# cryptovision CAmelot

## Modular construction kit for PKI components

With cryptovision CAmelot you can create a Public Key Infrastructure (PKI) that is tailor-made for your individual needs. Existing cryptovision CAmelot PKIs are easy to alter and extend. As an especially flexible solution, cryptovision CAmelot supports both enterprise (X.509) and government PKIs (CV certificates). In addition, Cryptovision CAmelot provides a powerful workflow engine and a PKI client.


### Management summary

If spies and hackers threaten your IT systems, you should react – before it is too late. Above all, authentication, digital signature and encryption are effective antidotes. For these security measures to work, you need private keys and digital certificates. The management of digital certificates is an important task. The components required for this are known as public key infrastructure (PKI).

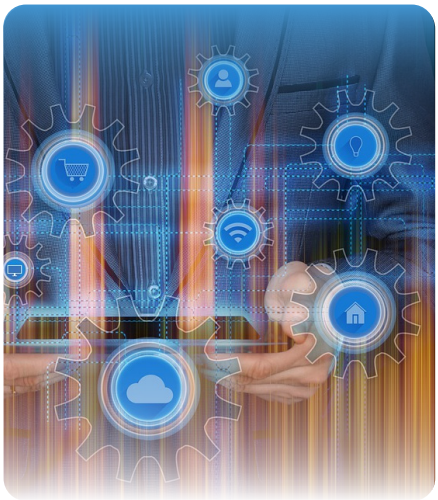
A PKI is always a very individual infrastructure. The exact implementation always depends on the IT environment, security requirements, the desired applications and many other factors. Often an existing PKI has to be changed afterwards. Cryptovision CAmelot, a product of Atos, is a highly flexible solution for the operation of a PKI that takes these requirements into account.

With cryptovision CAmelot you can build a PKI that is tailor-made for your individual needs. Existing cryptovision CAmelot PKIs are easy to change and extend. One of the reasons cryptovision CAmelot is so flexible is that it is based on a completely modular architecture. In addition to the standard modules, further modules can be developed according to your requirements.

As one of the most flexible PKI solutions worldwide, cryptovision CAmelot supports both enterprise PKIs (X.509 certificates) and PKIs for eID documents (CV certificates). In addition, cryptovision CAmelot's modular architecture enables different security levels. High security architectures can thus be realized as well as cost-effective infrastructures for pragmatic security requirements. Unneeded modules are omitted, which also significantly simplifies administration.


## Why do I need a PKI?

Private and public keys play a major role for authentication, encryption, and digital signature. However, a private/public key pair is only of use if it is bound to a digital identity (this can be a person or a device). This binding is achieved with a digital certificate. A Public Key Infrastructure (PKI) is the combination of components and processes necessary for managing digital certificates. Typical parts of a PKI include a certification authority, a certificate repository, and PKI applications.



## What is a PKI workflow?

A PKI workflow is defined by the sequence of persons and components that are involved in a PKI process – especially certificate enrollment and renewal – and by the data that is processed. Workflow design plays a crucial role in a PKI. In order to make a PKI process effective, secure, and compliant to certain rules, it is necessary to specify exactly, which party processes which data in which order.

## What is a PKI client?

A PKI client is a component that is installed on the user platform. It is responsible for client-side communication with other PKI components. It supports the user in using and administering his private keys and certificates. For instance, a PKI client can automatically renew a digital certificate when it expires.

Atos

## Basics

### Cryptovision CAmelot

Cryptovision CAmelot is a Certification Authority (CA) software. The CA is the core component of a Public Key Infrastructure (PKI).

### For Individual PKIs

With cryptovision CAmelot you can easily configure your own individual PKI architecture. Cryptovision CAmelot supports all scenarios from simple PKIs with one CA to complex certification hierarchies. Changes in the PKI setting are easily possible.

### For Extensible PKIs

With cryptovision 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.

### Certificates for eIDs

Cryptovision CAmelot is an ideal solution for electronic identity documents (eIDs). It supports both X.509 and card verifiable (CV) digital certificates. It can also be operated as an ICAO Document Signer. Due to its modularity it easily scales to hundreds of millions of users.

### Certificates for Enterprises

Cryptovision CAmelot is ideally suitable for enterprise certificate lifecycle management. It can be easily integrated into existing IT environments and provisioning processes. Instead of introducing a new infrastructure cryptovision CAmelot is designed according to the philosophy that existing infrastructure should be used and that different components with similar tasks should be avoided.

### Platform-independent

Cryptovision CAmelot is completely realized in JAVA. Therefore, it can easily be operated on many different platforms.

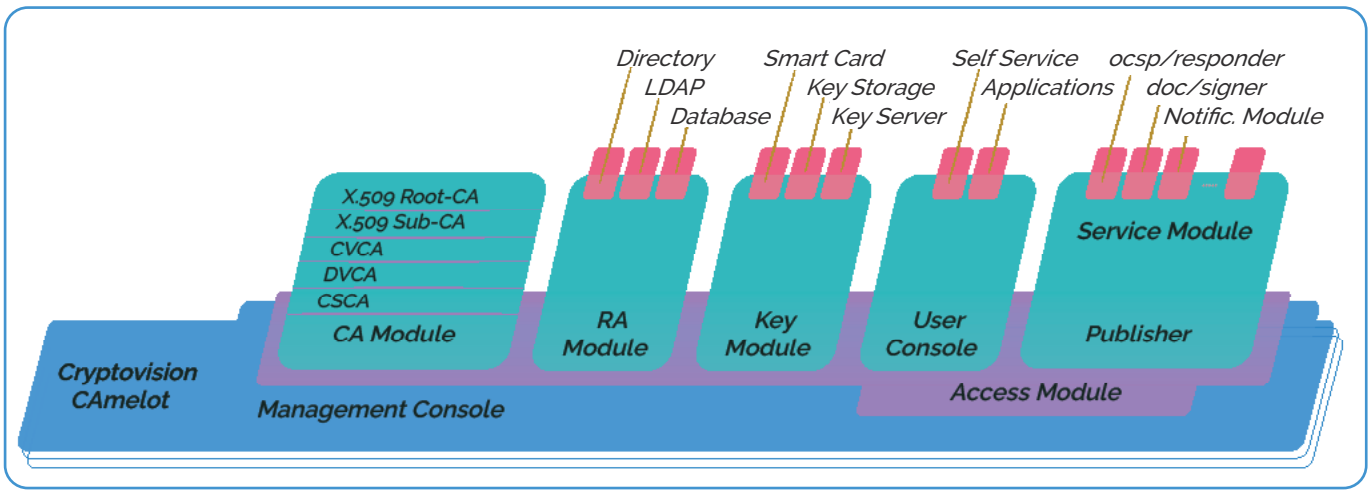
### High Security

Based on the modular architecture cryptovision CAmelot supports PKIs on different security levels. From a high security PKI (e.g. for corporate infrastructures) to a cost-effective PKI with medium security requirements all scenarios are possible. It supports HSMs, flexible roles, strong admin authentication and more.

### Advanced Features

Cryptovision CAmelot supports a sophisticated logging function, several kinds of auto-enrolment and many other advanced features.

# Product architecture




Cryptovision CAmelot has a fully modular architecture. The core functionality is provided by one or several CA modules, while six other module types are responsible for access control and communication with other components.

# Architecture

Cryptovision CAmelot was designed as a CA software that provides maximum flexibility and extensibility. Virtually every usage scenario of a PKI can be covered. Later changes are easily possible. The flexibility cryptovision CAmelot provides is based on a fully modular design. All modules are independent entities that can easily be replaced. The core functionality of cryptovision CAmelot is provided by one or several CA modules, while six other module types are responsible for tasks like access control and communication with other components.

# Cryptovision Camelot modules

### Protocol Handler Modules
This module type communicates with control units, especially with a management console.

### CA modules:
This is the core component, responsible for generating and signing digital certificates.

### Key manager modules
Key manager modules communicate with the key stores used by cryptovision CAmelot, typically smart cards, Hardware Security Modules (HSMs) or key files.

### Certifier modules
Modules of this type assemble the content of digital certificates and prepare them for signing. There are modules for X.509 certificates and card verifiable (CV) certificates.

### Publisher modules
Modules of this type are responsible for publishing digital certificates generated by cryptovision CAmelot. Especially, modules for LDAP servers, databases, and files can be used.

### Certificate template modules:
A Certificate template module provides one or more specific certificate extensions which are encoded in a certificate.

### Access module:
The access module (there is only one of its kind) is responsible for access control within the cryptovision CAmelot architecture. It verifies the access conditions from external systems and also for the internal connections between the modules.

In all, cryptovision CAmelot provides the most flexible approach in CA architecture that is thinkable.

# Add-ons

The functionality of CAmelot can be enhanced with the PKI client Pendragon and the workflow engine Shalott. With the help of these solutions, an almost arbitrary enrollment process can be defined, while working with keys and digital certificates becomes extremely simple and user-friendly.

# Success story

With almost 30 million inhabitants, Ghana is an important country in West Africa. As an major project for the future, the Ghanaian government has launched an electronic identity card, the GhanaCard. The GhanaCard can not only be used as an identity document but also as a passport replacement within the West African ECOWAS region. In addition, the GhanaCard enables strong authentication – as a secure password replacement for online services. Digital signatures and payment are supported, too.

For the realization of the GhanaCard, the Ghanaian government relies on cryptovision (now part of Atos) technology. The software on the GhanaCard, the associated Public Key Infrastructure (PKI), and the token-based access to the PKI were implemented by cryptovision. The Certification Authorities (CAs) are operated with cryptovision CAmelot. The PKI of the GhanaCard, developed for 16 million users, is one of the most modern worldwide On 15 September 2017, Ghanaian President Nana Akufo-Addo received the first GhanaCard.

### Supported systems
- Windows Server 2016 / 2019
- CentOS 6/7 64 bit
- Red Hat 6/7 64 bit
- LDAP capable user directory service
- HSMs from Bull, Utimaco, Thales, SafeNet

### Customers
Cryptovision CAmelot is used (among others) by the following customers:
- Identity authorities of emerging nations: Citizens of several emerging nations receive eID cards with private keys and certificates.
- German defense supplier: Uses cryptovision CAmelot for authentication.
- Car manufacturer: A Japanese car manufacturer uses cryptovision CAmelot for protecting the internal IT infrastructure.

# About Atos

Atos is a global leader in digital transformation with 109,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea), listed on Euronext Paris and included in the CAC 40 ESG and Next 20 Paris Stock indexes.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Find out more about us
atos.net
atos.net/career

Let's start a discussion together

For more information: info@cryptovision.com