
cisco Live!
Let's go

The bridge to possible

Building & Maintaining Trust in Service Provider Networks

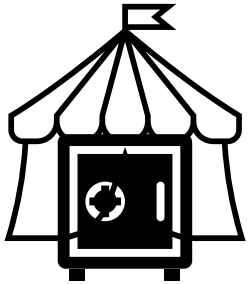
Rakesh Kandula, Technical Marketing Engineer

cisco Live!

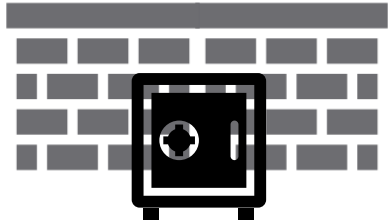
BRKSPG-2868

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



Steel door is useless if you are protecting a tent



Steel door is useful only when you are protecting a concrete structure

Operational security is useful only when the underlying router has trust built into it from the hardware layer

Agenda

- Trustworthy Platforms Overview
- IOS-XR Operational Security
- Automating Security Workflows
- Conclusion

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

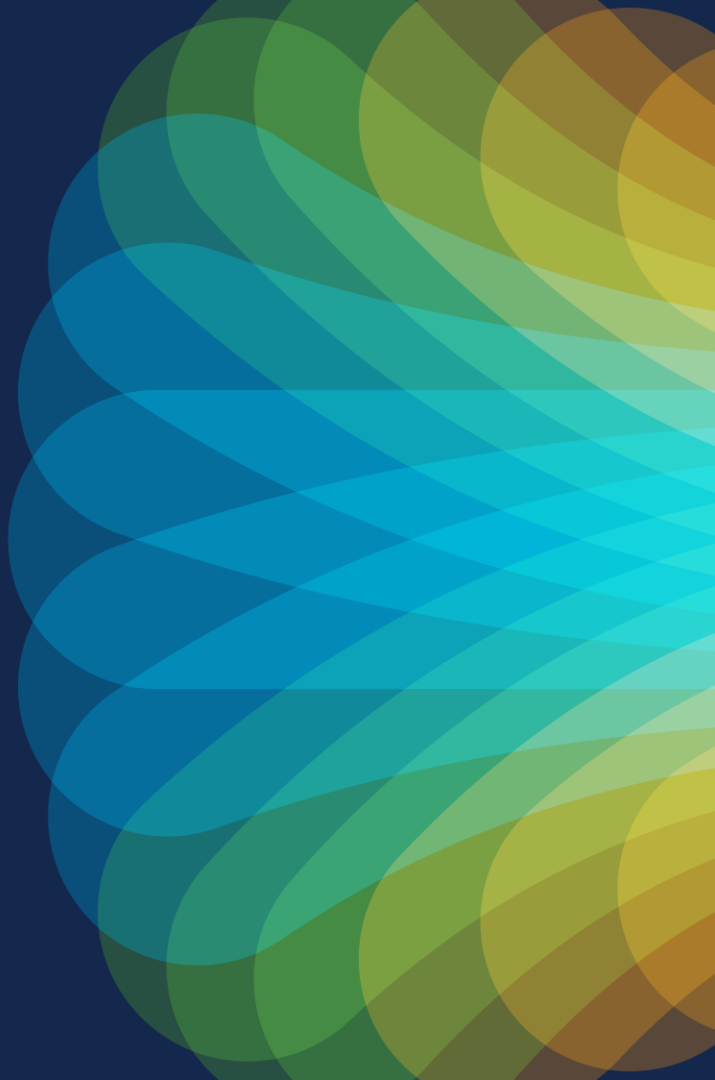
Loss of Revenue

Brand Reputation Loss

Impact to SLAs

Legal Implications

Trustworthy Platforms Overview



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

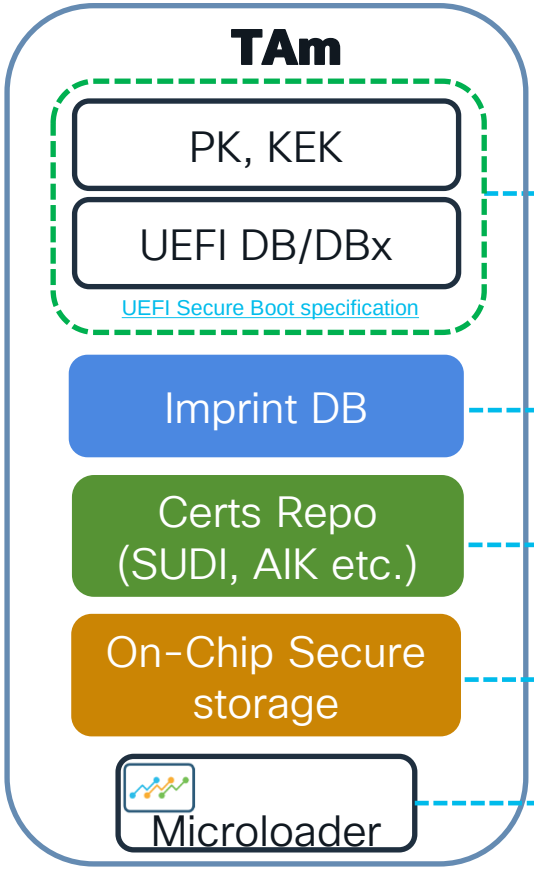
Maintaining Trust at Runtime

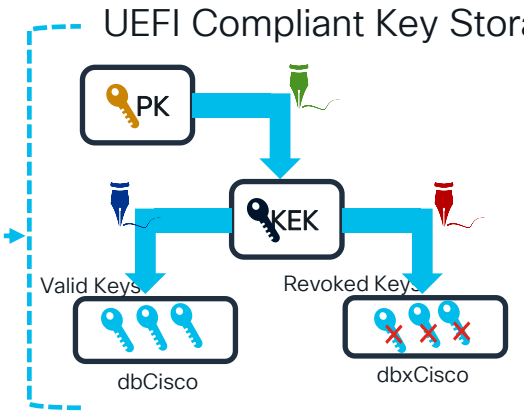
Run-time Defenses, Config Encryption, DDoS Protection

Visualize and Report on Trust

Trust Dossier & Crosswork Trust Insights

Enabling Trust in Hardware – Cisco's TAm* Chip





Provides Chip Guard functionality

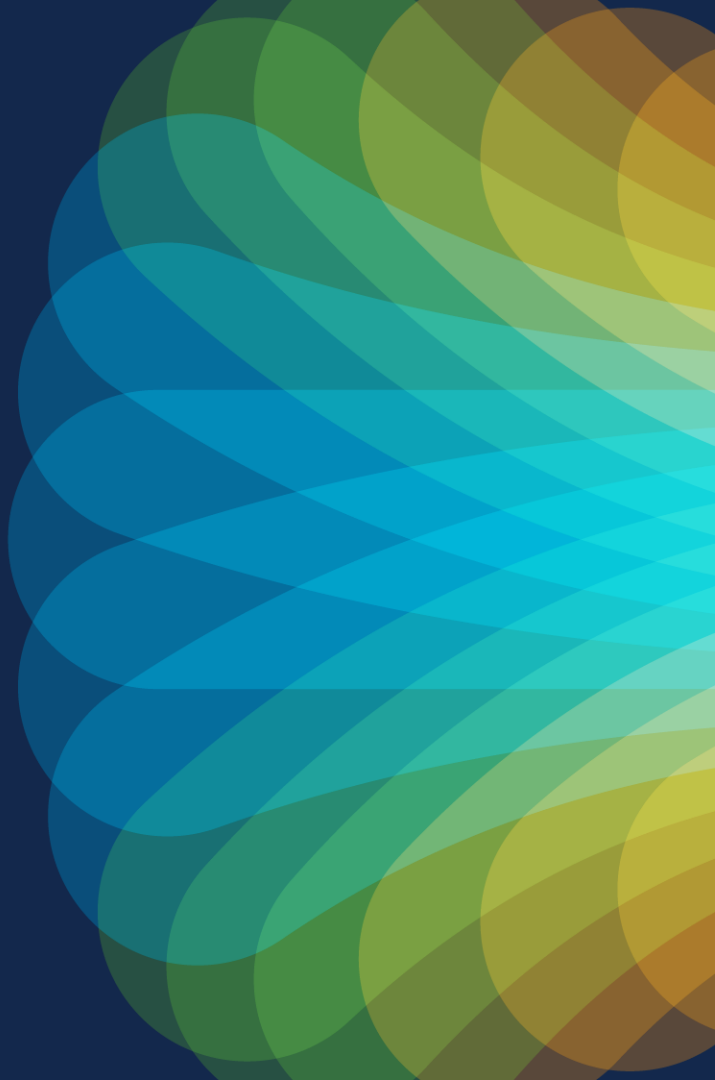
Provides unique device identity

Stores additional keys, certs, flags, etc.

Anchor for Secure boot

*Trust Anchor Module

IOS-XR Operational Security



Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

Data Protection

Data-at-rest protection & data sanitization

Remote Attestation

Periodic validation of device integrity

Ownership Establishement

Ownership Vouchers & MASA Service

Consent Based Security Features

Additional consent for critical security features

Counterfeit Protection

SUDI Authentication For Hardware Integrity

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

Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

Data Protection

Data-at-rest protection & data sanitization

Remote Attestation

Periodic validation of device integrity

Ownership Establishement

Ownership Vouchers & MASA Service

Consent Based Security Features

Additional consent for critical security features

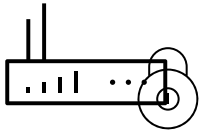
Counterfeit Protection

SUDI Authentication For Hardware Integrity

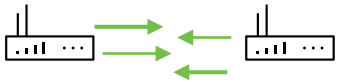
Config Encryption For Routers

1. Provides data-at-rest protection
2. Encrypts disk partition holding configuration data
3. Encryption key protected by TAm
4. Zeroization CLI for RMA scenarios

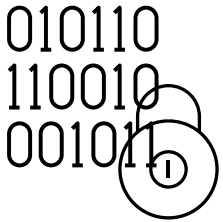
Data Protection and the missing element



Data At Rest



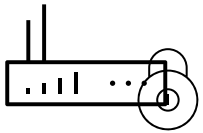
Data In Transit



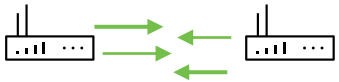
Data In Use

And...

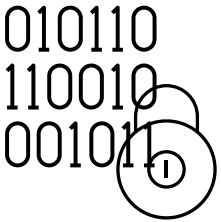
Data Protection and the missing element



Data At Rest



Data In Transit



Data In Use

Data Sanitization

Data Sanitization

1. Setup de-commissioning process for data-bearing components
2. Use IOS-XR's factory reset feature
3. Statement of Volatility available on Trust portal guide

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

Remote Attestation

Periodic validation of device integrity

Ownership Establishement

Ownership Vouchers & MASA Service

Consent Based Security Features

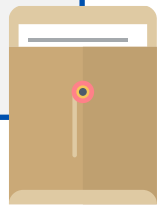
Additional consent for critical security features

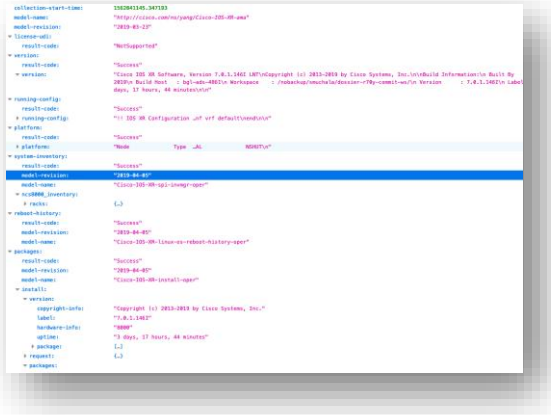
Counterfeit Protection

SUDI Authentication For Hardware Integrity

Example of 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

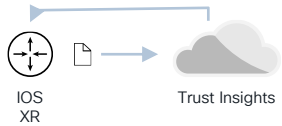




- Human-readable JSON formatted output via CLI command
- Signed envelope (not encrypted)

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

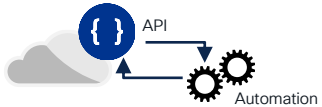
3

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.

Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

Data Protection

Data-at-rest protection & data sanitization

Remote Attestation

Periodic validation of device integrity

Ownership Establishement

Ownership Vouchers & MASA Service

Consent Based Security Features

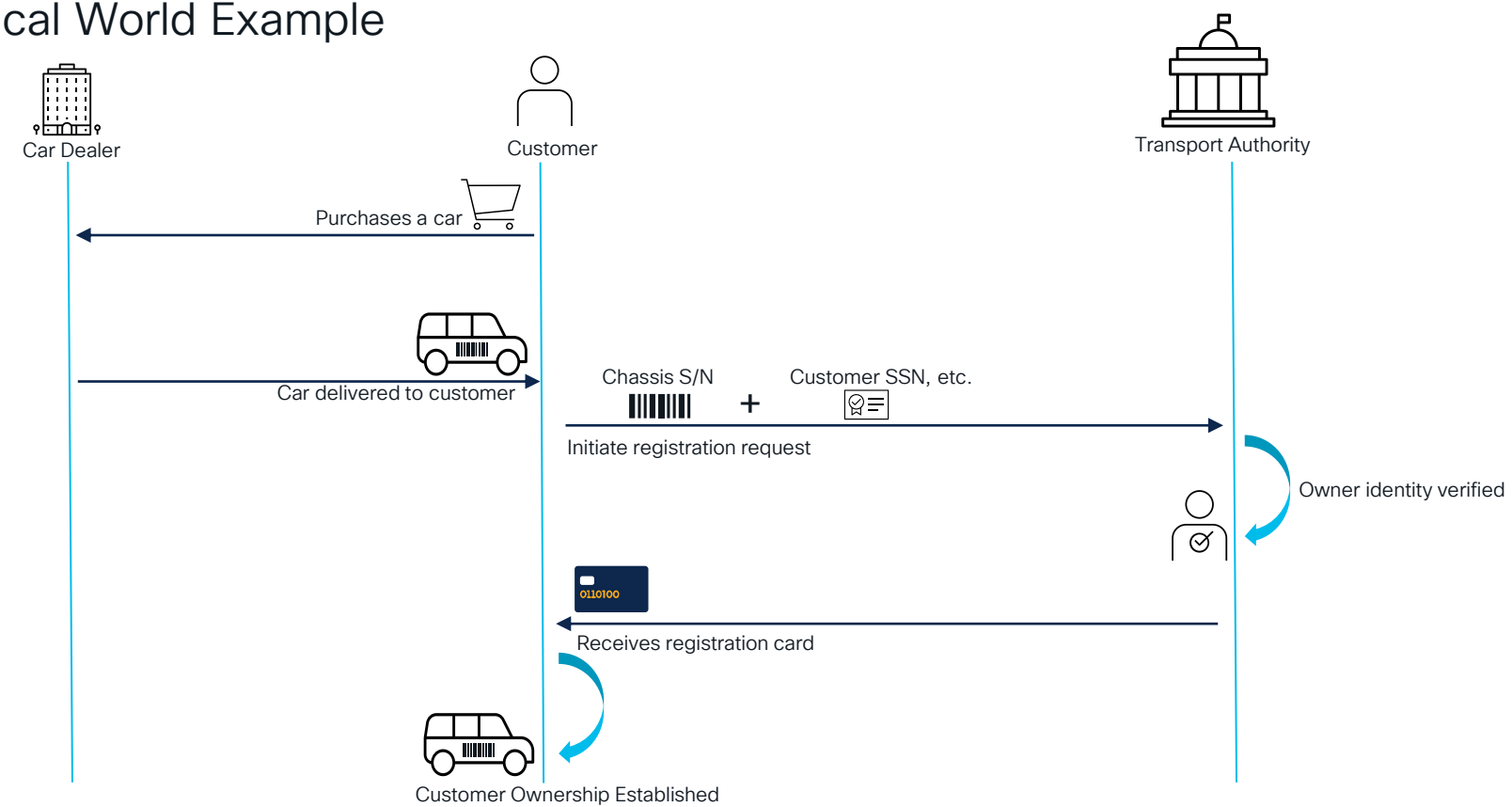
Additional consent for critical security features

Counterfeit Protection

SUDI Authentication For Hardware Integrity

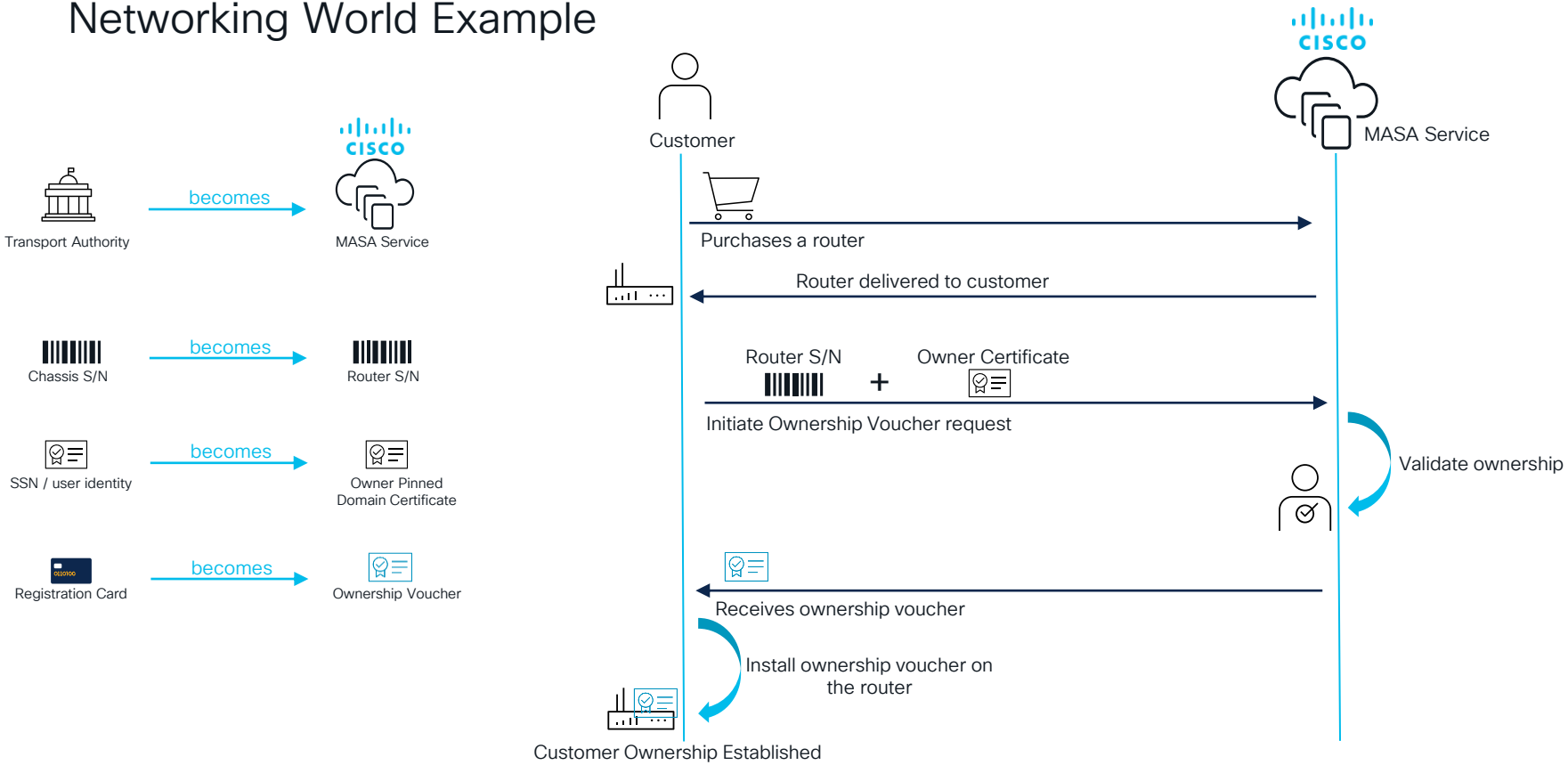
What is Ownership Establishment?

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.

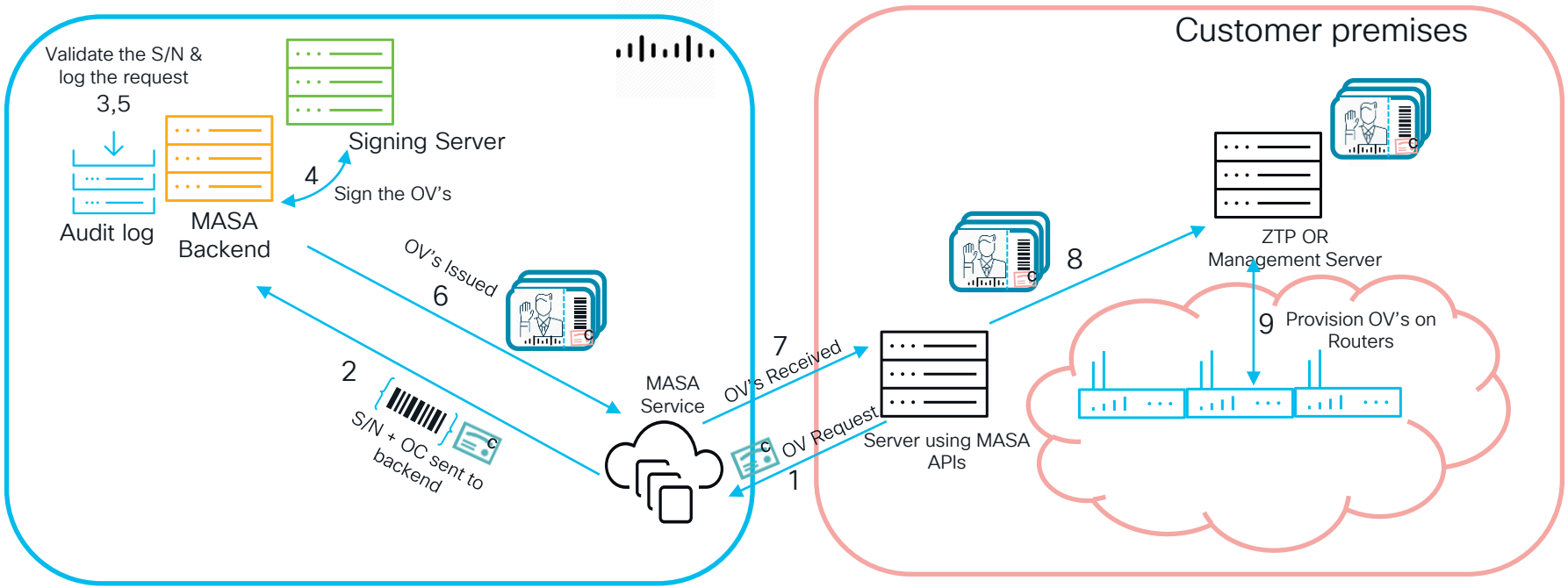
```
module: ietf-voucher

  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
```

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?

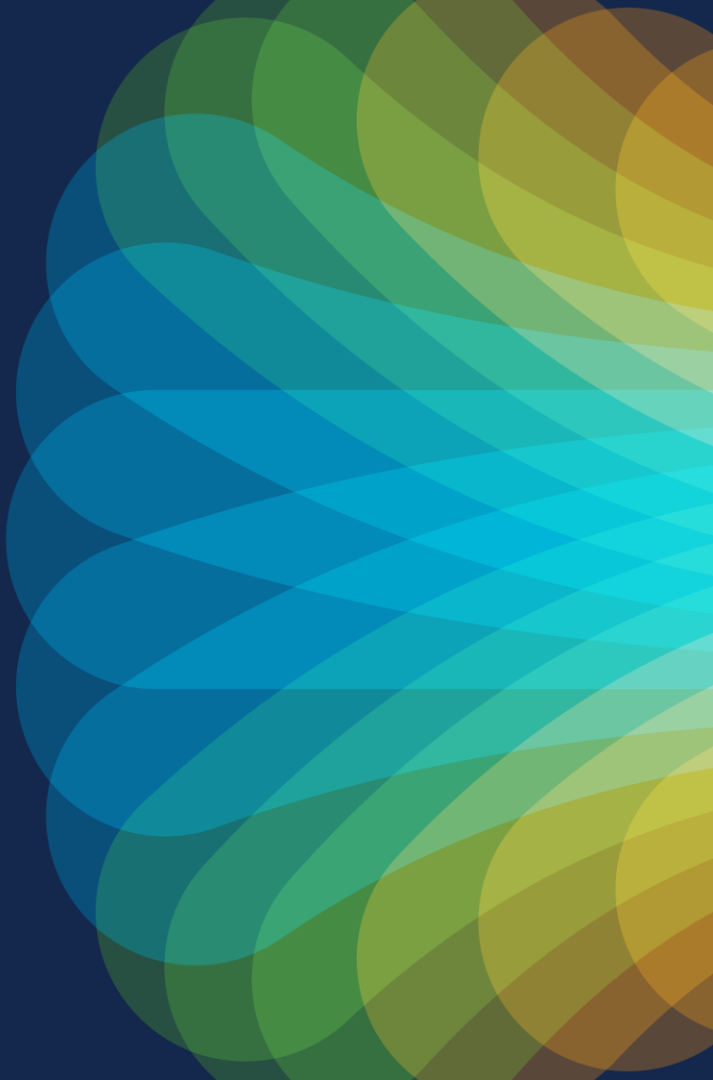
Automated MASA Service Workflow



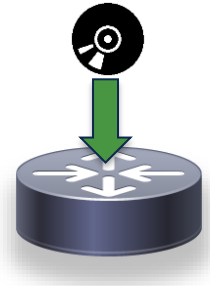
MASA - Manufacturer Authorized Signing Authority

MASA Demo

Why Establish Ownership?



Ownership Establishment – Use cases



Secure Zero Touch Provisioning (SZTP)

RFC8572 compliant secure zero touch provisioning of routers

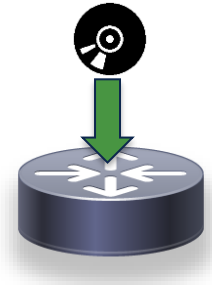
Application Signing

Onboard Key Package for Signed Apps

Consent Based Security Features

Additional consent for critical security features

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

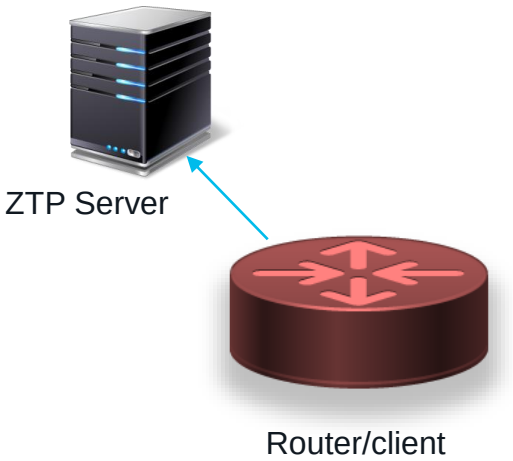
Consent Based Security Features

Additional consent for critical security features

Security Considerations for Zero Touch Provisioning (ZTP)

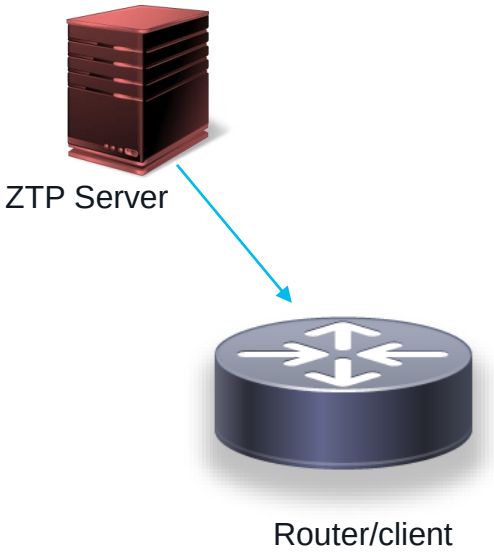
Router/Client Validation

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



Server Validation

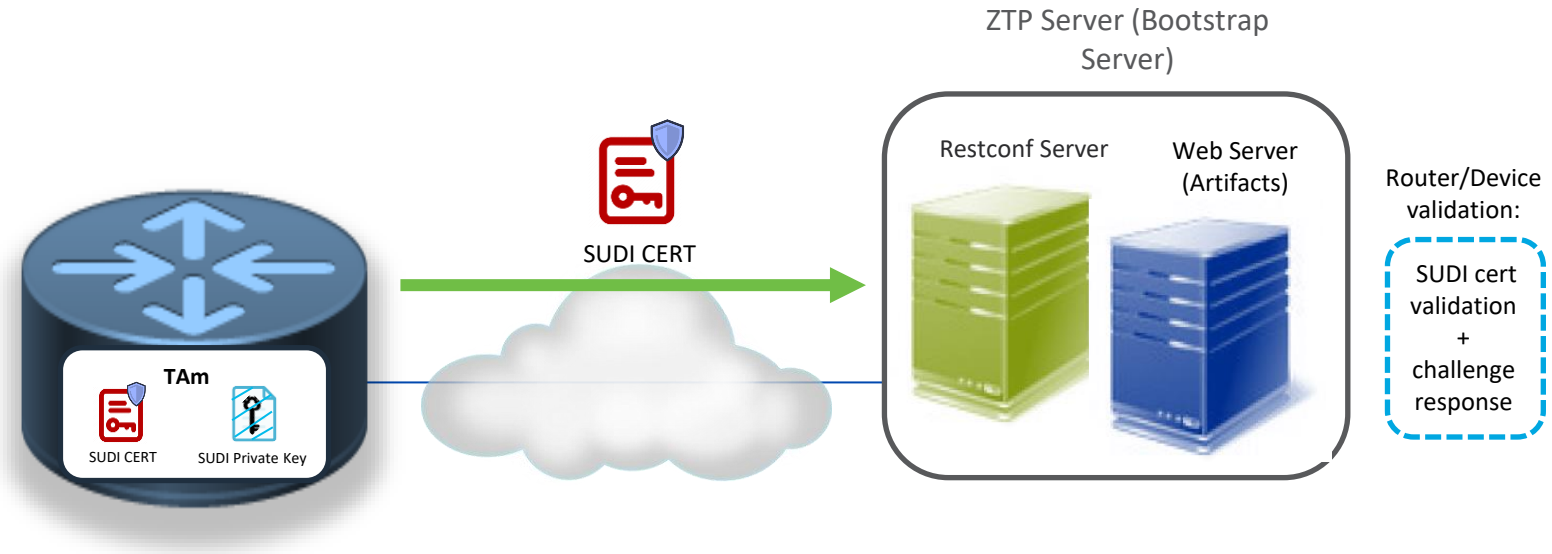
Router/client must validate the server offering artifacts



Artifact Validation

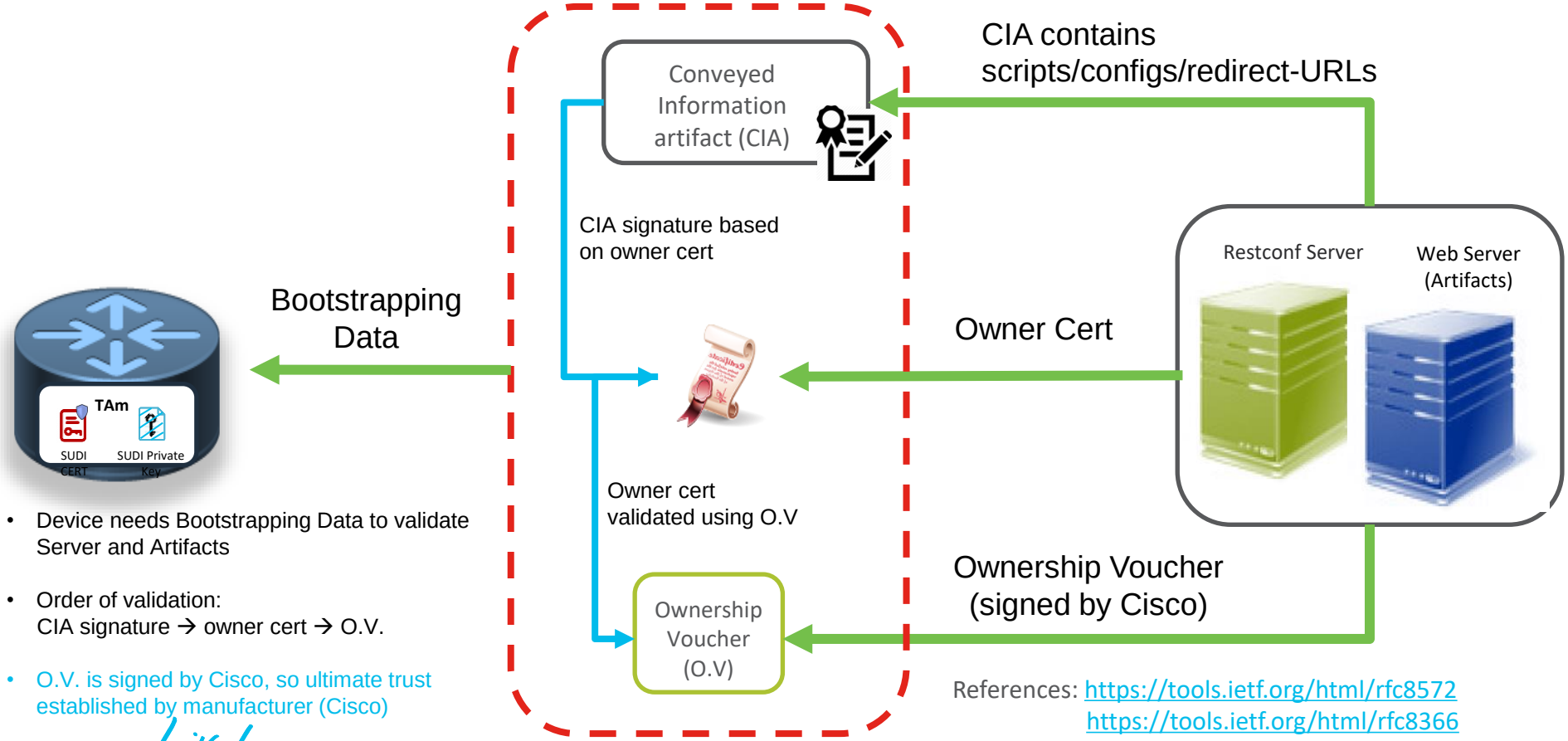
The artifact downloaded from the ZTP/Web server must be validated before being loaded/executed

Secure ZTP (RFC8572): Router Validation



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

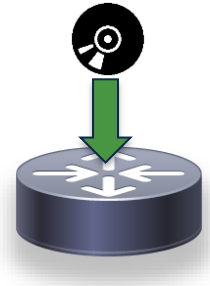
SZTP Artifacts : ZTP Server + Artifact Validation



- 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

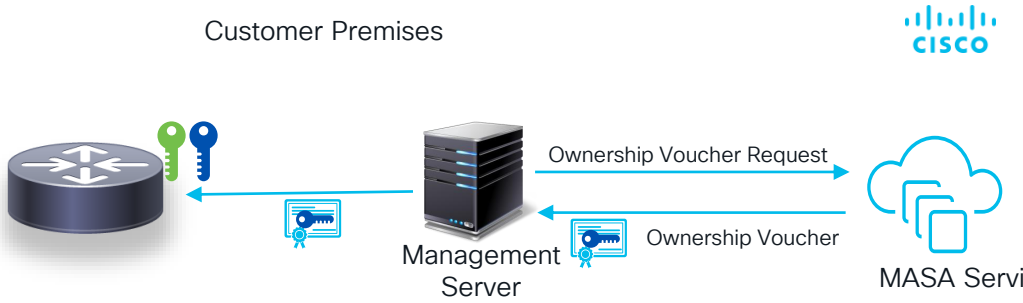
Additional consent for critical security features

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

Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

Data Protection

Data-at-rest protection & data sanitization

Remote Attestation

Periodic validation of device integrity

Ownership Establishement

Ownership Vouchers & MASA Service

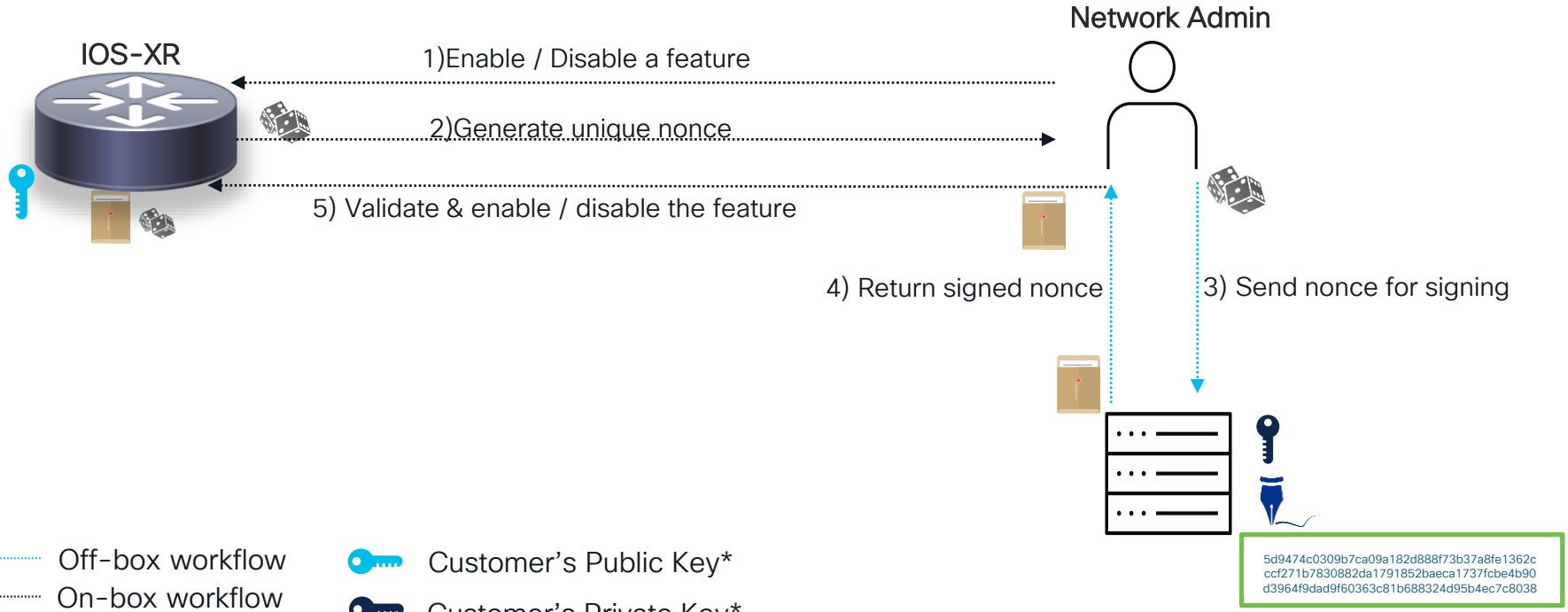
Consent Based Security Features

Additional consent for critical security features

Counterfeit Protection

SUDI Authentication For Hardware Integrity

CLI Challenge / Response – Consent Workflow



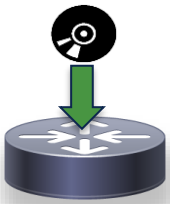
Consent Based Security Features

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...

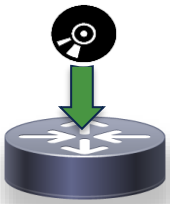
Consent Based Security Features

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

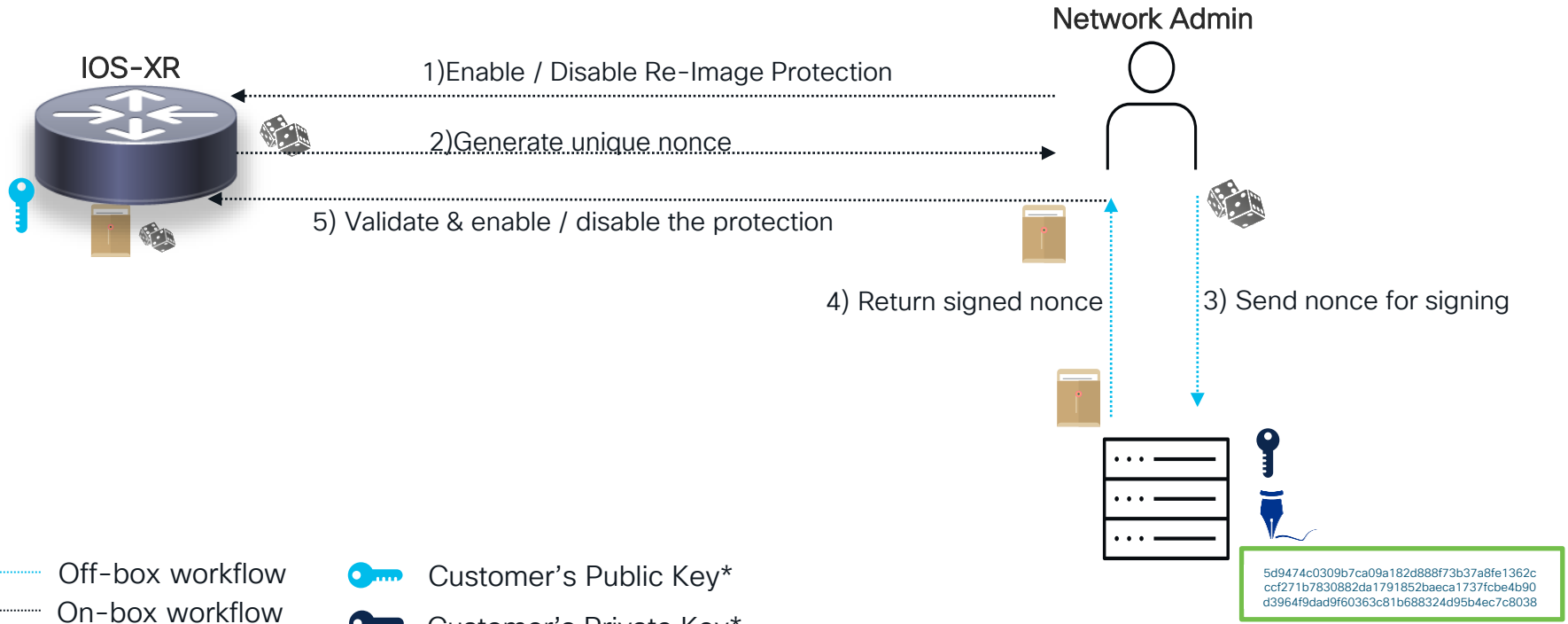
1. Increasing incidents of cell site routers in remote locations being stolen
2. The stolen routers are factory reset by booting through USB or PXE boot that erases the older running config too
3. These routers are then sold in illegal markets
4. Some incidents involve rogue internal employees too

Re-Image Protection For Routers

Workflow

1. New XR CLI with additional consent to disable USB/PXE boot
2. Store the flag in the tamper-resistant on-chip TAm secure storage
3. Persistent across disk erasure & reload
4. BIOS disables USB/PXE boot if flag is enabled

Re-Image Protection – Consent Workflow



*Applicable for Customer Consent Only

Operational Security Focus Areas

User Identity Access

Adopting Passwordless SSH, MFA, AAA controls, etc.

Data Protection

Data-at-rest protection & data sanitization

Remote Attestation

Periodic validation of device integrity

Ownership Establishement

Ownership Vouchers & MASA Service

Consent Based Security Features

Additional consent for critical security features

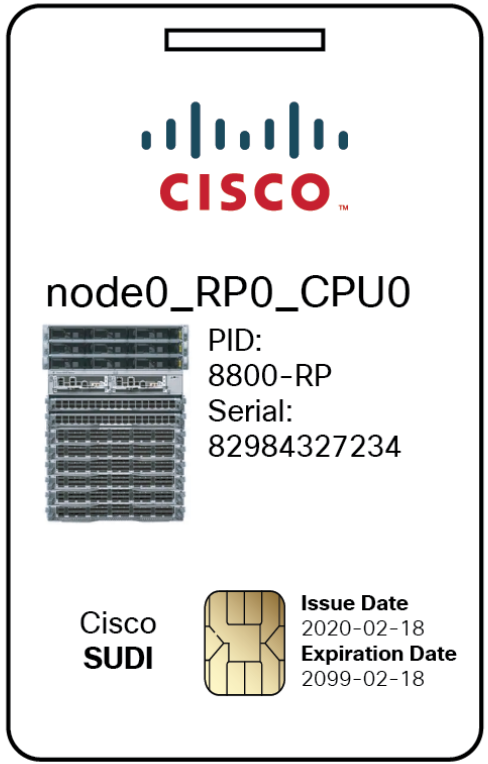
Counterfeit Protection

SUDI Authentication For Hardware Integrity

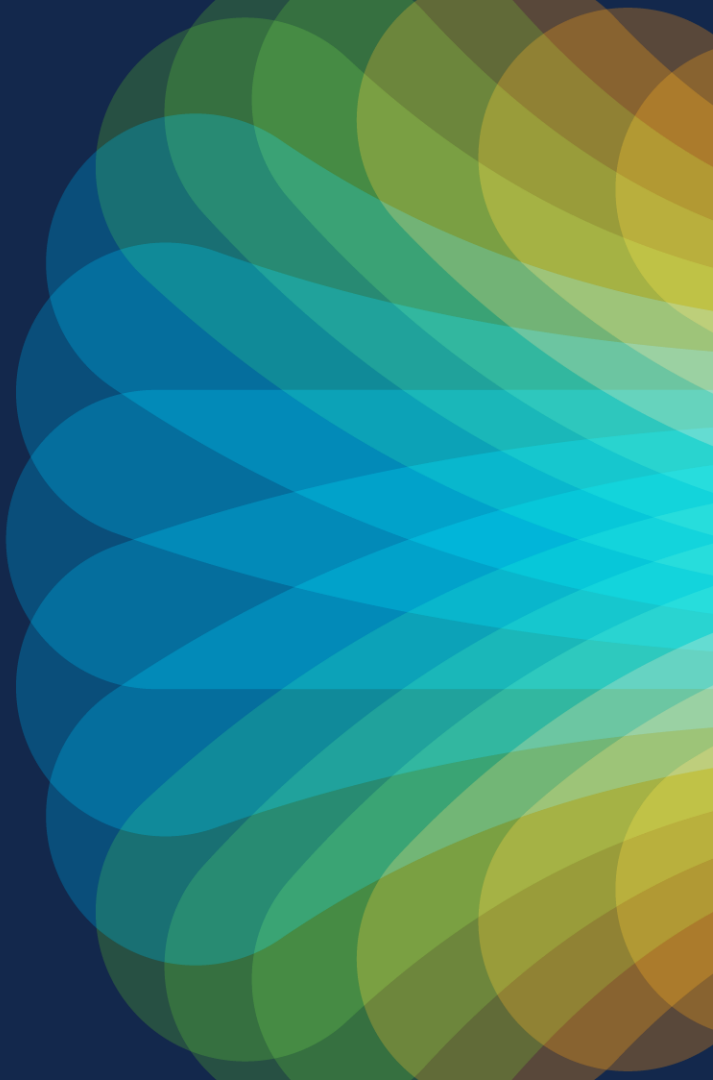
Secure Unique Device Identity (SUDI)

"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

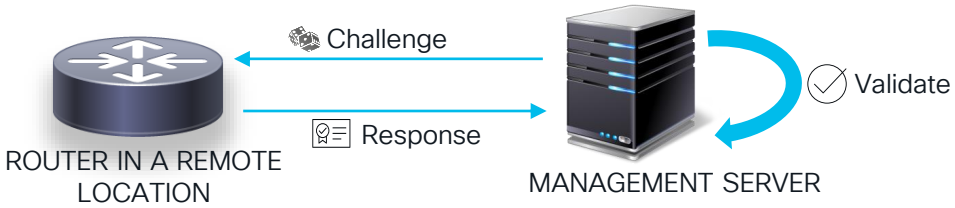


Automating Security Workflows



cisco Live!

SUDI Workflow For Hardware Integrity Validation



Challenge

1. Challenge the remote router with a unique nonce to provide it's SUDI certificate.
2. The nonce 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 nonce is included in the response signature.

Validate

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 Cisco PKI

Counterfeit Hardware Detection Demo

SUDI Based CLI Signature Utility

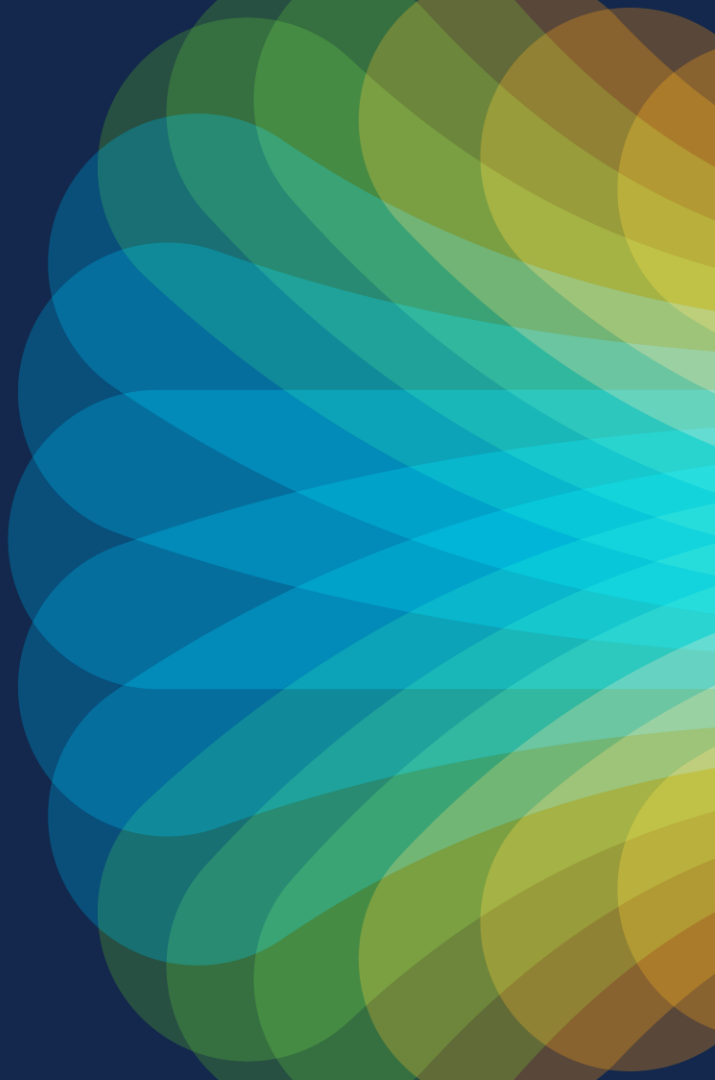
IOS-XR supports a CLI signature utility based on SUDI private key

1. Any IOS-XR CLI output can be signed by SUDI private key using the signature utility
2. This is to ensure the output is from a genuine device and not a replay from meddler-in-the-middle (MITM) attack
3. The signature of the signed CLI response can be validated first using the SUDI public key before consuming the CLI output

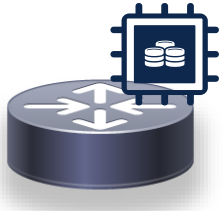
SUDI Based CLI Signature Utility - Example

RP/0/RP0/CPU0:Galapagos#show version | utility sign nonce ABCD
Tue Mar 7 06:31:00.071 UTC
{
"cli-output": "Cisco IOS XR Software, Version 7.4.1 LNT\nCopyright (c) 2013-2021 by Cisco Systems, Inc.\n\nBuild Information:\n Built By : ingunawa\n Built On : Wed Aug 04 08:28:43 UTC 2021\n Build Host : iox-lnx-021\n Workspace : /auto/srcarchive17/prod/7.4.1/ncs540l-aarch64/ws\n Version : 7.4.1\n Label : 7.4.1\n\ncisco NCS540L\ncisco N540X-8Z16G-SYS-A processor with 8GB of memory\nGalapagos uptime is 6 weeks, 6 days, 19 hours, 9 minutes\nCisco NCS 540 Series Fixed Router 12x1G, 4 xCu, 8x1/10G, AC\n\n",
"signature-envelop": {
"nonce": "ABCD",
"signature-version": "02",
"sudi-signature": "Ugj00x78n3hXD1nzymEOpUsR143N3Zgz8g15m40eQmrO6yQ0etqGM+10vkSEoz9zTnQ+qicufZyp+Vx4MRLagnFXOoQubAY94CB/85qmrLi1is9phjPJ0uDhK5bpF8bQZtZbQ3PcLOyfx1sG8Gk13I0xQaWdgbB1daz3setsjHkjvHzFSu2aTtKW+DdZSUOxOaCXgSxazwDbE/v826Lng31JzFfgh9SLQEijp3IfdmKFeRpdK4fOSZN1tXdwlfXRo2YpRPEf9oPEYXI91/b5Bjaz+kCamGintVeqV5XiBxLvpVLtxIymoZtJuDdX/NYe/5UGtjG/wAMcgbN/1JKlBQ=="
}
}

Conclusion



Building Trustworthy Network Includes



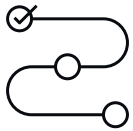
Validating hardware integrity

Enabling boot integrity

Periodic evaluation of device posture during runtime

Updating operational security features

Having stronger data protection policies



Automating operational security

02/07/24 @ 08:45 AM & 02/08/24 @ 10 AM

FULL CONFERENCE | IT LEADERSHIP

Cisco Secure Edge Protection–Protecting the 5G Edge against DDoS Attacks - BRKSPG-2401

Mike Geller, Distinguished Architect, Radware

The rapid expansion of 5G has led to a diverse threat surface threatening the availability and sustainability of desired low-latency outcomes (virtual reality, IoT, etc.). One of the newer threats is the attack from rogue IoT devices and UE (phones, iPads and other 5G attached devices). This session covers the different angles and approaches to dealing with these threats, otherwise known as "protecting the 5G N3." The Cisco Secure Edge Protection service is a container and controller (to aggregate feedback from tens of thousands of cell site routers or "edge routers") that today is offered in the NCS 540 Cell Site Router and will be expanded to other IOS-XR platforms, including white box platforms. Please come to this session to learn how to protect your network, your customers, and the SLAs bound to the current and next-generation services. The widely distributed nature of the 5G network means that customers should expect to be able to see and mitigate DDoS services as far out to the edge as possible. You'll learn about the supporting technology and see a live demonstration of how it works.

Technical Level: Intermediate

Technology: 5G, Security

Session Type: Breakout

Session Length: 90 Minutes

Percentage of New Content: 75% New

Eligible for Continuing Education Credit: Yes

You are a Speaker **Tuesday, Feb 6 | 4:45 PM - 6:15 PM CET**


cisco
The bridge to possible
Thank you
cisco Live!


cisco Live!
Let's go