EVIDEN

CASE STUDY

PKI-basierte Identitäts- und Code-Signing-Infrastruktur für eine Organisation im Verteidigungsumfeld

DIE AUSGANGSSITUATION

Ein international tätiger Anbieter sicherheitskritischer System- und Softwarelösungen entwickelt und betreibt Lösungen für Einsatzumgebungen mit besonders hohem Schutzbedarf. Ziel ist es, Authentizität, Integrität und Nachvollziehbarkeit von Software und Systemkomponenten über den gesamten Lebenszyklus konsistent sicherzustellen – von der Entwicklung bis zum Betrieb.

Mit steigenden Sicherheits- und Zulassungsanforderungen sowie zunehmender Haftung für Softwareintegrität wird Code Signing damit nicht als technisches Detail, sondern als Voraussetzung für Zulassung, Betrieb und Langzeitverfügbarkeit sicherheitskritischer Systeme bewertet. In diesem Umfeld tragen OEMs und Systemhäuser die Gesamtverantwortung:

Schwächen im Code-Signing-Ansatz wirken sich unmittelbar auf Zulassung, Haftung und Einsatzfähigkeit aus – über lange Betriebszeiträume hinweg.

DIE HERAUSFORDERUNG

Die Organisation stand vor der Aufgabe, ein automatisiertes Code-Signing-System aufzubauen; die dafür erforderliche PKI-Architektur war das sicherheitskritische Fundament, um Signaturen, Identitäten und Nachweise konsistent abzusichern:

- **EINDEUTIGE** Identifikation und Authentifizierung von Personen, Komponenten und Software in sicherheitskritischen Systemen
- **END-TO-END-SCHUTZ** der Software Supply Chain durch autorisiertes Code Signing und verifizierbare Software-Integrität
- **ZUVERLÄSSIGER** Betrieb in isolierten und air-gapped Umgebungen ohne Internetzugang
- **ERFÜLLUNG** von Audit- und Revisionsanforderungen in hochregulierten Programmen
- **VERWALTUNG** mehrerer tausend Identitäten bei minimalem Administrationsaufwand
- **HOHE** Verfügbarkeit und Robustheit bei begrenzten Ressourcen (Hardware, Personal, Betrieb)
- **FLEXIBILITÄT** und Modularität für unterschiedliche Plattformen, Systemgenerationen und Einsatzszenarien
- **LANGFRISTIGE** kryptographische Sicherheit, inklusive
- **VORBEREITUNG** auf Post-Quantum-Kryptographie (PQC)

In der Analyse zeigte sich zudem, dass klassische Enterprise-PKI- oder DevOps-Ansätze häufig an den Rahmenbedingungen scheitern: Cloud-PKIs und Online-Validierung sind in vielen Programmen nicht zulässig, und die PKI muss in segmentierten, isolierten Netzen belastbar betrieben und geprüft werden.

DIE LÖSUNG

Zur Umsetzung wurden zwei voneinander getrennte PKI-Architekturen konzipiert und umgesetzt – realisiert durch Eviden Cybersecurity Products mit einem abgestimmten Portfolio aus PKI-, Signatur- und HSM-Komponenten.
Der Ansatz ist von Beginn an auch für air-gapped und hochregulierte Umgebungen ausgelegt: nativ offline-fähig, auditierbar und mit klarer Root-of-Trust-Architektur.

Die Vertrauenskette endet nicht an der Netzwerkgrenze.

01 CODE-SIGNING-PKI

Eine dedizierte PKI-Domäne bildet die Grundlage für sichere Zertifikatsprozesse und kontrollierte Signaturen, u. a. als Enabler für Zulassung und Betrieb:

- **Aufbau** einer PKI zur Verwaltung von Komponenten- und Systemidentitäten
- **Automatisiertes** Code Signing über eine zentrale Signatur-Engine (API-gestützt), geeignet für CI/CD-Integrationen
- **Offline-fähige** Signierprozesse für Umgebungen mit eingeschränkter oder fehlender Konnektivität
- **Zeitstempelung** (Timestamping) zur langfristigen Beweissicherung und Nachvollziehbarkeit von Signaturen – auch wenn Signaturzertifikate später ablaufen oder widerrufen werden
- **Klare** Rollen- und Rechtekonzepte sowie revisionssichere Protokollierung der Signatur- und Zertifikatsprozesse

02 MULTI-APPLIKATIONS-PKI

Für Umgebungen ohne externe Konnektivität wurde eine modulare Multi-Applikations-PKI vorgesehen, die unter Segmentierung und Isolation zuverlässig funktioniert:

- **AUSLEGUNG** auf streng kontrollierte, air-gapped Szenarien, in denen Online-Mechanismen wie OCSP oder externe CRL-Verteilung nicht praktikabel sind
- **IMPLEMENTIERUNG** als geschlossenes Trust-Ökosystem mit internen Richtlinien und lebenszyklusorientierten Gültigkeitskonzepten
- **UNTERSTÜTZUNG** typischer Plattform-Use-Cases wie TLS-Absicherung, Geräte-/Komponenten-Authentisierung und weitere plattformspezifische Vertrauensfunktionen
- **BEDARFSGERECHTE** Bereitstellung eigenständiger PKI-Instanzen pro Segment/Zone – passend zu Missionsprofil und Systemkonfiguration
- **MODULAR** und skalierbar: Anpassbar an bestehende Produktlinien, herstellerübergreifend einsetzbar und übergabefähig an Betreiber und Behörden
- **TEMPLATE-BASIERTES** Ausrollen von PKI-Komponenten, abgestimmt auf die spezifischen Anforderungen der Zielplattform
- **RESSOURCENSCHONENDER** Betrieb: Schlanke, modular zuschaltbare Komponenten reduzieren Systemlast – ein Vorteil, wenn Energie und Infrastruktur in air-gapped Szenarien begrenzt sind.

Vertrauenswürdige Kommunikation muss auch ohne externe Validierungsdienste funktionieren.

03 MAXIMALE SCHLÜSSEL- UND KRYPTOSICHERHEIT

HSM + Kryptographische Agilität

Die Lösung sieht eine durchgängige Absicherung kritischer Schlüssel vor:

- **STRIKTE** Trennung der Vertrauensdomänen zwischen Code-Signing- und Multi-Applikations-PKI zur Minimierung von Angriffsflächen
- **HSM-GESTÜTZTE** Schlüsselverwaltung für Root-, CA- und TSP-Schlüssel
- **FLEXIBLE** Nutzung verschiedener Schlüsselträger für die Anwendungen, abhängig von den spezifischen Anforderungen der Zielplattform. Möglich ist etwa die Nutzung von HSMs, Smartcards und virtuellen Smartcards
- **VOLLSTÄNDIGE** Nachvollziehbarkeit durch Audit-Logs und zentrale Protokollierung relevanter Aktionen
- **KRYPTOGRAPHISCHE** Agilität inklusive Re-Signing- und Migrationsstrategien zur Post Quanten Kryptographie

04 „MADE IN EUROPE“
Souveränität und Vertrauen als Sicherheitskriterium

In Verteidigungs- und Hochsicherheitsumgebungen beeinflussen Herkunft, Zertifizierbarkeit und rechtlicher Rahmen die Sicherheitsbewertung von Kernkomponenten. Eviden Cybersecurity Products adressiert diese Dimension mit einem souveränen Portfolio an Cybersecurity-Produkten, das in Europa entwickelt und hergestellt wird und damit die Ausrichtung auf europäische Standards, Datenschutzprinzipien und Anforderungen der digitalen Souveränität unterstützt.

In Hochsicherheitsumgebungen wird Herkunft selbst zum Sicherheitskriterium.

Die zugrundeliegende Engineering- und R&D-Basis ist u. a. in Frankreich und Deutschland verankert; damit lässt sich der „Made in Europe“-Ansatz auch organisatorisch (Kompetenzen, Verantwortung, Produktpflege) nachvollziehbar abbilden – ein relevanter Punkt für Beschaffungs- und Governance-Vorgaben.

LEISTUNGSBAUSTEINE

Neben der Technologie wurden auch die begleitenden Bausteine für einen zulassungs- und auditfähigen Betrieb adressiert:

ARCHITEKTUR- und Designberatung zur Ableitung einer zulassungsfähigen Root-of-Trust- und PKI-Struktur

IDENTIFIKATION der Anwendungsfälle

AUFBAU von Signier- und HSM-Infrastruktur sowie Definition der Betriebs- und Sicherheitsgrenzen (Trust Domains)

PROZESSE, Richtlinien und Audit-Vorbereitung inklusive Dokumentation und Nachweisführung

ROLLOUT der Eviden Kernkomponenten: Modulare CA (CAmelot), Public-Key-Infrastruktur (ID PKI), Signatur-Engine (ID Sign), virtuelle Smartcard (SCinterface VSC), Timestamping (ID TSP) und HSMs (Proteccio).

Die Leistungsfähigkeit der Architektur wurde in einem Proof of Concept erfolgreich demonstriert und dient als Grundlage für den produktiven Rollout.

DAS ERGEBNIS

Mit der implementierten Architektur profitiert die Organisation von einer konsistenten Kette von Identität und Vertrauen über den gesamten Lebenszyklus ihrer Systeme:

- **NACHWEISBARE** Authentizität und Integrität von Softwareartefakten – vom Build bis zur Auslieferung und Nutzung
- **BETRIEBSSICHERHEIT** in isolierten Einsatzumgebungen, ohne Abhängigkeit von externen Validierungsdiensten
- **SKALIERBARE** Verwaltung von Identitäten und Zertifikaten mit standardisierten, automatisierbaren Workflows
- **REVISIONSSICHERE** Transparenz durch Auditierbarkeit und klare Rollen-/Rechtezuweisungen

Die im Proof of Concept validierten Ergebnisse wurden erfolgreich in die laufende Projektumsetzung überführt und bilden die Grundlage für den produktiven Rollout sowie die weitere Härtung des Betriebsmodells.

Eine konsistente Kette von Identität und Vertrauen – vom Build bis zum produktiven Einsatz.

MEHRWERT FÜR DIE ORGANISATION

REDUZIERTES PROJEKT- UND HAFTUNGSRISIKO

Ein kontrollierter, nachvollziehbarer Signatur- und Trust-Ansatz reduziert Risiken in der Lieferkette und dem Betrieb – einschließlich Haftungsfragen bei Softwareintegrität.

ZUKUNFTSSICHERER LANGZEITBETRIEB

Defense-Systeme werden über lange Zeiträume betrieben. Kryptographische Agilität, Re-Signing-/Migrationsstrategien und die Vorbereitung auf PQC tragen zur Betriebssicherheit über den Lebenszyklus bei.

SICHERER BETRIEB IN AIR-GAPPED SZENARIEN

Die Multi-Appplikations-PKI ist auf Isolation ausgelegt und ermöglicht Trust-Entscheidungen ohne externe Abhängigkeiten – passend zu segmentierten und offline betriebenen Umgebungen. Gleichzeitig bleibt der Betrieb ressourcenschonend, da schlanke, modular zuschaltbare Komponenten Systemlast reduzieren – ein Vorteil, wenn Energie und Infrastruktur in air-gapped Szenarien begrenzt sind.

BESCHLEUNIGTE AUDITFÄHIGKEIT

Durch Prozesse, Richtlinien und Audit-Vorbereitung (inkl. Dokumentation) werden Nachweise konsistenter, wodurch Prüf- und Freigabeprozesse in hochregulierten Programmen planbarer werden.

MODULAR UND SKALIERBAR – ÜBERGABEFÄHIG

Der Ansatz ist modular, an bestehende Produktlinien anpassbar, herstellerübergreifend einsetzbar und in Betriebsorganisationen sowie Behördenübergaben integrierbar.

MADE IN EUROPE / SOUVERÄNITÄT

Ein in Europa entwickeltes und hergestelltes Produktportfolio unterstützt Anforderungen an Governance und digitale Souveränität und adressiert Herkunfts- und Kontrollanforderungen in sensiblen Beschaffungsumgebungen.

EXECUTIVE SUMMARY

Die Eviden-Lösung stellt Integrität, Authentizität und Nachvollziehbarkeit von Softwareartefakten, Komponenten und Identitäten entlang des gesamten Lebenszyklus sicher – einschließlich auditierbarer Prozesse und Protokollierung. Sie ermöglicht verlässliche Trust-Entscheidungen und Validierung auch in air-gapped Umgebungen ohne externe Abhängigkeiten.

Durch die modulare Architektur ist der Ansatz an unterschiedliche Plattformen, Systemgenerationen und Betriebskonzepte anpassbar und deckt vielfältige Einsatzszenarien über Zonen/Segmente und Missionsprofile ab.

Vertrauenswürdige Software Supply Chains müssen auch unter Isolation belastbar funktionieren.

Der Betrieb ist ressourcenschonend ausgelegt, da schlanke, modular zuschaltbare Komponenten die Systemlast reduzieren – ein relevanter Faktor, wenn Energie und Infrastruktur in isolierten Umgebungen begrenzt sind. In einem Umfeld erhöhter geopolitischer Unsicherheit unterstützt das Konzept den planbaren, belastbaren Betrieb und eine nachhaltige, digital souveräne Absicherung der Software Supply Chain.

Eviden Digital Identity

Munscheidstr. 14
D 45886 Gelsenkirchen

T: +49 209 16724 - 50
F: +49 209 16724 - 61

Weitere Informationen:

2026-5-22