JFrog 2024 swampUP

Trustworthiness-centric Software Supply Chain Security

Regulations, Requirements & Solutions

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

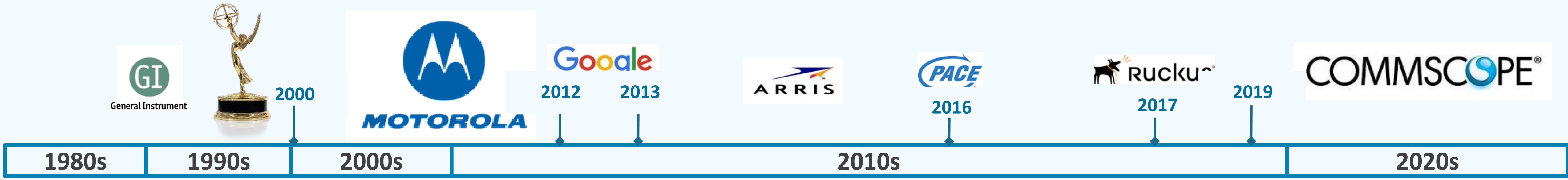
COMMSCOPE®

About CommScope

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

Sr. Director at CommScope PKI Center & Security Solutions:

I lead a diverse team in R&D, security operations, and product marketing, 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

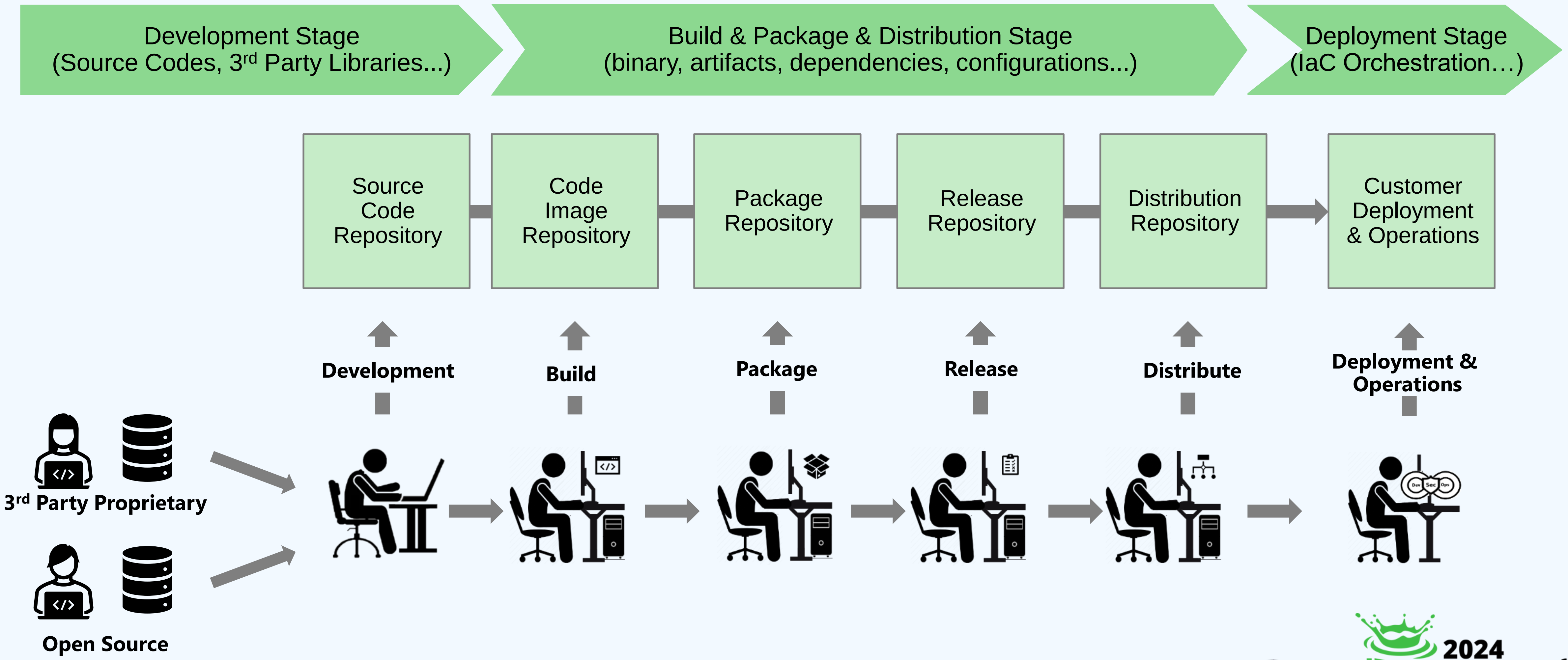
CommScope Solution for SSC Security

Collaborative Solutions from JFrog and CommScope (demo)

Forward Looking: Post-Quantum Code Signing

Conclusions

Software Supply Chain (SSC)



Development Stage
(Source Codes, 3rd Party Libraries...)

Build & Package & Distribution Stage
(binary, artifacts, dependencies, configurations...)

Deployment Stage
(IaC Orchestration…)

Source Code Repository

Code Image Repository

Package Repository

Release Repository

Distribution Repository

Customer Deployment & Operations

Development

Build

Package

Release

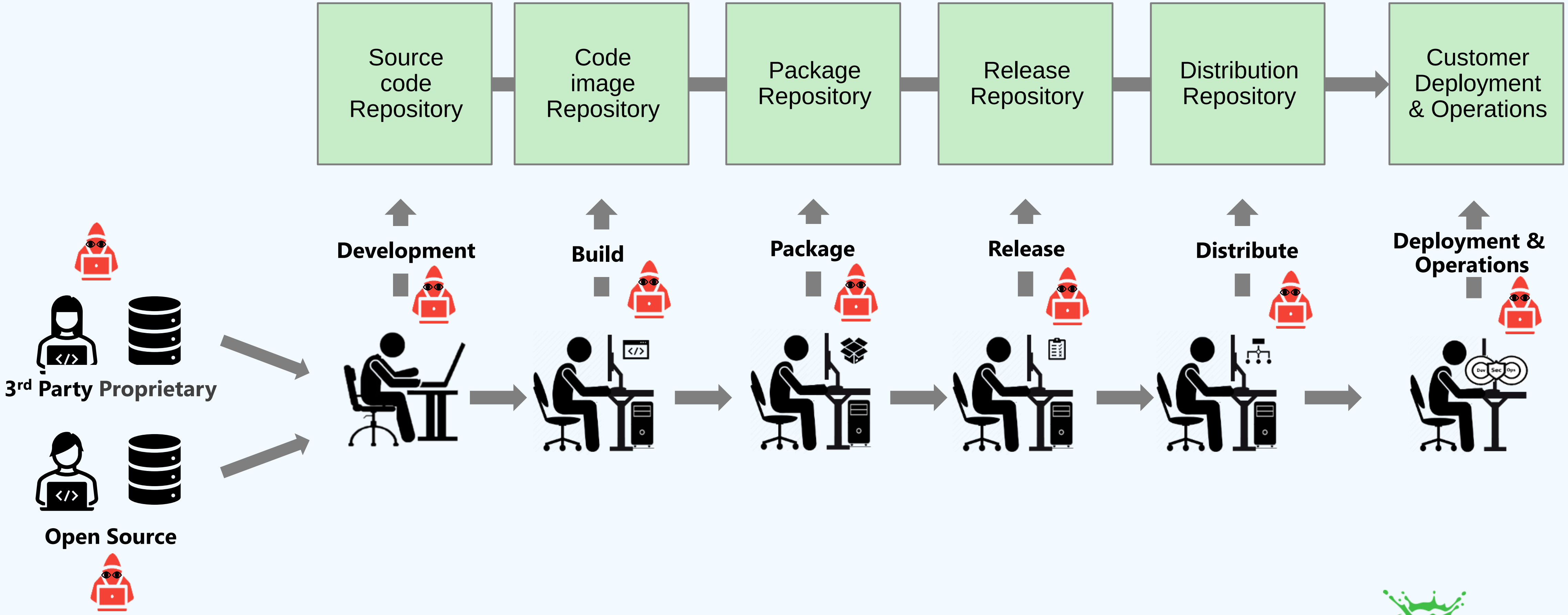
Distribute

Deployment & Operations

3rd Party Proprietary

Open Source

Typical Threats in Software Supply Chain



Code Tampering

Key Compromise

Malicious Injection

JFrog 2024 swampUP

Emerging Government Regulations

United States
NIST National Institute of Standards and Technology U.S. Department of Commerce
CISA
NTIA
Communications Security Establishment
Canadian Centre for Cyber Security
Canada
Council of the European Union
European Union
National Cyber Security Centre
United Kingdom
ASD Australian Signals Directorate
ACSC
Australia
National Cyber Security Centre
New Zealand
National Cyber Security Centre Ministry of Justice and Security
Netherlands
NSM Norwegian National Cyber Security Centre
Norwegian
BSI
Germany
NISC
内閣サイバーセキュリティセンター
Japan
KISA Korea Internet & Security Agency
South Korea
CSA Singapore
Singapore

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 Consortiums and Initiatives

industrial internet CONSORTIUM

Software Trustworthiness Best Practices

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

SLSA

Safeguarding artifact integrity across any software supply chain

SLSA • Supply-chain Levels for Software Artifacts

TrustedFirmware

Trusted Services

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

PKI Consortium Best Practices for Code Signing

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

CISQ

Consortium for Information & Software Quality™

SOFTWARE QUALITY STANDARDS – ISO 5055

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

OpenSSF

OPEN SOURCE SECURITY FOUNDATION

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/

TRUSTED® COMPUTING GROUP

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

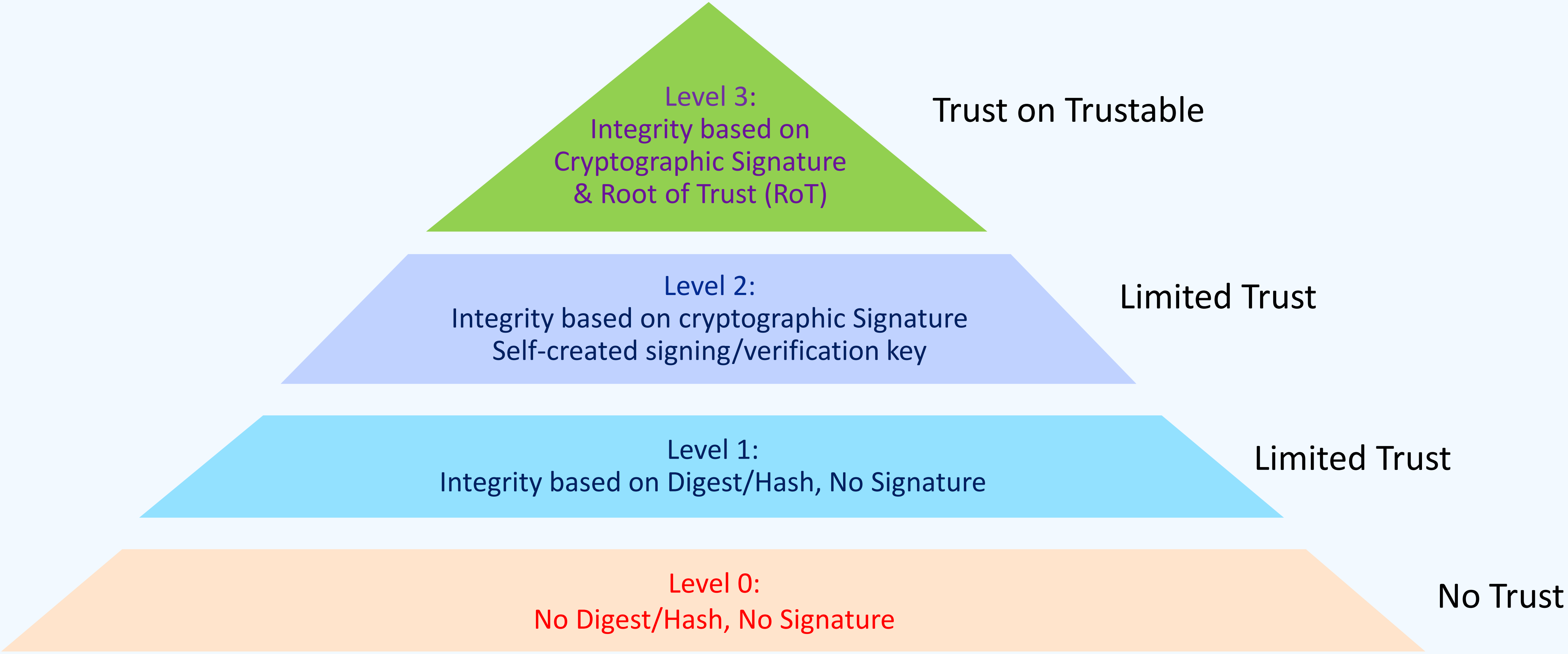
Software Operation

- 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



Level 3:
Integrity based on
Cryptographic Signature
& Root of Trust (RoT)

Trust on Trustable

Level 2:
Integrity based on cryptographic Signature
Self-created signing/verification key

Limited Trust

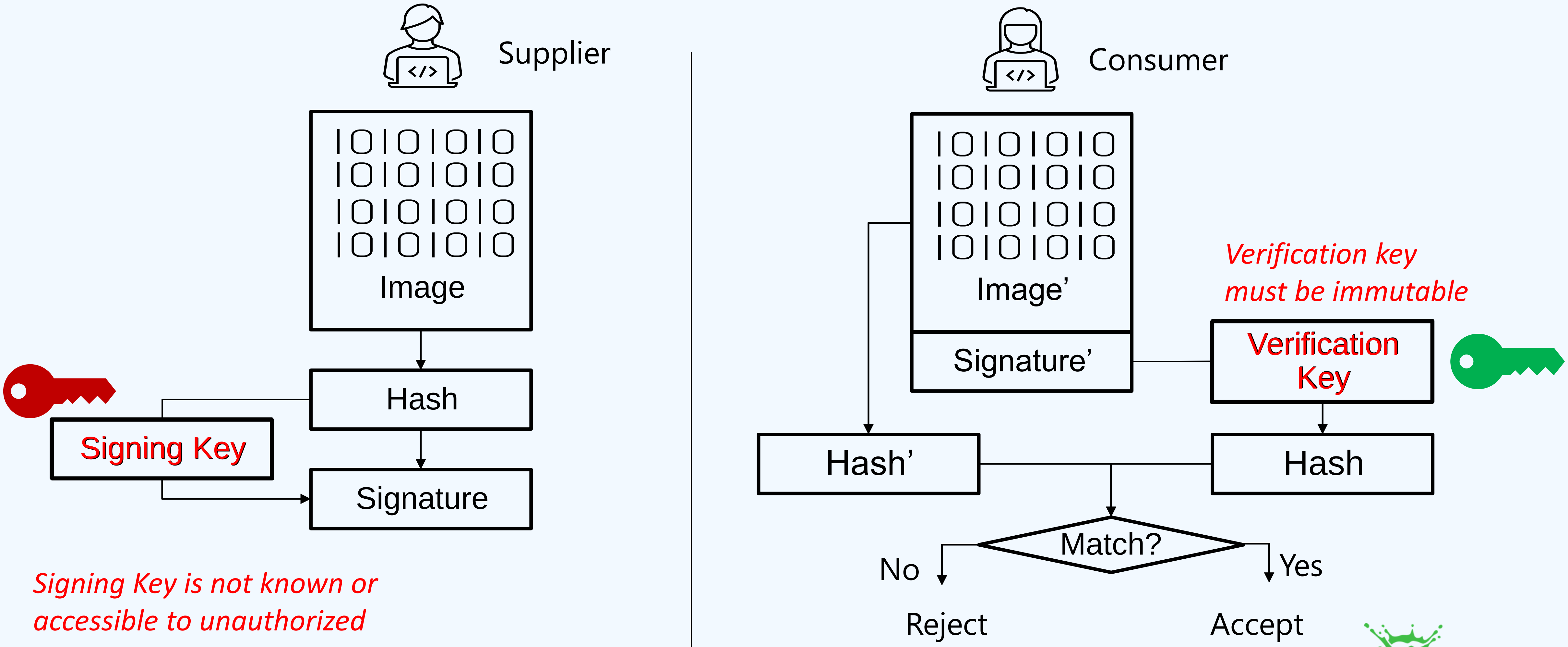
Level 1:
Integrity based on Digest/Hash, No Signature

Limited Trust

Level 0:
No Digest/Hash, No Signature

No Trust

Basics: Software Integrity via Code Signing



Supplier

10101010
10101010
10101010
10101010
Image

Hash

Signing Key

Signature

Consumer

10101010
10101010
10101010
10101010
Image’

Signature’

Verification Key

Hash’

Hash

Match?

No

Yes

Reject

Accept

Verification key must be immutable

Signing Key is not known or accessible to unauthorized parties

Ensuring Trustworthiness in Code Signing

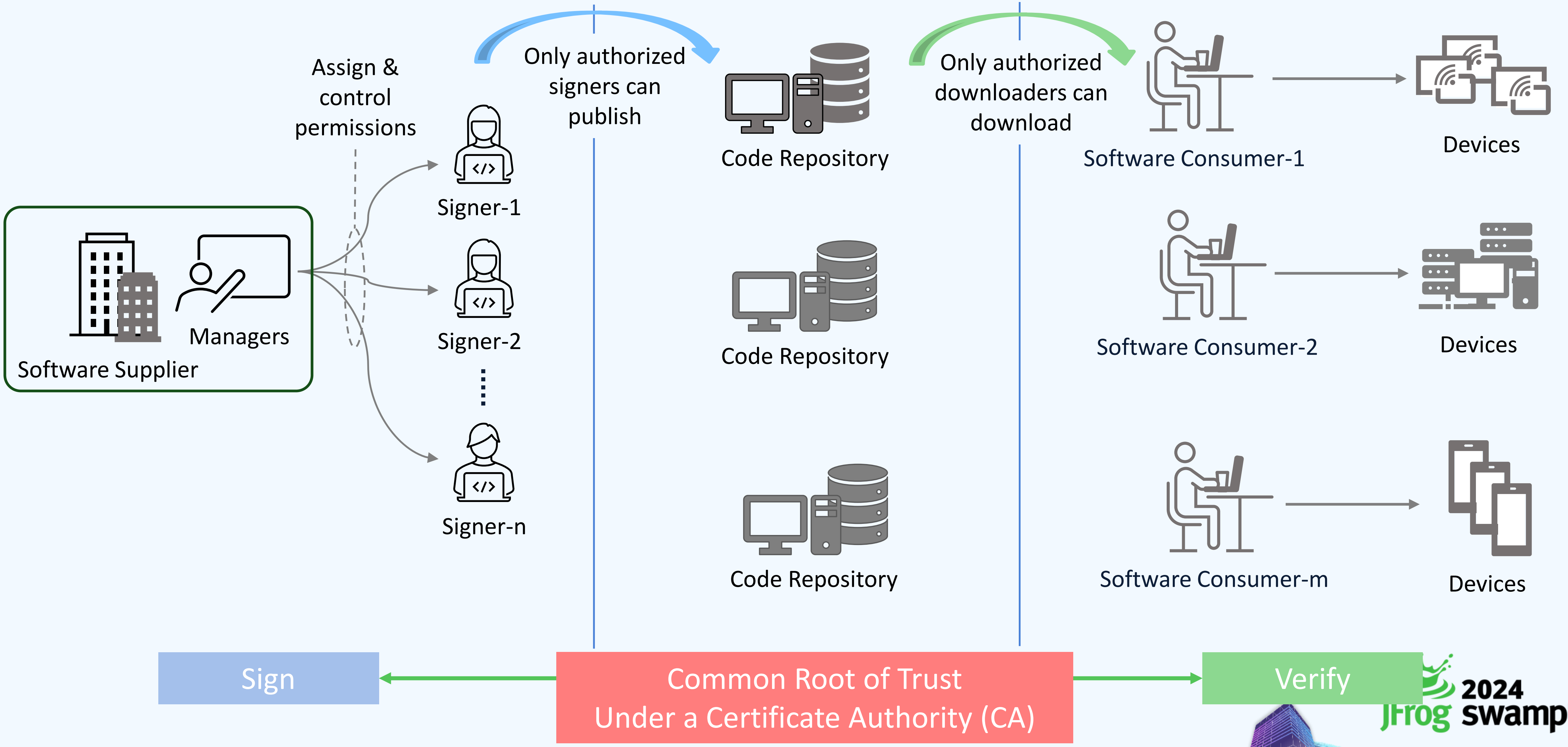
Signing and Verifications Keys

- 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

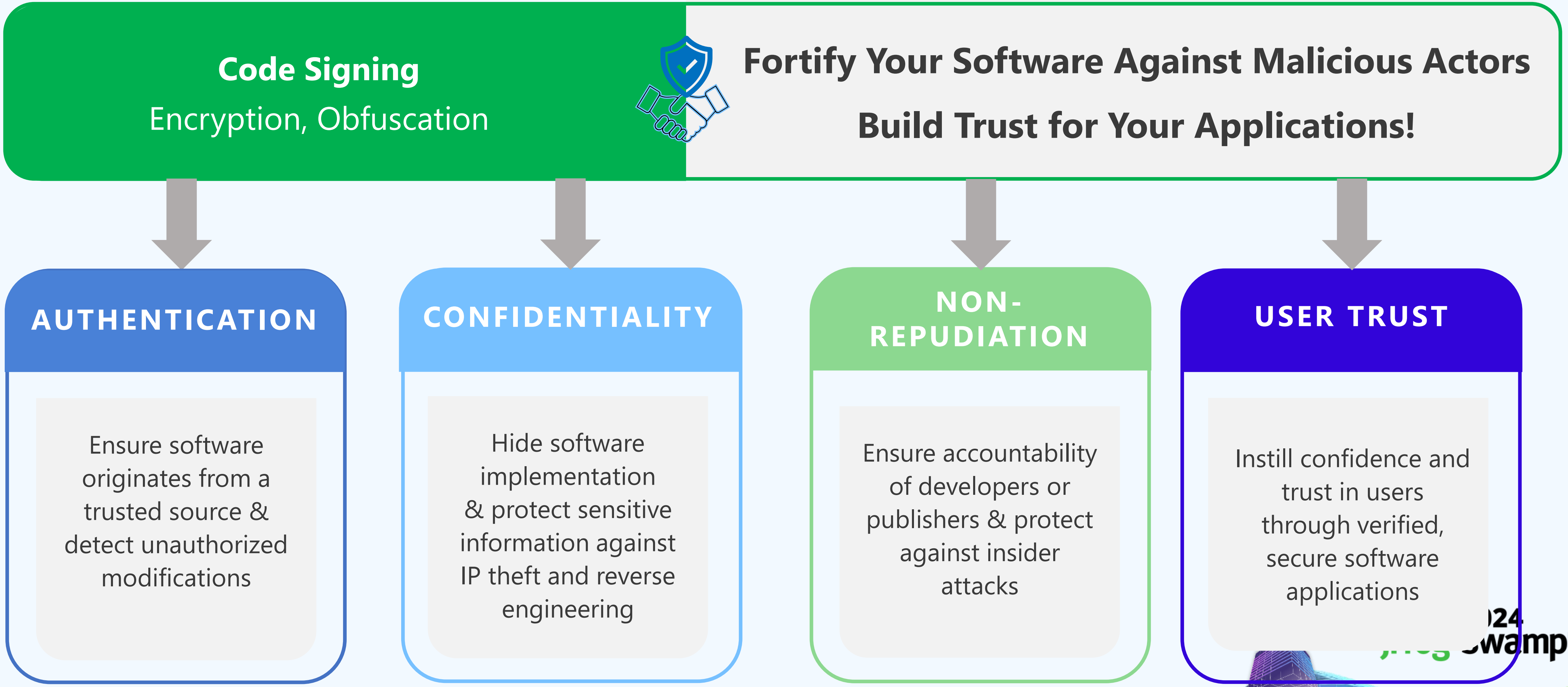
- Lack of signer verification diminishes confidence in the integrity of the code
- Absence of signer activity tracking hinders accountability, undermining trust and the integrity of the signing process

A Trust Framework for Code Signing in SSC



CommScope's Code Signing Platform

CommScope's Solution: PRiSM (*P*ermission *Ri*ghts *S*igning *M*anager)



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

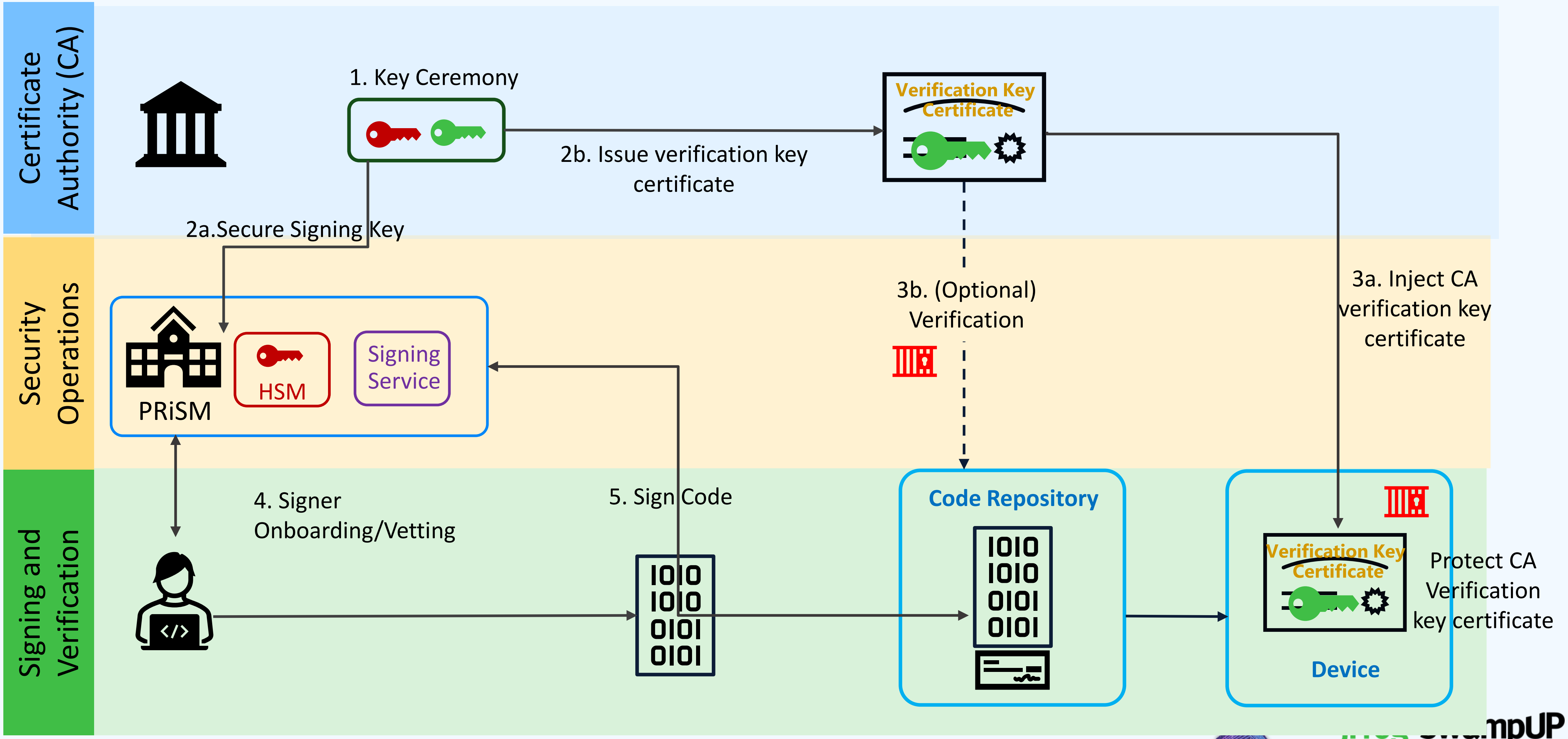
NON-REPUDIATION

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


Certificate Authority (CA)
Security Operations
Signing and Verification
1. Key Ceremony
2b. Issue verification key certificate
Verification Key Certificate
2a.Secure Signing Key
3b. (Optional) Verification
3a. Inject CA verification key certificate
PRiSM
HSM
Signing Service
4. Signer Onboarding/Vetting
5. Sign Code
1010
1010
0101
0101
Code Repository
1010
1010
0101
0101
Verification Key Certificate
Protect CA Verification key certificate
Device

Term: HSM – Hardware Security Module

Software Verification

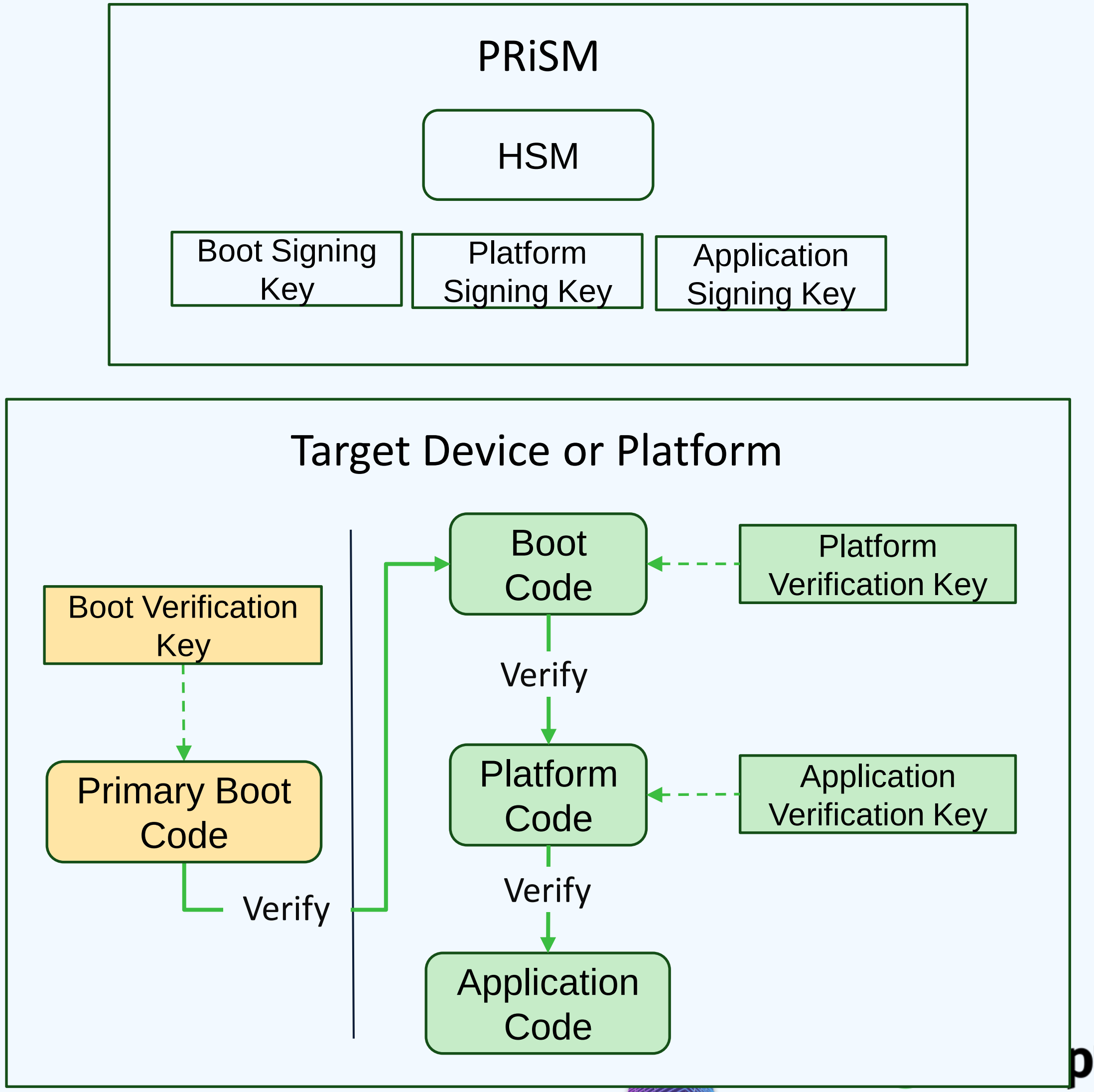
how to prevent sophisticated attackers from bypassing code authentication?

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.

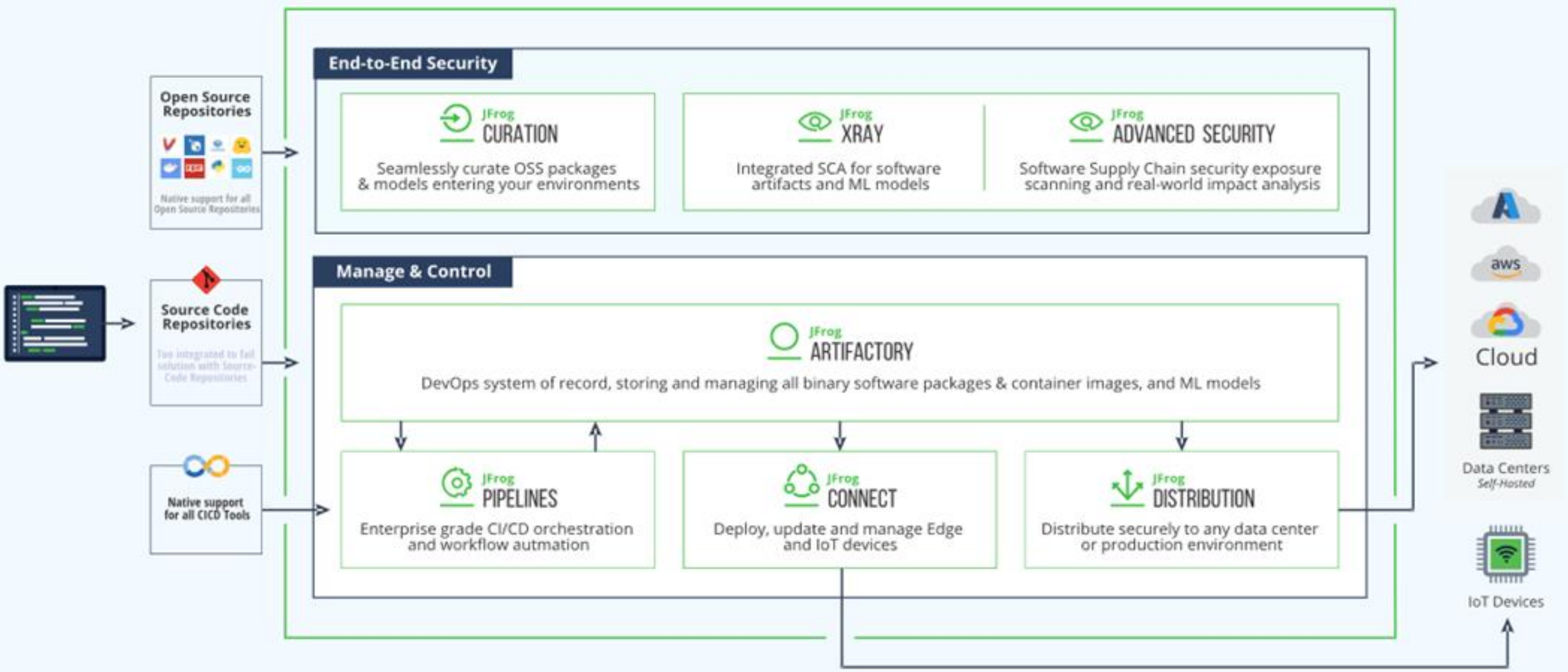
Signing key in operations:

- 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



Open Source Repositories

Native support for all Open Source Repositories

Source Code Repositories

Too integrated to fail solution with Source-Code Repositories

Native support for all CICD Tools

End-to-End Security

JFrog CURATION

Seamlessly curate OSS packages & models entering your environments

JFrog XRAY

Integrated SCA for software artifacts and ML models

JFrog ADVANCED SECURITY

Software Supply Chain security exposure scanning and real-world impact analysis

Manage & Control

JFrog ARTIFACTORY

DevOps system of record, storing and managing all binary software packages & container images, and ML models

JFrog PIPELINES

Enterprise grade CI/CD orchestration and workflow autmation

JFrog CONNECT

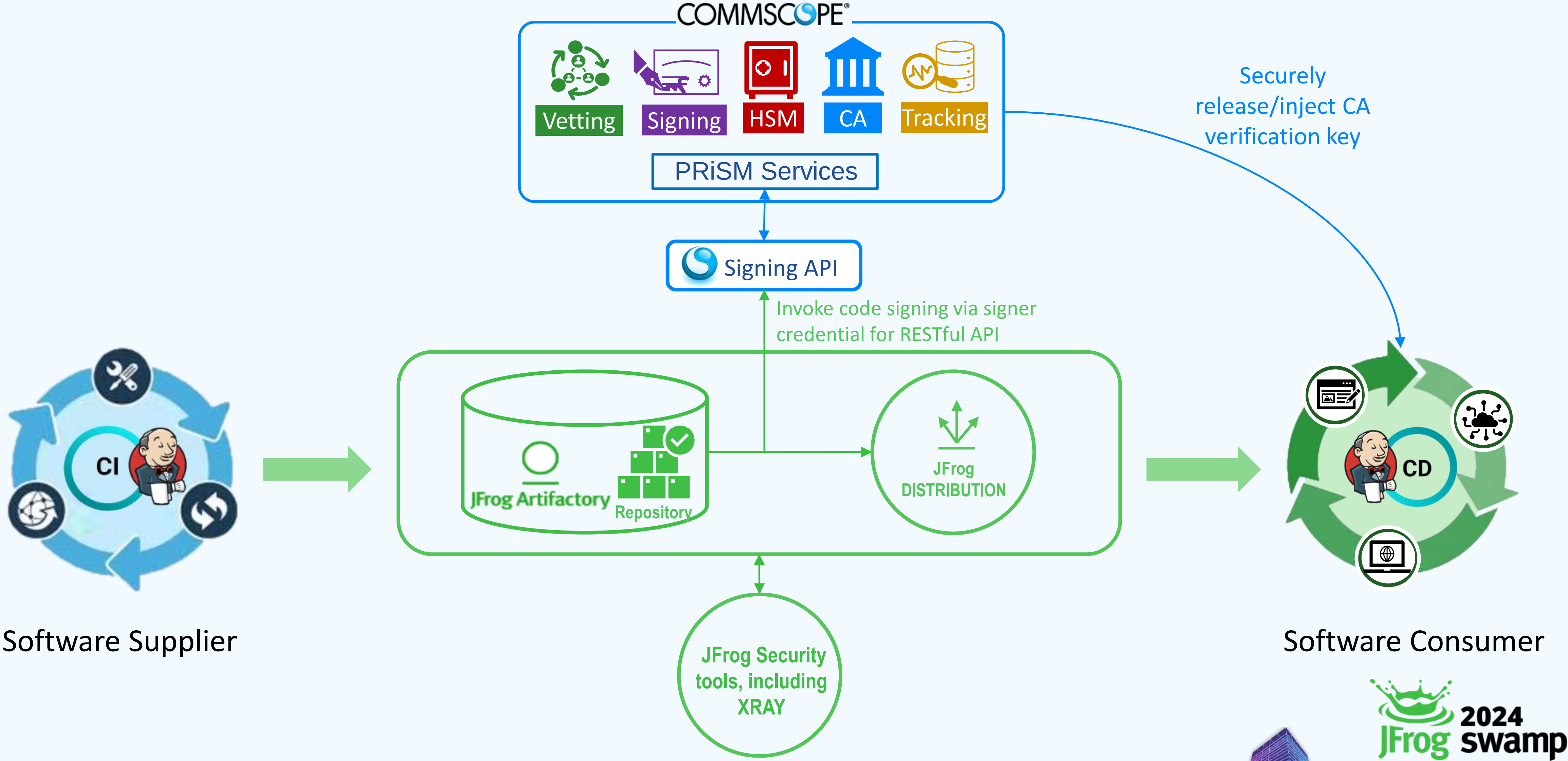
Deploy, update and manage Edge and IoT devices

JFrog DISTRIBUTION

Distribute securely to any data center or production environment

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

JFrog and CommScope Integrated Solution



How This Solution Helps JFrog's Customers

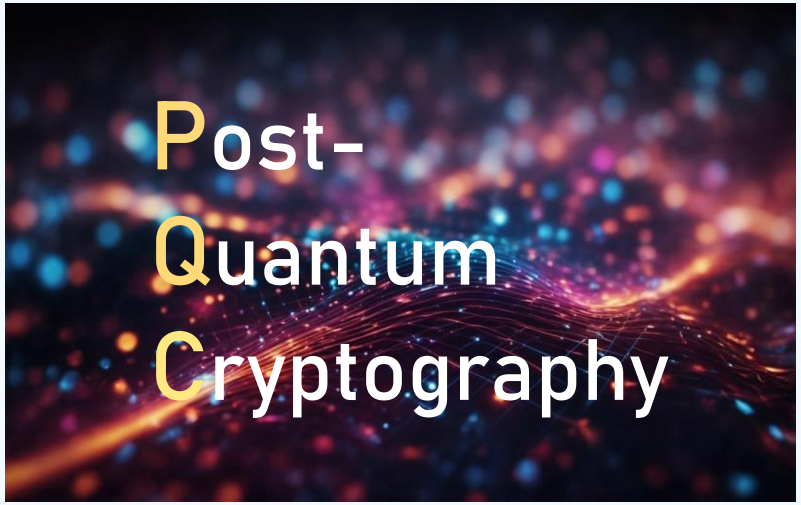
- Protect your SSC from unauthorized access to signing keys and avoid irreversible security risks.
- Enable robust security measures without significant investment in technical expertise or infrastructure to meet industry standards and regulations.
- Access a pre-integrated solution that simplifies implementation,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

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