cryptoVision
an atos company

Product Brief

CAmelot

Modular construction kit for PKI components

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

CAmelot, a product of cryptovision, is a highly flexible solution for the operation of a PKI that takes these requirements into account.

With CAmelot you can build a PKI that is tailor-made for your individual needs. Existing CAmelot PKIs are easy to change and extend. One of the reasons 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, CAmelot supports both enterprise PKIs (X.509 certificates) and authority PKIs (CV certificates). In addition, 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..

Version: 10/2021

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.

THE BASICS

CAmelot

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

For Individual PKIs

With CAmelot you can easily configure your own individual PKI architecture. 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 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

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

CAmelot is ideally suitable for enterprise certificate lifecycle management. Due to its modular architecture it can be easily integrated into existing IT environments and provisioning processes. Instead of introducing a new infrastructure 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

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

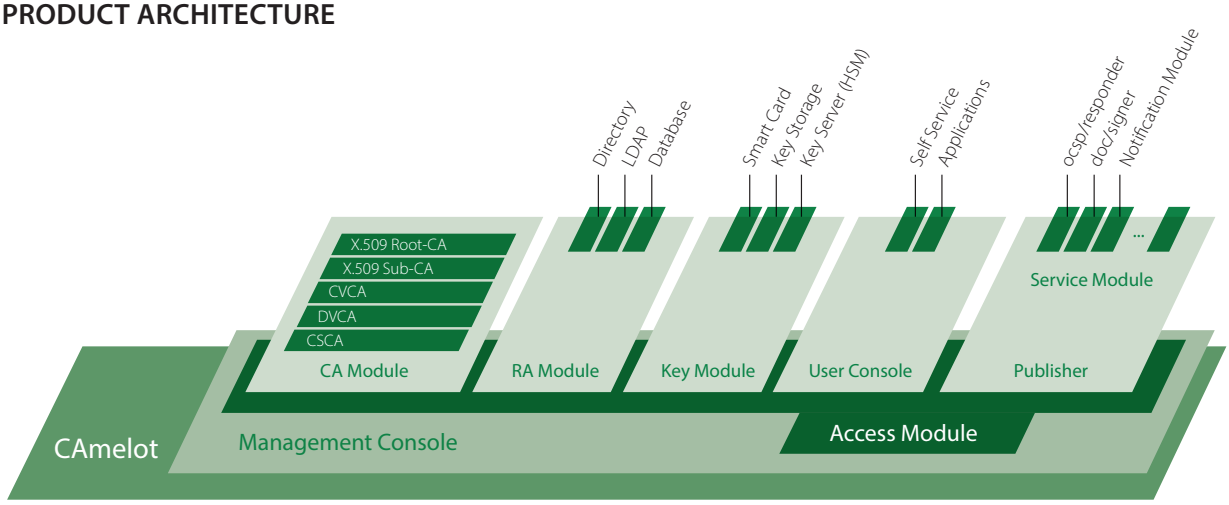
High Security

Based on the modular architecture 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. CAmelot supports HSMs, flexible roles, strong admin authentication and more.

Advanced Features

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

PRODUCT ARCHITECTURE



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.

Camelot modules:

Protocol Handler Modules

This module type communicates with control units, especially with a management console.

Key manager modules

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

Publisher modules

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

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.

CA modules:

This is the core component, responsible for generating and signing digital certificates..

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 CAmelot architecture. It verifies the access conditions from external systems and also for the internal connections between the modules.

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

CAmelot Architecture

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 CAmelot provides is based on a fully modular design. All modules are independent entities that can easily be replaced. Communication between the modules is achieved via documented "orders". The core functionality of 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.

SUPPORTED SYSTEMS

- Windows Server 2016 / 2019
- CentOS 6/7 64 bit
- Redhat 6/7 64 bit
- LDAP capable user directory service
- HSMs from Utimaco, Thales, Bull, SafeNet

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 technology. Both the software on the GhanaCard as well as the associated Public Key Infrastructure (PKI) and the token-based access to the PKI were implemented by cryptovison. The Certification Authorities (CAs) are operated with CAmelot. The PKI of the GhanaCard, which was developed for 16 million certificate holders, is one of the most modern worldwide.

On 15 September 2017, Ghanaian President Nana Akufo-Addo received the first GhanaCard.

CUSTOMERS

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 CAmelot for authentication.
- Car manufacturer: A Japanese car manufacturer uses CAmelot for protecting the internal IT infrastructure.

cryptovision

cv cryptovision GmbH is one of the leading specialists for modern, user-friendly cryptography and secure electronic identities. With its solutions, over 250 million people worldwide and a multitude of institutions in the digital world protect themselves against hacker attacks, manipulation, misuse of identities and espionage.

cryptovision addresses various industries such as public administration, health, automotive, finance & insurance, energy or IT. Its customers include countries such as Nigeria, Ghana and Ecuador, institutions such as the German Armed Forces, the German Federal Office for Information Security (BSI), the city of New York and companies such as E.ON, VW and Allianz. Since 31 August 2021, cryptovision is part of Atos.

KONTAKT

cv cryptovision GmbH
Munscheidstr. 14
D 45886 Gelsenkirchen

T: +49 209 16724-50
F: +49 209 16724-61
info@cryptovision.com

www.cryptovision.com