cryptoVision
an atos company

Product Brief

# CAmelot

## Modulare Software-Lösung für PKI-Komponenten

**Mit CAmelot können Sie eine Public-Key-Infrastruktur (PKI) aufbauen, die genau auf Ihre Anforderungen passt. Bestehende CAmelot-PKIs lassen sich leicht ändern und erweitern. Als eine der flexibelsten PKI-Lösungen weltweit unterstützt CAmelot sowohl Unternehmens- als auch Behörden-PKIs. Zusätzlich bietet CAmelot eine leistungsfähige Workflow-Engine und einen PKI-Client.**

## MANAGEMENT SUMMARY

Wenn Spione und Hacker Ihre IT-Systeme bedrohen, sollten Sie reagieren – bevor es zu spät ist. Vor allem Authentifizierung, digitale Signatur und Verschlüsselung haben sich als Gegenmaßnahmen bewährt. Damit diese funktionieren, benötigen Sie private Schlüssel und digitale Zertifikate. Das Management digitaler Zertifikate ist hierbei eine wichtige Aufgabe. Die für diesen Zweck eingesetzten Komponenten werden als Public-Key-Infrastruktur (PKI) bezeichnet.

Eine PKI ist immer eine sehr individuelle Infrastruktur. Die genaue Realisierung hängt stets von der IT-Umgebung, Sicherheitsanforderungen, den gewünschten Anwendungen und vielen anderen Faktoren ab. Oft muss eine vorhandene PKI nachträglich geändert werden.

CAmelot, ein Produkt von cryptovision, ist eine hochflexible Lösung für den Betrieb einer PKI, die diesen Anforderungen Rechnung trägt.

Mit CAmelot können Sie eine PKI aufbauen, die maßgeschneidert für Ihre individuellen Bedürfnisse ist. Bestehende CAmelot-PKIs sind leicht zu ändern und zu erweitern. CAmelot ist unter anderem deshalb so flexibel, weil es auf einer vollständig modularen Architektur beruht. Zusätzlich zu den bereits vorhandenen Modulen lassen sich weitere nach Ihren Anforderungen entwickeln.

Als eine der flexibelsten PKI-Lösungen weltweit unterstützt CAmelot sowohl Unternehmen-PKIs (X.509-Zertifikate) als auch Behörden-PKIs (CV-Zertifikate). Zudem ermöglicht die modulare Architektur von CAmelot unterschiedliche Sicherheitsniveaus. Hochsicherheitsarchitekturen lassen sich damit genauso realisieren wie kostengünstige Infrastrukturen für pragmatische Sicherheitsanforderungen. Nicht benötigte Module werden weggelassen, was nebenbei die Administration deutlich vereinfacht.

Version: 01/2022

## Wozu benötigt man eine PKI?

Private und öffentliche Schlüssel spielen eine wichtige Rolle für die Authentifizierung, die Verschlüsselung und die digitale Signatur. Ein Paar aus privatem und öffentlichen Schlüssel ist jedoch nur dann von Nutzen, wenn es an eine digitale Identität gebunden ist (dies kann eine Person oder ein Gerät sein). Diese Bindung wird von einem digitalen Zertifikat gewährleistet. Eine Public-Key-Infrastructure (PKI) ist die Kombination von Komponenten und Prozessen, die für die Verwaltung digitaler Zertifikate erforderlich sind. Typische Bestandteile einer PKI sind eine Zertifizierungsstelle, eine Registrierungsstelle, ein Verzeichnisdienst für Zertifikate und diverse PKI-Anwendungen.

## Was ist ein PKI-Workflow?

Ein PKI-Workflow wird durch die Abfolge der Personen und Komponenten, die an einem PKI-Prozess – insbesondere der Zertifikatsregistrierung und -erneuerung – beteiligt sind, sowie durch die zu verarbeitenden Daten definiert. Die Gestaltung des Workflows spielt in einer PKI eine entscheidende Rolle. Um einen PKI-Prozess effektiv, sicher und regelkonform zu gestalten, muss genau festgelegt werden, welche Partei welche Daten in welcher Reihenfolge verarbeitet.

## Was ist ein PKI-Client?

Ein PKI-Client ist eine Komponente, die auf der Benutzerplattform installiert wird. Er ist für die clientseitige Kommunikation mit anderen PKI-Komponenten zuständig. Er unterstützt den Benutzer bei der Verwendung und Verwaltung seiner privaten Schlüssel und Zertifikate. Ein PKI-Client kann zum Beispiel ein digitales Zertifikat automatisch erneuern, wenn es abläuft.

GRUNDLAGEN

### CAmelot

CAmelot ist eine Software für den Betrieb einer Zertifizierungsstelle (CA). Die CA ist die Kernkomponente einer Public-Key-Infrastruktur (PKI).

### Für individuelle PKIs

Mit CAmelot können Sie eine PKI vollständig nach Ihren Anforderungen gestalten. CAmelot unterstützt von einer pragmatischen Mini-PKI bis zu komplexen CA-Hierarchien jedes Szenario. Nachträgliche Änderungen sind problemlos möglich.

### Für erweiterbare PKIs

Mit CAmelot können Sie eine bestehende PKI beliebig erweitern. Sie können vorhandene Module nutzen oder Module entwickeln. Bestehende Module können angepasst werden.

### Zertifikate für eIDs

CAmelot ist die ideale PKI-Lösung für elektronische Ausweise. Sowohl X.509- als auch CV-Zertifikate werden unterstützt. CAmelot kann zudem als ICAO-9303-Document-Signer betrieben werden. Aufgrund seiner Modularität lässt sich CAmelot leicht skalieren – bis hin zu Hunderten von Millionen von Ausweisinhabern.

### Zertifikate für Unternehmen

CAmelot ist ideal für den Einsatz im Unternehmen. Durch die vollständig modulare Architektur lässt sich CAmelot leicht in bestehende IT-Umgebungen und Provisioning-Prozesse integrieren. Statt eine neue Infrastruktur aufzubauen, wird die bestehende genutzt. So wird eine Doppelung von IT-Komponenten vermieden.

### Plattform-unabhängig

CAmelot ist vollständig in Java realisiert. Daher kann es auf vielen unterschiedlichen Plattformen eingesetzt werden.

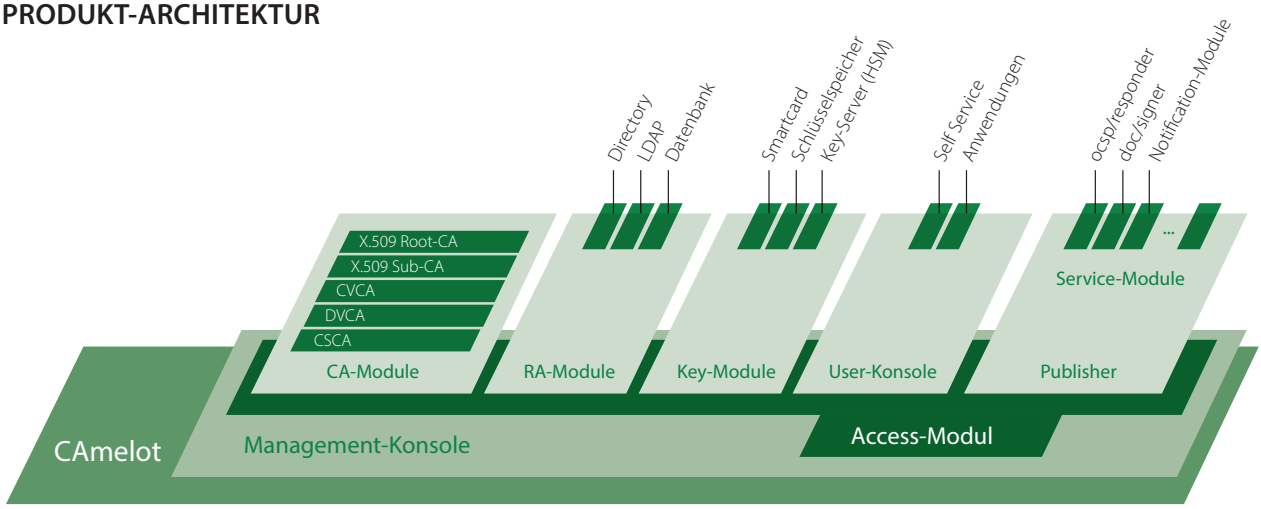
### Hohe Sicherheit

CAmelot unterstützt PKIs in verschiedenen Sicherheitsstufen. Von einer Hochsicherheits-PKI (beispielsweise im Militärwesen) bis zur kostengünstigen Infrastruktur mit pragmatischem Sicherheitskonzept sind so gut wie alle Szenarien möglich.

### Zahlreiche Features

CAmelot bietet ein flexibles Rollenkonzept, starke Administratoren-Authentifizierung, eine leistungsfähige Log-Funktion, Auto-Enrolment und zahlreiche weitere innovative Features.

## PRODUKT-ARCHITEKTUR




*CAmelot hat eine vollständig modulare Architektur. Die Kernfunktionalität wird von einem oder mehreren CA-Modulen bereitgestellt, während sechs weitere Modultypen für die Zugriffskontrolle und die Kommunikation mit anderen Komponenten zuständig sind.*

## Camelot-Module

### Protocol-Handler-Module

Dieser Modul-Typ kommuniziert mit der Management-Konsole und anderen Steuerungseinheiten.

### Key-Manager-Module

Key-Manager-Module kommunizieren mit den von CAmelot verwendeten Schlüsselspeichern – in der Regel Chipkarten, Hardware-Sicherheitsmodule (HSMs) oder Schlüssel-Dateien.

### Publisher-Module

Module dieses Typs sind für die Veröffentlichung von digitalen Zertifikaten verantwortlich. Insbesondere können sie für LDAP-Server, Datenbanken und Dateien verwendet werden.

### Certifier-Module:

Module dieses Typs stellen den Inhalt von digitalen Zertifikaten zusammen und bereiten sie für die Signierung vor. Es gibt Module für X.509-Zertifikate und CV-Zertifikate.

### CA-Module

Diese Komponenten sind für die Signierung digitaler Zertifikate verantwortlich.

### Certificate-Template-Module:

Ein Certificate-Template-Modul stellt eine oder mehrere Zertifikatserweiterungen bereit, die in einem Zertifikat kodiert werden.

### Access-Modul:

Das Access-Modul (es gibt nur eines dieser Art) regelt die Zugriffskontrolle in der CAmelot-Architektur.

**Insgesamt bietet CAmelot den flexibelsten Ansatz für eine CA-Architektur, der denkbar ist.**

## Architektur

CAmelot wurde als CA-Software konzipiert, die maximale Flexibilität und Erweiterbarkeit bietet. Praktisch jedes Einsatzszenario einer PKI lässt sich mit CAmelot abdecken. Spätere Änderungen sind problemlos möglich.

Die Flexibilität von CAmelot basiert auf einem vollständig modularen Design. Jedes Modul kann einfach ausgetauscht werden. Die Kommunikation zwischen den Modulen wird über dokumentierte „Aufträge“ erreicht. Die Kernfunktionalität von CAmelot wird von einem oder mehreren CA-Modulen bereitgestellt, während sechs weitere Modultypen für Aufgaben wie Zugriffskontrolle und Kommunikation mit anderen Komponenten zuständig sind.

### UNTERSTÜTZTE SYSTEME

- Windows Server 2016 / 2019
- CentOS 6/7 64 bit
- Red Hat 6/7 64 bit
- LDAP-fähiger Verzeichnisdienst
- HSMs von Utimaco, Thales, Bull, SafeNet

## Referenzprojekt

Mit fast 30 Millionen Einwohnern ist Ghana ein wichtiges Land in Westafrika. Als großes Zukunftsprojekt hat die ghanaische Regierung einen elektronischen Personalausweis, die GhanaCard, eingeführt. Die GhanaCard kann nicht nur als Identitätsdokument, sondern auch als Passersatz innerhalb der westafrikanischen ECOWAS-Region verwendet werden. Darüber hinaus ermöglicht die GhanaCard eine starke Authentifizierung – als sicherer Passwort-Ersatz für Online-Dienste. Auch digitale Signaturen und Zahlungen werden unterstützt.

Bei der Realisierung der GhanaCard setzt die ghanaische Regierung auf die Technologie von cryptovision. Sowohl die Software auf der GhanaCard als auch die zugehörige Public-Key-Infrastruktur (PKI) und der Token-basierte Zugang zur PKI wurden von cryptovision implementiert. Die Zertifizierungsstellen (CAs) werden mit CAmelot betrieben. Die PKI der GhanaCard, die für 16 Millionen Zertifikatsinhaber entwickelt wurde, ist eine der modernsten weltweit.

Am 15. September 2017 erhielt der ghanaische Präsident Nana Akufo-Addo die erste GhanaCard.

### KUNDEN

CAmelot wird (unter anderem) von folgenden Kunden genutzt:

- Identitätsbehörden von Schwellenländern: Die Bürger mehrerer Schwellenländer erhalten eID-Karten mit privaten Schlüsseln und Zertifikaten.
- Deutscher Rüstungslieferant: Verwendet CAmelot zur Authentifizierung.
- Autohersteller: Ein japanischer Automobilhersteller verwendet CAmelot zum Schutz der internen IT-Infrastruktur.

## cryptovision

Die cryptovision GmbH ist ein führender Spezialist für moderne, benutzerfreundliche Kryptografie und sichere elektronische Identitäten. Über 250 Millionen Menschen und zahlreiche Institutionen weltweit schützen sich mit cryptovision-Lösungen gegen Hacker-Angriffe, Manipulation, Identitätsmissbrauch und Spionage.

cryptovision ist in zahlreichen Branchen aktiv – unter anderem im öffentlichen Sektor, im Gesundheitswesen, in der Automobilbranche, im Finanz- und Versicherungswesen, in der Energieversorgung und der Informationstechnik. Zu den cryptovision-Kunden gehören Staaten wie Nigeria, Ghana und Ecuador; staatliche Organisationen wie die Bundeswehr, das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Stadt New York, sowie Unternehmen wie E.ON, Volkswagen und Allianz. Seit dem 31. August 2021 ist cryptovision ein Teil von 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