Software Signing in the Quantum Age

Keyfactor Tech Days 2023

Antonio Vaira – Siemens AG

SIEMENS

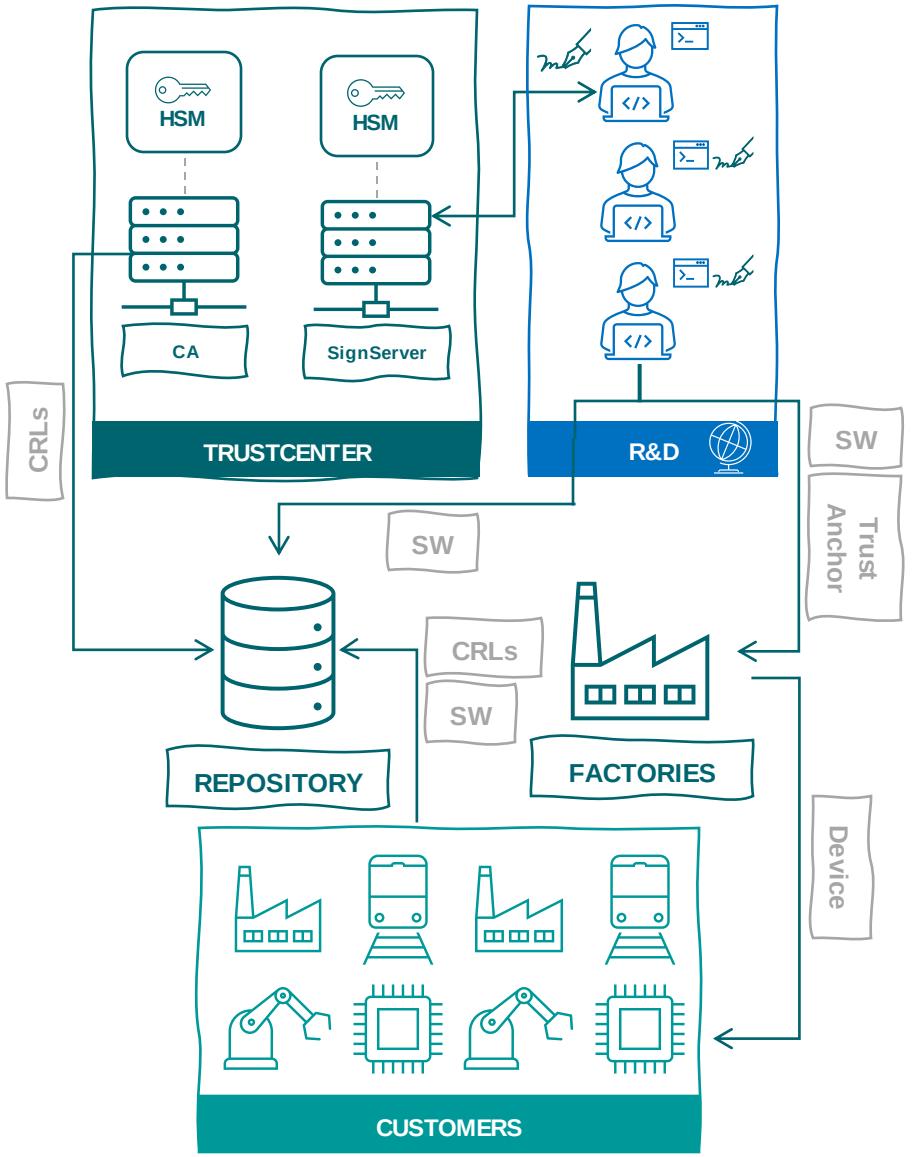
Table of contents
Agenda

- Use Case Definition: Software Signing
- Upcoming Challenges with Software Signing
- Modified Solution: Post-Quantum Software Signing
- PoC with Keyfactor
- Required Next Steps

SIEMENS

Use Case Definition: Software Signing

- Signing of software artifacts ensures their **authenticity**.
- Several types of software signature types can be supported, e.g., plain **signatures**, CMS, etc., in accordance with OEM requirements.
- A centralized software signing service moves security and compliance **burdens** away from R&D:
  - consistent use of HSMs,
  - secure backup/restore mechanism,
  - disaster recovery strategies.

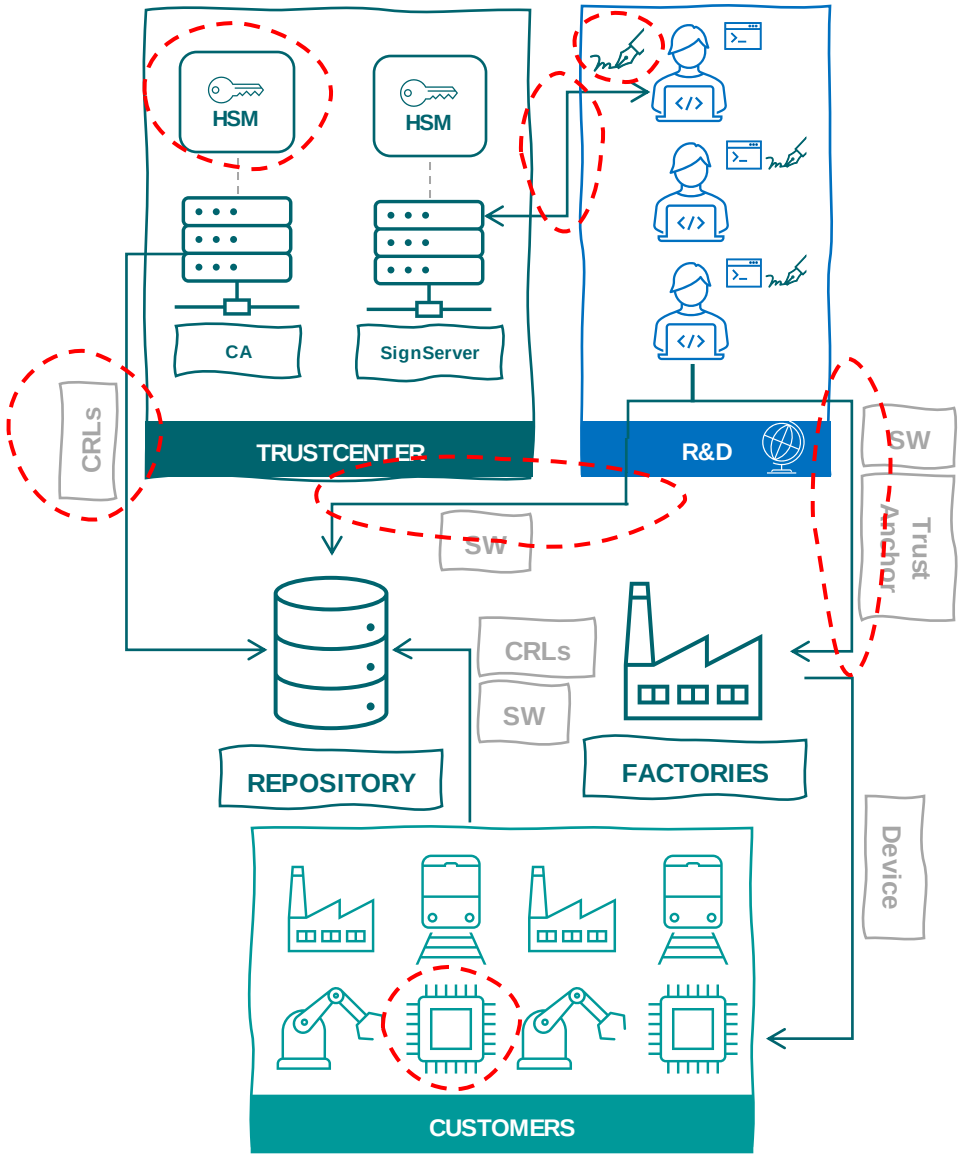


CMS: Cryptographic Message Syntax (RFC5652)
OEM: Original Equipment Manufacturer
HSM: Hardware Security Module

SIEMENS

Upcoming Challenges with Software Signing

- Quantum computers will make RSA/ECC **obsolete**.
- Post-quantum cryptography (PQC) will have to progressively **replace** RSA/ECC in the entire technology stack: coordinated effort.
- In the industrial world we need to migrate **soon** due to long lived security requirements of software in products and difficulty to replace trust anchors.
- Authorities, and customers, are starting to set the **pace** for migration: NSA provides a migration timelines for NSS in CNSA 2.0.

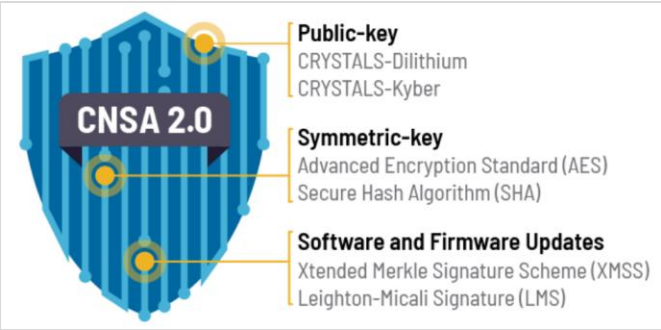


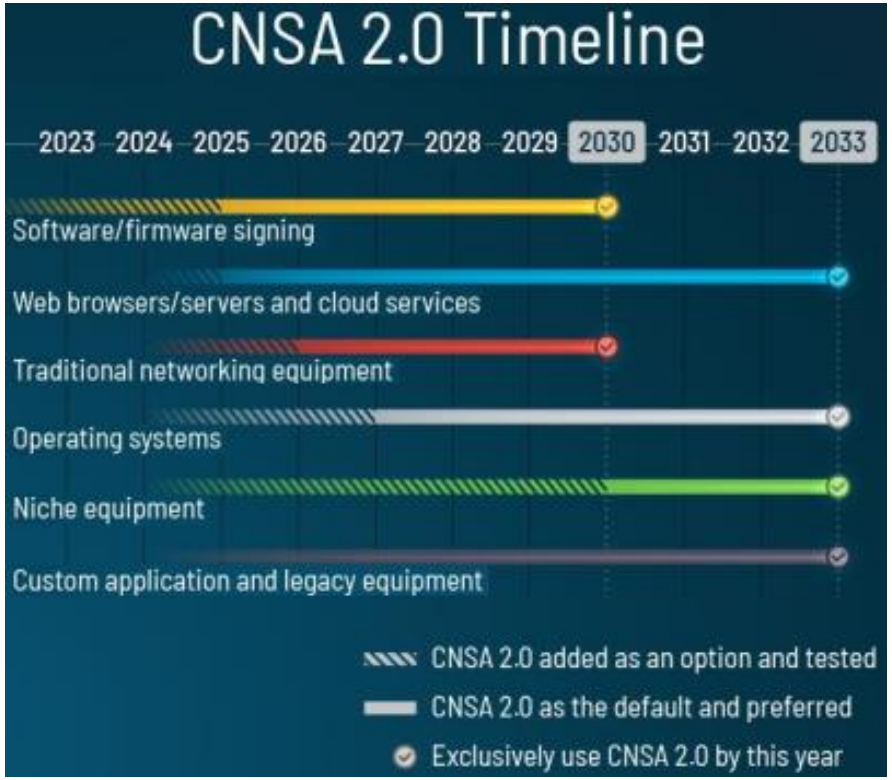
ECC: Elliptic-Curve Cryptography
NSA: National Security Agency
CNSA: Commercial National Security Algorithm Suite 2.0

SIEMENS

Modified Solution: Post-Quantum Software Signing

- Being **crypto-agile** and migrating to stronger cryptography, i.e., post-quantum cryptography.
- Post-quantum digital signature algorithms, from **NIST 3rd round** standardization are slightly more difficult to use than traditional ones.
- **Stateful** "Hash Based Signature" schemes are much more difficult to operate securely. They are preferred in CNSA 2.0 for **SW/FW signing.**
- CNSA 2.0 is the first concreate example but we should expect more to come.





NIST: National Institute of Standards and Technology
SW/FW: software/firmware
CNSA: Commercial National Security Algorithm Suite 2.0

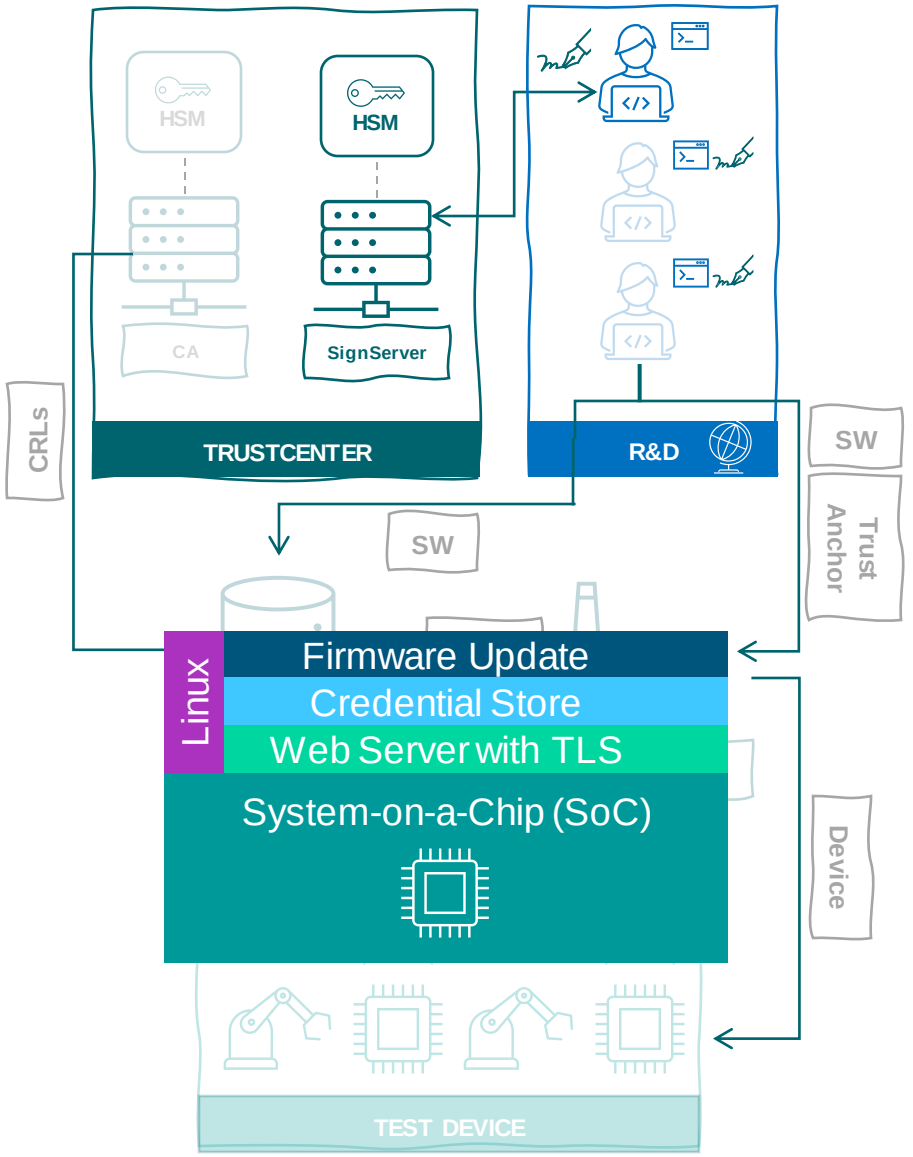
SIEMENS

PoC with Keyfactor

- In a funded project, called AQUORYPT, we did the following on a **test device**:
  - Sign a software update, with post-quantum crypto libraries and trust anchor,
  - Update the device to post-quantum crypto,
  - Deliver post-quantum signed updates.

- Now we focus on the **SignServer** to support software signing with post-quantum cryptography: SPHINCS+ first, and after with Dilithium and Falcon.

- Software updates may be signed with a traditional and a post-quantum signature in the **same CMS**.



Aquorypt: https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/aquorypt
BMBF-FKZ. : 16KIS1021

SIEMENS

Required Next Steps

- Continuation and extension of the **proof-of-concept** on PQC support for digital signature and certificate management use cases,
- Support all **NIST 3rd round** post-quantum algorithms for issuance of certificates, including certifying KEM public keys, and signing of software artifacts,
- Support **stateful hash based signature algorithms**, like XMSS and LMS (c.f. NIST SP 800 208), for signing software artifacts and root CA certificates,
- After their standardization is finalized, support the diverse **certificates formats**, like hybrid composite and non-composite as discussed in IETF and specified in ITU-T,
- Provide guidance on how to **migrate** and securely **operate** Keyfactor products.

IETF: Internet Engineering Task Force
ITU: International Telecommunication Union
ITU-T: ITU Telecommunication Standardization Sector (ITU-T)

Contacts

Siemens AG

Antonio Vaira

Cybersecurity Expert - PKI

T CST SEA
Otto Hahn Ring 6
81739 Munich
Germany

E-mail:
antonio.vaira(at)siemens.com

SIEMENS