Technical Data Sheet

cryptovision CAmelot

Certificate Lifecycle Management for Government and Enterprises

cryptovision CAmelot empowers you to operate a Certification Authority (CA) that is tailor-made to your individual needs. It is ideal for governments issuing digital certificates for electronic identity (eID) documents, as well as for enterprises managing their own internal PKIs. Thanks to its modular design, CAmelot offers seamless scalability—from simple test CAs to large-scale PKI environments.

Functions	• Advanced CA solution for sophisticated PKI environments • Consists of modules for certificate generation, publishing, revocation, renewal, role-based administration and more • Various pre-installed Certificate Templates (e.g. client authentication, server authentication, Windows smart card logon, OCSP server, code signing, domain controller, EFS, EFS recovery, email signature, email signing, Sub CA, Document Signer, Document Verifier) • Certificate management via web interface • Logging via Apache Commons Logging • Monitoring

Features	• Fully modular architecture:
	  • Every component can be customized or replaced separately to build the CA you want
	• Java-based and therefore platform independent:
	  • Change of the OS any time
	  • Sub-CA may run on another platform than CA
	• Makes PKI a feature of Identity Management:
	  • CAmelot can be integrated into virtually any LDAP-based data vault including identity management systems
	• Scalable from small special-purpose PKIs to nationwide government PKIs
	• Future-proof technology with
	  • multi-tenancy
	  • X.509 and cv certificate
	  • OCSP
	  • CRLs
	  • ECC
	  • Support of smart cards / USB tokens / HSMs
	• TR-03129 support

Technical Data Sheet - CAmelot

Scope of Supply	Standard, customizable modules and additional ones for higher security level, more convenience or further applications:
	• **CA Modules**: core component
	  • X.509 CA
	  • CSCA, DVCA, CVCA
	• **Access Module**: for access control within the CAmelot architecture
	• **Protocol Handler Modules**: communicate with management console
	• **Publisher Modules**: for publishing certificates via LDAP, data-bases and files
	• **Key Manager Modules**: communicate with the key stores (HSMs, smartcards or key files)
	• **Certifier Modules**: assemble the content of digital certificates and prepare them for signing
	• **Certificate Template Modules**: for certificate extensions
	• **Revocation Modules**: manages and encodes CRLs
	• **Scheduler Modules**: for handling recurring jobs like certificate renewal and update of CRLs
	• **Notification Modules**: notify users and administrators (i.e. in case of an error or to remind for renewal)
	• **Service Modules**: for PKI related services like Document Signer according to [9303v2], CMC, OCSP
	• Additional application:
	  • Auto-enrolment for workstations (**workstation/cic**)

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

Technical Data Sheet - CAmelot

Supported Applications	**X509** • Certificate-based login to Linux, Active Directory, Lotus Notes • NetIQ (formerly Novell) eDirectory • SSL authentication (Internet Explorer, Firefox, ...) • Certificate-based login to NetWeaver Portal • Login Client • Digital signature and encryption for emails (GreenShield, Mozilla Thunderbird, Outlook, HCL Notes) • VPN protection (Check Point, Windows, Cisco, NCP) • Disk encryption with Pre-Boot Authentication: • Signing of documents with IDnomic Sign MS Office, Open Office, LibreOffice, Adobe Acrobat • Microsoft Terminal Server and Citrix XenApp protection • Encrypted and signed data according to S/MIME, PKCS#7, XML • Encryption, XML Digital Signature, and other formats and many others • Identity documents: passport, electronic identity card, driving license, health card, signature card and many others
Supported Certificate Types	**X509 certificate types** (examples) • CA and Sub CA • TLS Client Authentication and TLS Server certificates • Domain Controller • Code Signing • Email (signing, encryption, signing and encryption) • Windows Smart Card Logon • OCSP Server • Masterlist signer and Deviationlist signer **CV certificate types** (examples) • CV CA • DV • Inspection System, Terminal Authentication and Signature Terminal

Technical Data Sheet - CAmelot

Supported HSMs	• Utimaco • Trustway
Supported Platforms	• CentOS 6/7 64 bit • Redhat 6/7 64 bit
Supported Algorithms	• RSA (up to 16384 bit) depending on HSM • ECC (up to 571 bit) depending on HSM • SHA-1 • SHA-2
Supported Data Bases	• Oracle • MySQL • MSSQL • H2
System Requirements	For CentOS / Redhat: • Java 17 • LDAP-capable user directory service

Trust Seal
www.teletrust.de/itsmie

Eviden Digital Identity
cv cryptovision GmbH
Munscheidstr. 14
D 45886 Gelsenkirchen

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

www.cryptovision.com