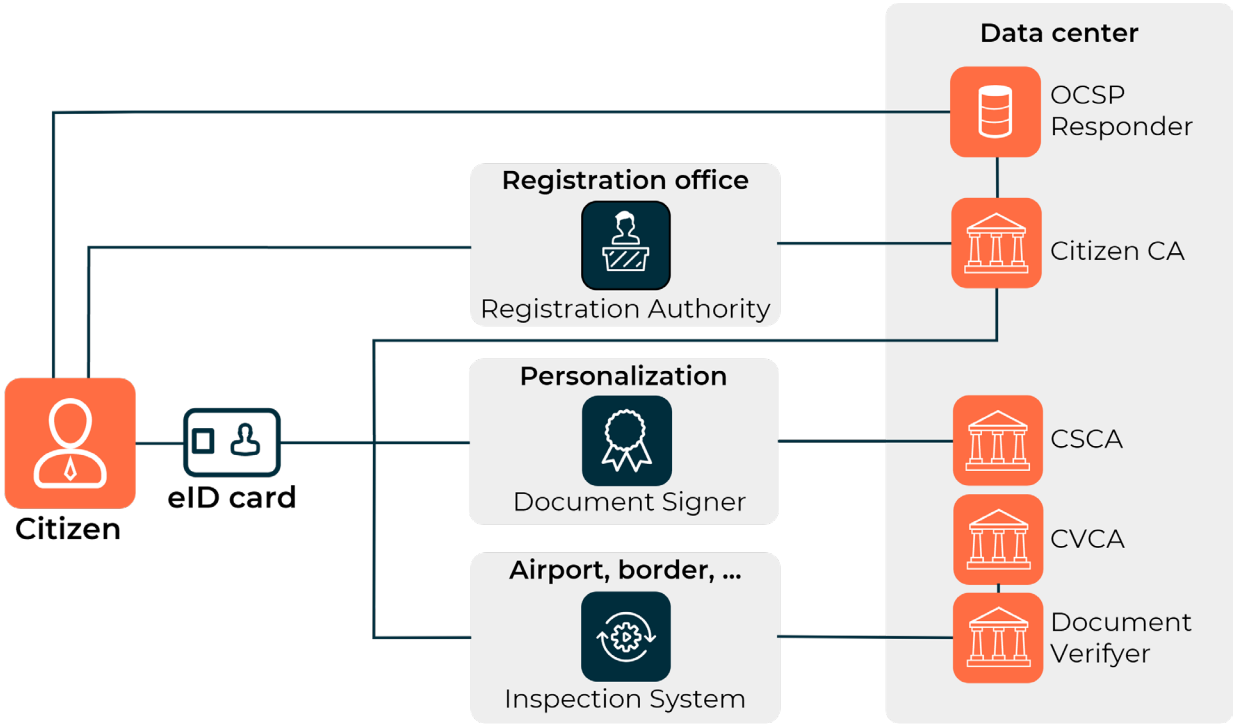
EVIDEN

cryptovision CAmelot

PKI for eID systems

With cryptovision CAmelot, governments can efficiently establish a Public Key Infrastructure (PKI) for electronic identity (eID) documents such as national ID cards, passports, and electronic driving licenses. Its modular design enables seamless scalability from straightforward test CAs to large-scale PKIs featuring multiple Certification Authorities and diverse certificate formats.



Every electronic identity (eID) system relies on a Public Key Infrastructure (PKI). A PKI typically consists of multiple certification authorities (CAs) along with various supporting components essential for secure certificate management.

Why do eID documents need a PKI?

Electronic identity cards, passports, health cards, driving licenses, and other forms of electronic identification (eID) rely extensively on asymmetric cryptography, specifically, the use of public and private key pairs. Each eID document is equipped with a unique key pair, enabling essential functions such as authentication, encryption, and digital signing. The issuing authority, typically a government agency, also uses its own key pair to digitally sign the data embedded in these documents.

The effectiveness of a key pair depends on its secure binding to a digital identity, whether that identity represents an individual or a device. This trust relationship is established through a digital certificate. Managing these certificates requires a Public Key Infrastructure (PKI), i.e. a comprehensive framework of technologies, policies, and procedures that governs the issuance, distribution, and lifecycle of digital certificates. A well-designed PKI is the foundational security layer of any robust eID system.

EVIDEN

How does an eID document PKI work?

Unlike enterprise PKIs, which primarily focus on user enrollment and internal access control, eID Public Key Infrastructures (PKIs)—especially those aligned with the Machine Readable Travel Documents (MRTD) standard and the Extended Access Control (EAC) model—are purpose-built to secure identity documents in international and high-security environments. At the core of this infrastructure is the Citizen CA, which issues and signs digital certificates for individual document holders. Complementing this, the Country Signing Certificate Authority (CSCA) is responsible for signing the data stored on the document itself. These cryptographic signatures ensure the authenticity and integrity of the document, allowing any attempt at tampering to be immediately detected during the verification process.

To protect access to sensitive biometric data, such as fingerprints or iris scans, EAC introduces a second trust path. The Country Verifying Certificate Authority (CVCA) issues certificates to Document Verifiers (DVs), which in turn authorize Inspection Systems (IS). This hierarchical structure ensures that only explicitly authorized systems can access protected data, enforcing confidentiality through cryptographic access control.

Our solution

Cryptovision CAmelot is a Certification Authority (CA) software solution purpose-built for issuing digital certificates for electronic identity documents. Designed with a fully modular architecture, CAmelot features independent, interchangeable components that offer exceptional flexibility and effortless customization.

CAmelot supports the operation of complex PKIs, including environments with multiple CAs and diverse certificate formats. Its architecture allows for seamless future modifications and upgrades. Through standardized interfaces, CAmelot integrates smoothly with external IT systems, streamlining essential processes such as user registration, certificate revocation, and distribution.

Key Features

Certificates for eIDs

CAmelot is a Certification Authority (CA) software specifically designed for digital certificates used in electronic identity documents. It supports operation in a variety of roles, including Citizen CA, CSCA, CVCA, and ICAO Document Signer. It supports both X.509 and card verifiable (CV) digital certificates.

Extensible

With CAmelot you can change or extend your PKI without touching the system core. You can choose from many existing modules. Additional modules can be developed, existing ones can be customized. Through standardized interfaces, CAmelot easily integrates with external IT systems such as directory services and workflow systems.

Secure

With its modular architecture, CAmelot supports PKIs from high-security infrastructures for eID documents all the way to cost-effective solutions for internal use. It offers security features, including support for Hardware Security Modules (HSMs), configurable role-based access control, and strong administrator authentication.

Flexible

With CAmelot you can easily configure your own individual PKI system. Thanks to its modular architecture, CAmelot supports all scenarios from simple test PKIs with one CA to complex certification hierarchies. It effortlessly scales to support hundreds of millions of users.

Platform-independent

CAmelot is completely realized in JAVA. Therefore, it can easily be operated on many different platforms, including Windows Linux, and macOS. Migration is easily possible.

Advanced features

CAmelot supports several kinds of enrollment processes, different renewal processes, OCSP status checks, numerous certificate profiles, a sophisticated logging function and many other advanced features.

EVIDEN

Who uses CAmelot?

CAmelot is deployed in numerous countries as a trusted Public Key Infrastructure (PKI) for electronic identity (eID) systems. Governments around the world rely on CAmelot to issue private keys and digital certificates for eID cards used by hundreds of millions of citizens. In addition, many countries use CAmelot as an ICAO Document Signer, enabling the secure digital signing of data stored on electronic identity documents.

Success story: GhanaCard

With a population of nearly 35 million, Ghana stands as a key nation in West Africa. To enhance identity management and digital services, the Ghanaian government has introduced the GhanaCard, a national electronic identity card for its citizens. Beyond serving as an official identity document, the GhanaCard functions as a passport substitute within the ECOWAS region and enables strong authentication for online services, acting as a secure alternative to traditional passwords. The latest generation of the card also supports digital signatures, further expanding its capabilities.

The GhanaCard project is powered by technology from cryptovision (now part of Eviden Digital Identity). Cryptovision provided the card's embedded software, the supporting Public Key Infrastructure (PKI), and token-based access to the PKI. The CAs are operated using CAmelot. Designed to serve over 17 million users, Ghana's PKI is considered one of the most advanced in the world.

Modules

CAmelot consists of the following modules:

- **Protocol handler modules**: These modules handle communication with control units, primarily through a management console.
- **CA modules**: The core components of CAmelot, CA modules are responsible for generating and signing digital certificates.
- **Key manager modules**: Key manager modules interface with the key stores used by CAmelot, typically smart cards, Hardware Security Modules (HSMs), or key files.
- **Certifier modules**: These modules assemble the content of digital certificates and prepare them for signing. Dedicated certifier modules are available for both X.509 and Card Verifiable (CV) certificate formats.
- **Publisher modules**: Publisher modules manage the distribution of certificates generated by CAmelot. They support a variety of targets, including LDAP servers, databases, and file-based systems.
- **Certificate template modules**: These modules define one or more specific certificate extensions to be encoded in the certificate, according to predefined templates.
- **Access module**: The single access module enforces access control across the CAmelot architecture. It verifies access permissions from external systems as well as internal module-to-module communication.

Thanks to its modular design, CAmelot offers the flexibility to adapt seamlessly to a wide range of customer needs.

Supported systems

- Windows Server 2016 / 2019
- Oracle Linux R9 64 bit
- Red Hat 9 64 bit
- LDAP-capable user directory service
- HSMs from Trustway, Utimaco, Thales, SafeNet

Find out more about us: www.cryptovision.com

Connect with us

Supported standards

- 509v3 certificates
- X.509v2 CRLs
- RFC 5280 (PKIX)
- RFC 2560 (OCSP)
- RFC 5272, RFC 5273 (CMC)
- IEEE 802.1x
- PKCS#1/#7/#8/#10/#11/#12
- SPKAC (Netscape signed public key and challenge format)
- TR-03129
- TR-03110-V2
- Card verifiable Certificates
- ICAO 9303 Part 12

eviden.com

 20251009