TeleTrusT-EBCA "PKI-Workshop" 2024

Berlin, 10.10.2024

"Einführung von Code-Signing-Lösung bei einem Vorreiter für Automationstechnik"

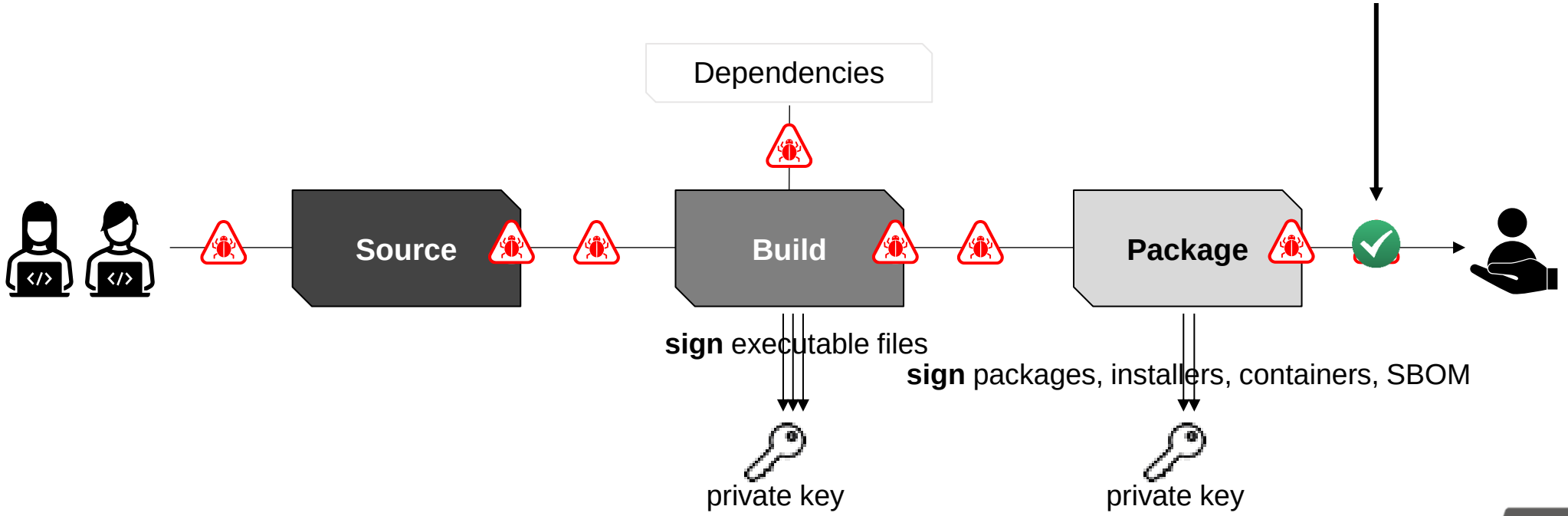
SignPath und NTT DATA Deutschland

Stefan Wenig, SignPath

Code Signing: authenticity and integrity

Authenticity: who published (signed) the code?
Integrity: was it modified after signing

If only the publisher has access to the private key



Code signing does not guarantee process integrity!

Source: slsa.dev

Hardware Security Modules

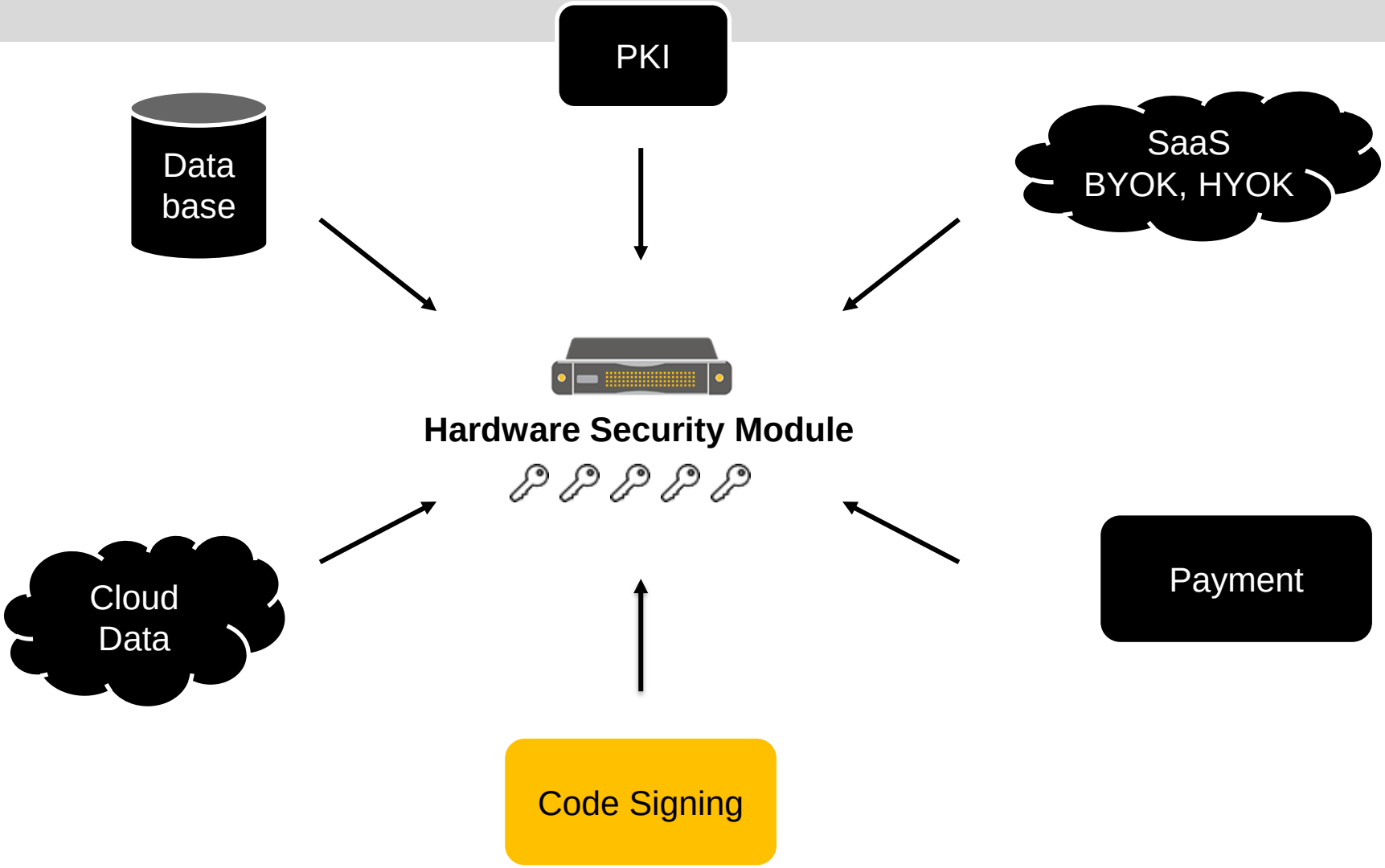
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Certified hardware
- **FIPS 140-2**
- **Common Criteria**

Lifetime security
for **secret keys**

Keys never
leave the HSM

Signing and
decryption
performed **by HSM**



What the HSM sees … and doesn't see

Developers

CI/CD build pipelines

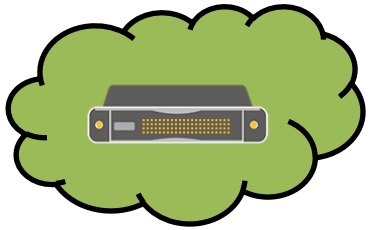
Build scripts

Dev tools

hash digest
8F58 2B0F 1CAE F03D …

password/token
****

signature block
E7BA F358 B20C AFE0 …



Code Signing Gateway

HSM

Platform-native Software Validation

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

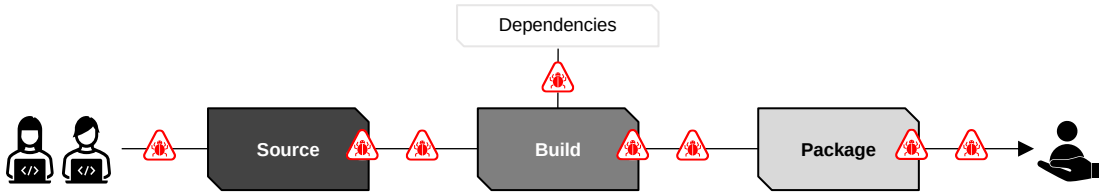
Platform	Standard Software	OSS	Components	Internal, Contractors
Windows	MS Update, MS Store, signing		signing?	
macOS, iOS	Apple Store, signing, notarization		signing, notarization	
Android	Play Store		?	signatures
Linux	distro, package repos		hash code? GPG signing?	
Containers	DCT, Notary, Cosign?		n/a	DCT, Notary, Cosign?
Java	signing (SE; EE?)		GPG signing (Maven Central)	signing?
Coding platforms	n/a	package managers, signing?		private pkg mgr? signing?
SBOMs, attestations	Cosign? CycloneDX XML/JSON signing?			
Other	scripts, config files, Helm charts, Terraform configs, Ansible playbooks …			

Different approaches

- file formats
  - generic vs. specific
  - embedded, envelope, detached
- algorithms (key, hash)
- root of trust, key distribution
  - certificate types (if any)
  - long-lived vs ephemeral
  - publisher vs. location
- online vs. offline
- content vs. metadata
- timestamping

Harden your Build Pipeline

SLSA Supply-chain Levels for Software Artifacts



Level	Requirements	Focus
L1	Produce provenance	Mistakes, documentation
L2	Hosted build platform, signing	Post-build tamper
L3	Hardened build platform	Build tamper

OWASP Top 10 CI/CD Security Risks

CICD-SEC-1	Insufficient Flow Control Mechanisms
CICD-SEC-2	Inadequate Identity and Access Management
CICD-SEC-3	Dependency Chain Abuse
CICD-SEC-4	Poisoned Pipeline Execution (PPE)
CICD-SEC-5	Insufficient PBAC (Pipeline-Based Access Controls)
CICD-SEC-6	Insufficient Credential Hygiene
CICD-SEC-7	Insecure System Configuration
CICD-SEC-8	Ungoverned Usage of 3rd Party Services
CICD-SEC-9	Improper Artifact Integrity Validation
CICD-SEC-10	Insufficient Logging and Visibility

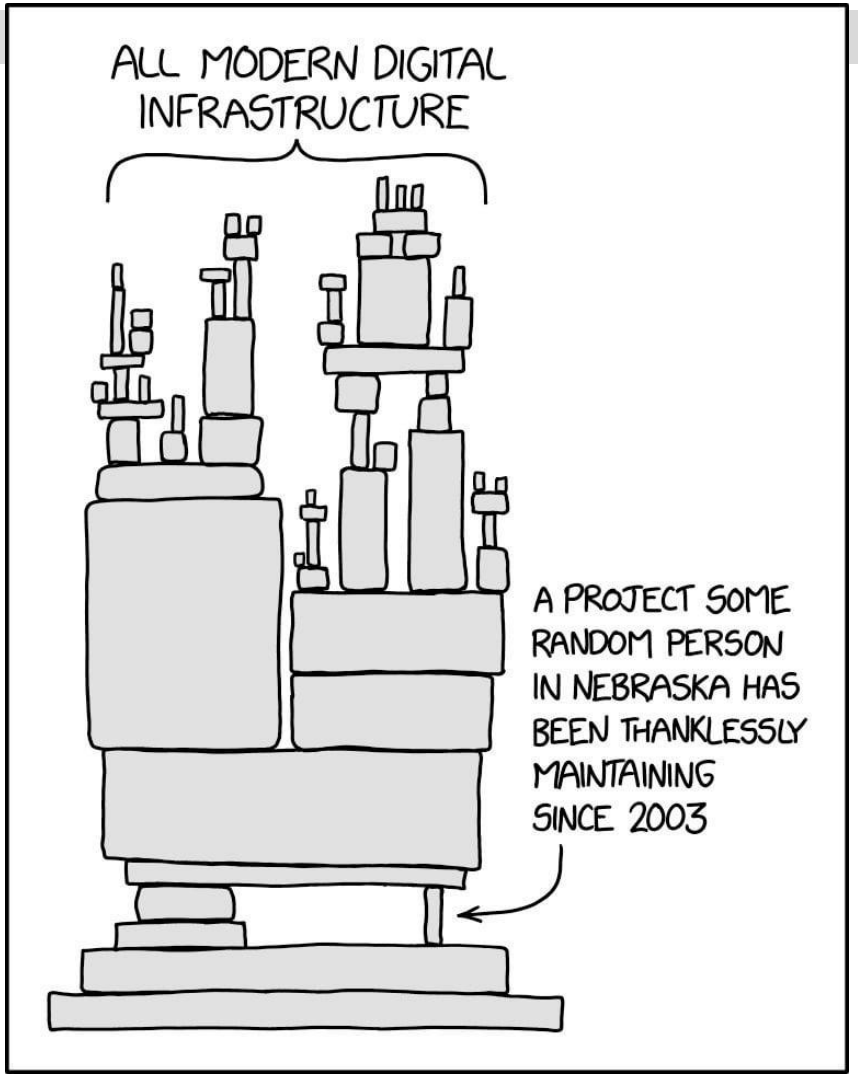
Source:
slsa.dev

Missing Control & Personal Trust Exploited
2024 XZ Utils Attack

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

OSS relies on source code reviews but **trusts individual maintainers** with **building & packaging**

- XZ Utils in many **Linux distros, macOS, embedded systems**
- **Social engineering** since 2021: bad actor achieved maintainer status
- **Attack implementation:**
  - Payload in forged binary test data
  - Not activated in GitHub source → **undetectable for reviewers**
  - Manually activated in source tarball
  - **Signed with bad maintainer's personal key**
- **Detected by Accident**



SignPath Code Integrity Platform

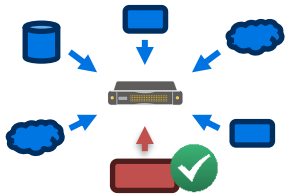
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

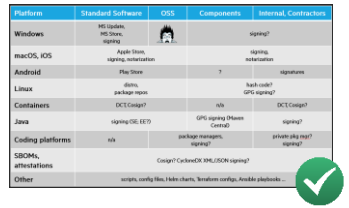
Pipeline Integrity

- **Zero-trust verification:** deep CI integration
  - Verify origin + build integrity
  - Source code and CI policies
- **Process and integration**
  - testing, approval, release candidates

Advanced Code Signing

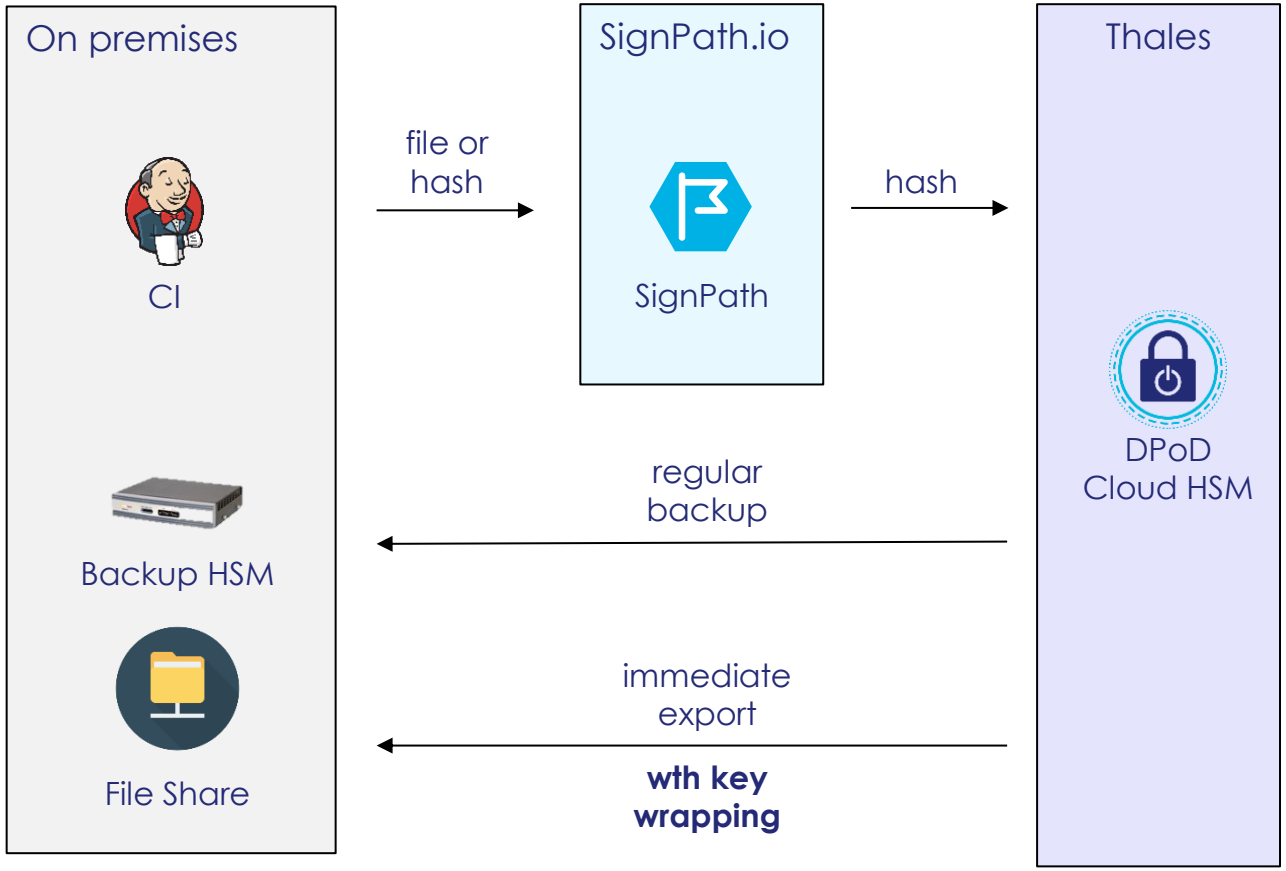
- Physical key security
- Platforms and Formats
- Package specs & constraints
- Declarative signing





Platform	Standard Software	OSS	Components	Internal, Contractors
Windows	MS Update, MS Store, signing		signing?	
macOS, iOS	Apple Store, signing, notarization		signing, notarization	
Android	Play Store		?	signatures
Linux	distro, package repos		hash code? GPG signing?	
Containers	DCT, Cosign?		n/a	DCT, Cosign?
Java	signing (SE, EE?)		GPG signing (Maven Central)	signing?
Coding platforms	n/a	package managers, signing?		private pkg repo? signing?
SBOMs, attestations	Cosign? CycloneDX XML/JSON signing?			
Other	scripts, config files, Helm charts, Terraform configs, Ansible playbooks ...			

Key custodianship and key archiving



Vielen Dank!

Stefan Wenig

SignPath GmbH
stefan.wenig@signpath.io