cryptovision

CAmelot

Highly Flexible Certificate Lifecycle Management

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

Today's IT managers are facing a wide variety of challenges. Especially, protection of data and infrastructures is becoming more and more important. To achieve this goal, authentication, digital signatures and encryption need to be used in an appropriate way. In order for these security measures to work, private keys and digital certificates are necessary.

Digital certificate management is therefore an important task. The components needed for this purpose are referred to as Public Key Infrastructure (PKI). A PKI is a highly individual construct. Its realization depends on the IT environment, security requirements, applications and many other factors.

cryptovision's CAmelot is a highly flexible solution for operating a PKI. CAmelot not only lets you build a PKI system tailor-made for your individual needs, but also provides a number of unique tools that make PKI operation easy – like the workflow engine Shalott and the PKI client Pendragon.

As one of the most flexible PKI solutions on the market, CAmelot supports both enterprise PKIs (X.509 certificates) and government PKIs (card verifiable certificates). The modular architecture of CAmelot enables different security levels. High security architectures can be realized, just as well as cost-effective implementations rendering medium security.

The worflow engine Shalott enables implementation of a company-wide PKI policy based on pre-configured workflows. Combined with the PKI client Pendragon, these workflows include enrollment and renewal processes that may require administrator approval based on predetermined rules. Thus, manual processing of certificate requests is reduced to a minimum.

BACKGROUND

Why do I need a PKI?

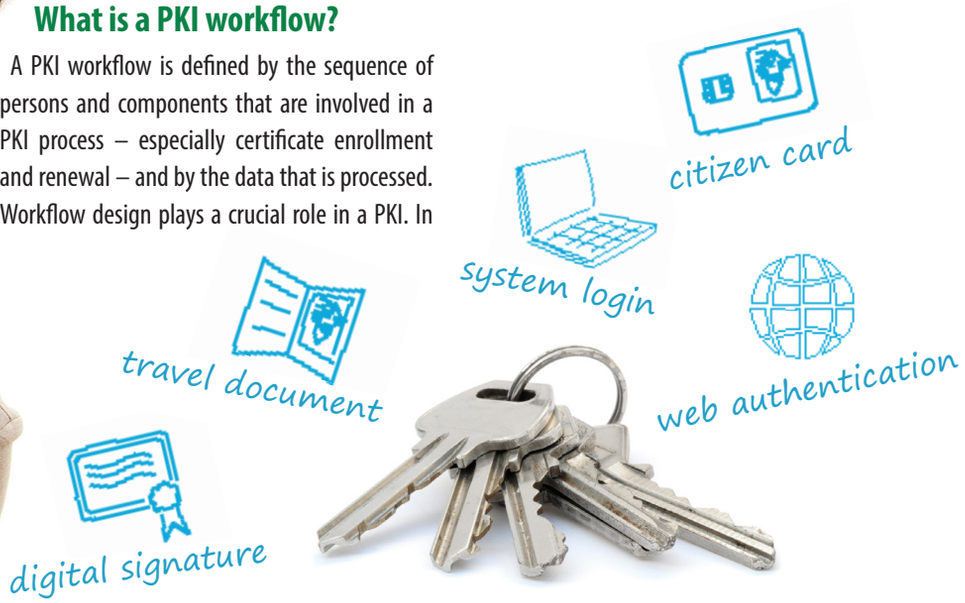
Private and public keys play a major role for authentication, encryption, and digital signature. However, a private/public key pair is only of use if it is bound to a digital identity (this can be a person or a device). This binding is achieved with a digital certificate. A Public Key Infrastructure (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).

Shalott

Shalott integrates a worflow engine into the PKI. PKI workflows based on Business Process Model and Notation (BPMN) can be graphically modeled and easily parameterized. Every certification request is processed according to predefined policies. Shalott simplifies PKI administration dramatically.

Pendragon

The PKI client Pendragon supports users in administering his certificates and keys, especially in enrollment and renewal.

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.

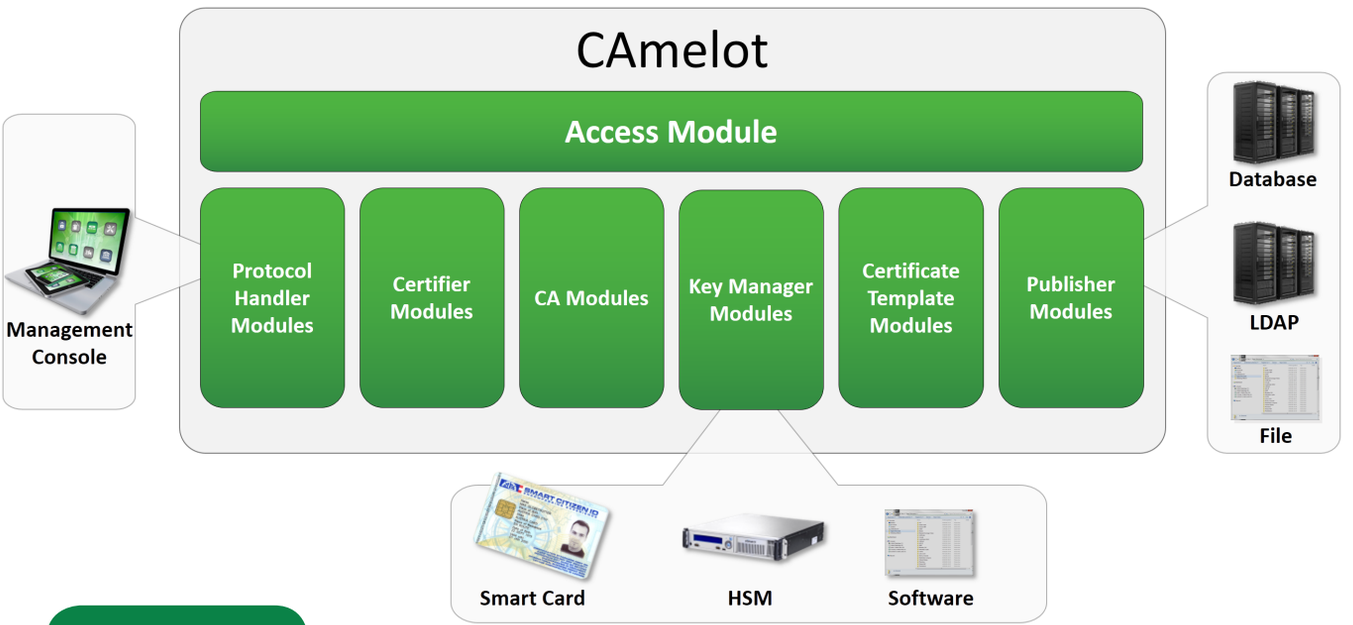
Advanced Features

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

cryptoVision

THE TECHNICAL PART

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.



THE MODULES

The following Module types exist:

- **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.

The 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 2008/2012 R2
- Redhat 6/7 64bit
- CentOS 6/7 64bit
- Any LDAP server supporting the entryDN attribute (RFC 5020)
- HSMs from Utimaco, Thales (nCipher), Bull, Gemalto (SafeNet)

THE MARKET PART

Success story

With close to 160 million citizens, Nigeria is Africa's most populous country. As part of an ambitious Presidential initiative, adult Nigerians and resident legal aliens currently receive advanced multipurpose electronic identity cards. cryptovision plays critical role in this mammoth project. The company is responsible for the deployment of the PKI which will be used to both electronically validate the card itself as well enable online digital signatures. One of the largest PKIs in the world, the full deployment will include least eight CAs and eventually issue certificates more than 100 million card holders. This PKI is unique as it serves as the backbone of the eID card which will be used many different government agencies and ministries. Card verifiable certificates ensure that only authorized agencies access relevant chip content specific to their organization. On the other hand, the same PKI will enables the eID holder to perfume advanced two factor authentication and to create digital signatures.

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.

About cryptovision

cryptovision is a leading supplier of innovative cryptographic IT security solutions. Based on its two decades of market experience and broad background in modern cryptographic techniques, such as Elliptic Curve Cryptography, all cryptovision products provide the most state-of-the-art and future-proof technologies. The company specializes in lean add-on components which can be integrated into nearly any IT system to gain more security in a both convenient and cost-effective way.

From small devices like citizen eID cards, all the way to large scale IT infrastructures, more than 500 million people worldwide make use of cryptovision products every day in such diverse sectors as defense, automotive, financial, government, retails and industry.

cv cryptovision GmbH
Munscheidstr. 14
D-45886 Gelsenkirchen

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

cv cryptovision
100 Park Avenue / Suite 1600
New York City, NY 10017, USA

T: +1 (212) 984 0750
F: +1 (212) 880 6499

www.cryptovision.com