EVIDEN

CASE STUDY

PKI-based identity and code-signing infrastructure for an organization in the defense sector

THE INITIAL SITUATION

An international provider of safety-critical system and software solutions develops and operates solutions for operational environments with particularly high security requirements. The goal is to consistently ensure the authenticity, integrity, and traceability of software and system components throughout their entire lifecycle – from development through to operation.

With rising security and certification requirements, as well as increasing liability for software integrity, code signing is no longer viewed as a technical detail but as a prerequisite for the certification, operation, and long-term availability of safety-critical systems. In this context, OEMs and system integrators bear overall responsibility:

Weaknesses in the code-signing approach have a direct impact on approval, liability, and operational readiness – over long periods of operation.

THE CHALLENGE

The organization was tasked with setting up an automated code-signing system; the required PKI architecture served as the security-critical foundation for consistently securing signatures, identities, and credentials:

- **UNIQUE** identification and authentication of individuals, components, and software components in safety-critical systems
- **END-TO-END PROTECTION** of the software supply chain through authorized code signing and verifiable software integrity
- **RELIABLE** operation in isolated and air-gapped environments without internet access
- **COMPLIANCE** with audit and review requirements in highly regulated programs
- **MANAGEMENT** of several thousand identities with minimal administrative effort
- **HIGH** availability and robustness despite limited resources (hardware, personnel, operations)
- **FLEXIBILITY** and modularity for different platforms, system generations, and application scenarios
- **LONG-TERM** cryptographic security, including
- **PREPARATION** for post-quantum cryptography (PQC)

The analysis also revealed that traditional enterprise PKI or DevOps approaches often fall short due to operational constraints: cloud-based PKIs and online validation services are not permitted in many programs, and the PKI must be operated and tested reliably in segmented, isolated networks.

THE SOLUTION

To implement this, two separate PKI architectures were designed and deployed – implemented by Eviden Cybersecurity Products using a tailored portfolio of PKI, signature, and HSM components. From the outset, the approach has been designed to support air-gapped and highly regulated environments: it is natively offline-capable, auditable, and features a clear root-of-trust architecture.

The chain of trust does not end at the network boundary.

01 CODE-SIGNING PKI

A dedicated PKI domain forms the foundation for secure certificate processes and controlled signatures, supporting certification and operational readiness:

- **Implementation** of a PKI for managing component and system identities
- **Automated** code signing via a central signing engine (API-based), suitable for CI/CD integrations
- **Offline-capable** signing processes for environments with limited or no connectivity
- **Time stamping** to ensure the long-term preservation of evidence and the traceability of signatures – even if signature certificates expire or are revoked at a later date
- **Clear** definitions of roles and rights, as well as audit-proof logging of signature and certificate processes

02 MULTI-APPLICATION PKI

For environments without external connectivity, a modular, multi-application PKI has been designed that operates reliably with segmentation and isolation:

- **DESIGNED** for strictly controlled, air-gapped scenarios in which online mechanisms such as OCSP or external CRL distribution are not feasible
- **IMPLEMENTATION** as a closed trust ecosystem with internal policies and lifecycle-based validity concepts
- **SUPPORT** for typical platform use cases such as TLS encryption, device/component authentication, and other platform-specific trust functions
- **PROVISIONING** of standalone PKI instances tailored to specific needs for each segment/zone – aligned with the mission profile and system configuration
- **MODULAR** and scalable: Adaptable to existing product lines, compatible with equipment from various manufacturers, and transferable to operators and government agencies
- **TEMPLATE-BASED** deployment of PKI components, tailored to the specific requirements of the target platform
- **RESOURCE-EFFICIENT** operation: Lean, modular components that can be added as needed reduce the system load – a benefit when energy and infrastructure are limited in air-gapped scenarios.

Trustworthy communication must work even without external validation services.

03 MAXIMUM KEY AND CRYPTO SECURITY

HSM + crypto agility

The solution provides end-to-end protection for critical keys:

- **STRICT** separation of trust domains between code-signing and multi-application PKIs to minimize the attack surface
- **HSM-BASED** key management for root, CA, and TSP keys
- **FLEXIBLE** use of various key storage mechanisms for the applications, depending on the specific requirements of the target platform. For example, HSMs, smart cards, and virtual smart cards can be used
- **COMPLETE** traceability through audit logs and centralized logging of relevant actions
- **CRYPTOGRAPHIC** agility including re-signing and PQC migration strategies

04 „MADE IN EUROPE“
Sovereignty and trust as a security criterion

In defense and high-security environments, the origin, certifiability, and legal framework of core components influence their security assessment. Eviden Cybersecurity Products addresses this aspect with a robust portfolio of cybersecurity products developed and manufactured in Europe, thereby supporting compliance with European standards, data protection principles, and digital sovereignty requirements.

In high-security environments, provenance itself becomes a security criterion.

The underlying engineering and R&D infrastructure is based in France and Germany, among other places; this allows the “Made in Europe” approach to be clearly reflected in organizational terms (responsibilities, accountability, product maintenance) – a key consideration for procurement and governance requirements.

SERVICE MODULES

In addition to the technology, the accompanying components required for compliance with regulatory requirements and audit readiness were also addressed:

ARCHITECTURE and design consulting for deriving an admissible root-of-trust and PKI structure

IDENTIFICATION of relevant applications

DEPLOYMENT of signature and HSM infrastructure as well as definition of operation and security boundaries (trust domains)

PROCESSES, guidelines and audit preparation, including documentation and record keeping

ROLLOUT of Eviden core components: modular CA (CAmelot), public-key infrastructure (ID PKI), signature engine (ID Sign), Virtual Smartcard (SCinterface VSC), time stamping (ID TSP), and HSMs (Proteccio)

The architecture's capabilities were successfully demonstrated in a proof of concept and serve as the basis for the production rollout.

With the implemented architecture, the organization benefits from a consistent chain of identity and trust throughout the entire lifecycle of its systems:

- **VERIFIABLE** authenticity and integrity of software artifacts – from build to deployment and operation
- **OPERATIONAL SECURITY** in isolated deployment environments, without reliance on external validation services
- **SCALABLE** management of identities and certificates with standardized, automatable workflows
- **AUDIT-PROOF** transparency through auditability and clear role/permission assignments

The results validated in the proof of concept were successfully transferred to the ongoing project implementation and form the basis for the production rollout as well as the further hardening of the operating model.

A consistent chain of identity and trust – from build to production.

ADDED VALUE FOR THE ORGANIZATION

REDUCED PROJECT AND LIABILITY RISK

A controlled, traceable approach to digital signatures and trust reduces risks in the supply chain and operations – including liability issues related to software integrity.

FUTURE-PROOF LONG-TERM OPERATION

Defense systems are operated over long periods of time. Cryptographic agility, re-signing and migration strategies, and preparation for PQC contribute to operational security throughout the system's lifecycle.

SECURE OPERATION IN AIR-GAPPED SCENARIOS

The multi-application PKI is designed for isolation and enables trust decisions without external dependencies – making it ideal for segmented and offline environments. At the same time, operations remain resource-efficient, as lean, modular components reduce system load – a key advantage when energy and infrastructure are limited in air-gapped scenarios.

ACCELERATED AUDIT READINESS

Processes, guidelines, and audit preparation (including documentation) help ensure that evidence is more consistent, making review and approval processes in highly regulated programs more predictable.

MODULAR AND SCALABLE – TRANSFERABLE

The approach is modular, adaptable to existing product lines, compatible with products from different manufacturers, and can be integrated into operational organizations and government agency transitions.

MADE IN EUROPE / SOVEREIGNTY

A product portfolio developed and manufactured in Europe supports governance and digital sovereignty requirements and addresses provenance and control requirements in sensitive procurement environments.

EXECUTIVE SUMMARY

The Eviden solution ensures the integrity, authenticity, and traceability of software artifacts, components, and identities throughout their entire lifecycle – including auditable processes and logging. It enables reliable trust decisions and validation even in air-gapped environments without external dependencies.

Thanks to its modular architecture, the approach can be adapted to different platforms, system generations, and operational concepts, covering a wide range of use cases across zones/segments and mission profiles.

Trustworthy software supply chains must remain resilient even under isolation.

The system is designed for resource efficiency, as lean, modular components that can be added as needed reduce the system load – a critical factor when energy and infrastructure are limited in isolated environments. In a climate of heightened geopolitical uncertainty, this approach supports predictable, resilient operations and ensures a sustainable, digitally sovereign software supply chain.

EVIDEN

Eviden Digital Identity

Munscheidstr. 14
D 45886 Gelsenkirchen

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

Further information:

2026-05-28