

Trustworthiness-centric Software Supply Chain Security

Regulations, Requirements & Solutions

Dr. Xin Qiu, Dr. James Ni, Dr. Lisa Yin

COMMScope®

About CommScope



Sr. Director at CommScope PKI Center & Security Solutions:

Dr. Xin Qiu has over 25 years of experience in Public Key Infrastructure (PKI), device, and software security, holding a portfolio of 80+ patents.

I lead a diverse team in R&D, security operations, product marketing and management, delivering security services to global device manufacturers and network operators.



Agenda

Typical Threats in Software Supply Chain (SSC)

Emerging Government Regulations and Industry Initiatives

Fundamentals of Software Supply Chain Security

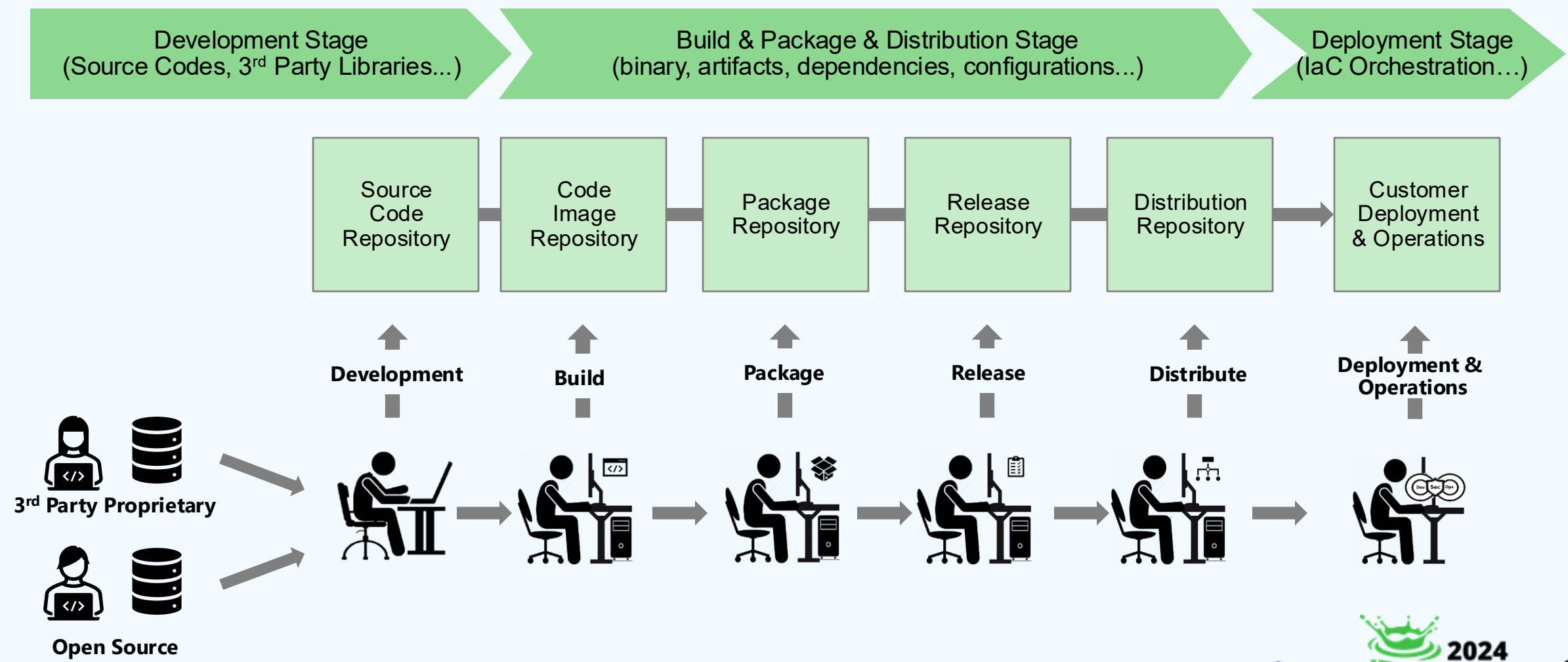
CommScope Solution for SSC Security

Collaborative Solutions from JFrog and CommScope (demo)

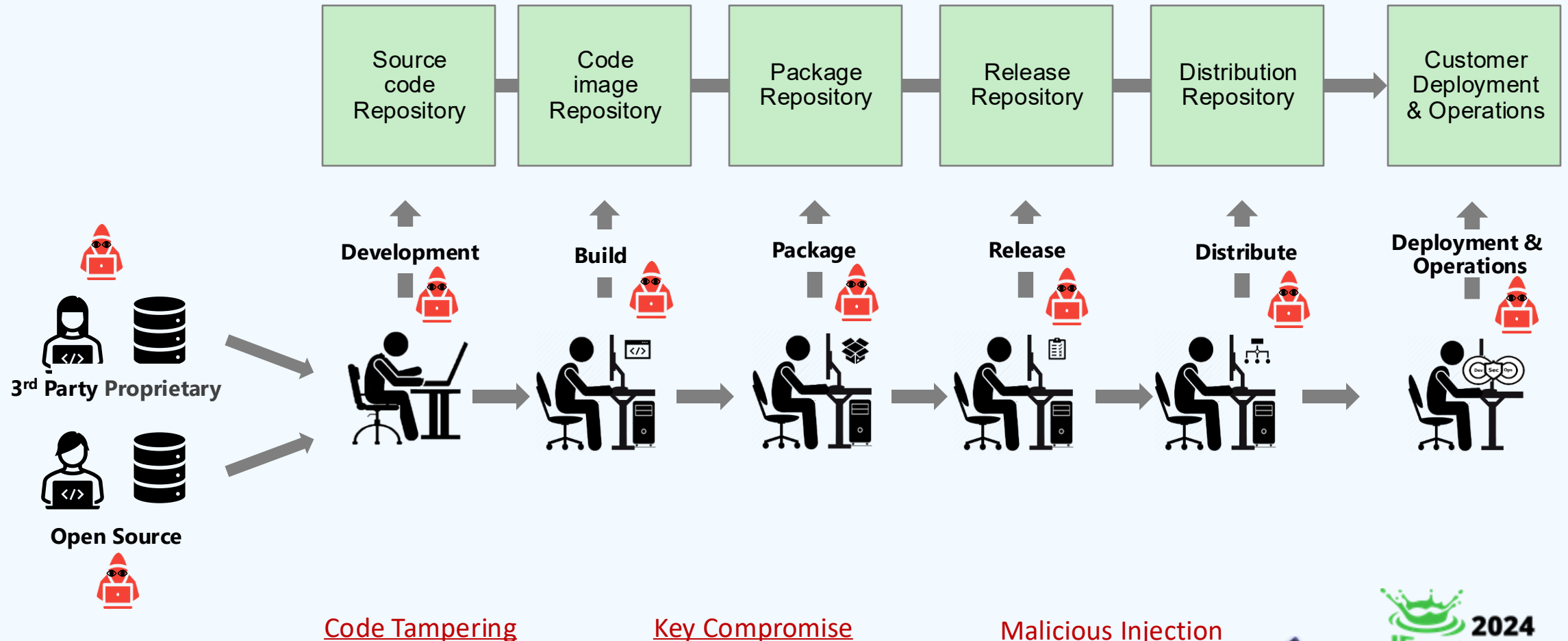
Forward Looking: Post-Quantum Code Signing

Conclusions

Software Supply Chain (SSC)



Typical Threats in Software Supply Chain



Emerging Government Regulations

United States



Globally, **new laws and regulations** are being enforced to require stronger measures for software supply chain security and application security.

Code Signing Requirement: Suppliers must perform code signing for all software/firmware delivered to customers & partners, to ensure security & integrity.

Risk Mitigation: Any gaps in code signing processes can expose customers to malicious or counterfeit components, damaging the supplier's brand, reputation, and business.

Securing the Software Supply Chain: Recommended Practices for Managing Open-Source Software and Software Bill of Materials



Industry Consortia and Initiatives



Software Trustworthiness Best Practices

https://www.iiconsortium.org/pdf/Software_Trustworthiness_Best_Practices_Whitepaper_2020_03_23.pdf



Safeguarding artifact integrity across any software supply chain

[SLSA • Supply-chain Levels for Software Artifacts](#)



The Trusted Services project provides a framework for developing and deploying device Root Of Trust (RoT)

<https://www.trustedfirmware.org/projects/trusted-services>



PKI Consortium Best Practices for Code Signing

<https://about.signpath.io/product/pkic-best-practices>



SOFTWARE QUALITY STANDARDS – ISO 5055

<https://www.it-cisq.org/standards/code-quality-standards/>



Scaling Up Supply Chain Security: Seamless Container Image Signing

<https://openssf.org/blog/2024/02/16/scaling-up-supply-chain-security-implementing-sigstore-for-seamless-container-image-signing/>



Creating the Complete Trusted Computing Ecosystem: An Overview of the Trusted Software Stack (TSS) 2.0

<https://trustedcomputinggroup.org/resource/creating-complete-trusted-computing-ecosystem-overview-trusted-software-stack-tss-2-0/>



Fundamentals of Software Supply Chain Security

Institutional Trust and Confidence

- Establishing trust and confidence in software's integrity among all stakeholders.

Software Lifecycle

- Addressing risks and weaknesses through a rigorous process of software design, development, testing, validation and deployment

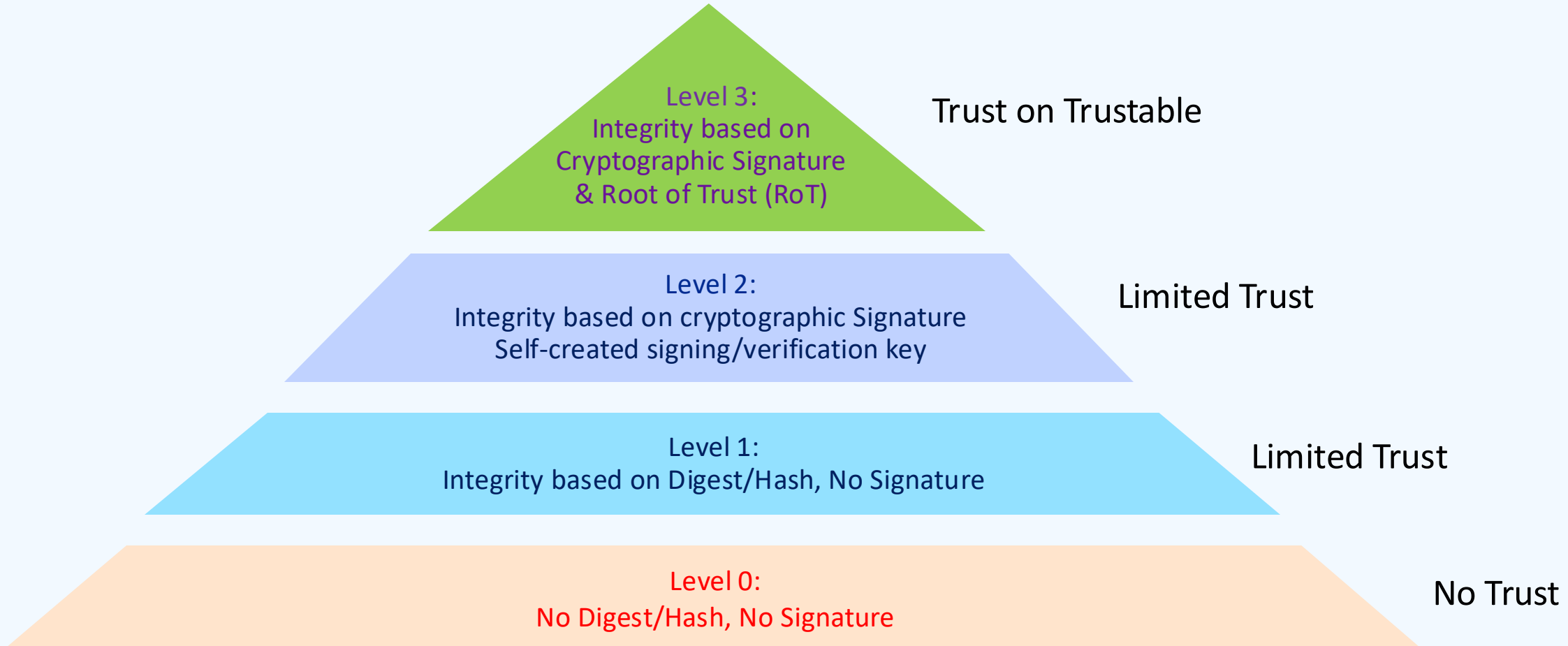
Software Operation

- Maintaining the integrity of software-at-rest and software-in-operation.

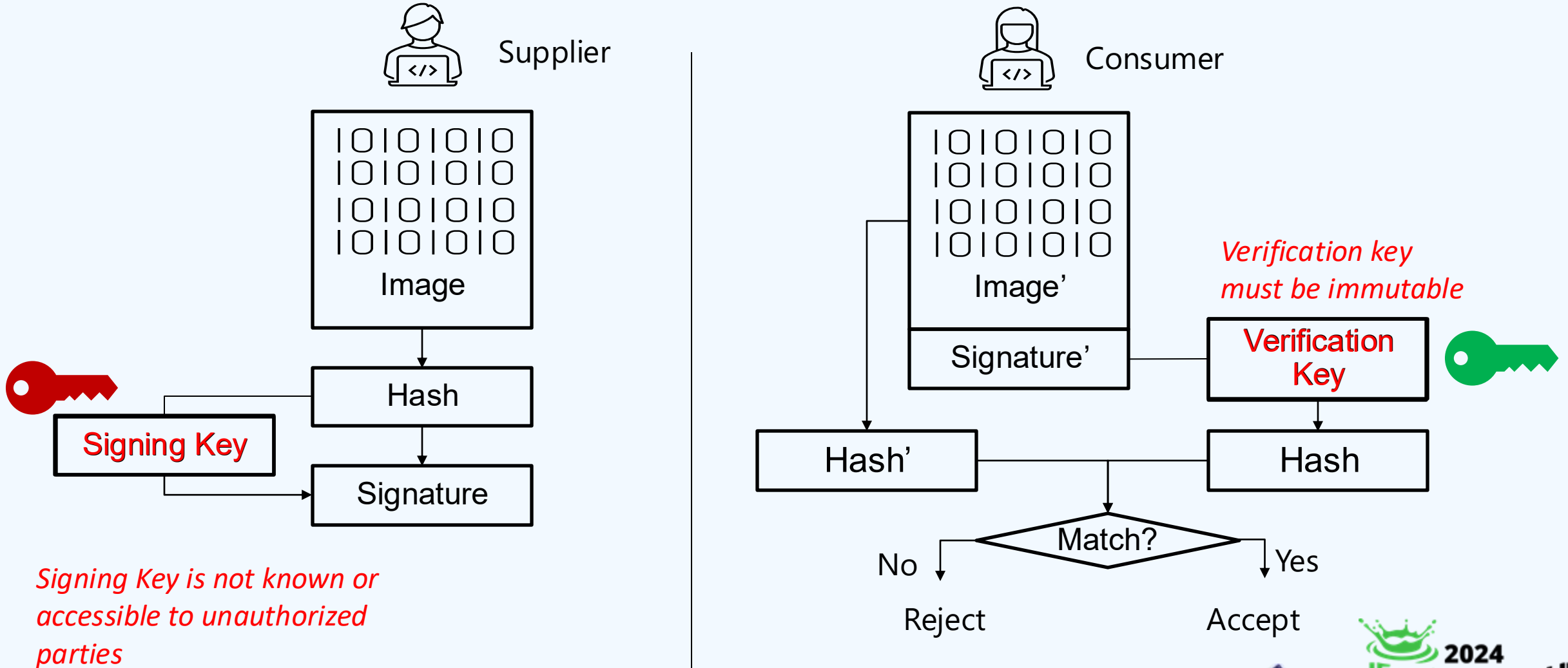
Software Protection

- Protecting software from unauthorized access and tampering.

Basics: Software Integrity – Levels of Trust



Basics: Software Integrity via Code Signing



Ensuring Trustworthiness in Code Signing

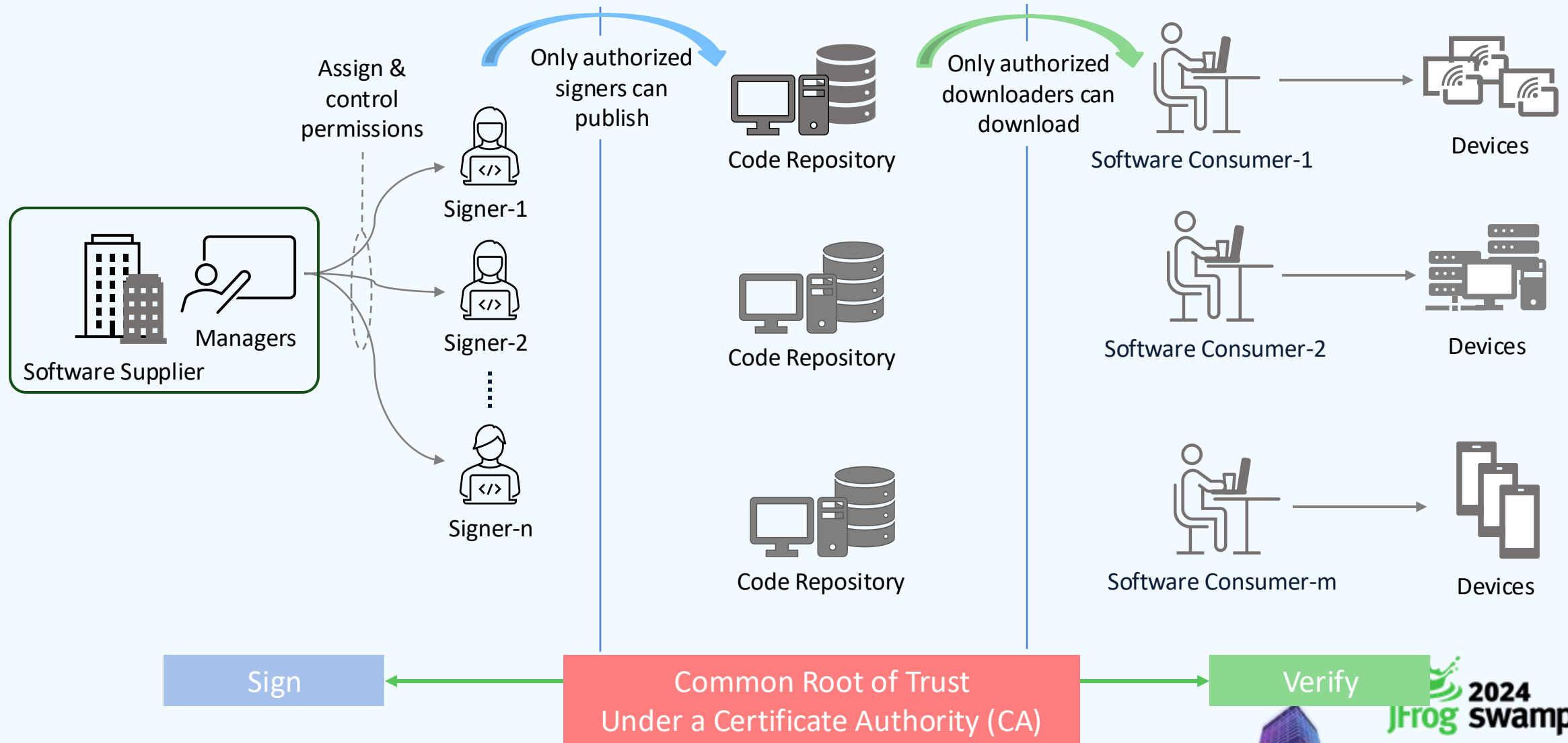
Signing and Verifications Keys

- Code signing without signing key protection leaves doors open to malicious injection threats
- Code signing without chaining verification key to a root of trust increases vulnerability to man-in-middle attacks

Signers and Signing Activities

- Lack of signer verification diminishes confidence in the integrity of the code
- Absence of signer activity tracking hinders accountability, undermining trust and the integrity of the signing process

A Trust Framework for Code Signing in SSC



CommScope's Code Signing Platform

CommScope's Solution: PRiSM (Permission Rights Signing Manager)

Code Signing
Encryption, Obfuscation



Fortify Your Software Against Malicious Actors
Build Trust for Your Applications!

AUTHENTICATION

Ensure software originates from a trusted source & detect unauthorized modifications

CONFIDENTIALITY

Hide software implementation & protect sensitive information against IP theft and reverse engineering

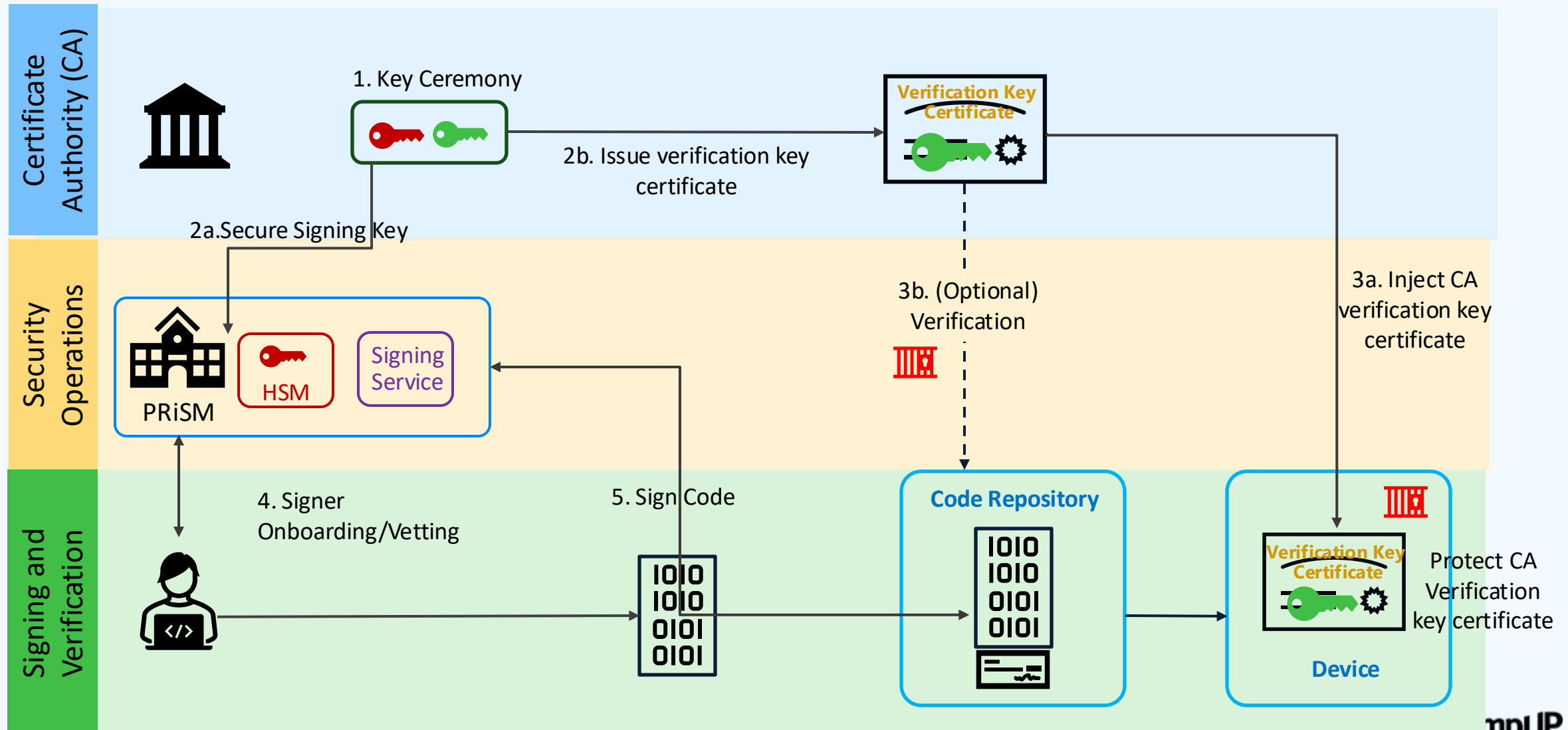
NON- REPUDIATION

Ensure accountability of developers or publishers & protect against insider attacks

USER TRUST

Instill confidence and trust in users through verified, secure software applications

CommScope's Code Signing Flow



Term: HSM – Hardware Security Module

Software Verification

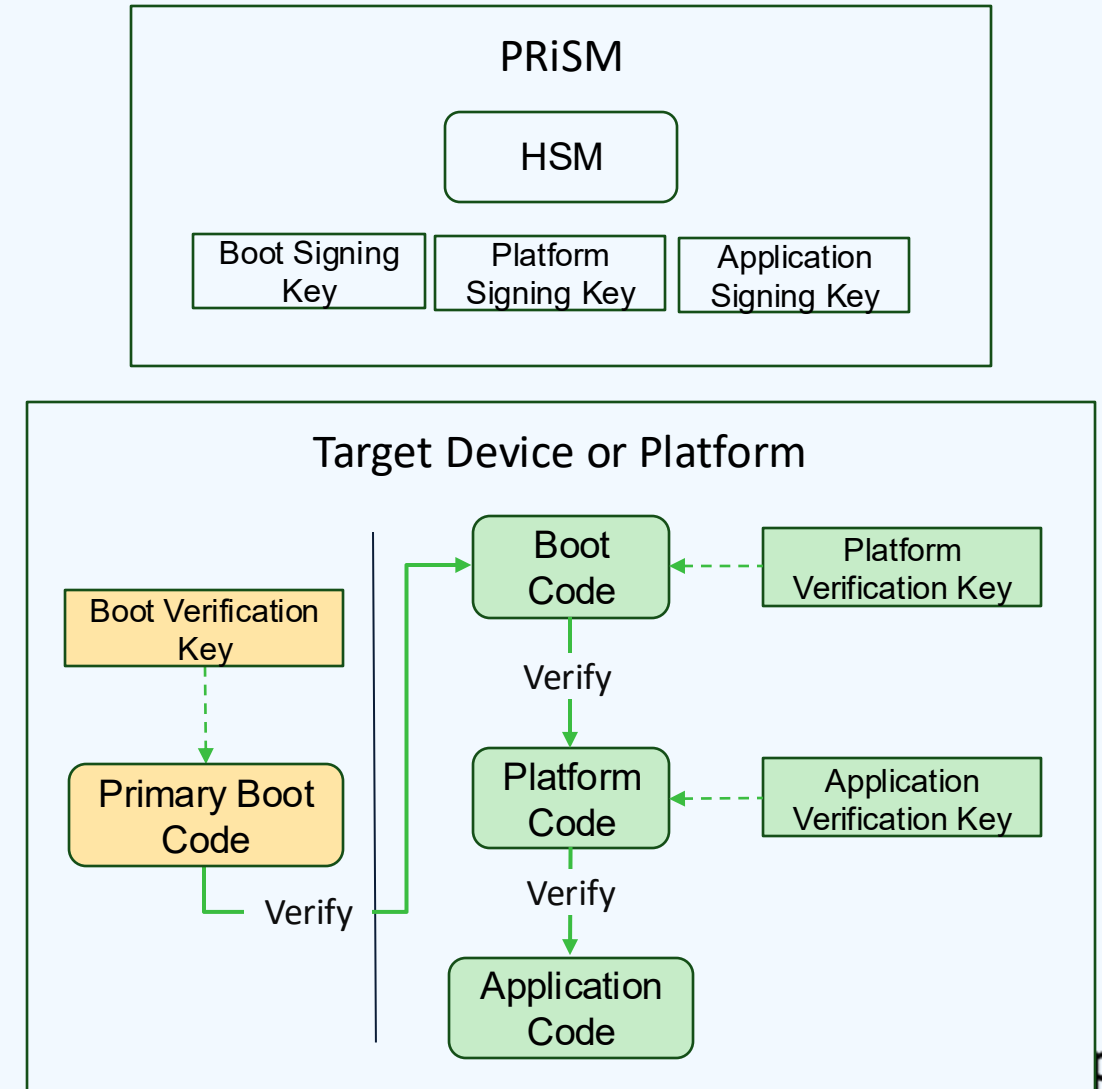
how to prevent sophisticated attackers from bypassing code authentication?

Follows a chain-of-trust model:

- Boot -> platform -> application
- Secure boot code & the root verification key are protected by **hardware**, establishing a root of trust (RoT) as the foundation.
- Later stage verification keys can vary and be updated for different reasons

Employs isolated execution environments to separate secure & non-secure operations.

Supports mechanisms for rollback protection, and anti-tampering measures.



Key Protection Gap in Vendor Secure Boot Solutions



Chip vendors often provide secure boot reference code with specifications but leave the responsibility of protecting software signing keys to device makers.

The reference code typically uses **software-based key** storage, which can be vulnerable if device makers do not implement robust key protection measures.



CommScope's extensive experience in implementing bootloader signing **with HSM-protected keys** for a wide range of chip vendors:

STMicroelectronics, Texas Instruments, Broadcom, Qualcomm, HiSilicon, Xilinx, MaxLinear, MediaTek, and Intel.

Signing Key Management

Signing key creation:

- All signing keys are generated centrally by the Certificate Authority (CA), not by individual signers.
- Signing keys are created through a multi-party controlled key ceremony.

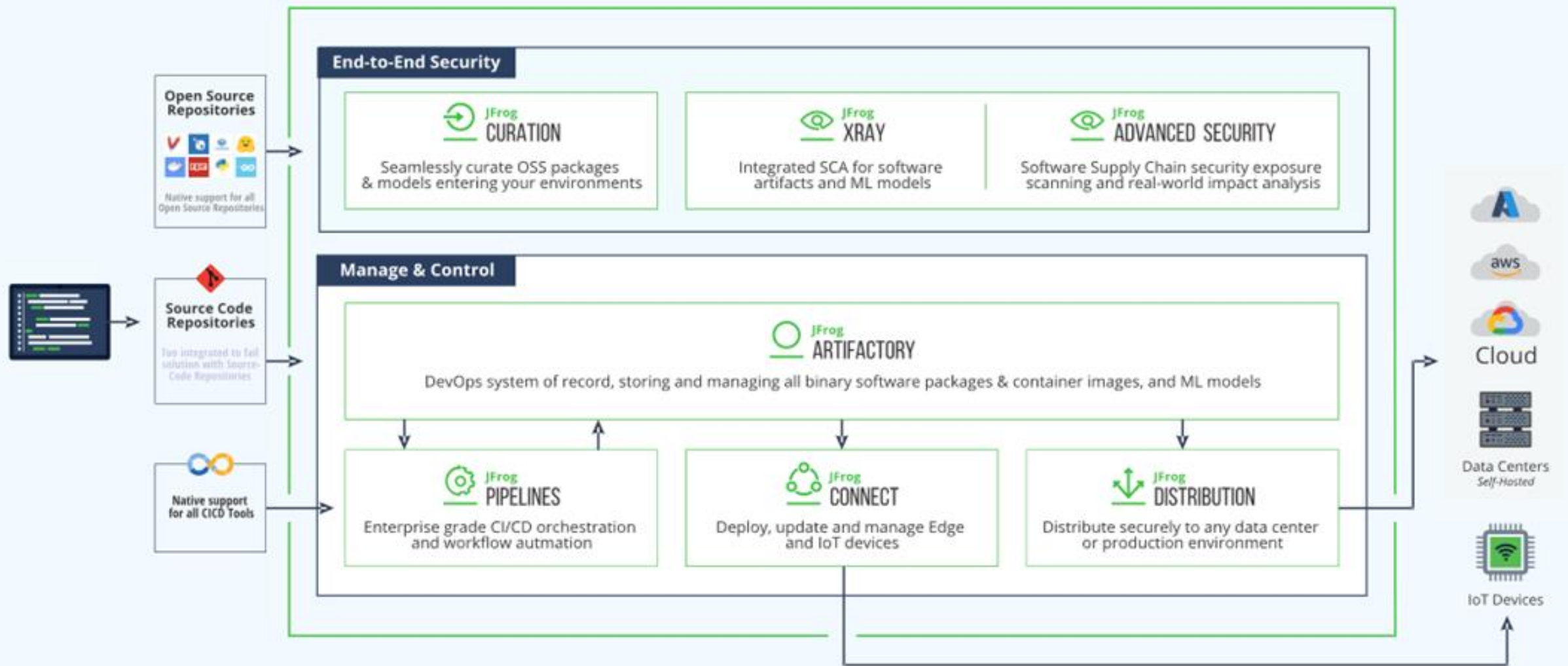
Signing key in operations:

- All signing keys are deployed to FIPS 140-2 compliant Hardware Security Modules (HSMs) hosted in PRiSM.
- Access to the backups of all signing keys is required by Two-Party Integrity (TPI) and is restricted to a list of trusted personnel

Signing key access permission:

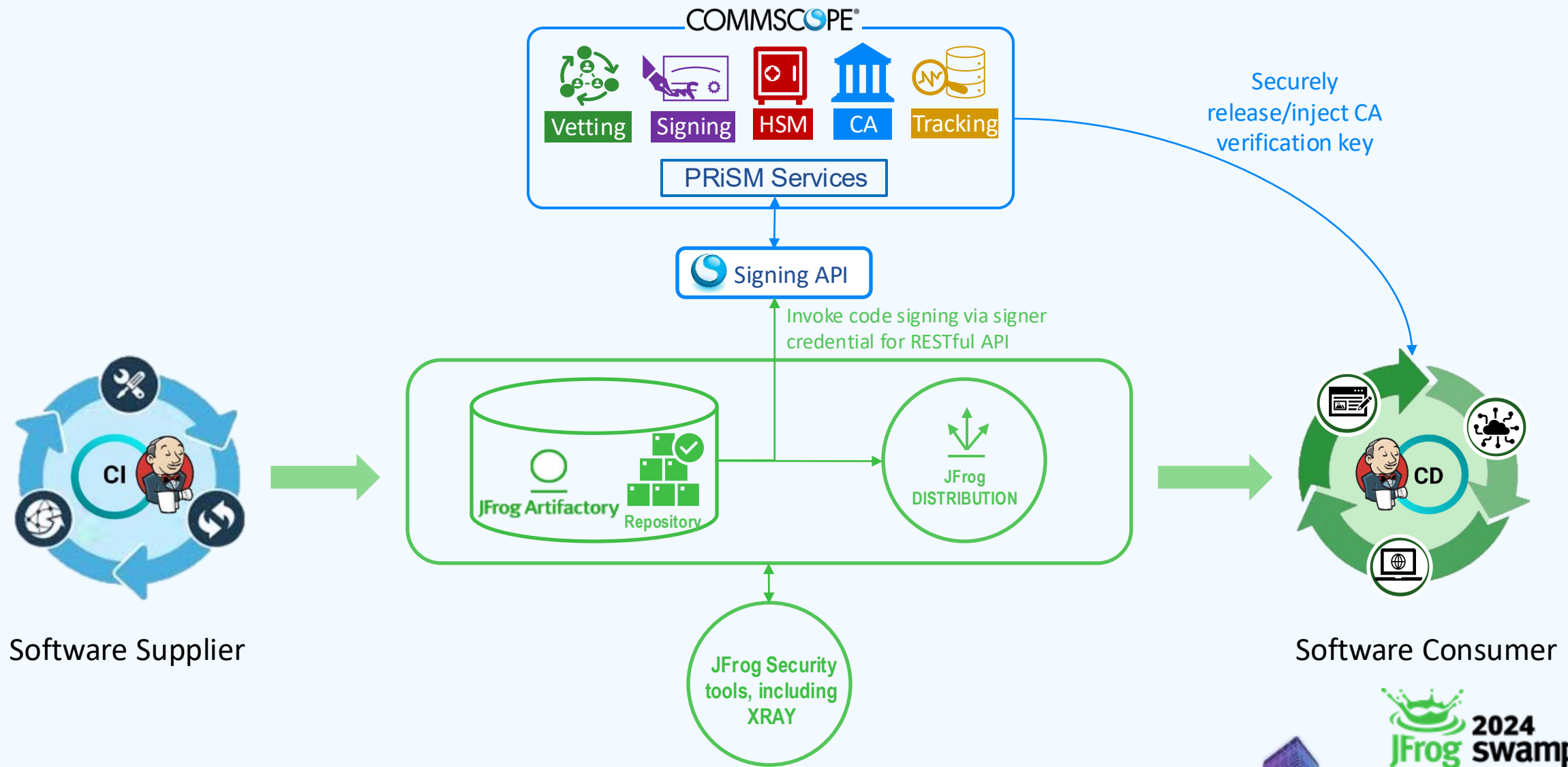
- All signing keys are associated with an enterprise, product family, and/or specific application as part of the signing configuration.
- Each code signer is assigned permissions to access one or more signing keys and configurations
- Every access and use of a signing key by a signer is logged to ensure non-repudiation.

The JFrog Platform



Source: <https://jfrog.com/platform/>

JFrog and CommScope Integrated Solution



A trustworthiness-centric software supply
chain security solution offered by



Integrated CommScope PRISM Signing with JFrog Software Supply Chain Platform in Jenkins Pipeline

How This Solution Helps JFrog's Customers

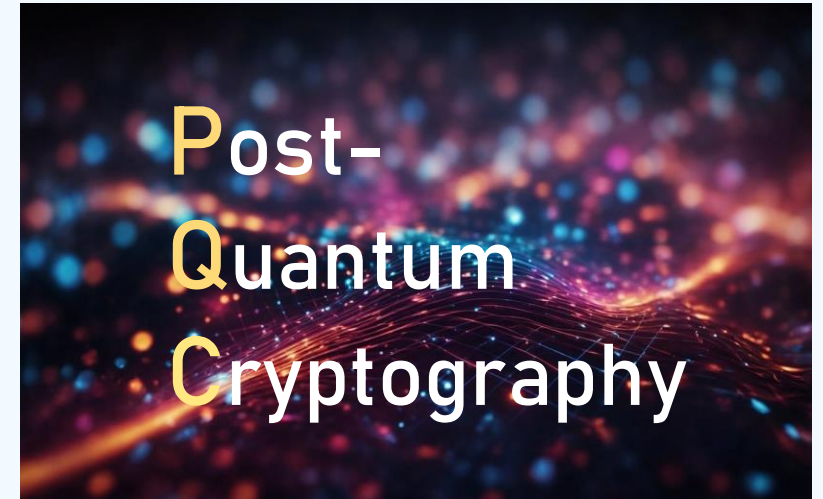
- Protect your SSC from unauthorized access to signing keys and avoid irreversible security risks.
- Enable robust security measures without significant investment in technical expertise or infrastructure to meet industry standards and regulations.
- Access a pre-integrated solution that simplifies implementation, reducing your development efforts.

Let us handle the complexity and cost, while you benefit from simplicity, productivity, and enhanced security.

Forward Looking: Post-Quantum Cryptography (PQC)

An Upcoming Major Security Event

- With quantum computers, current public-key algorithms for code signing, like RSA and ECDSA, face significant vulnerabilities.
- Similar to Y2K, the impending "Y2Q" crisis is projected to occur between 2030 and 2035.
- Risk is now: "Harvest" encrypted data today, decrypt it after "Q-Day"
- NIST released the first set of PQC standards in August 2024.



As a first step, code-signing software itself needs to be migrated to PQC.

Forward Looking: PQC-based Code Signing



CommScope PKI Center

Scalable, Secure, Robust
PKI infrastructure in
production for 25+
years

Extensive experience
and expertise,
combating real-world
cyber threats



PQC Based Code Signing

Close collaborations
with chip and HSM
vendors implementing
PQC-based code
signing and encryption
solutions

**PQC-based code
signing is expected by
Q4 2024**



PQC Credential Provisioning

Both Factory and in-
field provisioning of
device credentials for
OEMs/ODMs and
service providers

**PQC-based device
credential
provisioning is
expected by Q1 2025**

Conclusions

Ensuring the trustworthiness of software is pivotal in software supply chain security.

The increased number of sophisticated attacks on SSC, both internal and external, demand rigorous and proactive approaches to security. Code signing is one such approach.

Code signing is not just about the signing action. It's crucial to protect both the signing and verification keys, as well as to trace all actions with supporting evidence.

A versatile code-signing solution allows seamlessly integration into various IDEs, source code repositories, CI/CD pipelines, and other components of SSC.

The integrated code-signing solution by CommScope and JFrog is rigorous yet easy-to-use, enabling companies to build better and more secure products.



Resources

<https://www.pki-center.com/partner/JFrog>

<https://pki-center.com>

[Xin \(Shing\) Qiu LinkedIn](#)

