Building Trustworthy Network Infrastructure

Rakesh Kandula
Technical Marketing Engineer, Cisco Systems

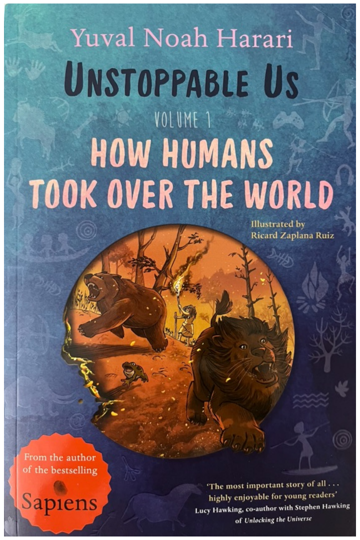
16th October 2023

About Me

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

“People need stories in order to cooperate, and they can change the way they cooperate by changing the stories they believe”

Yuval Noah Harari



Agenda

1. Service Provider Security Concerns
2. Trustworthy Platforms – Challenges & Solutions
3. Strengthening Operational Security

Threat Landscape For Service Provider Networks

Deployment Challenges For Service Providers

Untrusted Remote Locations

Support Critical Infrastructure

Global Scale

Impact of Attacks on Service Providers

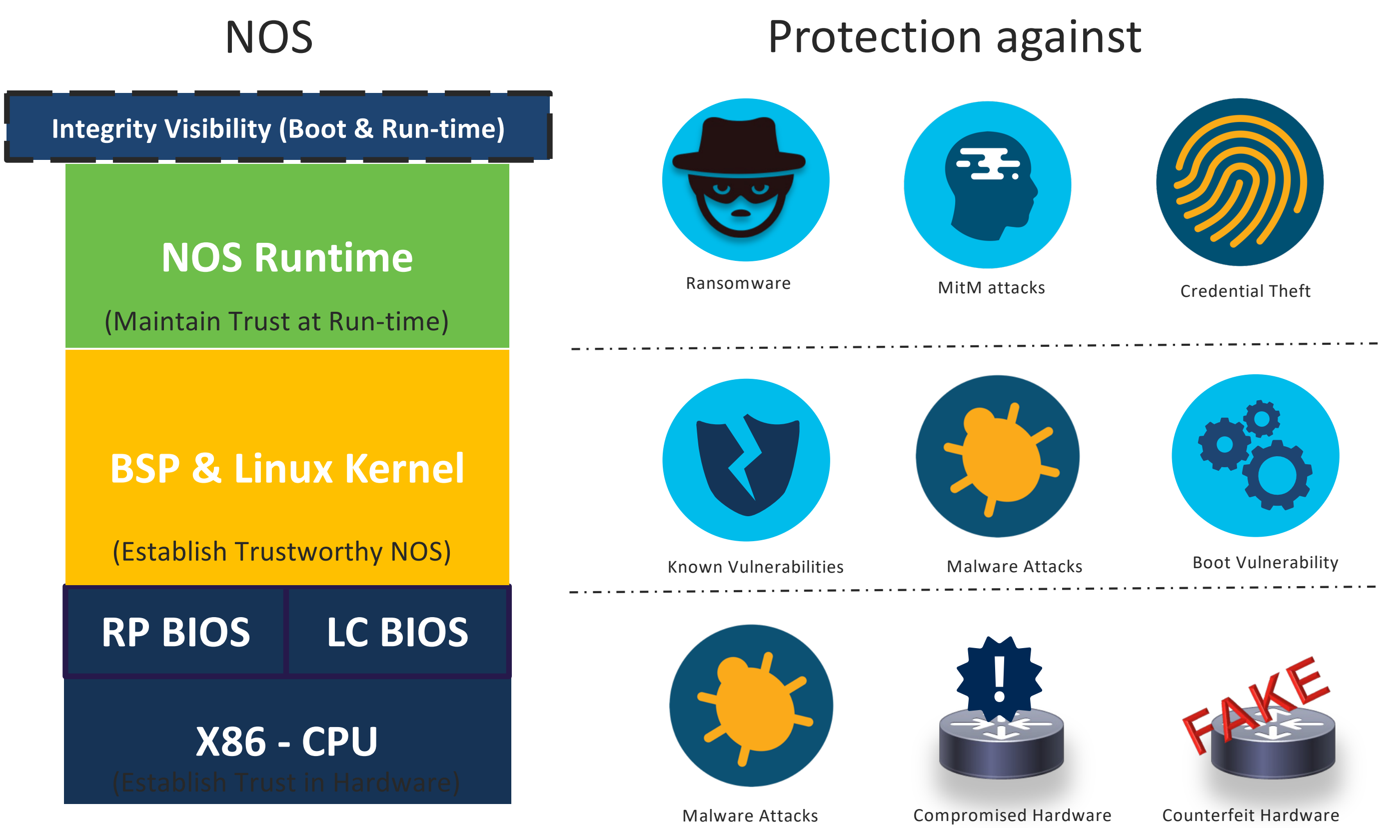
Loss of Revenue

Brand Reputation Loss

Impact to SLAs

Legal Implications

Threats to Network Devices – Layered View



Trustworthy Platforms Overview

Trustworthy

Trust Begins in Hardware

Ensuring Hardware Integrity

Enabling Trust in the Network OS

Ensuring Integrity of the Boot Process

Maintaining Trust at Runtime

Run-time Defenses, Data Protection, DDoS Protection

Visualize and Report on Trust

Continuous Posture Evaluation

Components of Trustworthy Platforms

Hardware Integrity

Ability to detect counterfeit hardware and act as a trust anchor

Boot Integrity

Ensuring integrity of the boot process

Runtime Integrity

Ensuring the integrity of the NOS runtime

Trust Visibility

Providing visualization of Trust

Components of Trustworthy Platforms

Hardware Integrity

Ability to detect counterfeit hardware and act as a trust anchor

Boot Integrity

Ensuring integrity of the boot process

Runtime Integrity

Ensuring the integrity of the NOS runtime

Trust Visibility

Providing visualization of Trust

Tampering of Critical Components

↑ Increase in Supply Chain Attacks

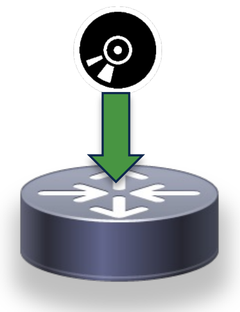
↑ Increasing attempts to put Trojans on Chips

- ✓ CPU Integrity
- ✓ ASIC Integrity
- ✓ Detect in-transit tamper
- ✓ Validate Mission Critical Components

Counterfeit Hardware & Unique Hardware Identity

1 Counterfeit hardware from illegal markets.

2 Tampered hardware sold in resale markets

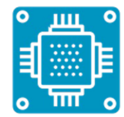


1 Ability to cryptographically identify a device uniquely

2 Adoption of secure & standards-based device onboarding / enrollment

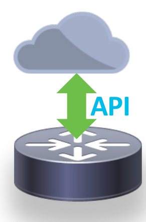
Solutions To Ensure Hardware Integrity

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



A platform security chip to ensure 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.)

Components of Trustworthy Platforms

Hardware Integrity

Ability to detect counterfeit hardware and act as a trust anchor

Boot Integrity

Ensuring integrity of the boot process

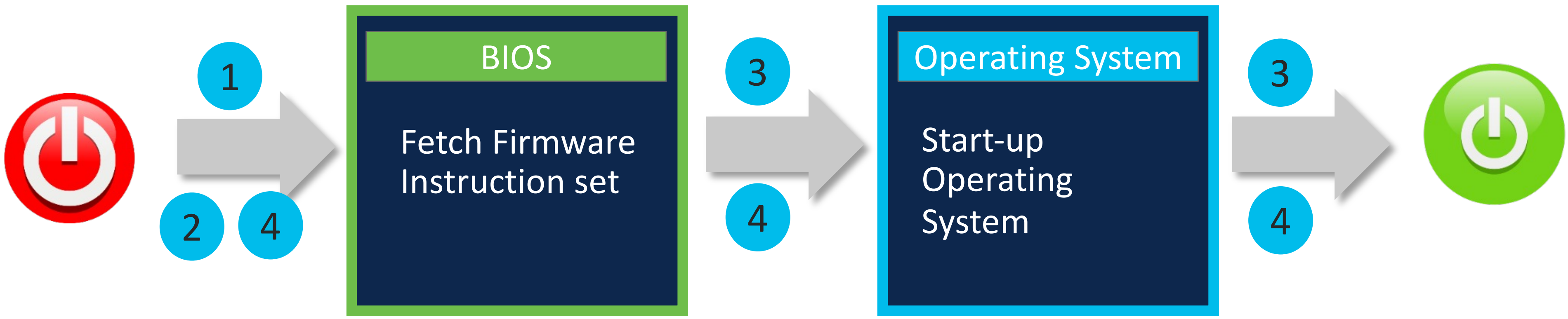
Runtime Integrity

Ensuring the integrity of the NOS runtime

Trust Visibility

Providing visualization of Trust

Attacking the Boot Sequence



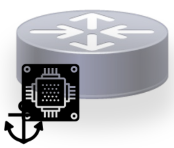
1 Changing the boot interface

2 Booting from alternate device

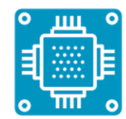
3 Bypassing Integrity checks

4 Adding persistent code

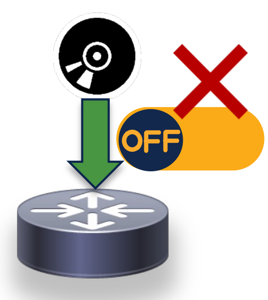
Ensuring Boot Integrity



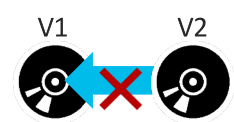
Secure boot anchored in an immutable hardware root of trust must be mandatory



Ability to validate boot artifacts and record boot measurements inside a TPM or similar security chip



Ability to prevent an adversary from disabling secure boot



Ability to prevent revoked images from booting (image downgrade protection)

Components of Trustworthy Platforms

Hardware Integrity

Provides counterfeit hardware protection and act as a trust anchor

Boot Integrity

Ensures integrity of the boot process

Runtime Integrity

Ensure integrity of the NOS runtime

Trust Visibility

Provides visualization of Trust

Runtime Integrity Challenges

1. Detecting tampering of Network Operating System (NOS) after secure boot process.

2. Ability to prevent processes from accessing unauthorized resources.

3. Ensuring the integrity of files before a process executes.

4. Preventing unverified 3rd party applications from running on the routers.

Maintaining Trust at Run-time

Application Containment and Policy

SELinux

- A Mandatory Access Control (MAC) facility built into the Linux Kernel
- Protection from malicious or misbehaving compromising the system

Integrity Visibility and Secure Measurement

Linux Integrity Measurement Architecture

- All processes executed by the kernel are securely measured and reported
- Kernel checks process signature to prevent unsigned code from executing

Linux Integrity Measurement Architecture (IMA)

IMA Logging


```
10 d93ea3e04ba8d68d7bf032f15963467a929a1e30 ima-sig
sha256:db48006f4c5decf1c70abdc849efa4618422420d031c202f6b99f0b185adc0a6 /bin/bash
0302046ebaed83010082223999846 3f30686f6c0946d4d0ebd95567469866c23a3de0fe210e4c84c3
ea95234a7dbf0565ed2549928b91a45f7bef59787460dc83ccd3ac9c6f39d7e7ef252f863f19afaf7
2fa9b0dbe2a96d2f84aa9ce9007b5bdcbb94d11d7085d9c25be68f6bd1566044f83ec17c770d66ccb
88b5db6a284527d95001d00cff92e14fd544bb2c4c9ffd17364d35c403f895f537c41da37e27b0284
b5f4ce1fde0d0730cef5e93b0971e4325a849e27ac85a6ec546631a3890808667d24411e80d430c7c
c0f93a8c6cf8ce9c5d3baf37423864d238540ea686569f685730a2e96e5fbefbc73be3d3eea716587
598e3df728f7fd3c64b3779d2b19d095c3405242fe40
```

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

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

Components of Trustworthy Platforms

Hardware Integrity

Provides counterfeit hardware protection and act as a trust anchor

Boot Integrity

Ensures integrity of the boot process

Runtime Integrity

Ensure integrity of the NOS runtime

Trust Visibility

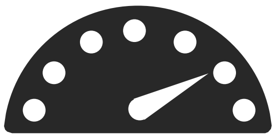
Provides visualization of Trust

Trust Visibility Components

1. Boot Integrity Visibility (BIV)
2. Runtime Integrity Visibility
3. Remote Attestation Workflow

How to establish Trust?

MEASURE

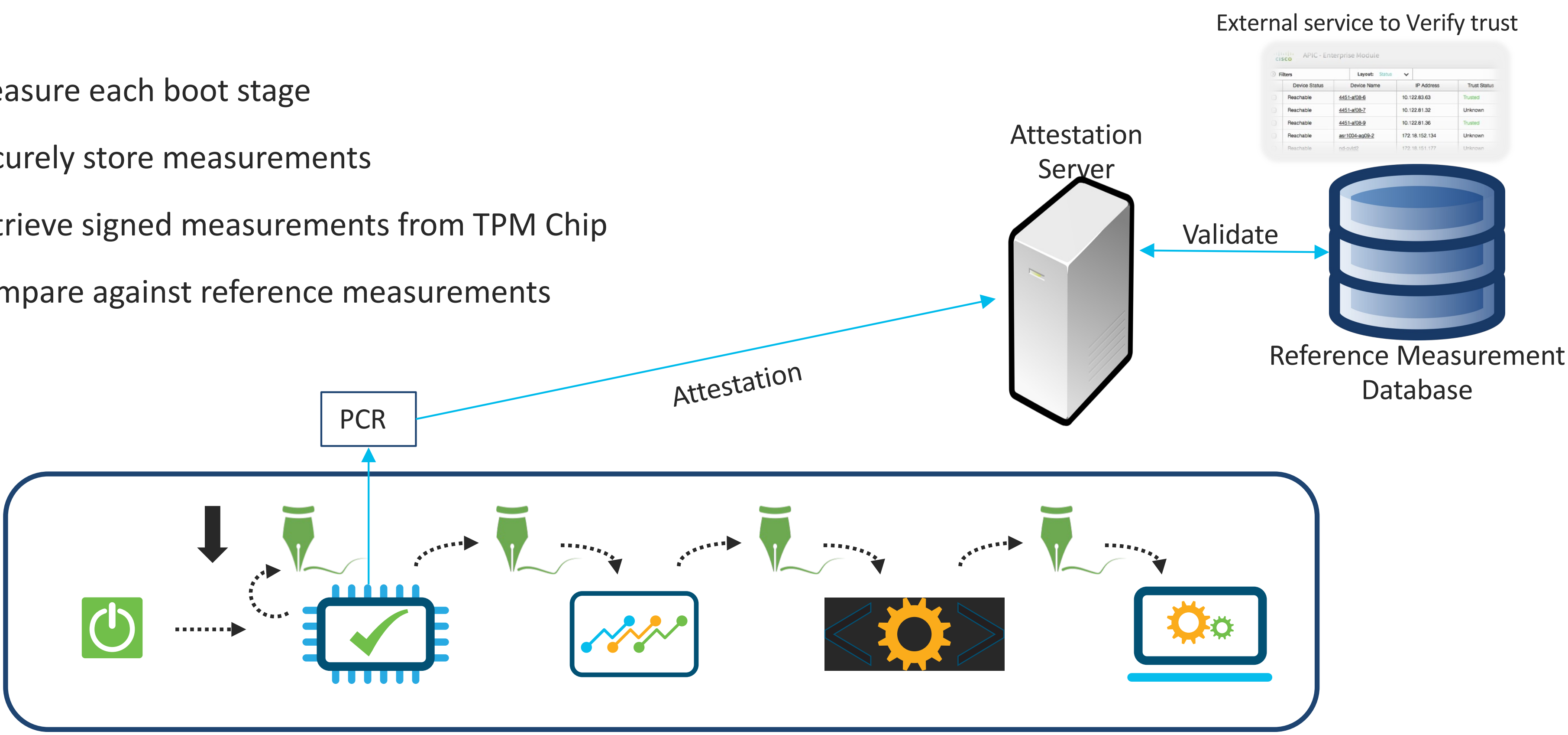


VERIFY

Boot Integrity Visibility (BIV)

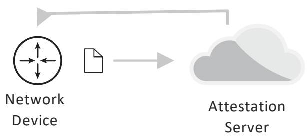
Boot Integrity Visibility (BIV) – Validate Trust

- Measure each boot stage
- Securely store measurements
- Retrieve signed measurements from TPM Chip
- Compare against reference measurements

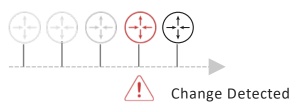


Remote Attestation Workflow

Remote Attestation Workflow

1 

Attestation server securely requests and collects signed evidence from network devices

2 

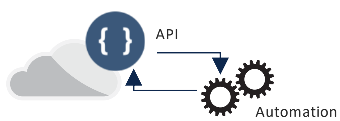
Collected evidence must be verified and added to timeline of running hardware and software

3 

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

4 

Dashboard for monitoring the posture of all devices in the network

5 

Additionally provide ability for closed loop automation to take actions based on the device posture

What About Operational Security?

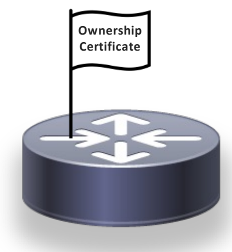
Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

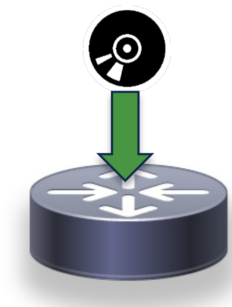
Data Protection

Data-at-rest protection & data sanitization



Ownership Establishement

Ownership Vouchers & MASA Service



Secure Device Onboarding

RFC8572 compliant secure zero touch provisioning of routers

Consent Based Security Features

Additional consent for critical security features

Quantum Security

Challenges posed by Quantum Computers

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

Other Measures

1. Using stronger password hashing mechanisms (Type-8, 9, 10)
2. Adopting secure transport methods (syslogs over TLS, SNMPv3, etc.)

*Discussed in later slides

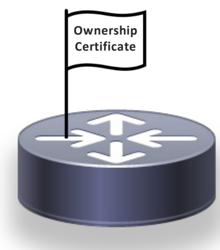
Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

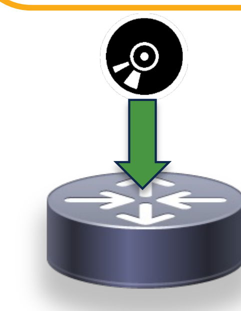
Data Protection

Data-at-rest protection & data sanitization



Ownership Establishement

Ownership Vouchers & MASA Service



Secure Device Onboarding

RFC8572 compliant secure zero touch provisioning of routers

Consent Based Security Features

Additional consent for critical security features

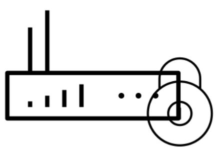
Quantum Security

Challenges posed by Quantum Computers

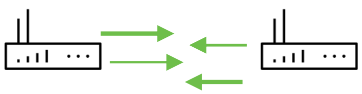
Sensitive Data Protection

1. Need data-at-rest protection
2. Full / Partial Disk Encryption
3. Encryption key protected by hardware
4. Support deletion of encryption keys

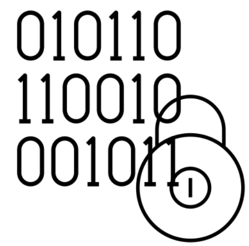
Data Protection and the missing element



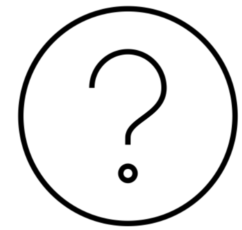
Data At Rest



Data In Transit

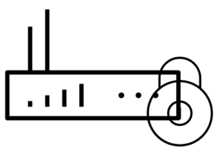


Data In Use

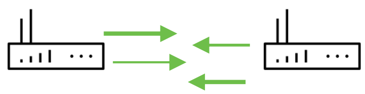


And…

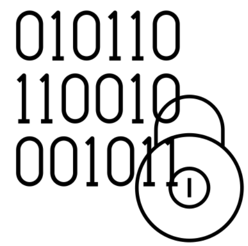
Data Protection and the missing element



Data At Rest



Data In Transit



Data In Use

Data Sanitization

Data Sanitization

1. Setup de-commissioning process for data-bearing components
2. Ensure all persistent data storage devices are safely erased
3. Implement an audit process for safe decommissioning of hardware
4. Critical for sustainability initiatives ensuring data protection

Data sanitization must be part of your organization's data security policies

Operational Security Focus Areas

User Identity Access

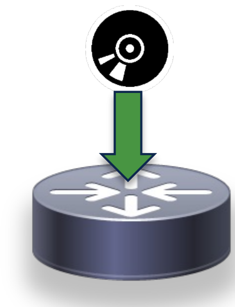
Adopting Passwordless SSH, MFA, AAA controls, etc.

Data Protection

Data-at-rest protection & data sanitization

Ownership Establishement

Ownership Vouchers & MASA Service



Secure Device Onboarding

RFC8572 compliant secure zero touch provisioning of routers

Consent Based Security Features

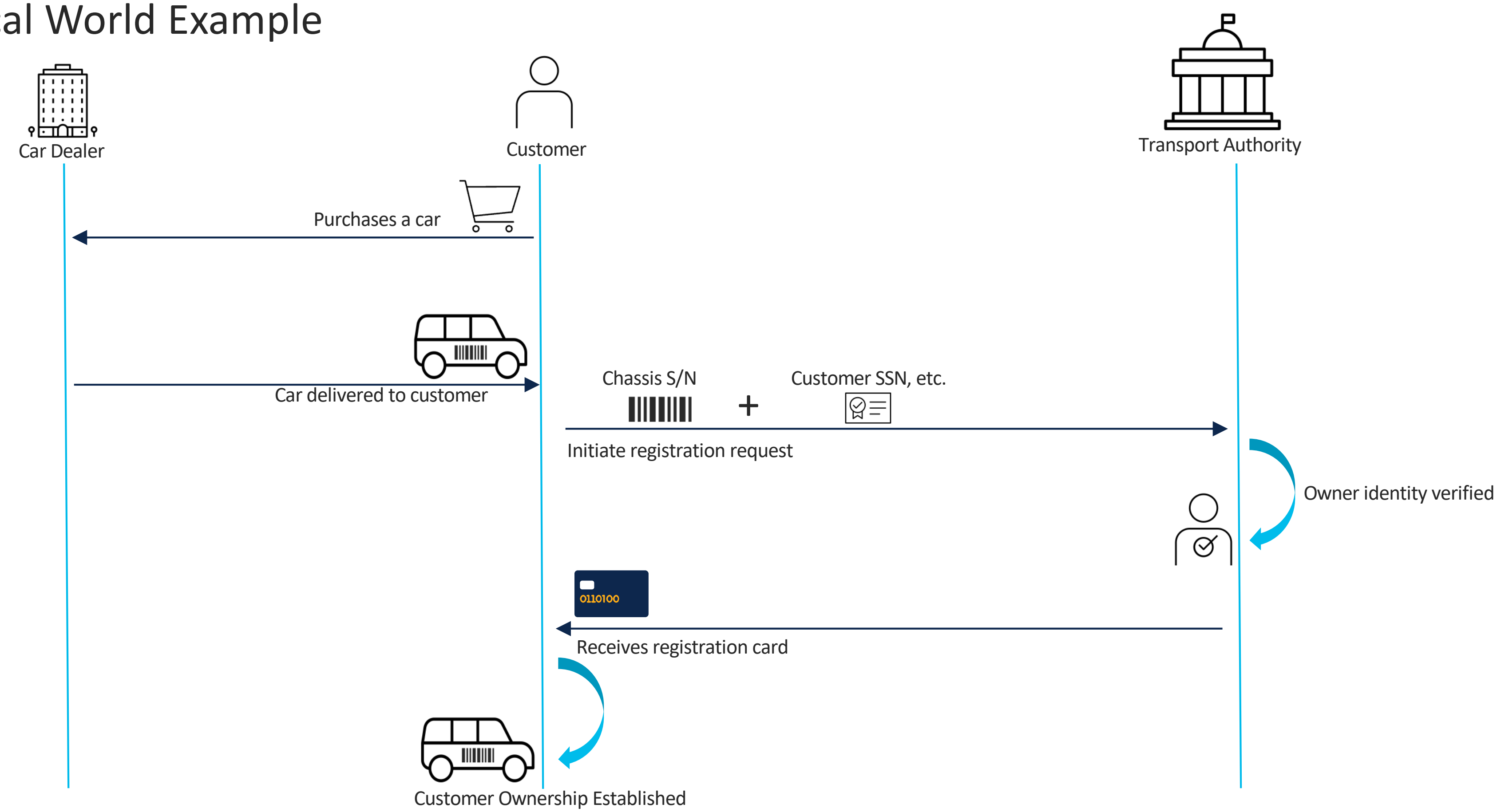
Additional consent for critical security features

Quantum Security

Challenges posed by Quantum Computers

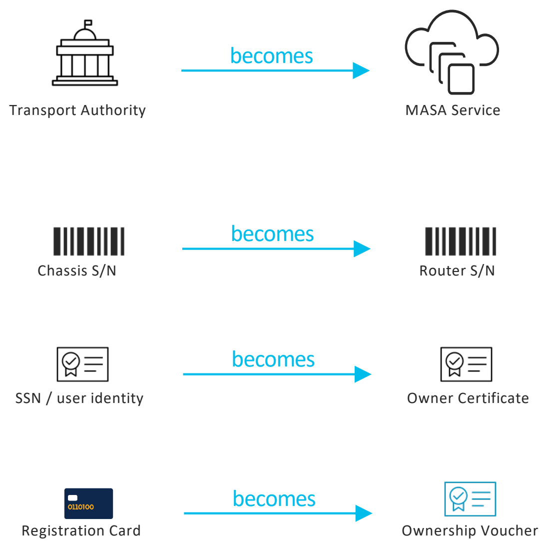
What is Ownership Establishment?

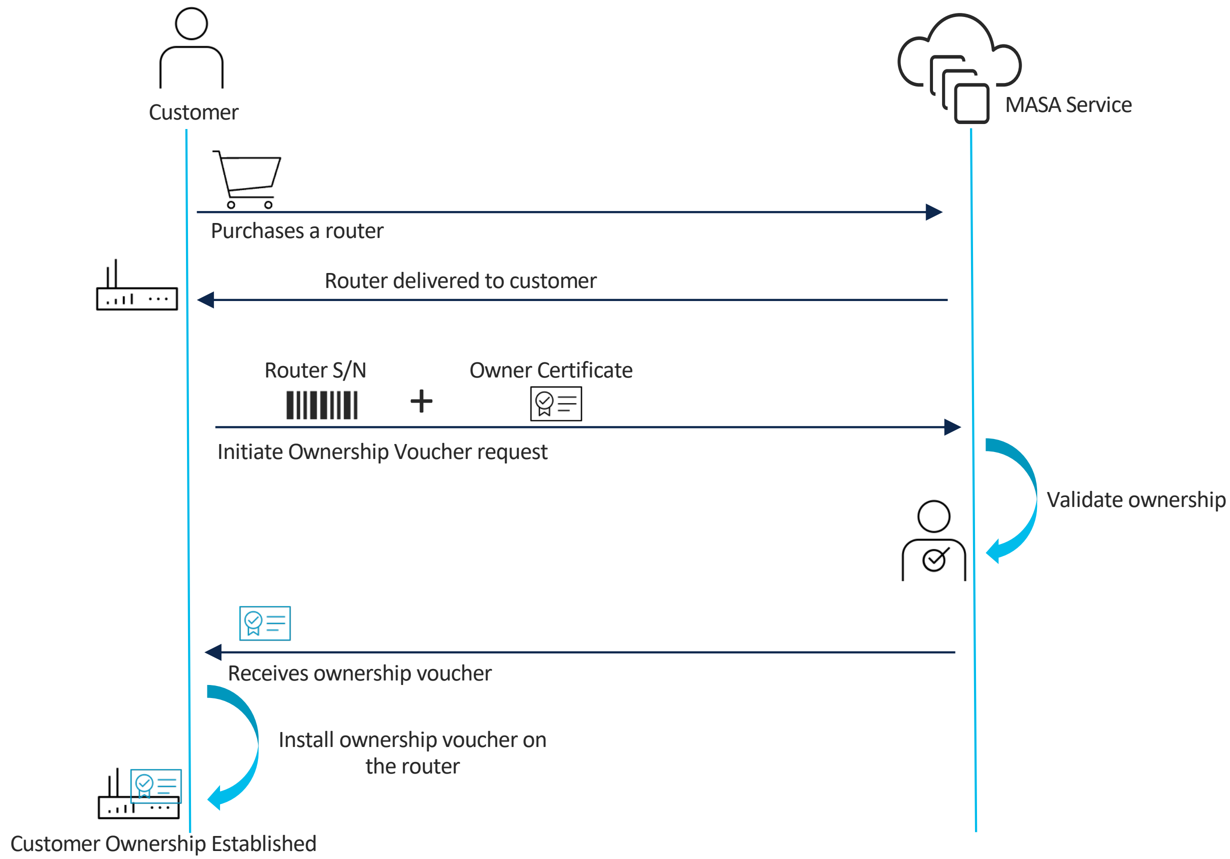
Physical World Example



What is Ownership Establishment?

Networking World Example





MASA - Manufacturer Authorized Signing Authority

Ownership Voucher (O.V) (RFC 8366)

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
```

- **Serial Number**: Serial number of the router/pledge being bootstrapped
- **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).

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

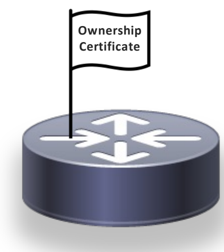
Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

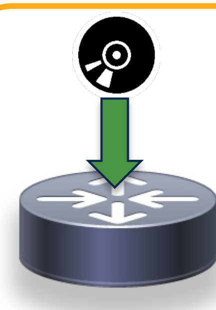
Data Protection

Data-at-rest protection & data sanitization



Ownership Establishement

Ownership Vouchers & MASA Service



Secure Device Onboarding

RFC8572 compliant secure zero touch provisioning of routers

Consent Based Security Features

Additional consent for critical security features

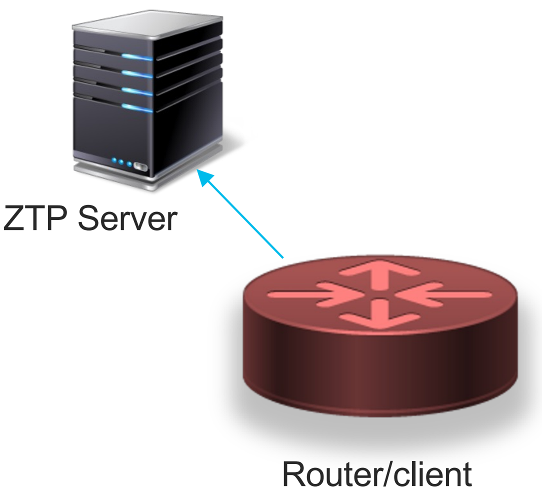
Quantum Security

Challenges posed by Quantum Computers

Security Considerations for Zero Touch Provisioning (ZTP)

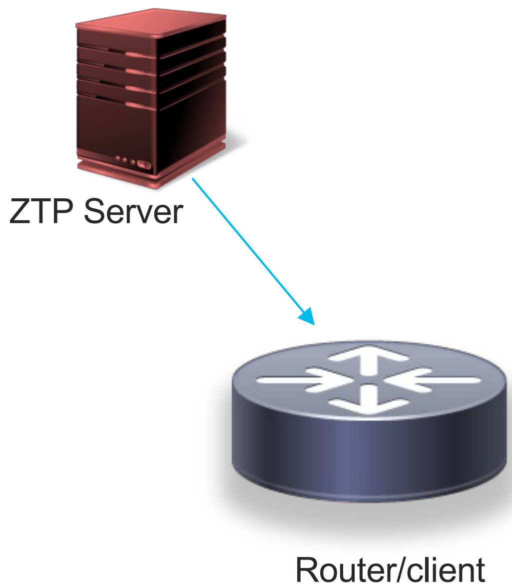
Router/Client Validation

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



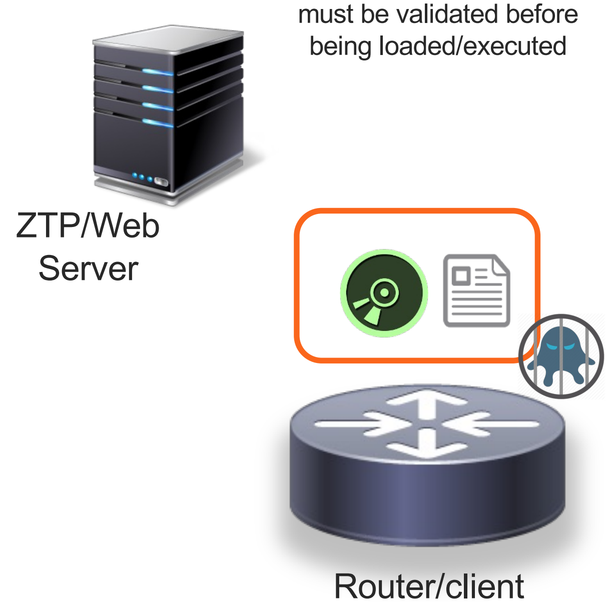
Server Validation

Router/client must validate the server offering artifacts

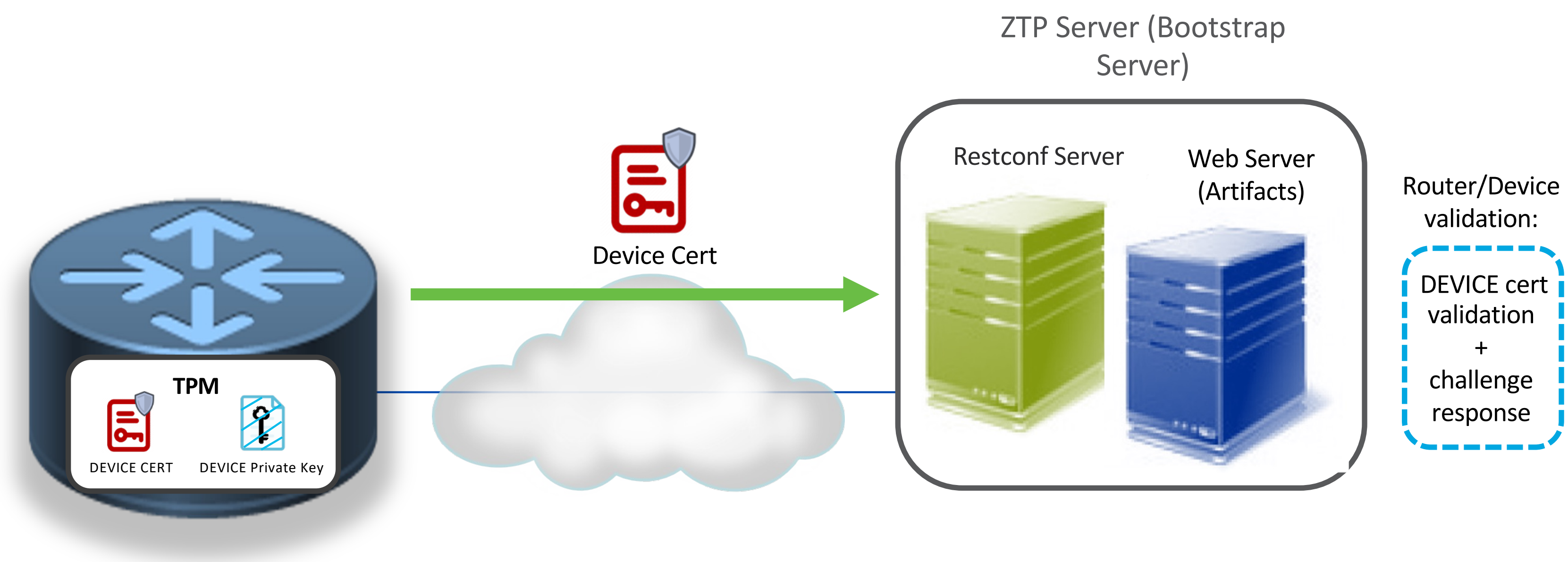


Artifact Validation

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

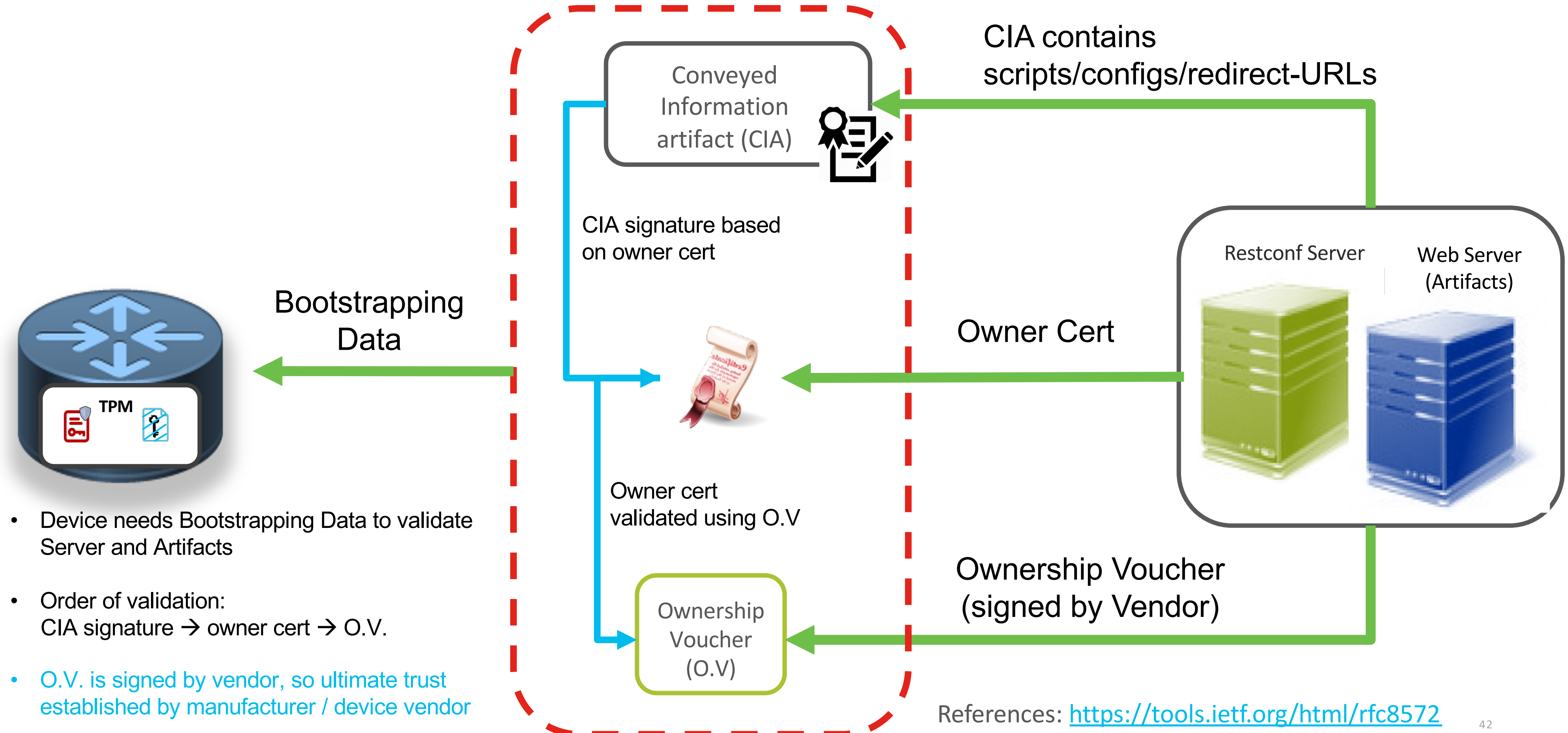


Secure ZTP (RFC8572): Router Validation



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

SZTP Artifacts (RFC 8572): 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 vendor, so ultimate trust established by manufacturer / device vendor

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

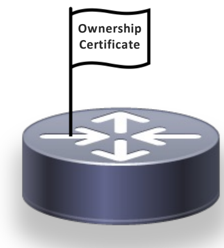
Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

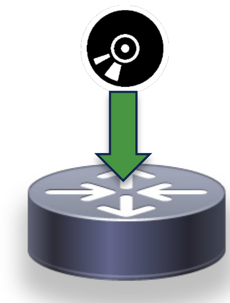
Data Protection

Data-at-rest protection & data sanitization



Ownership Establishement

Ownership Vouchers & MASA Service



Secure Device Onboarding

RFC8572 compliant secure zero touch provisioning of routers

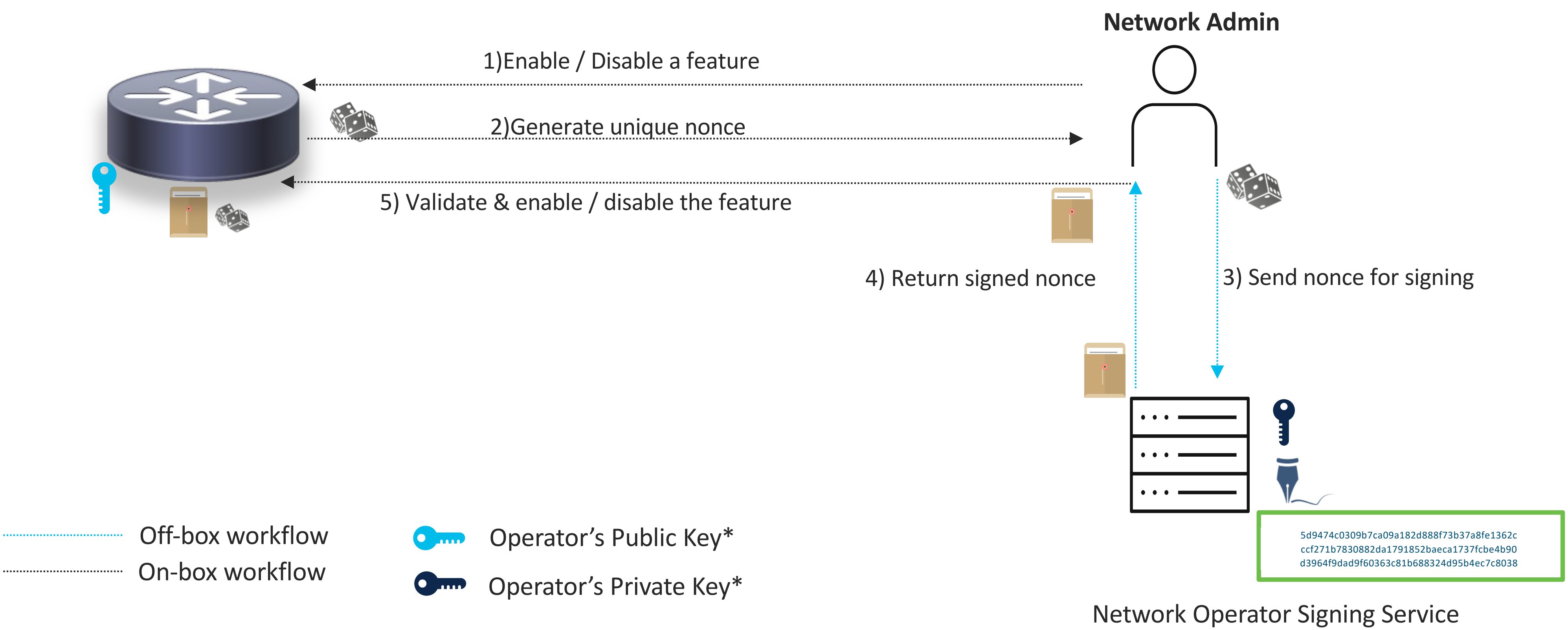
Consent Based Security Features

Additional consent for critical security features

Quantum Security

Challenges posed by Quantum Computers

CLI Challenge / Response – Consent Workflow



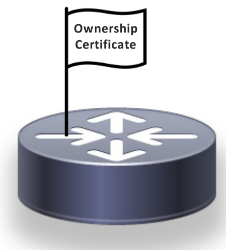
Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

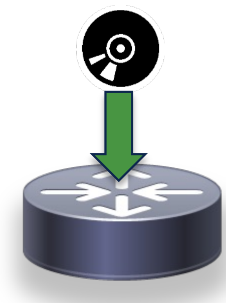
Data Protection

Data-at-rest protection & data sanitization



Ownership Establishement

Ownership Vouchers & MASA Service



Secure Device Onboarding

RFC8572 compliant secure zero touch provisioning of routers

Consent Based Security Features

Additional consent for critical security features

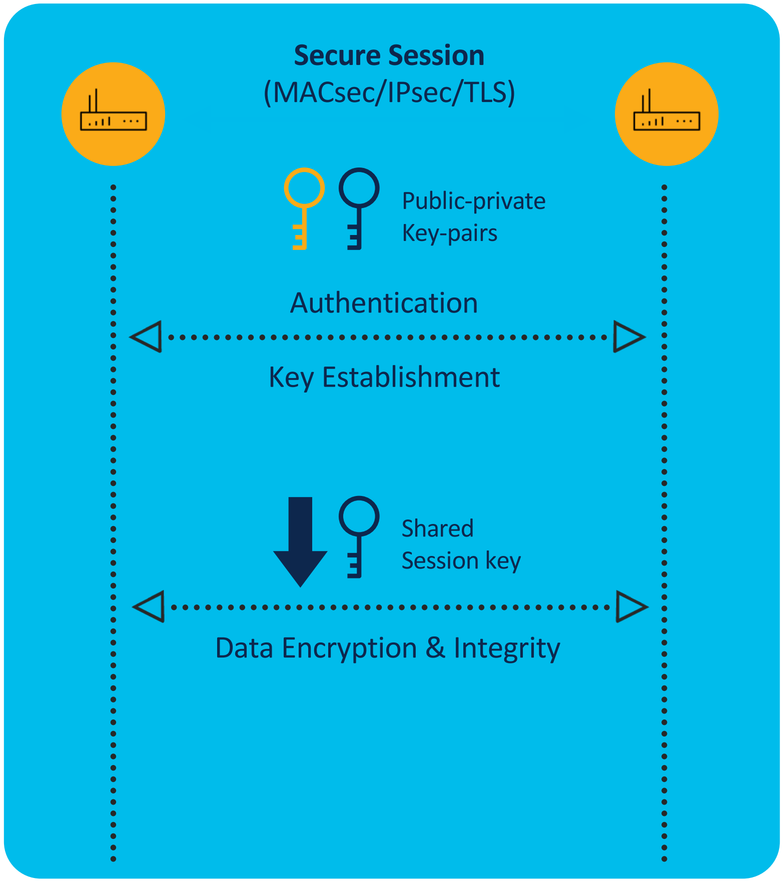
Quantum Security

Challenges posed by Quantum Computers

People are making incremental efforts in developing a **Quantum Computer.**

Once they have one which is sufficiently large and reliable, they could use it to **Break Current Encryption!** (public key algorithms)

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
- Example: RSA, DH, ECC

Large reliable Quantum computers can break RSA, DH, ECC!

Symmetric Cryptography

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

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

Why should we care about Quantum Threats **now**?

1. Attackers can tap the 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!!!

   a) Military or other defense networks
   b) Federal or other government agencies
   c) Financial institutions and banks
   d) Service provider networks catering to enterprises having sensitive data

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

Available Options

Symmetric Cryptography

- ✓ Long symmetric keys are Quantum Safe
- ⚠ Issues with distributing keys and trust

Quantum Key Distribution

- ✓ Use Quantum Mechanics to protect the data
- ⚠ Some limitations

Postquantum Cryptography

- ✓ Replace current public key algorithms with new ones
- ⚠ Still need to vet the algorithms and update the protocols

To Summarize…

Threats to Network Devices & Solutions

NOS

Integrity Visibility (Boot & Run-time)

NOS Runtime

(Maintain Trust at Run-time)

BSP & Linux Kernel

(Establish Trustworthy NOS)

RP BIOS | **LC BIOS**

X86 - CPU

(Establish Trust in Hardware)

Protection against

Solutions

- Disk Encryption
- Remote Attestation
- Secure Onboarding
- Operational Security Features

- Measured Boot
- Security Enhanced Linux
- Integrity Measurement Arch.

- Unique Hardware Identity
- Platform Security Chip like TPM
- Hardware anchored Secure Boot

Questions?