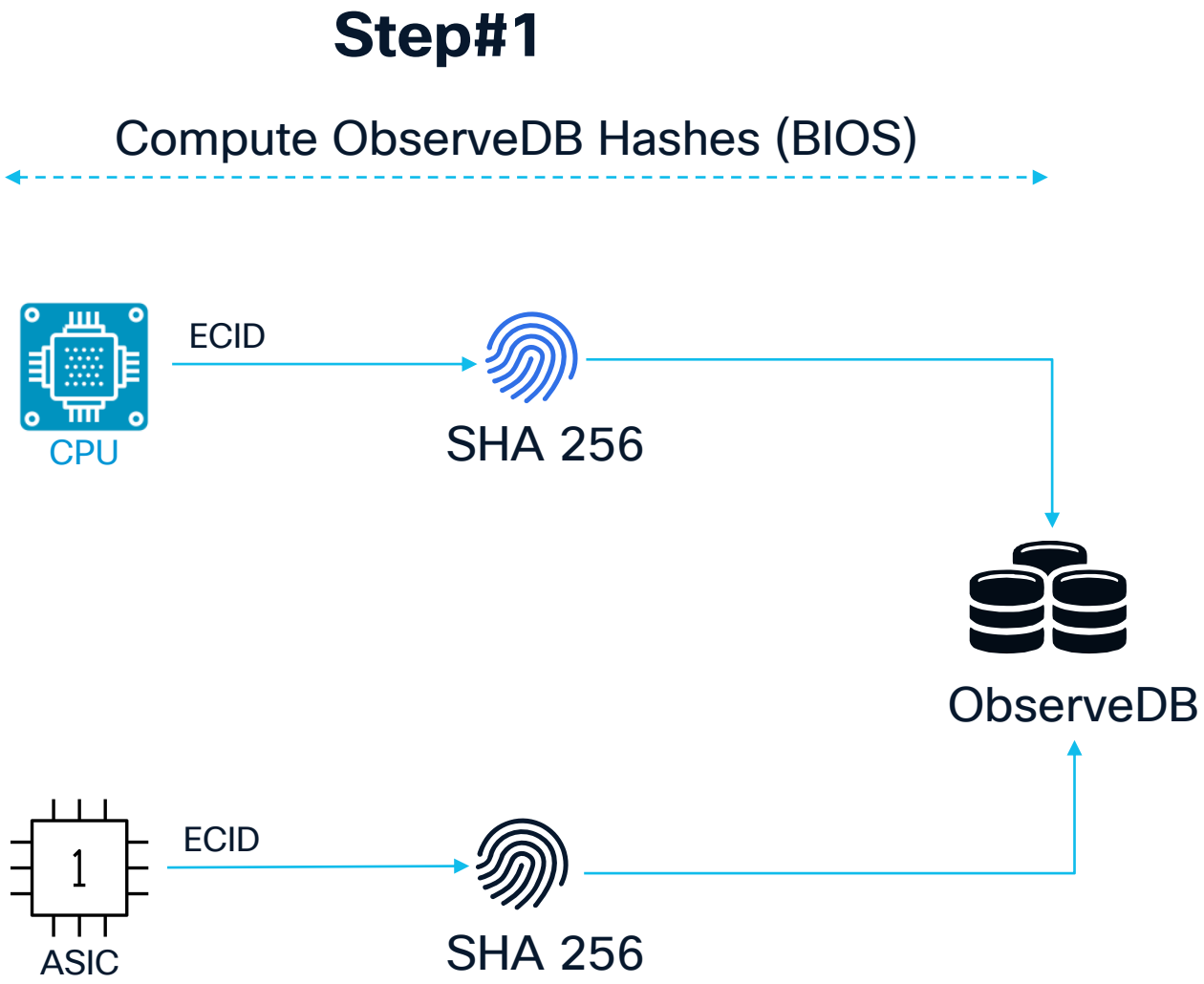
- During manufacturing, the SHA-256 hash of the ECID* of the CPU and NPU are calculated
- These hashes are then programmed inside the TAm chip
- The programmed hash values form the ImprintDB inside the TAm chip
- The ImprintDB cannot be modified during runtime

***E**lectronic **C**hip **ID**

ImprintDB



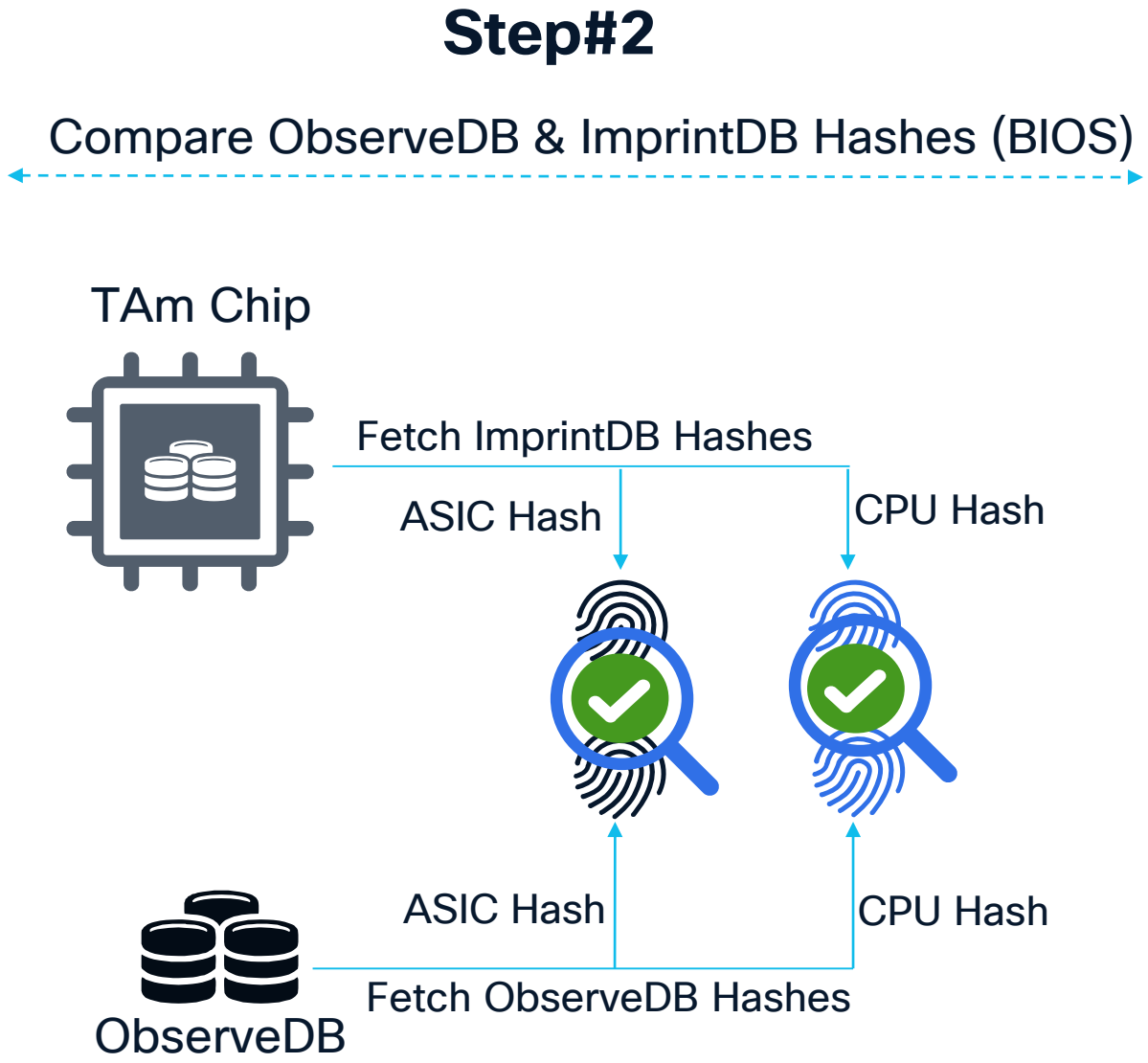
Chip Guard Workflow (BIOS)



- BIOS reads the ECID of the chips and computes their hashes
- Each of the hashes is then extended into a PCR inside TAm chip
- These set of observed hashes forms the ObserveDB

Chip Guard Workflow (BIOS)

- BIOS fetches the factory programmed hash values from ImprintDB
- The hash values are compared with the ObserveDB generated in the previous step
- BIOS continues with boot process if and only if the hashes match

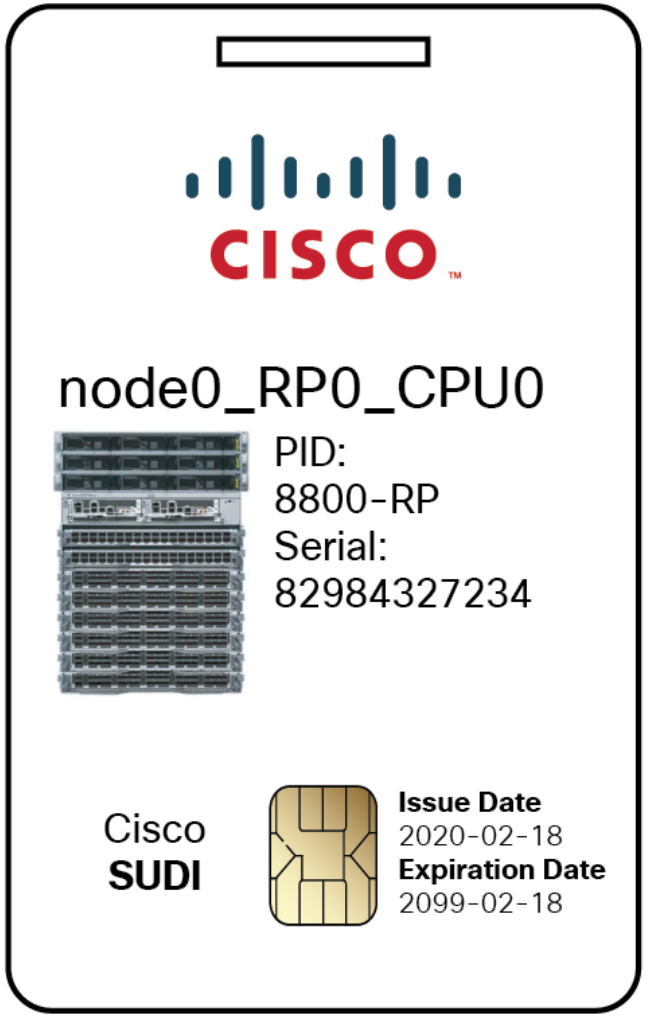


Tackling Counterfeit Hardware

Secure Unique Device Identity (SUDI)

"How do I know this is really my router?"

- Unique cryptographic key embedded in hardware trust anchor module within every IOS XR Router
  - Secure Unique Device Identifier (SUDI)
  - Provides 802.1AR Secure Device Identity
  - Immutable key imbedded in Trust Anchor Module at time of manufacture
  - Signed by Cisco for proof of authenticity
  - Includes PID and Serial number of device
- Cryptographically strong identification of remote hardware
- Establishes unique, immutable hardware identity



SUDI Workflow For Hardware Integrity Validation

Challenge

1. Challenge the remote router with a random number to provide it's SUDI certificate.
2. The random number is used to ensure the freshness of the response received from the router.

Response

1. Router responds back with the SUDI certificate chain signed by the router unique SUDI private key.
2. The random number is included in the response signature.

Validation

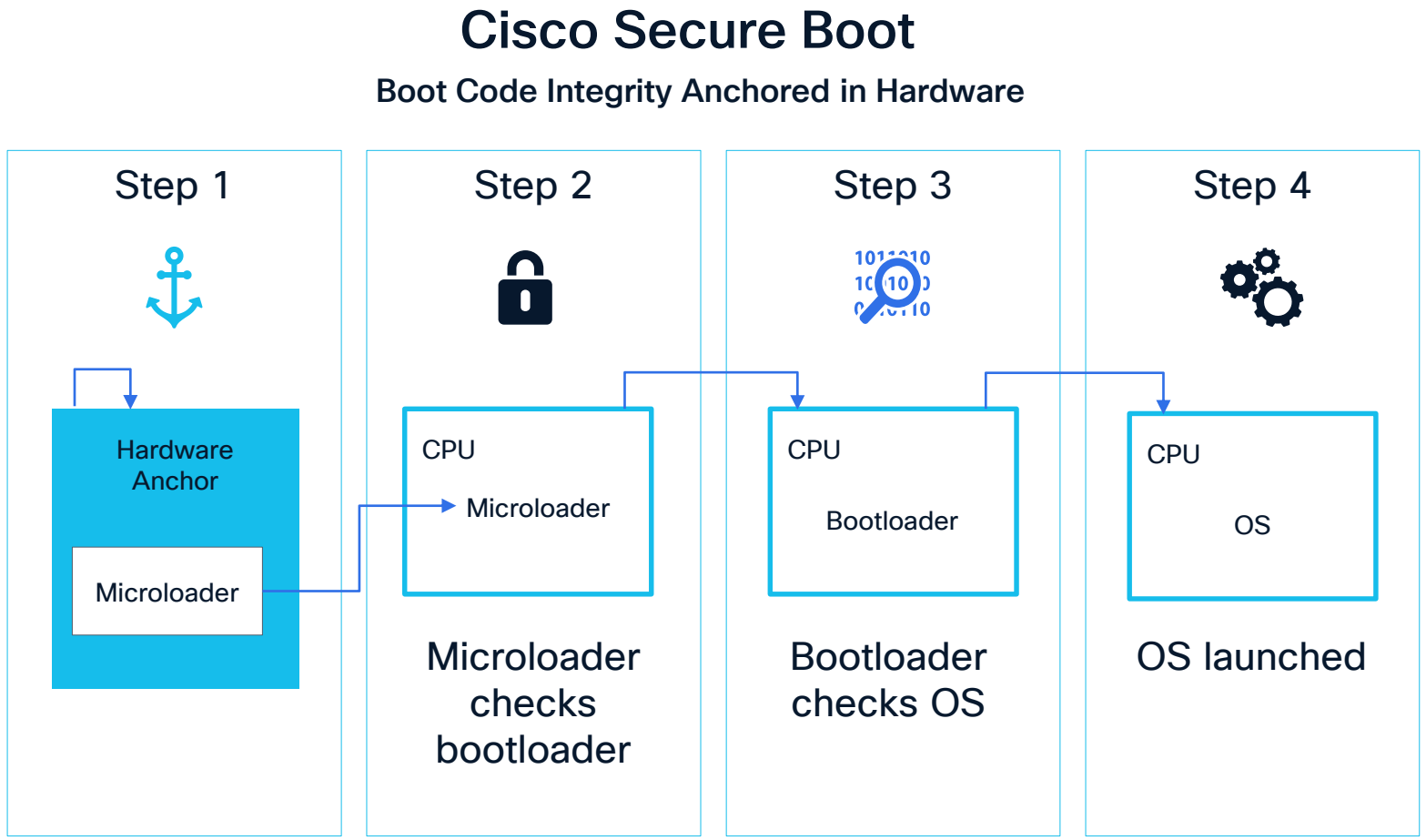
1. Verify the signature of the SUDI response using the the SUDI leaf cert.
2. Verify the SUDI leaf certificate chain using the root & Sub-CA certs from Cisco.

Link to SUDI verifier scripts - https://github.com/ios-xr/sudi_verifier

Secure Deployment

Cisco Secure Boot – Overview

Anchors Secure Boot in Hardware to Create a Chain of Trust

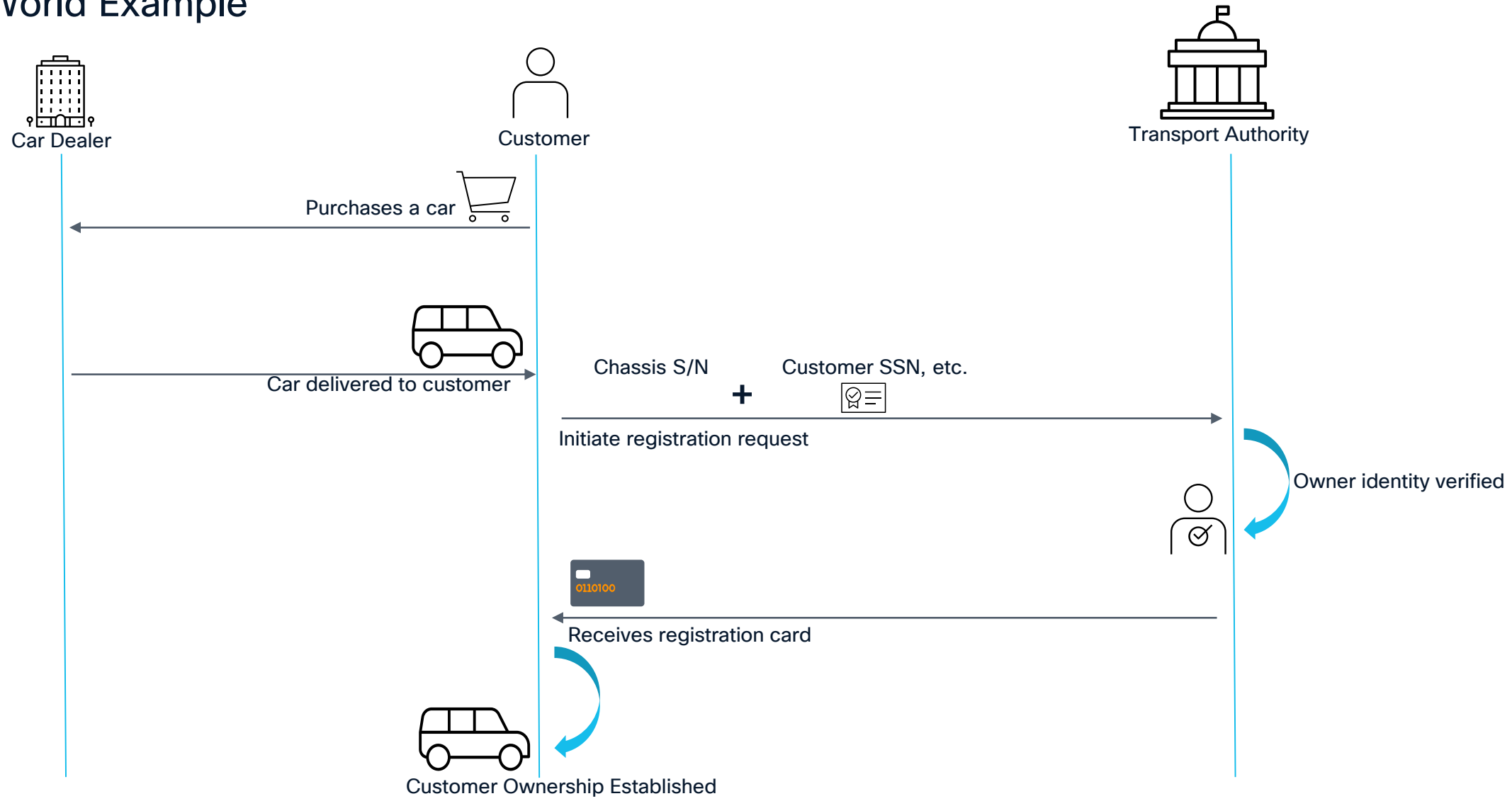


Software Authenticity:

- Only authentic signed Cisco software boots up on a Cisco platform
- The boot process stops if any step fails to authenticate
- Each step validates the signature of the next stage before proceeding
- The TAm chip acts as an anchor to the secure boot and the chain of trust starts from hardware

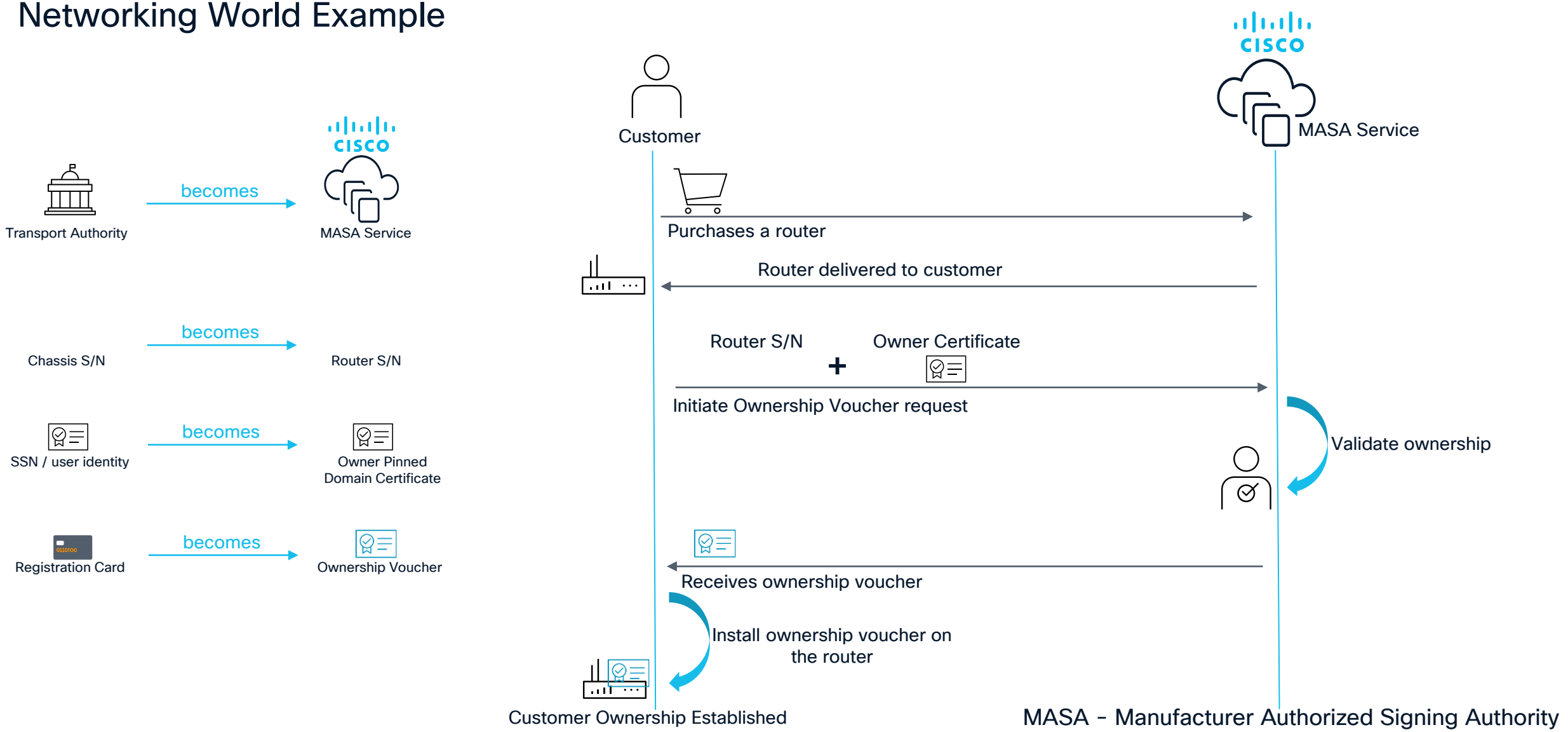
What is Ownership Establishment?

Physical World Example



What is Ownership Establishment?

Networking World Example



Ownership Voucher (O.V) (RFC 8366)

Reference Slide

Yang model for O.V.

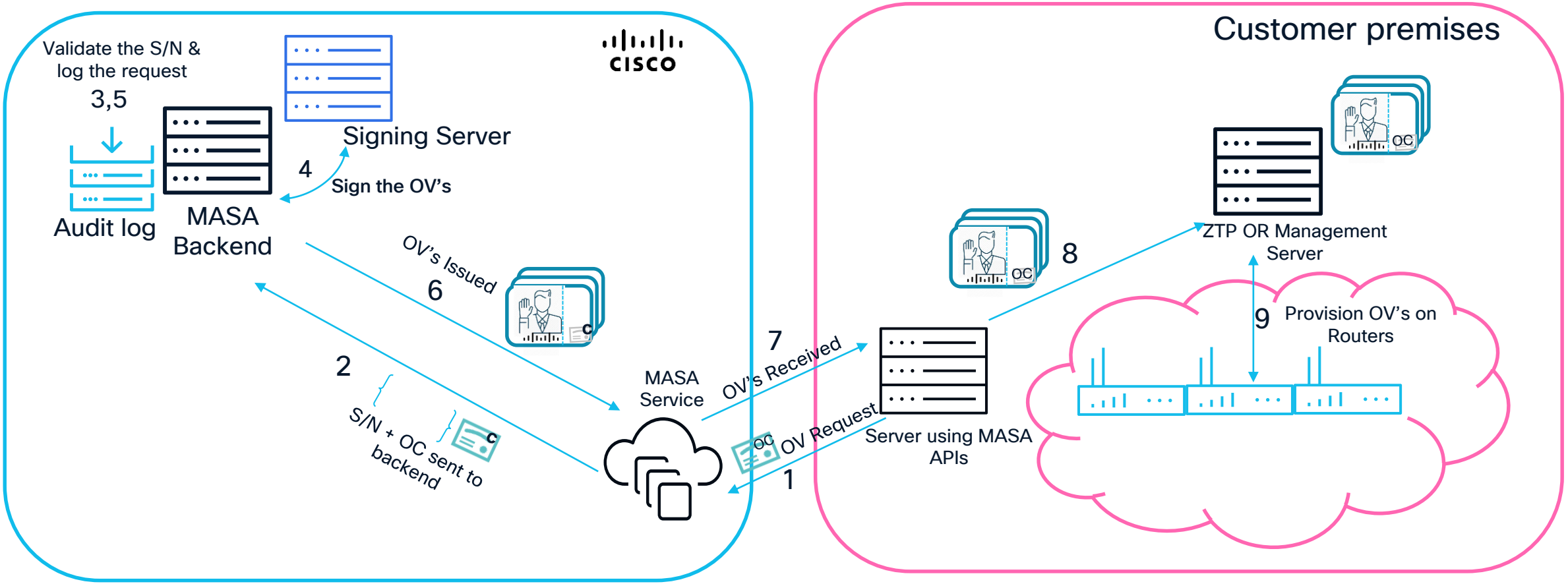
```
module: ietf-voucher

  yang-data voucher-artifact:
      +---- voucher
         +---- created-on                          yang:date-and-time
         +---- expires-on?                         yang:date-and-time
         +---- assertion                           enumeration
         +---- serial-number                       string
         +---- idevid-issuer?                      binary
         +---- pinned-domain-cert                  binary
         +---- domain-cert-revocation-checks?      boolean
         +---- nonce?                              binary
         +---- last-renewal-date?                  yang:date-and-time
```

Reference: https://tools.ietf.org/html/rfc8366

- Ownership Voucher is an artifact coming from the manufacturer (MASA*) of the router being bootstrapped into the network.
  * MASA – Manufacturer Authorized Signing Authority
- JSON artifact modeled as shown in YANG and signed using a CMS structure.
- The primary purpose of an Ownership Voucher is to securely convey a customer provided certificate, the "Pinned-Domain-Cert" (PDC) to the router being onboarded.
- Pinned-domain-cert (PDC): The owner cert is rooted to the chain of trust leading to the pinned-domain cert. This means PDC can be the root cert for OC or an intermediate cert for OC or the same as OC (self-signed).

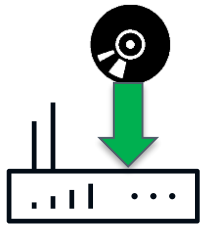
How To Establish Ownership?

Automated MASA Service Workflow



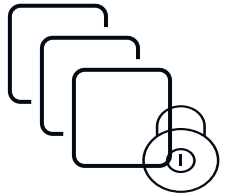
MASA - Manufacturer Authorized Signing Authority

Ownership Establishment – Use cases



Secure Zero Touch Provisioning (SZTP)

RFC8572 compliant secure zero touch provisioning of routers



Application Signing

Onboard Key Package for Signed Apps

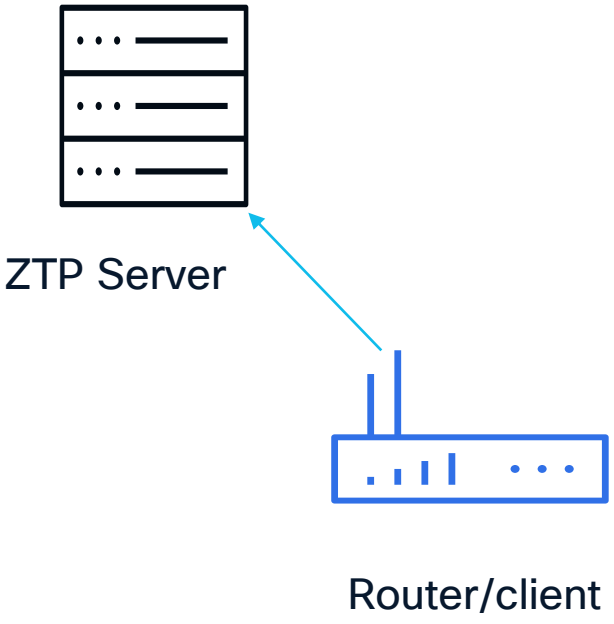
Consent Based Security Features

Additional consent for critical security features

Security Concerns for Zero Touch Provisioning (ZTP)

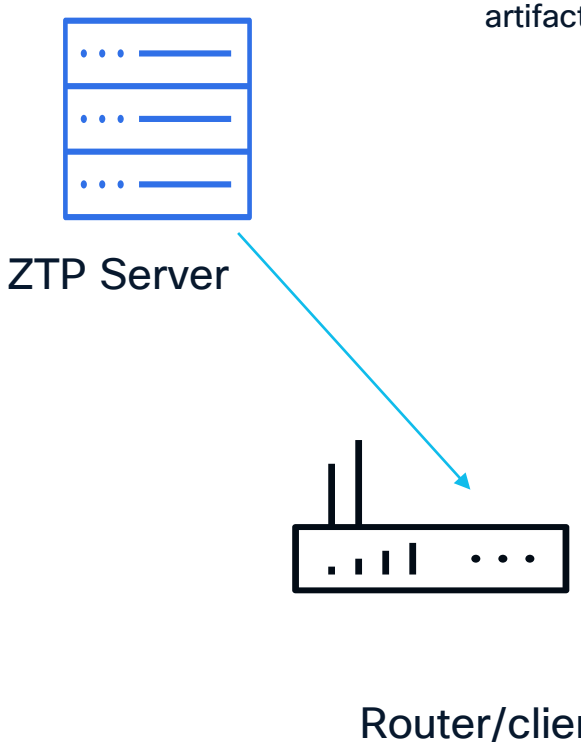
Router/Client Validation

Server must validate router/client cert (SUDI cert) before offering artifacts/secrets/configs



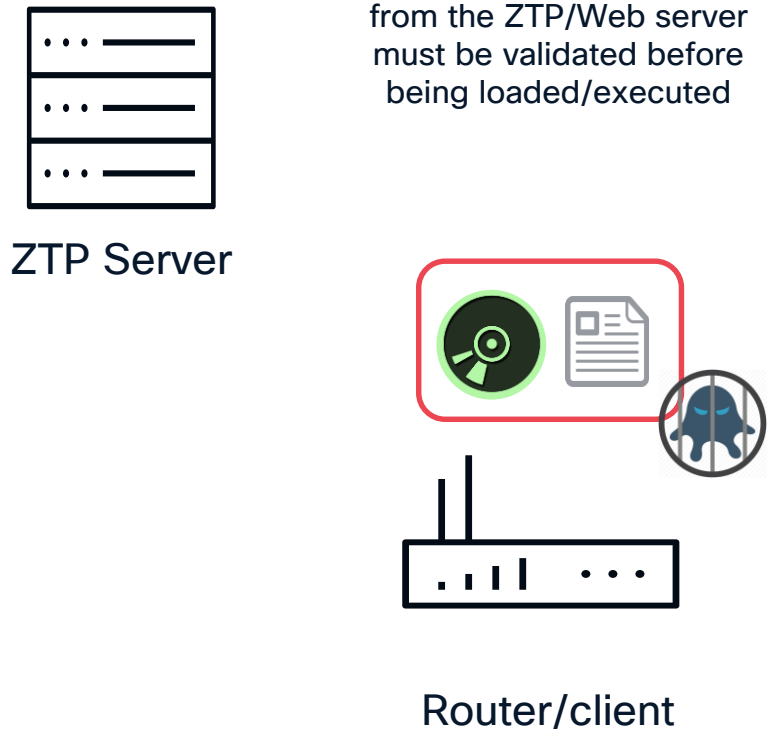
Server Validation

Router/client must validate the server offering artifacts

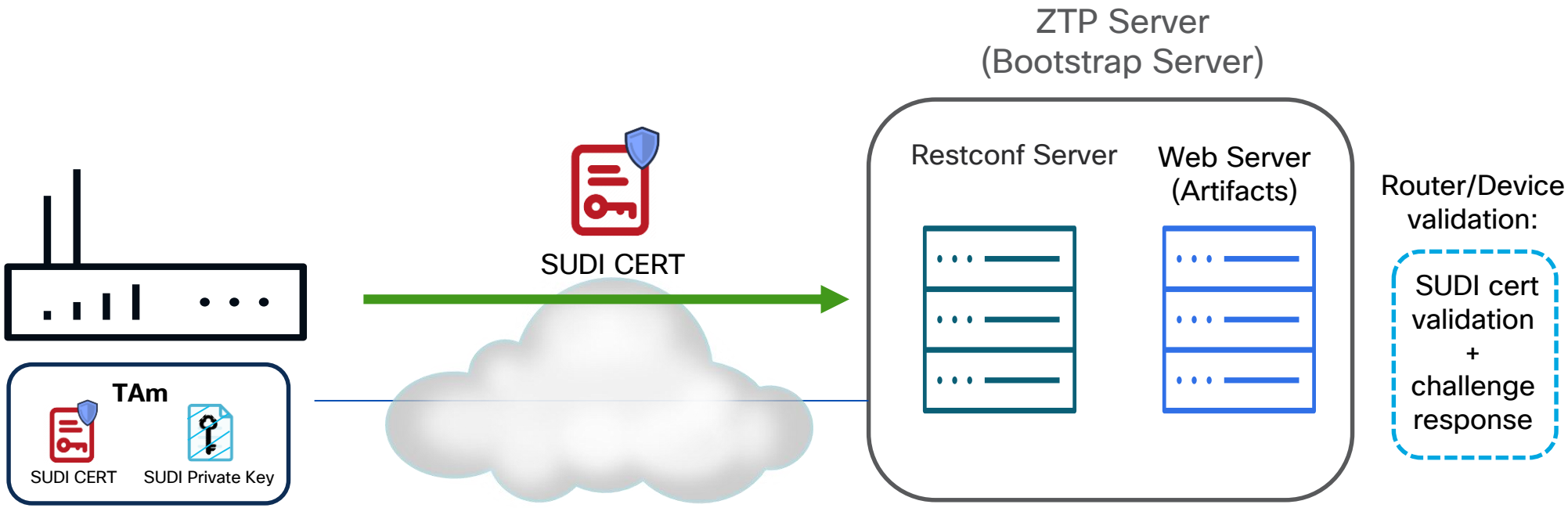


Artifact Validation

The artifact downloaded from the ZTP/Web server must be validated before being loaded/executed

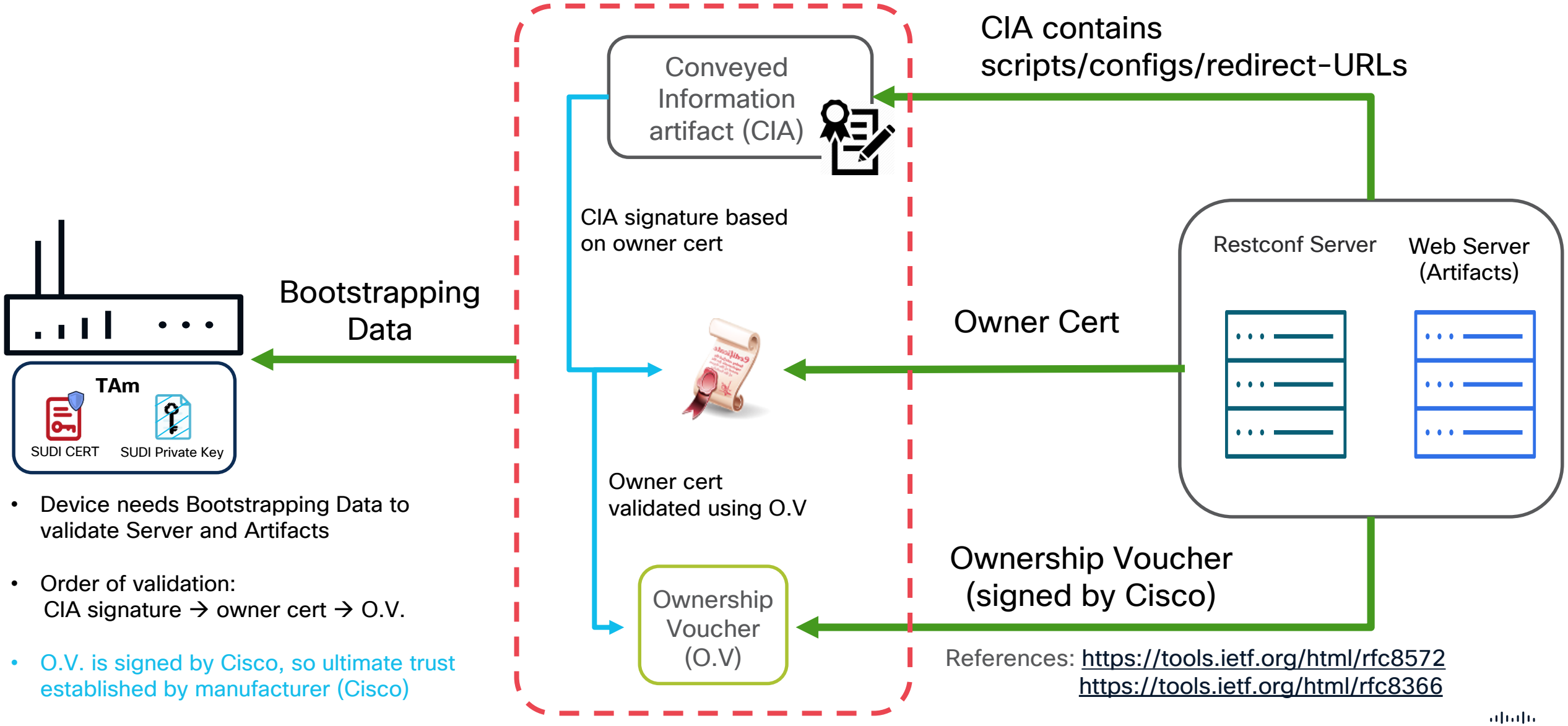


Secure ZTP (RFC8572): Router Validation



Reference: https://tools.ietf.org/html/rfc8572

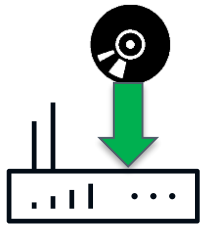
SZTP Artifacts : ZTP Server + Artifact Validation



- Device needs Bootstrapping Data to validate Server and Artifacts
- Order of validation:
  CIA signature → owner cert → O.V.
- O.V. is signed by Cisco, so ultimate trust established by manufacturer (Cisco)

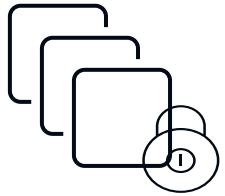
References: https://tools.ietf.org/html/rfc8572
https://tools.ietf.org/html/rfc8366

Ownership Establishment – Use cases



Secure Zero Touch Provisioning (SZTP)

RFC8572 compliant secure zero touch provisioning of routers



Application Signing

Onboard Key Package for Signed Apps

Consent Based Security Features

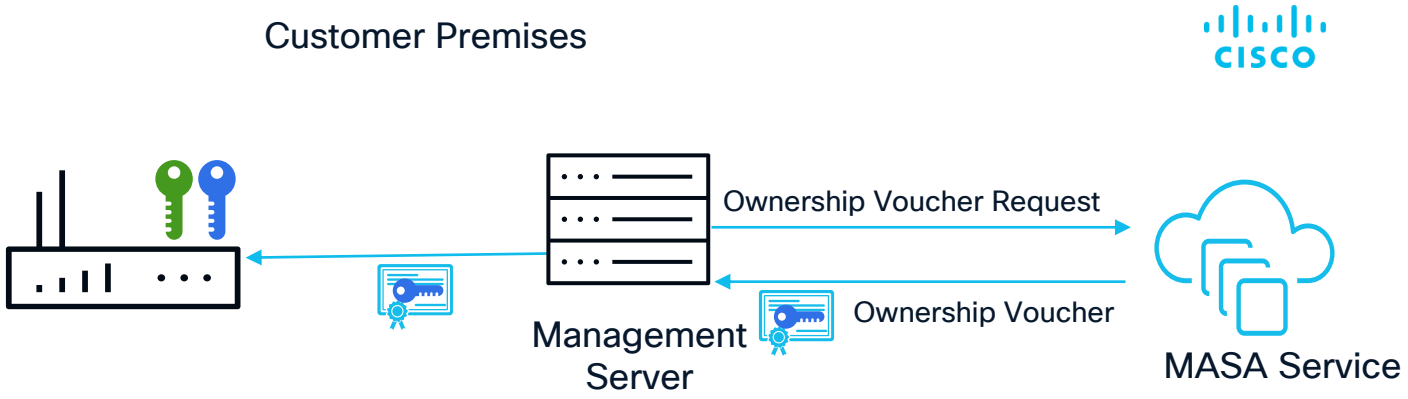
Additional consent for critical security features

Application Signing Use case – Step#1

Factory-shipped Initial State

1. The router has only Cisco's public key
2. This key can verify only Cisco signed artefacts
3. Customer signed artefacts cannot be verified at this stage

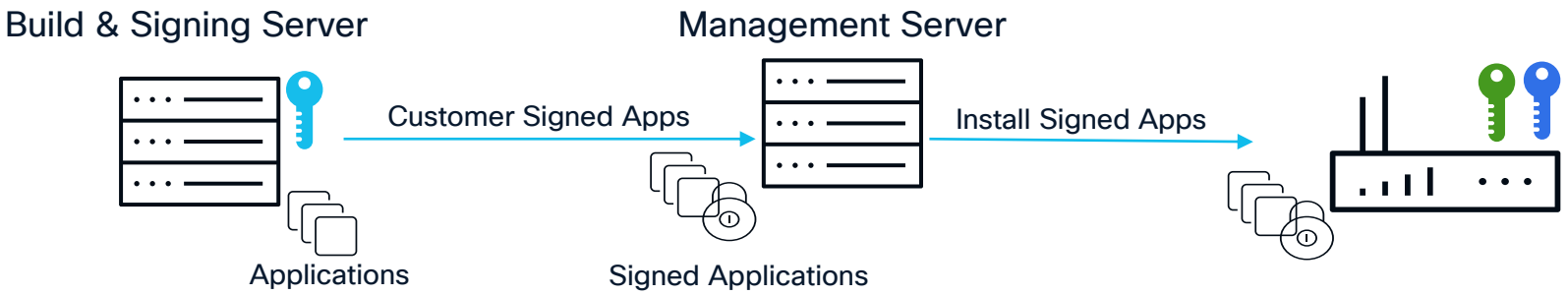
Ownership Established State



1. The router now has Cisco's & customer public keys
2. The customer key will be used to verify signed artefacts from customers like signed apps
3. Multiple keys can be onboarded using key packages

Cisco Public Key Customer Private Key Customer Public Key

Application Signing Use case – Step#2

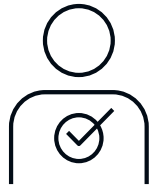


1. Customers can build their apps in their own environment and sign them with their own private key.
2. The signed customer app can then be installed on the router through their management or provisioning servers.
3. The same ownership key can be used to sign the apps or customers can create different keys for each of their use cases.
4. Multiple keys can be onboarded on the router using key packages once the ownership is established.
5. Customers can sign their own key packages with the ownership key

Cisco Public Key Customer Private Key Customer Public Key

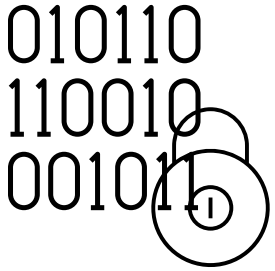
Beyond Deployment

Maintaining Operational Security



User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.



Data Protection

Various data protection aspects

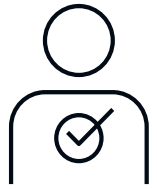
Remote Attestation

Periodic validation of device integrity

Consent Based Security Features

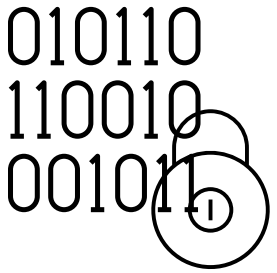
Additional consent for critical security features

Maintaining Operational Security



User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.



Data Protection

Various data protection aspects

Remote Attestation

Periodic validation of device integrity

Consent Based Security Features

Additional consent for critical security features

User Identity & Access Controls

SSH

1. Adopting Password less SSH
   a) Public-Key based authentication
   b) Certificate-based authentication
2. Disabling weaker ciphers

Multi Factor Authentication

1. Two-factor authentication for admins accessing the devices
2. Additional consent-based security* mechanism for sensitive features

AAA Controls

1. Using dynamic authentication and proper segregation of roles for users
2. Implementing stronger password policies & hashing mechanisms (Type-8, 9, 10)

Other Measures

1. Enabling Management Plane Protection (MPP)
2. Adopting secure transport methods (syslogs over TLS, SNMPv3, etc.)

*Discussed in later slides

Type-5 & Type-7 Deprecation Note

1. Type-5 secret configuration uses MD5 which is not secure and is being deprecated from 24.4.1 release.

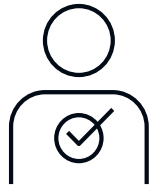
2. Type-7 password configuration is also not secure and is being deprecated from 24.4.1 release.

3. Existing configurations & upgrades will be supported till 25.2.1 and full deprecation is planned in 25.2.1 release.

4. Default option going forward will be type-10 secret configuration. Existing type-8 & type-9 methods will also continue to be supported.

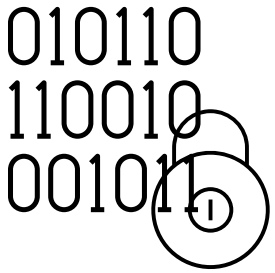
More deprecation details can be found here.

Maintaining Operational Security



User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.



Data Protection

Various data protection aspects

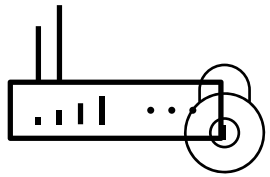
Remote Attestation

Periodic validation of device integrity

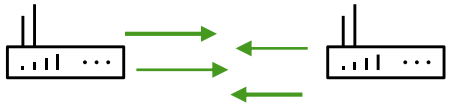
Consent Based Security Features

Additional consent for critical security features

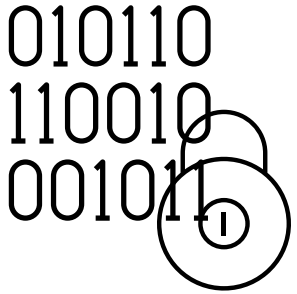
Various aspects of data protection



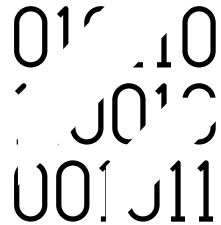
Data At Rest



Data In Transit



Data In Use



Data Sanitization

Data-At-Rest Protection

Configuration Encryption

1. Threat is from bad actors having offline physical access to routers
2. Must protect sensitive configuration data on the disk
3. Config encryption feature encrypts disk partition holding config data
4. Zeroization CLI for crypto erase operation during decommissioning

Data-In-Transit Protection

Transport Security

1. SSH, TLS, SNMPv3 for management plane & control plane data
2. New IPsec feature to protect management plane traffic
3. RADIUS over TLS (RFC6614) support from IOS-XR 24.3.1 release
4. Enable MACsec for line-rate data path traffic protection

Data-In-Use Protection

Runtime Security

1. Protect runtime data & processes from unauthorized access
2. SELinux support to provide access controls at process level
3. Kernel supports IMA (Integrity Measurement Architecture) for file integrity checks when files are accessed
4. Filesystem inventory* for a full inventory of files hashes for integrity checks even if a file wasn't accessed

*Details in later slides

Data Sanitization

Safe Decommissioning

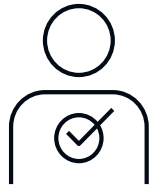
1. Persistent data from decommissioned devices can be a liability / security risk to operators.

2. IOS-XR's factory reset & zapdisk features help with disk wiping.

3. Statement of volatility available on trust portal to sanitize various data-bearing components on the routers.

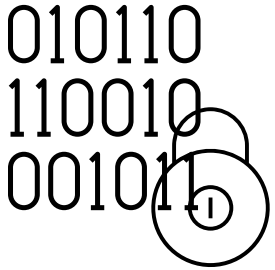
4. Make data sanitization as part of your organization's data security policies.

Maintaining Operational Security



User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.



Data Protection

Various data protection aspects

Remote Attestation

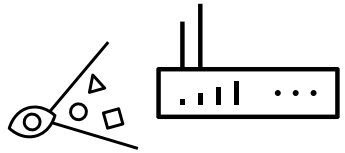
Periodic validation of device integrity

Consent Based Security Features

Additional consent for critical security features

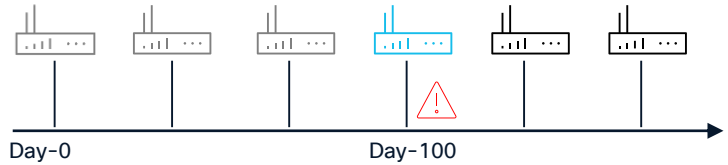
Remote Attestation – What & Why?

Visibility of device posture



1. Ability to verify device posture remotely
2. Device posture could be
   a) Hardware Identity
   b) Boot integrity status
   c) Runtime integrity status
   d) Modification of running configuration (hash)
   e) Hardware & Software inventory

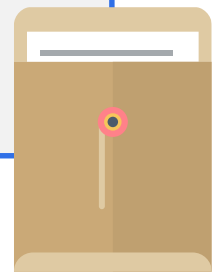
Device posture can change over time

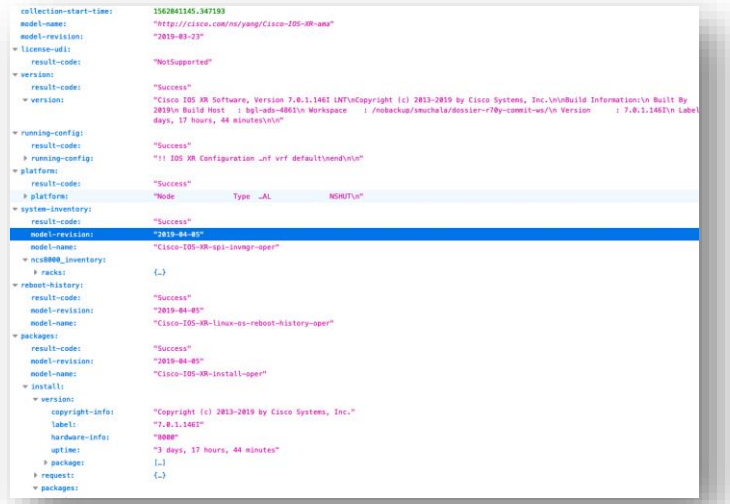


1. Routers deployed in remote locations have a potential of being tampered at hardware layer
2. Device posture could change over time and any changes need to be alerted
3. Posture changes could be both hardware & software
4. Routers must have a native mechanism to provide reporting on trust

Reporting on Trust – IOS-XR Trust Dossier

- OS Version + Platform Output
- Anti-Replay Nonce
  - Specified as CLI option
- System Hardware inventory
  - Cisco-IOS-XR-invmgr-oper.yang
  - Cisco-IOS-XR-spi-invmgr-oper.yang
- Hardware Attestation Data
  - Cisco-IOS-XR-remote-attestation-act.yang
- SUDI (Hardware Identity) Certificate
  - Separate signature per FRU (includes nonce)
- Software Package inventory
  - Cisco-IOS-XR-spirit-install-instmgr-oper.yang
  - Cisco-IOS-XR-install-oper.yang
- Reboot History
  - Cisco-IOS-XR-linux-os-reboot-history-oper.yang
- Rollback History
  - Cisco-IOS-XR-config-cfgmgr-exec-oper.yang

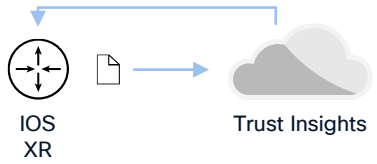




- Human-readable JSON formatted output via CLI command
- Signed envelope (not encrypted)

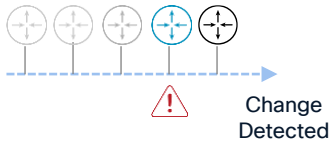
How Remote Attestation Works – Trust Insights

1



Trust Insights securely requests and collects signed evidence (trust dossier)from IOS XR devices

2



Dossier evidence verified and added to timeline of running hardware and software

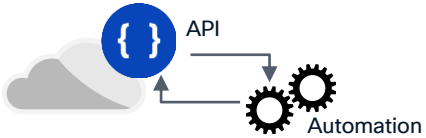
3

Trust data verified against Known-Good-Values (KGV) for hardware and software from Cisco

4

Trust Insights delivers assured inventory reporting with history, and trust visibility for IOS XR systems

5

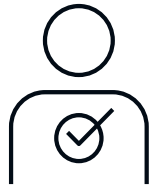


Trust and Assured Inventory data accessible via API to enable Closed-Loop Automation

File System Inventory

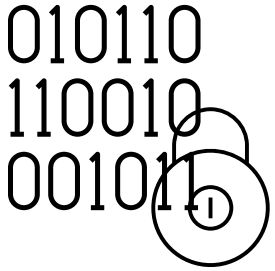
1. Provides an on-demand snapshot of all XR files.
2. This is optional and must be explicitly enabled.
3. All the file hashes are collected irrespective of a file being accessed or not.
4. Users can configure the snapshot timer. The default timer interval is 15 mins.
5. During bootup a complete snapshot of all files in the rootfs will be created.
6. Later incremental snapshots (includes only modified files) would be created based on monitoring interval.

Maintaining Operational Security



User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.



Data Protection

Various data protection aspects

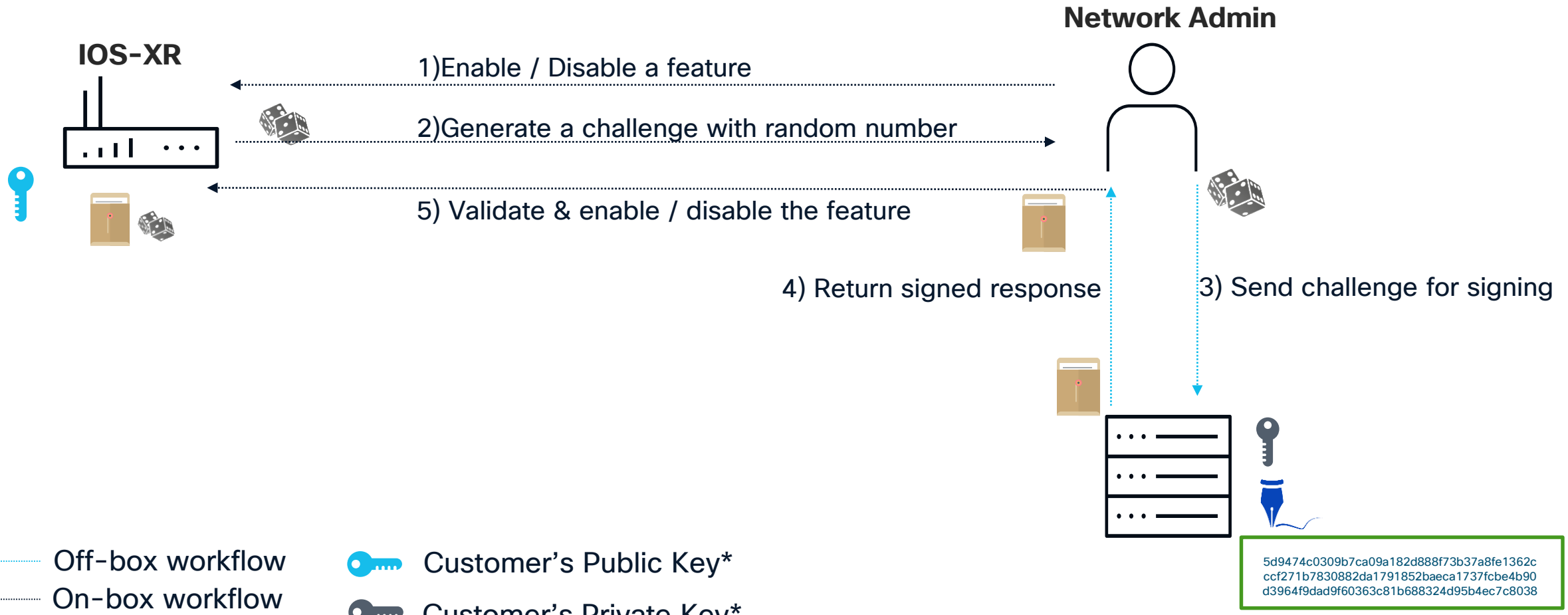
Remote Attestation

Periodic validation of device integrity

Consent Based Security Features

Additional consent for critical security features

CLI Challenge / Response – Consent Workflow



Off-box workflow

On-box workflow

Customer's Public Key*

Customer's Private Key*

*Applicable for Customer Consent Only

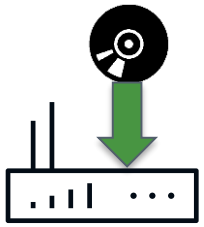
Consent Based Security Features

Re-Image Protection

Provides re-image protection for routers to deter thefts

Gating Lawful Interception

Ability to control enable/disable of Lawful Interception



Disabling Secure ZTP

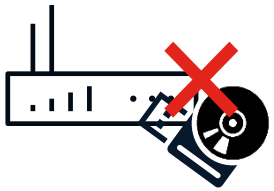
Consent to downgrade the security posture of Zero Touch Provisioning (ZTP)

Factory Reset

Consent to perform factory reset, manufacturing key restore, etc.

And more...

Consent Based Security Features

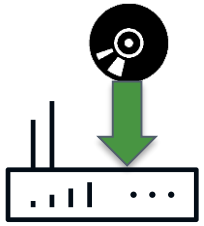


Re-Image Protection

Provides re-image protection for routers to deter thefts

Gating Lawful Interception

Ability to control enable/disable of Lawful Interception



Disabling Secure ZTP

Consent to downgrade the security posture of Zero Touch Provisioning (ZTP)

Factory Reset

Consent to perform factory reset, manufacturing key restore, etc.

And more...

Re-Image Protection For Routers

Consent Based Security Features Use case

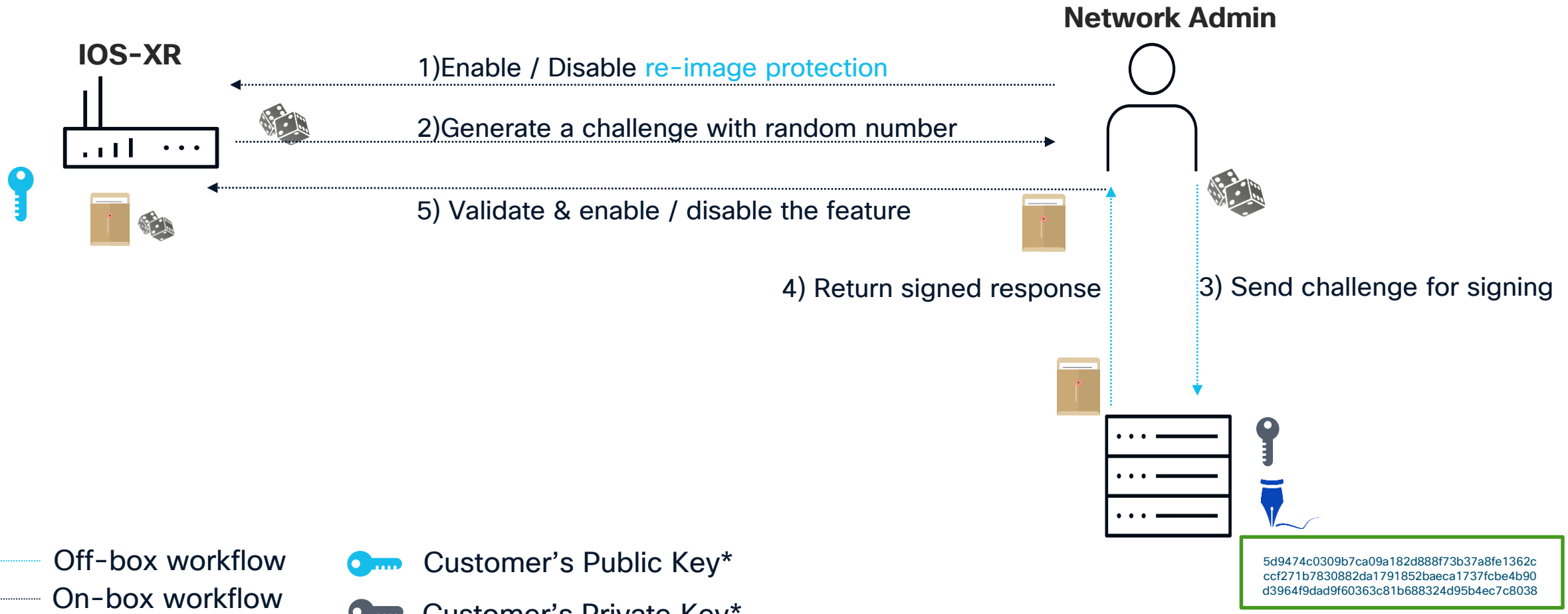
1. Increasing incidents of cell site routers in remote locations being stolen
2. The stolen routers are factory reset by booting through USB or PXE boot that erases the older running config too
3. These routers are then sold in illegal markets
4. Some incidents involve rogue internal employees too

Re-Image Protection For Routers

Feature Workflow

1. New IOS-XR CLI with additional consent to disable USB/PXE boot.
2. Feature enablement flag (status) is stored inside the tamper-resistant on chip TAm secure storage.
3. Feature enablement status is persistent across reloads & disk erasures.
4. During Cisco's Secure boot workflow, BIOS reads the feature status and disables USB/PXE boot if feature is enabled.

Re-Image Protection – Consent Workflow



*Applicable for Customer Consent Only

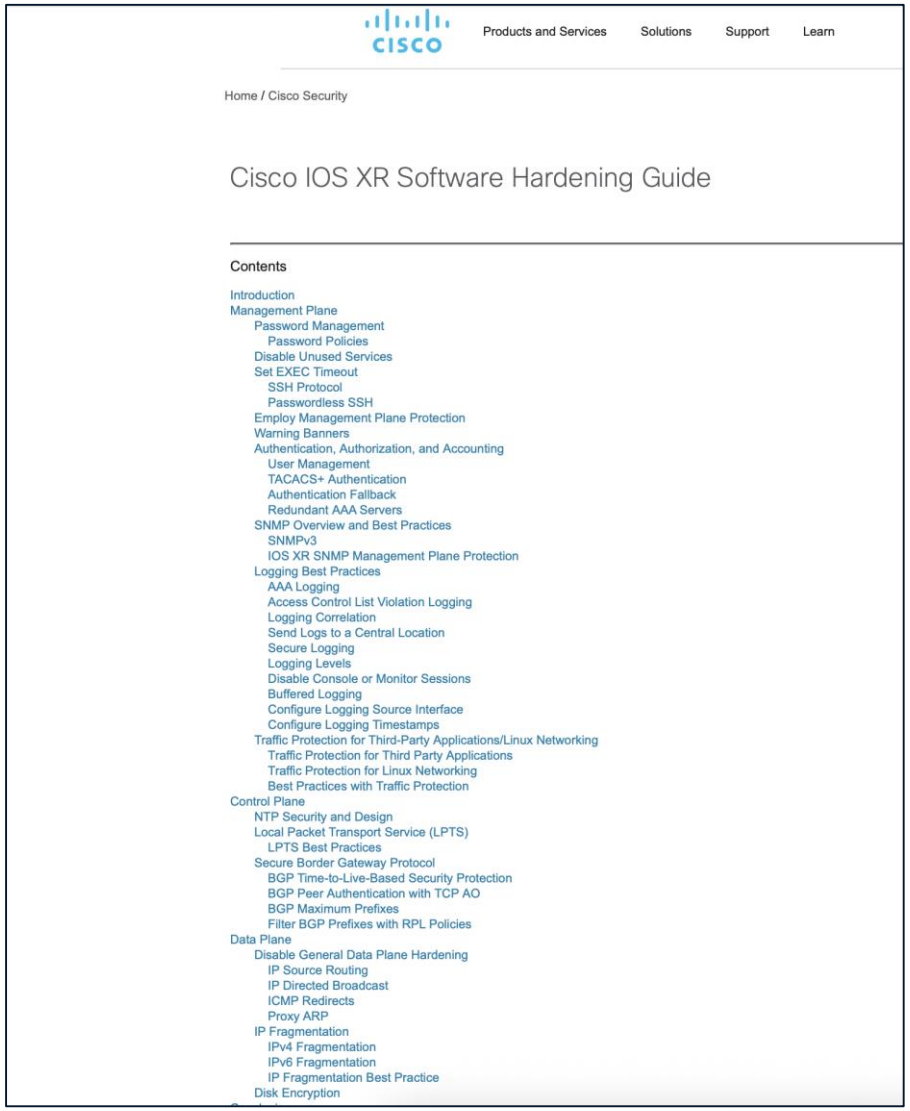
IOS-XR Operational Security Enhancements

1. RADIUS over TLS (RFC 6614) from 24.3.1 release.
2. SELinux in enforcement mode for Cisco 8000 from 24.4.1 release.
3. Certificate enrollment using EST* (RFC 7030) from 25.1.1 release.
4. Secure Disk Erase on Cisco 8000 platforms from 25.2.1 release.
5. Full disk encryption on Cisco 8000 platforms in 25.2.1 release.
6. TACACS+ over TLS in 25.2.1 release.

*Enrollment over Secure Transport

Operational Security is a journey...

1. Control Plane Protection
2. Routing Protocols Security
3. Certificates / Key rotation
4. Accounting, NetFlow for visibility
5. And many more ...



cisco Products and Services Solutions Support Learn

Home / Cisco Security

Cisco IOS XR Software Hardening Guide

Contents

IOS-XR Hardening Guide - https://sec.cloudapps.cisco.com/security/center/resources/Cisco-IOS-XR-HardeningGuide

Breakout Session on Salt Typhoon Attack & Security Hardening

June 11th, 2:30 pm

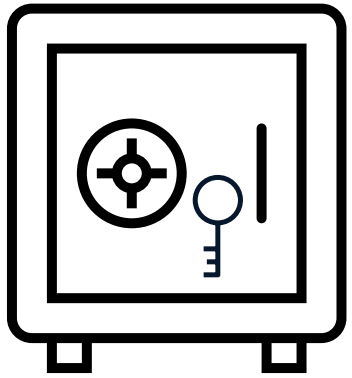
Quantum Safe Security

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

Public Key



Private Key

Digital Signatures

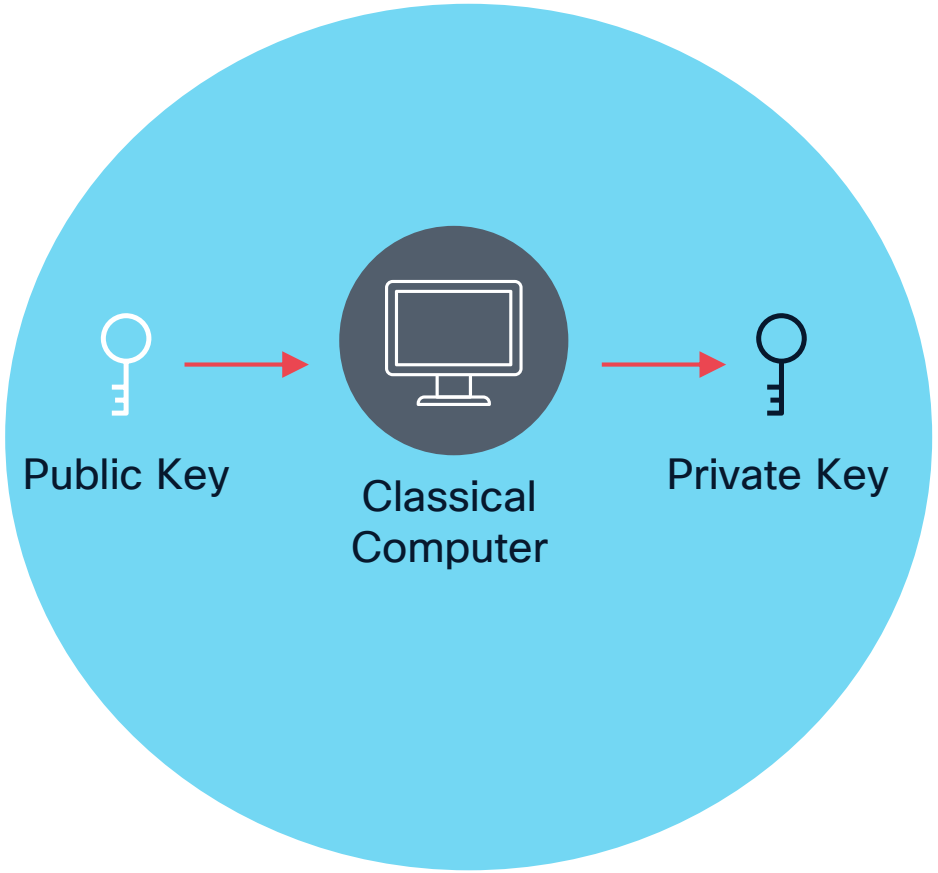
Encrypt with private key

Identity

Encrypt with private key

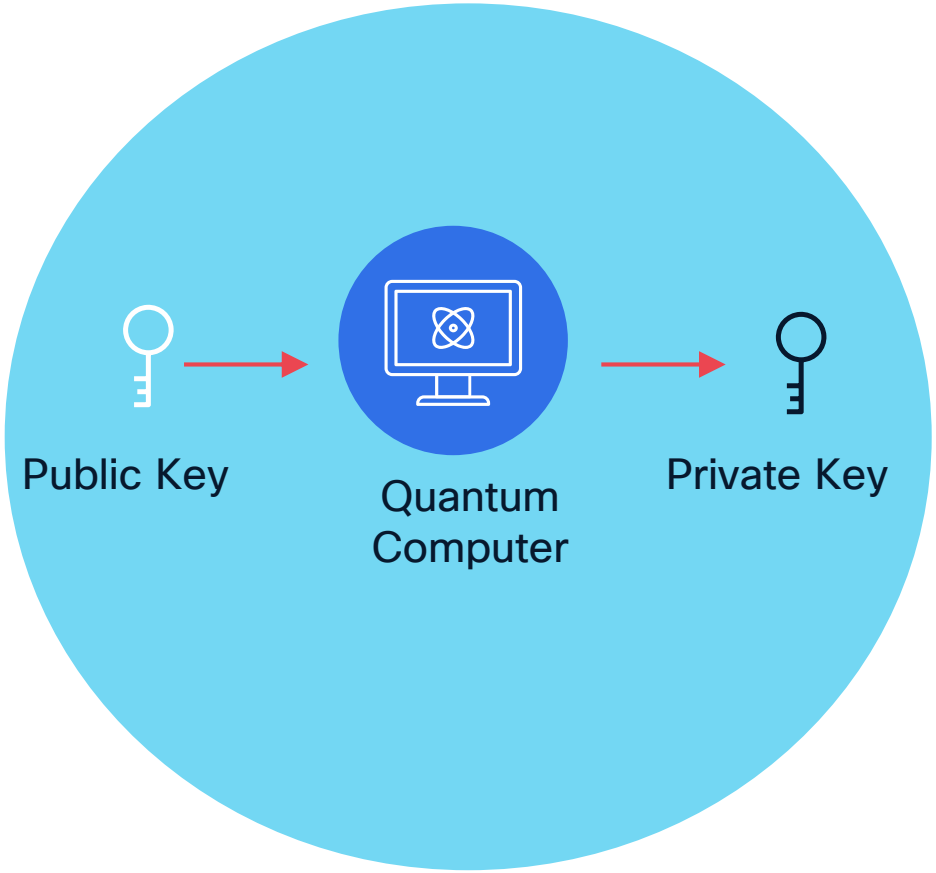
Key Negotiation

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

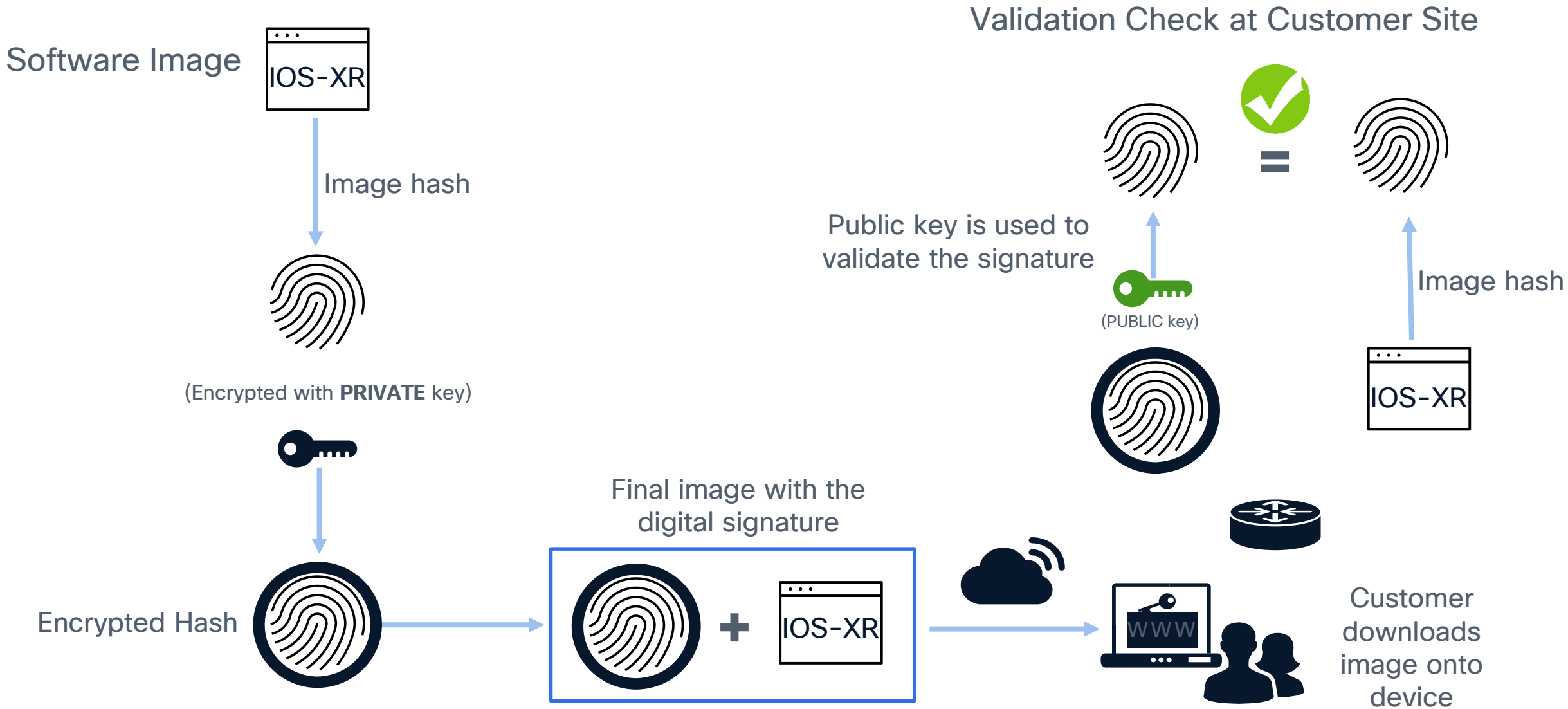
Scope of post-quantum threat

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

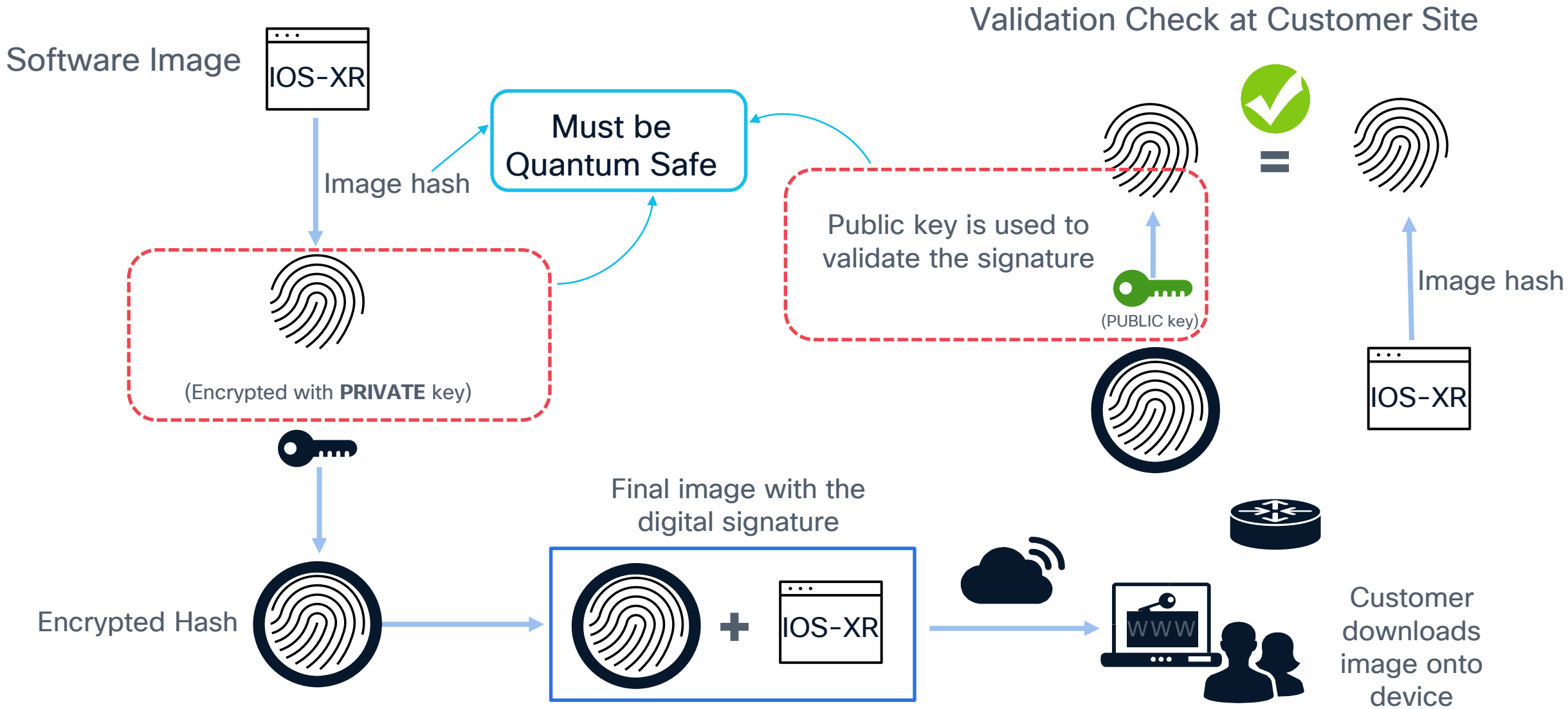
*IMA – Integrity Measurement Architecture

**SUDI – Secure Unique Device Identifier

Firmware/Software Integrity – Generic Workflow



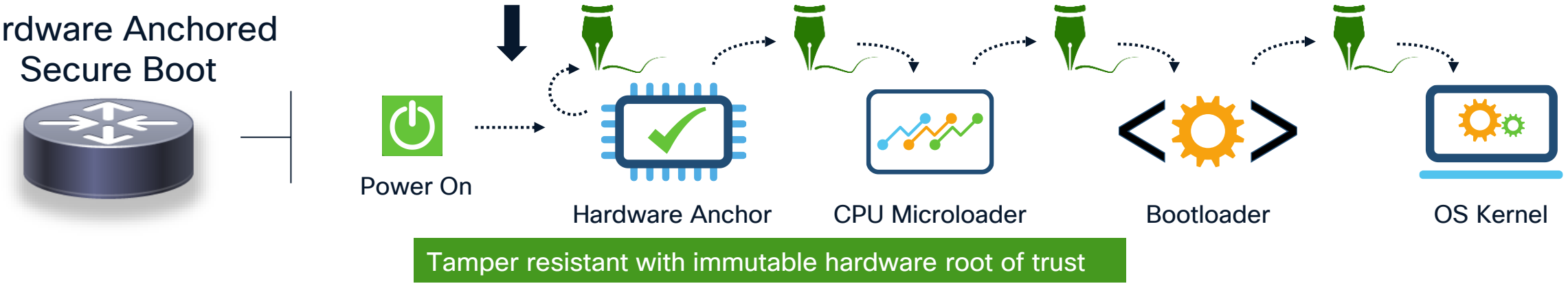
Firmware/Software Integrity – Generic Workflow



Quantum Threat To Secure Boot Workflow

Chain-of-Trust starts at Hardware

Hardware Anchored Secure Boot



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*

IMA Logging

Must be Quantum Safe

```
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

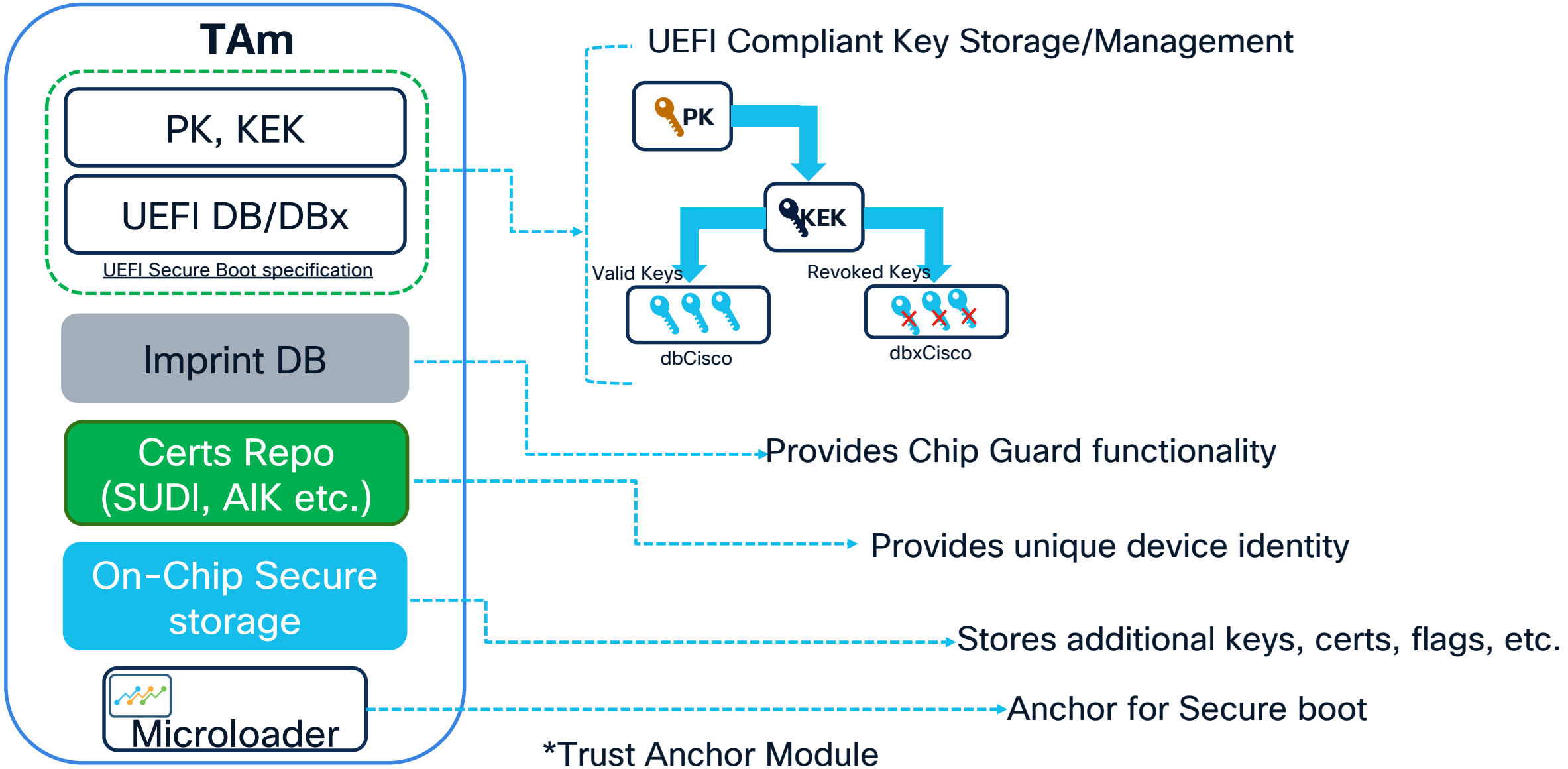
1. The effort to find pre-image hash by a quantum computer is n/2 or n/3 (with Grover's algorithm) where n is the output size of the hash.
2. This would mean we need at least 384-bit hashes to be used to get the 128-bit equivalent security in a post quantum world.
3. Recommendation would be to use SHA-512 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 Integrity

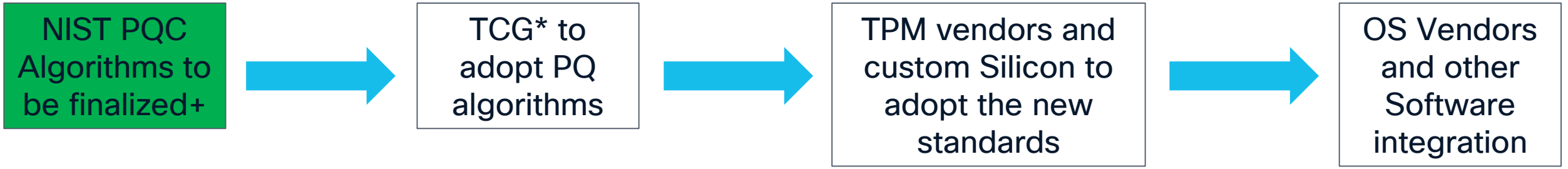
Enabling Trust in Hardware – Cisco's TAm* Chip



Some Open & Proprietary Security Chips

Open Titan	Caliptra	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 Safe Hardware Considerations



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

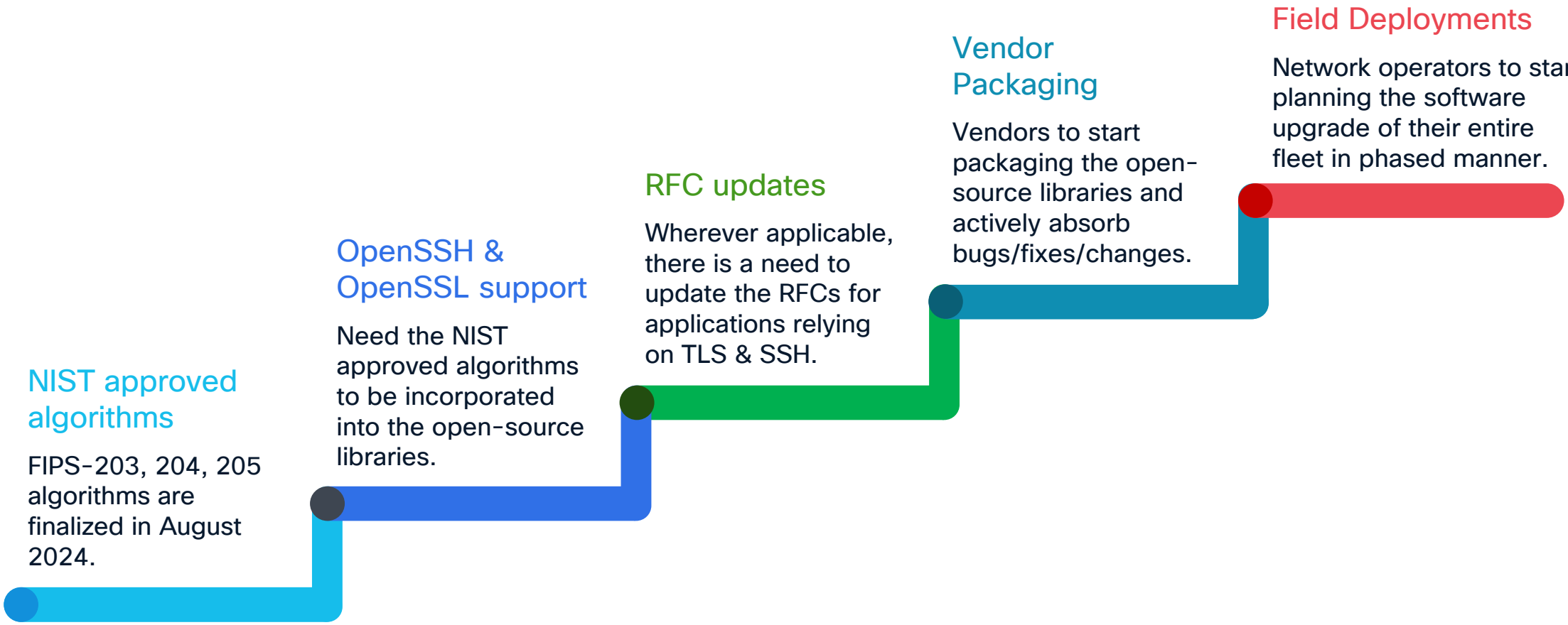
Impact to Operational Security

Operational Security Features For Network Devices

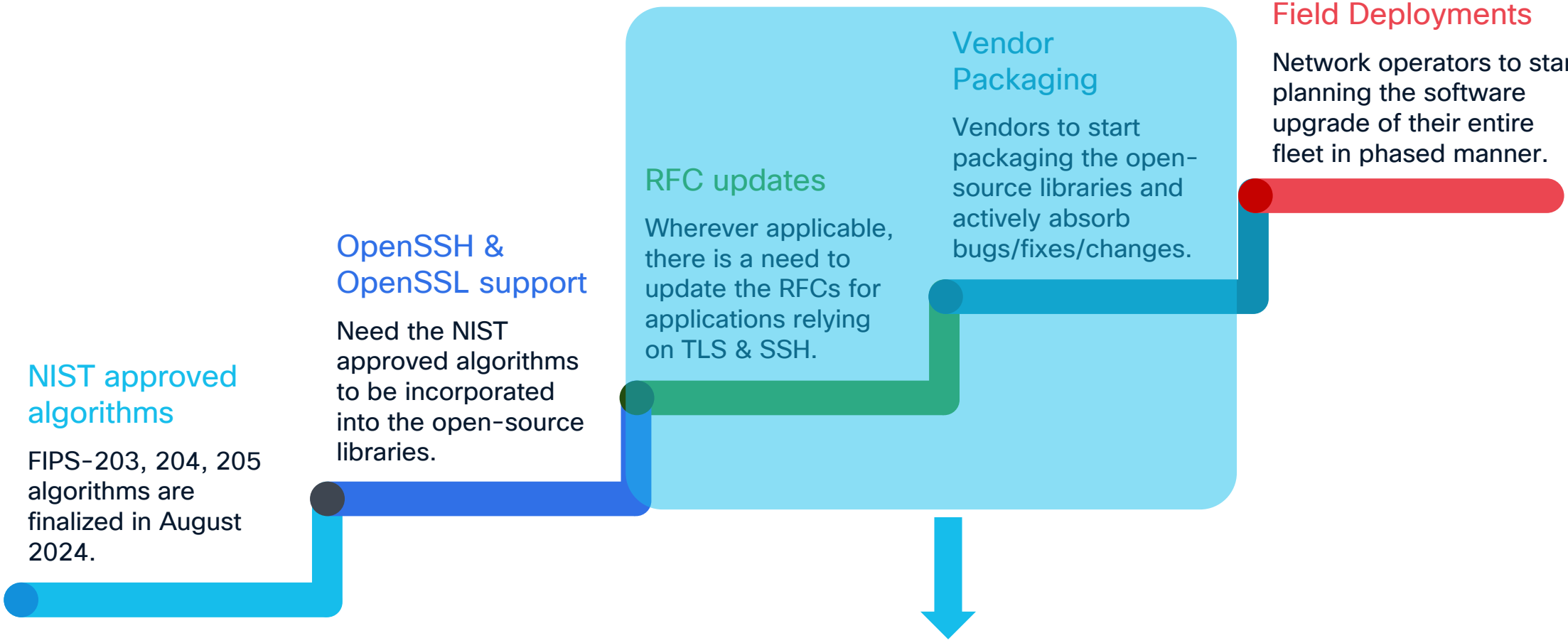
1. SSH connections to manage the network devices.
2. TLS connections for gRPC or other mechanisms to mange the devices.
3. Monitoring the network devices using syslogs over TLS, etc.
4. RADIUS over TLS (RFC 6614) or TACACS+ over TLS for user authentications and command authorizations.

And so on…

Path To PQC Software Support



Path To PQC Software Support – Where are we?



1. Cisco's SSH & SSL libraries with PQ support are being integrated by various business units.
2. IOS-XR is trending towards PQ SSH & TLS support by end of CY'25*

*Tentative

CNSA Recommended Algorithms and Use cases

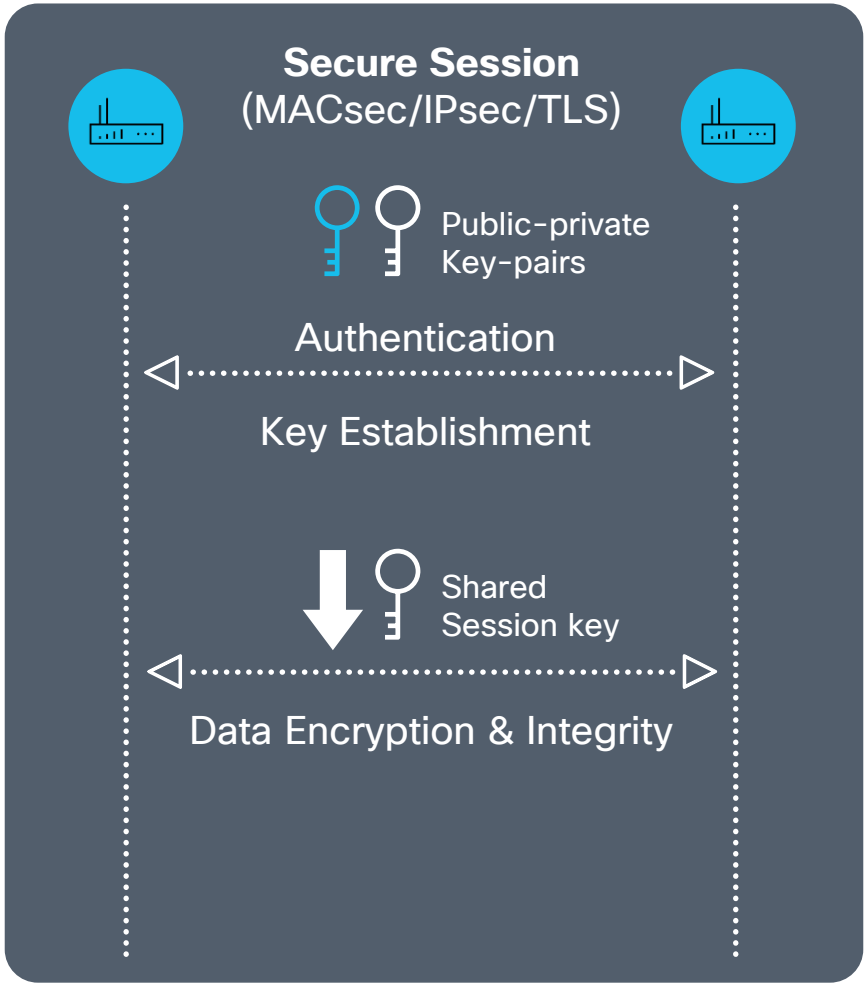
Reference Slide

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

CNSA – Commercial National Security Algorithm Suite

Transport Security Impact

Quantum computing impact on transport protocols



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

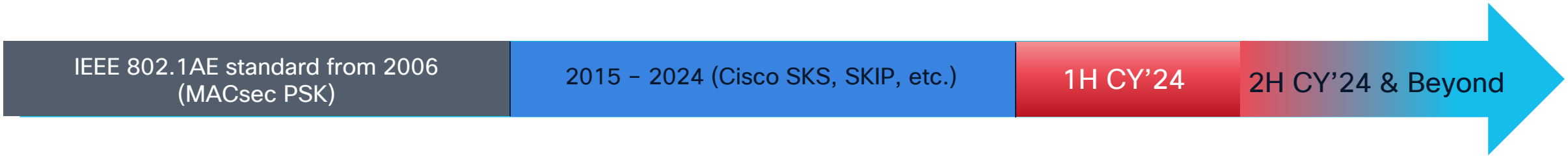
Symmetric crypto with large and high-entropy keys is resistant to quantum computer attacks

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.

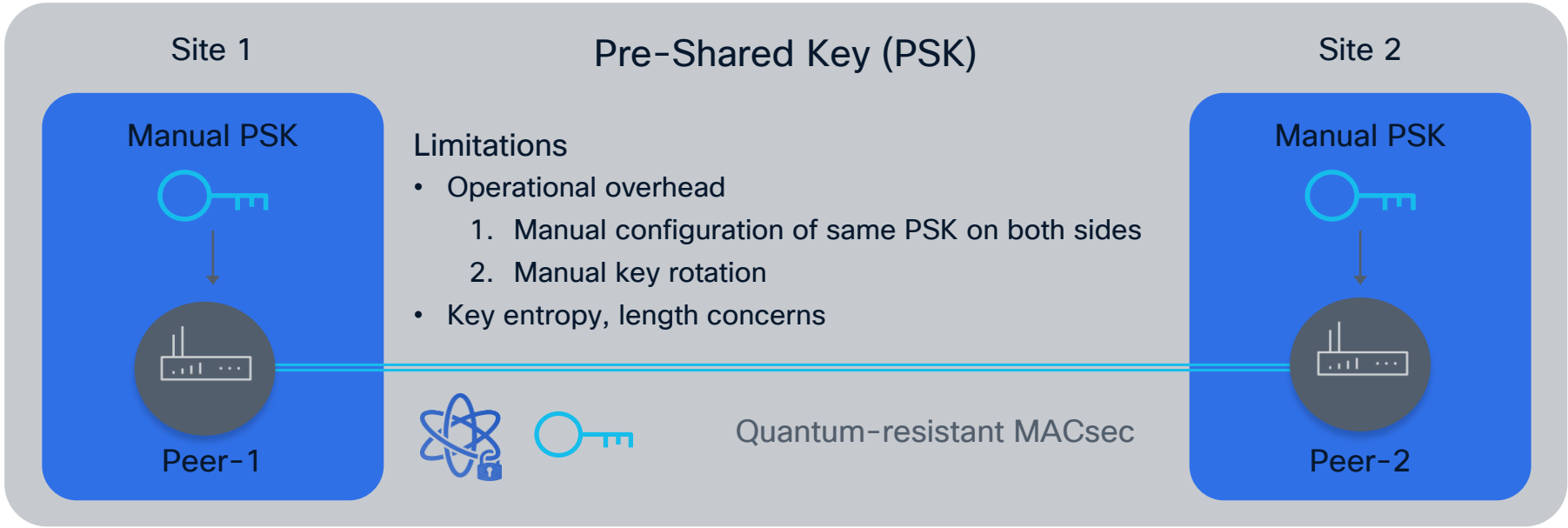
Quantum Safe Transport Security Solutions

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.



Quantum-safe MACsec

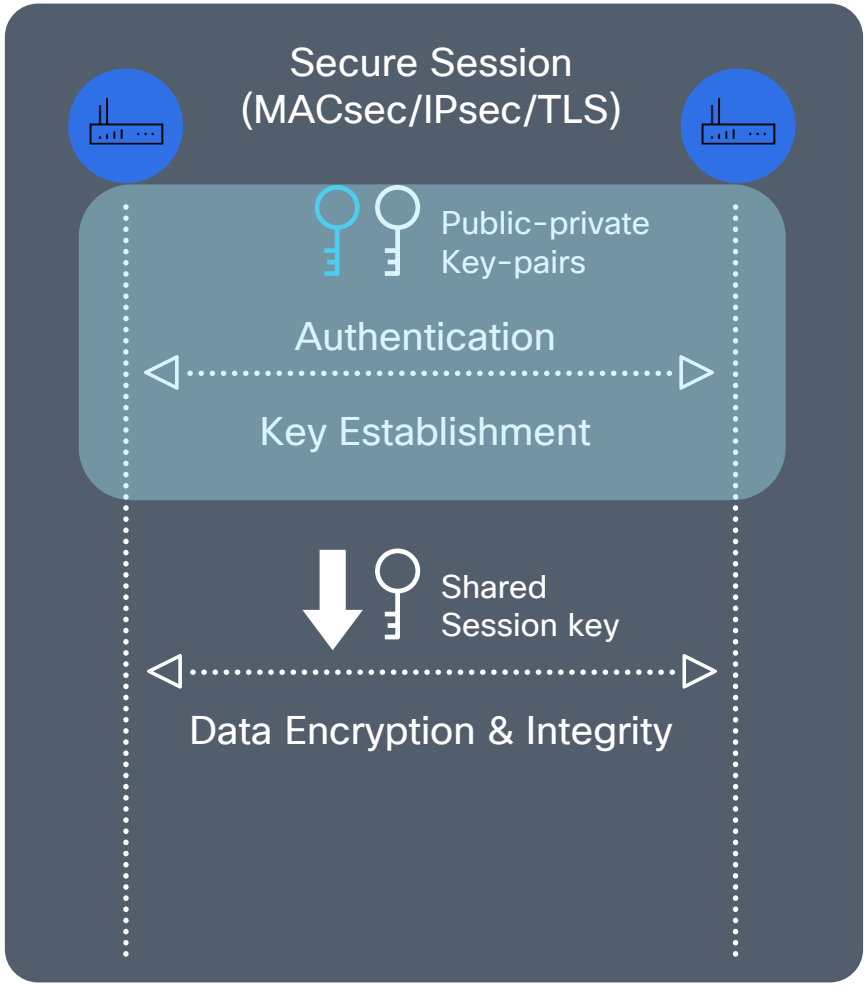
Pre-shared key (PSK) option

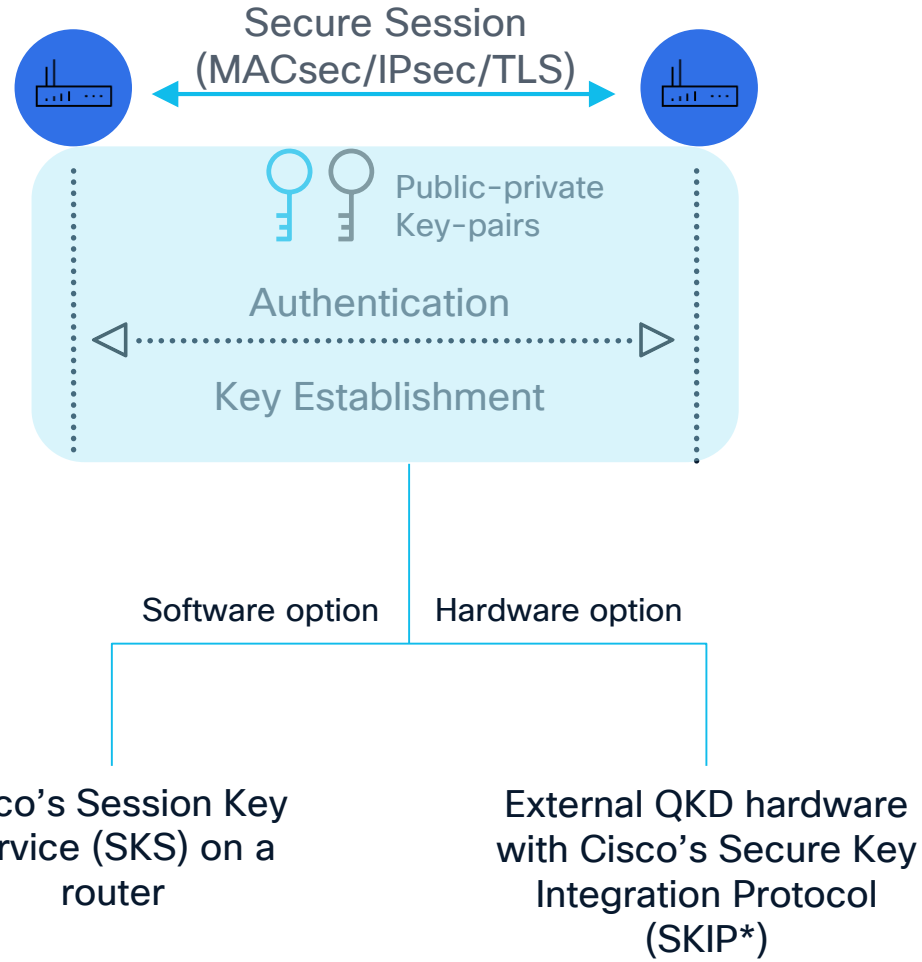


1. MACsec with PSK option is already supported and used by customers.
2. There is no need for additional hardware (like QKD*) or software upgrade.
3. Quantum-safe as this is based on symmetric cryptography (which is quantum-resistant).

*Quantum Key Distribution

Cisco's Quantum key distribution options

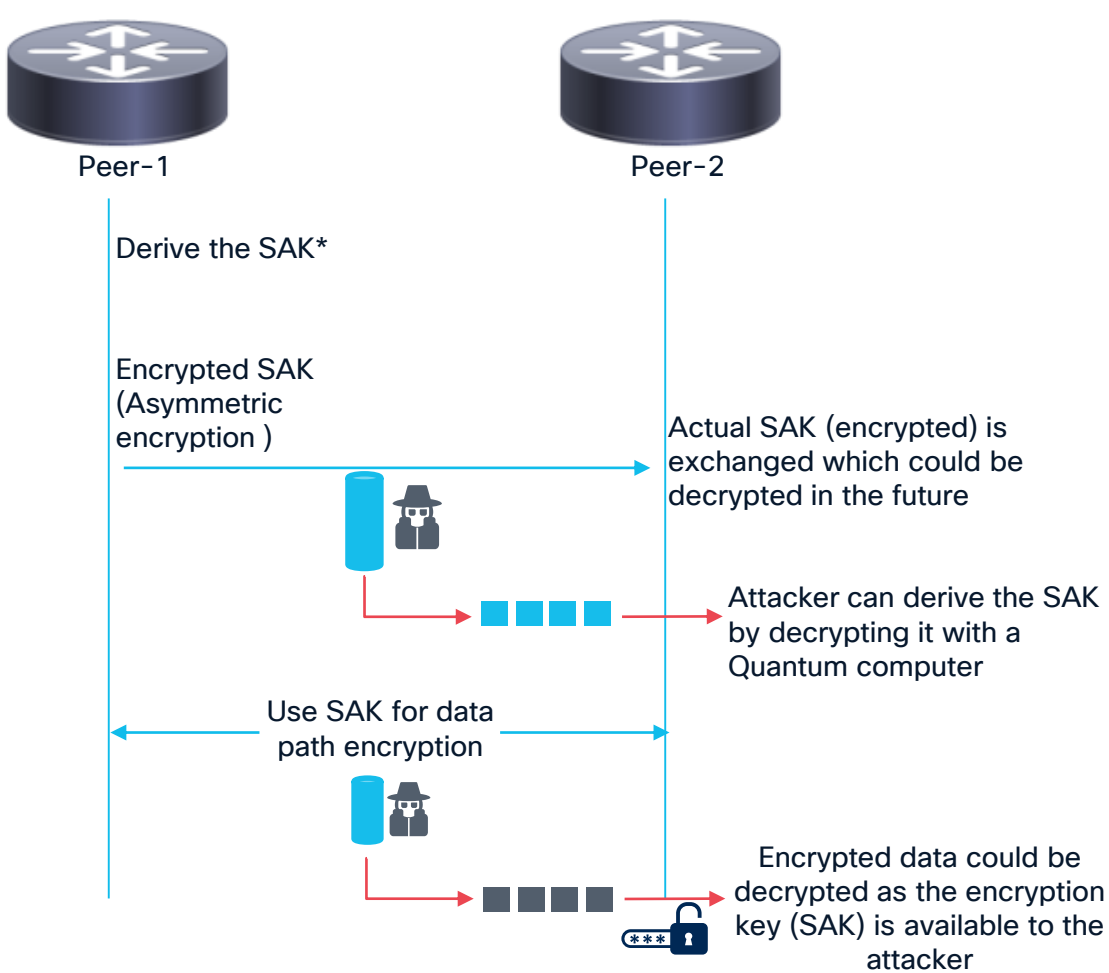




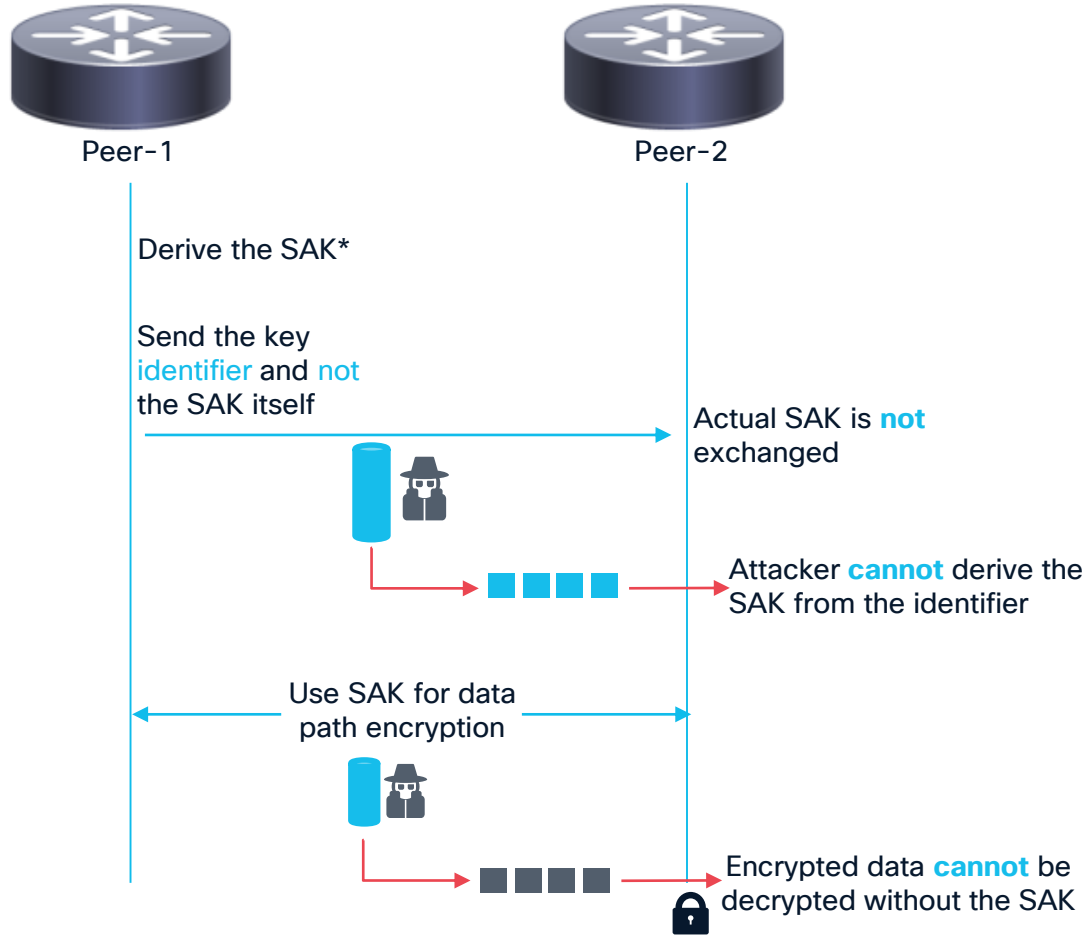
*SKIP Specification - https://www.ietf.org/archive/id/draft-cisco-skip-00.html

Quantum key distribution – Basic principle

Existing method

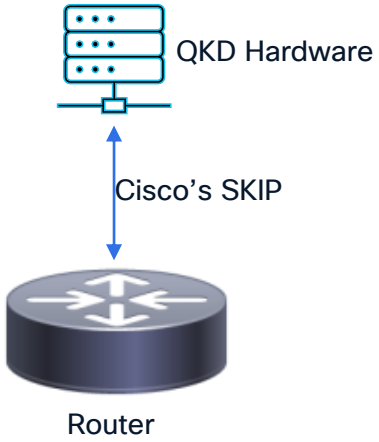


QKD method

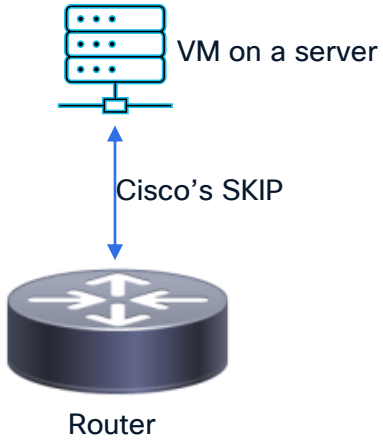


*SAK – Security Association Key

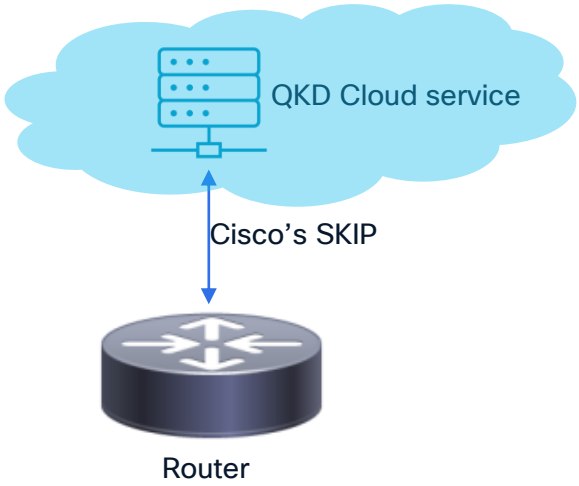
Bring Your Own Key Approach



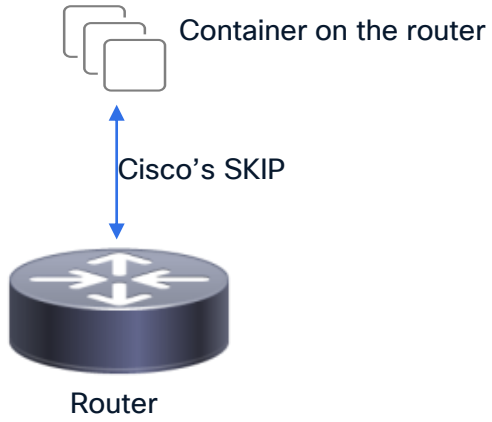
Physical QKD Appliance



Virtual Machine Approach



Keys From a Cloud Service

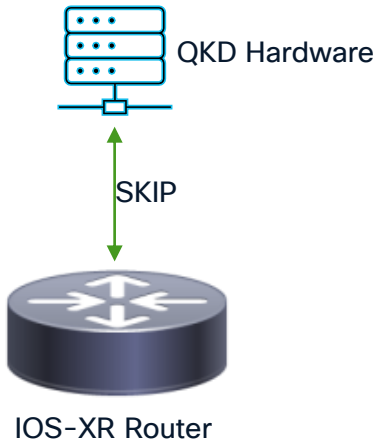


Container as key source

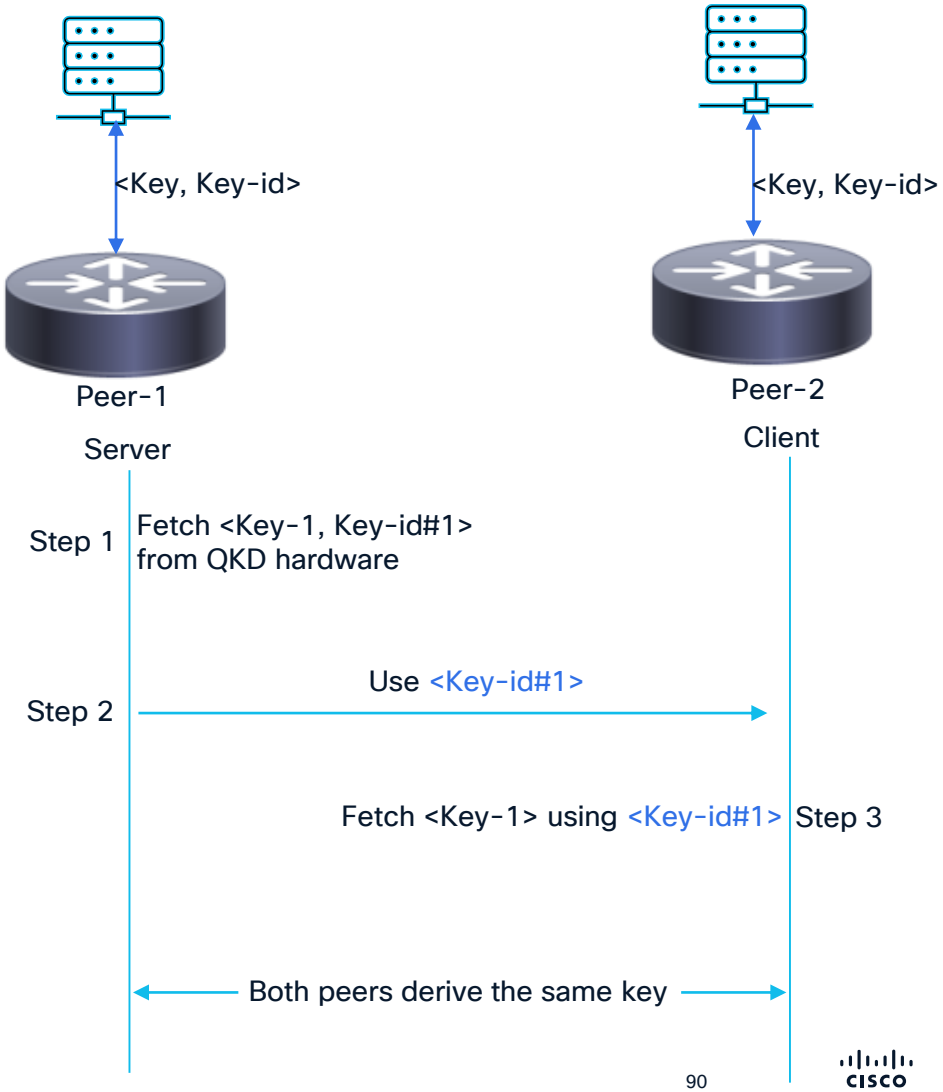
1. The key source option is up to the customers based on their use case, cost constraints, level of security needed, etc.
2. Cisco devices support the SKIP interface to fetch the keys from any of the key sources.

Quantum key distribution options

External Key Source with Cisco's Session Key Import Protocol (SKIP)

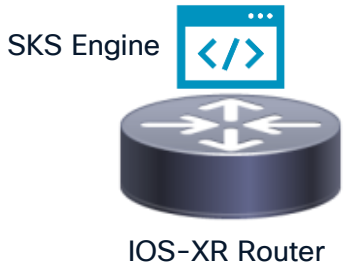


1. Dedicated hardware to generate the session keys and key-id's
2. The QKD hardware for a given pair of devices would be in sync
3. Each peer fetches the key and key-id from the QKD hardware over a TLS connection
4. Only key-id is sent on the wire, and the peer fetches the key from the QKD hardware

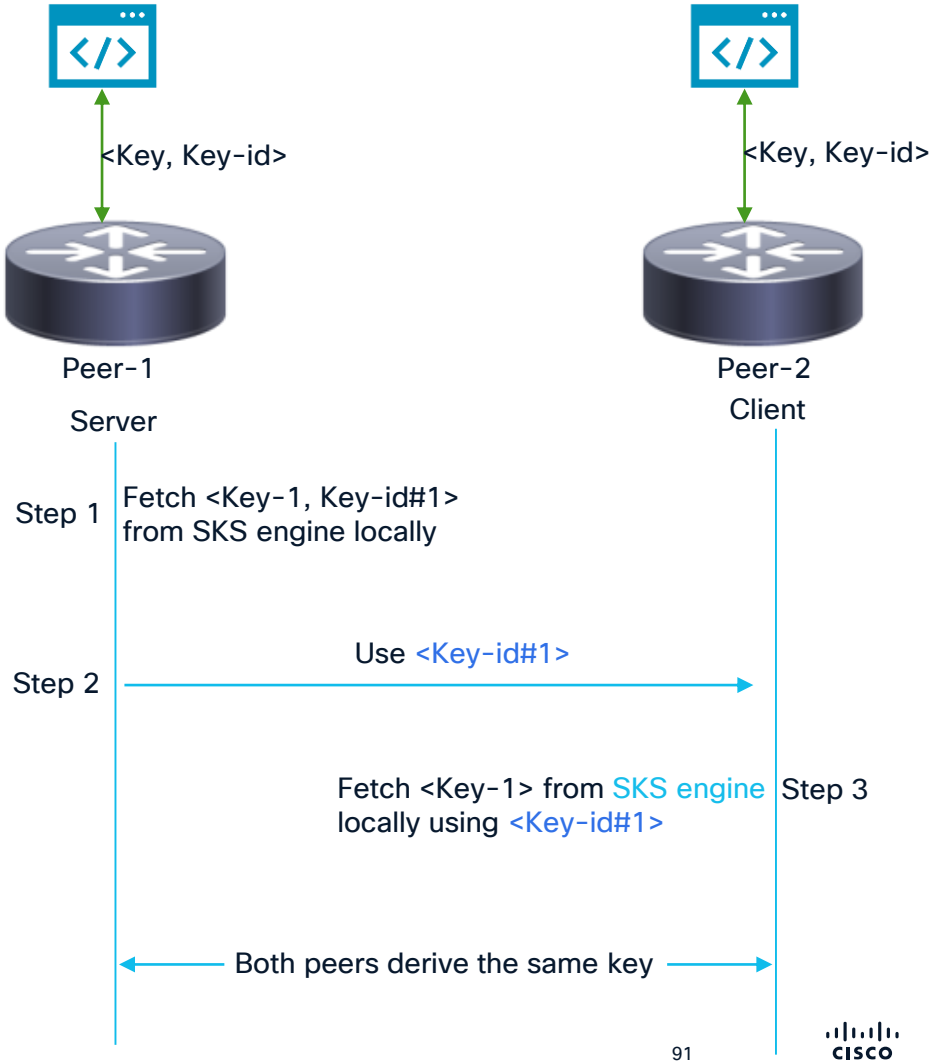


Quantum key distribution options

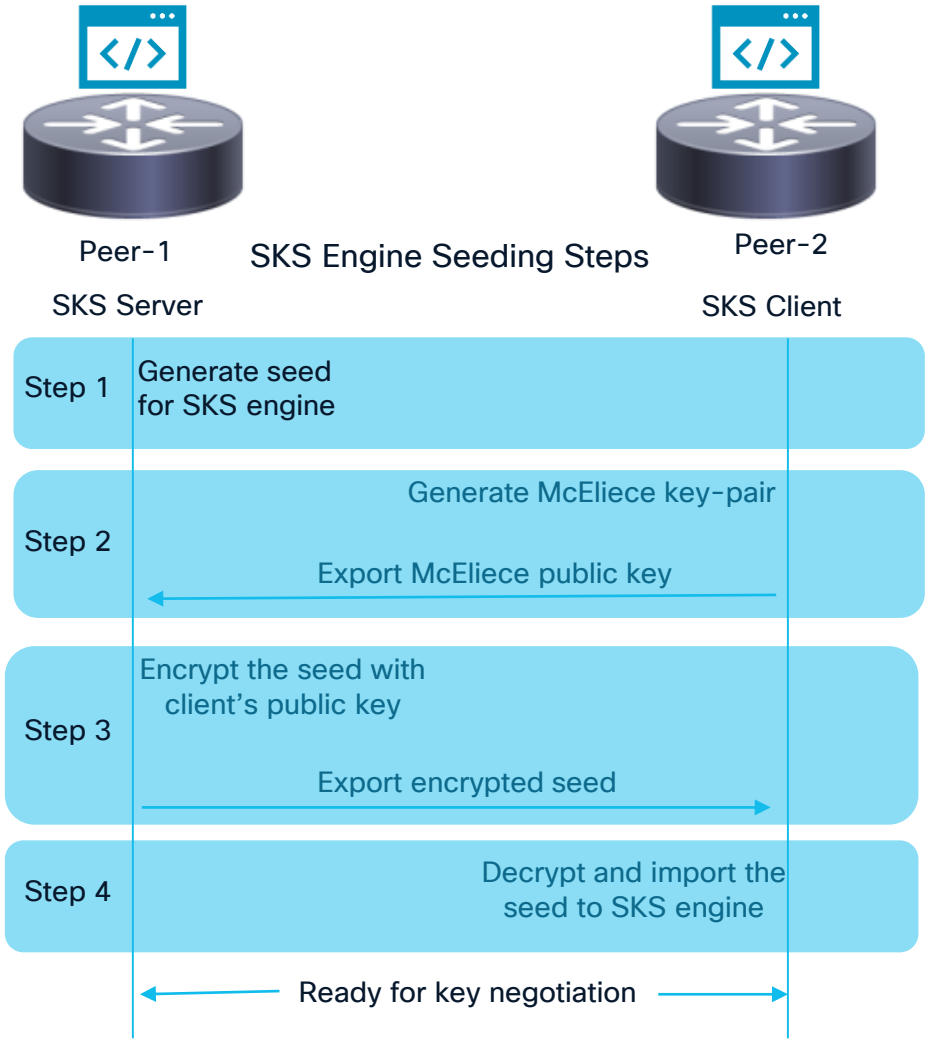
Cisco's Session Key Service (SKS) on the router



1. SKS engine on the router generates the keys
2. No additional hardware required
3. The SKS engine must be seeded with the same seed on both the peers
4. The seed is protected by McEliece cryptosystem which is quantum-resistant
5. Only key-id is sent on the wire, and the peer derives the key from its local SKS engine



Cisco Session Key Service workflow



1. The SKS engines on both routers generate the keys in same order as they are initialized with the same initial seed.

2. McEliece cryptosystem is proven to be Quantum Safe. Used typically for one-time operations as it is computationally intensive and has long keys not suitable for line-rate applications.

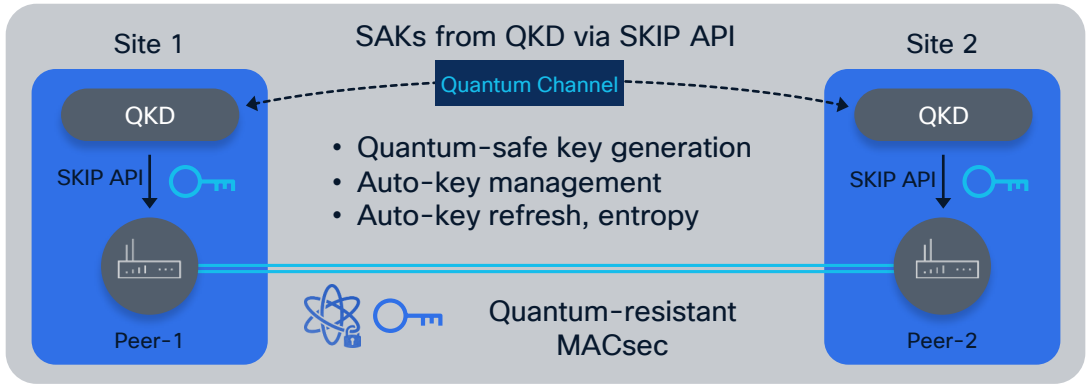
3. One-time seeding operation to generate the keys in the same order.

4. The routers only exchange the key identifiers making it Quantum Safe.

Quantum-safe MACsec

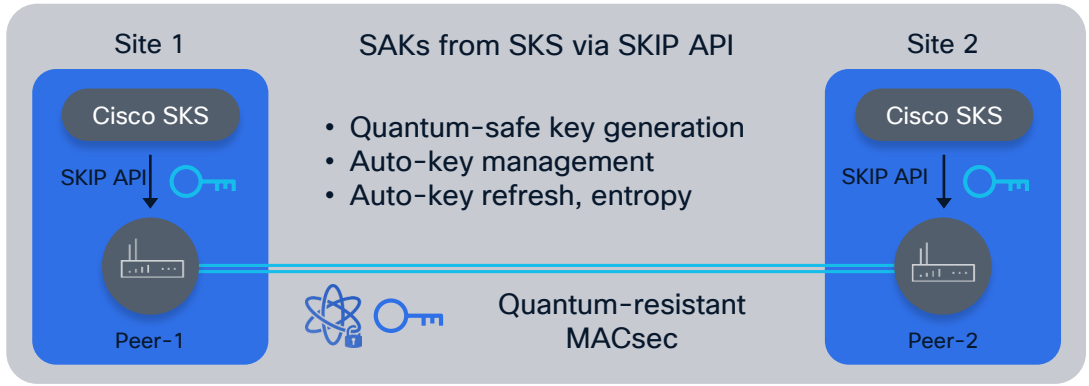
Quantum key distribution options

External QKD hardware



1. Hardware-based key source
2. Dedicated optical fiber (up to 100 km supported)
3. QKD hardware per-site/peer
4. Very expensive
5. Supported from IOS-XR 7.9.1 release

Cisco SKS server



1. Software-based key source
2. No dedicated circuit or distance limitations
3. No additional hardware requirement
4. No additional cost
5. Supported from IOS-XR 7.4.1 release

Path to Post Quantum Cryptography

Reference Slide

PQC Algorithms & Standards

LMS – RFC8554 – approved

XMSS – RFC8391 – approved

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

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

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

FIPS-205 SLH-DSA – approved
- 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.

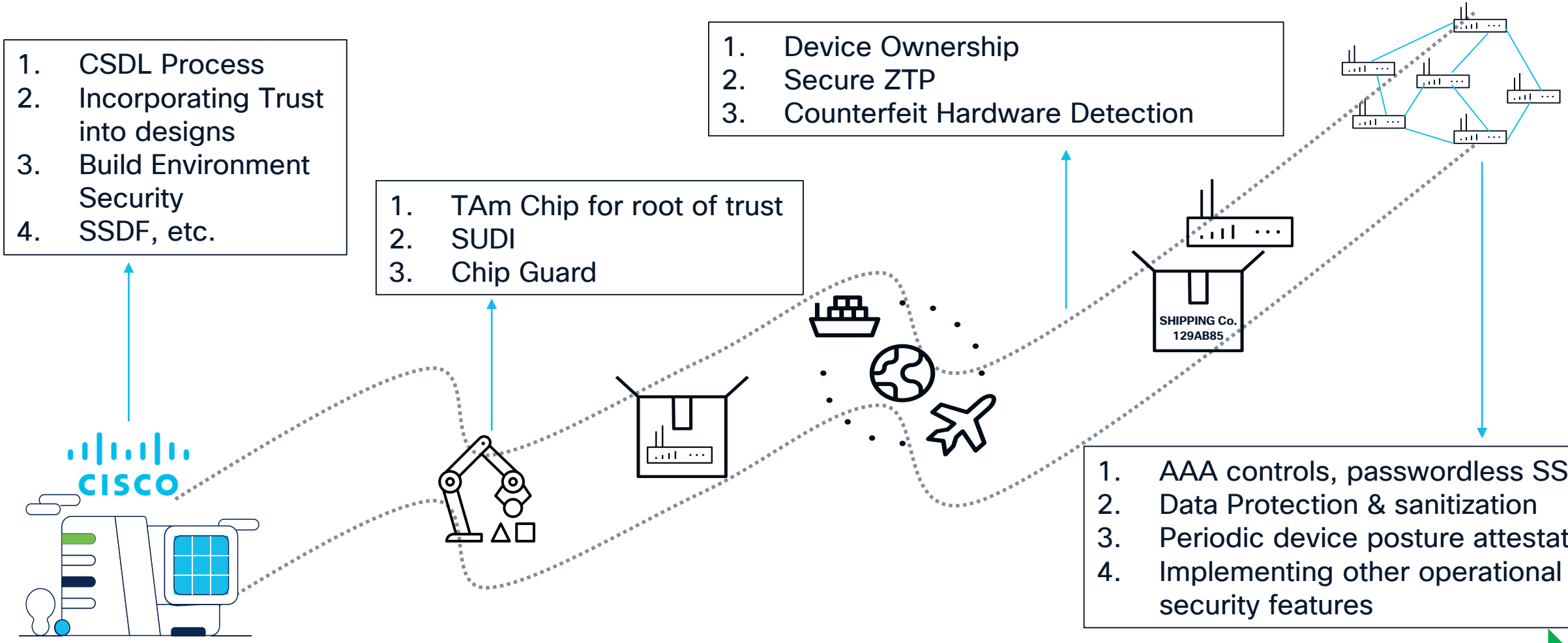
Conclusion

Secure By Design At Every Stage

1. CSDL Process
2. Incorporating Trust into designs
3. Build Environment Security
4. SSDF, etc.

1. TAm Chip for root of trust
2. SUDI
3. Chip Guard

1. Device Ownership
2. Secure ZTP
3. Counterfeit Hardware Detection



1. AAA controls, passwordless SSH
2. Data Protection & sanitization
3. Periodic device posture attestation
4. Implementing other operational security features

SECURE BY DESIGN AT EVERY STAGE

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

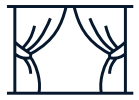
Walk-in-lab on DDoS Edge Protection Solution

Monday - Thursday

Breakout Session on DDoS Edge Protection Solution

June 11th 4 pm

Continue your education



Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: https://www.linkedin.com/in/rakeshreddy/

Thank you

cisco Live !


CISCO