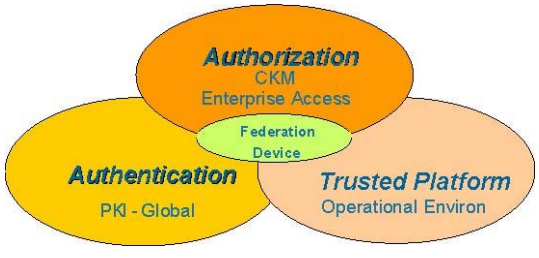
Technologies Juxtaposed: PKI & CKM®- A Winning Combination

Do PKI and CKM® relate and if so, how?

These technologies are complementary in application and CKM® products are designed accordingly. CKM® is interoperable with all of the leading PKI vendors (see attached overview) and has incorporated PKI functionality into its CKM® Desktop product.



Viewing assured information in a federated manner presents three basic components:

- An *Authorization* system that controls rights of users on networks - where authorized
- An *Authentication* system that verifies the identity of users – as they move about
- A *Trusted Platform* on which to operate

Authorization

CKM® applications permit the Enterprise Owner to establish controls for access to and protection of information on the network. The Enterprise is able to distribute, manage and revoke single or multiple rights, or authorizations for each user; even involving multiple applications, including over numerous domains. The Enterprise Owner defines domains, defines the authority of each domain and establishes authorization policies and standards.

CKM® is a standards-based key management system that grants and administers authorizations and enforces them cryptographically. The encryption system also provides persistent content protection. Message encryption takes place with the originator at the client.

Keys are created for the message and destroyed. Keys are not transferred, nor are they stored. Key recovery is 100%; but only through the Enterprise owner. The server does not have to be involved in the transmission of an encrypted message. The message recipient with the right authorizations can decrypt the message (or that portion of the message she/he is allowed to see).

CKM® provides dynamic assured information sharing at the Basic Robustness level and is consistent with DOD Directive 8500 (1&2). CKM® is designed for one-to-many communications.

Authentication

PKI – designed primarily for one-to-one communications – supplies the Authentication component and provides its own key management mechanism that offers a mathematically precise way to authenticate

that a source or action originated from a recognized point or party. In addition, by policy adherence, a level of non-repudiation can be associated to that source or action.

Stated another way, PKI substantiates a specific numeric value, assigns it to a specific person or action in a mathematical process. The verifying action is then a complementary mathematical process attested to by a trust system. In this manner, PKI serves as a mechanism for Identification (John Doe is precisely the John Doe who lives at 515 Main Street, Dublin, Ohio, who was born in Columbus on November 5, 1970 and is a US citizen). PKI authenticates this identity electronically.

Trusted platform

CKM® and PKI can be supported on a trusted platform where supplementary security and assurance enhancements are available. These security enhancements may be found in designated operating systems, platforms, or selected hardwire devices.

Summary

The juxtaposition of CKM® and PKI on a Trusted Platform (including on a hard token) provides a federated system that enables:

- Assured information sharing within a need to know environment
- Secure one-to-one and one-to-many communications
- End-to-end security
- On-line or off-line capability
- Persistent protection of information down to the object level (transit & storage)
- 100% key recovery
- Authentication and identification
- Revocation
- Scaleability – large scale
- Non-repudiation
- Confidentiality
- Authorization and role based access control – enforced through cryptography

An overview of existing PKI product's interoperability with CKM® follows.

Copyright 2010
All Rights Reserved

PKI Interoperability with CKM®[1]

Interoperable with CKM Desktop / RTE	CKM Cryptographic Service Provider (1024 bit keys)	Revocation Checking: CRL DP[2]	Revocation Checking: OCSP[3]	Client Authentication (bilateral SSL)	S/MIME[4]
ACES (issued by DST)	Yes	Yes	Yes	Yes	Yes
Alacris	n/a	Yes	Yes	Yes	Yes
Baltimore UniCERT v3.5.3	Yes	Yes	n/a	Yes	Yes
beTRUSTed	Yes	Yes	Yes	Yes	Yes
CertCo CertValidator	n/a	No, next update field is not present in CRL	Yes	n/a - no private key	n/a - no private key
Comodo	Yes	Yes	n/a	unknown	n/a
Comtrust	Yes	No	n/a	Yes	Yes
Digital Signature Trust (DST)	Yes	Yes	Yes	Yes	Yes
DoD IECA (issued by DST)	Yes	Yes	n/a	Yes	Yes
e-Certify	Yes	Yes	n/a	Yes	Yes
Entrust PKI v6.0	Yes	Yes	n/a	Yes	Yes
GeoTrust	Yes	Yes	n/a	Yes	Yes
Global Sign	Yes	No, cert does not have CRL DP field	n/a	Yes	Yes
iPlanet Certificate Management System v4.2 SP2	Yes	Yes	Yes	Yes	Yes
Ksign PKI 2.0	n/a	Yes	Yes	Yes	Yes
Microsoft Windows 2000 PKI	Yes	Yes	n/a	Yes	Yes
Microsoft Windows Server 2003	Yes	Yes	n/a	Yes	Yes

[1] Internal testing with the exception of RSA Security. RSA Security also performed testing of CKM products and certified them as RSA Secured Keon Ready.
[2] Certificate must have CRL Distribution Points field (with a URL).
[3] Certificate must have Authority Information Access field.
[4] Tested using Microsoft Outlook 2000 to send a signed message with the certificate and key pair stored on a CKM Token.

Interoperable with CKM Desktop / RTE	CKM Cryptographic Service Provider (1024 bit keys)	Revocation Checking: CRL DP[2]	Revocation Checking: OCSP[3]	Client Authentication (bilateral SSL)	S/MIME[4]
OpenValidation	n/a	No, cert does not have CRL DP field	Yes	Yes	Yes
QuoVadis	n/a	Yes	No -only supports https	Yes	Yes
RSA Security Keon CA v6.0.2	Yes	Yes	Yes	Yes	Yes
SafeScrypt	Yes	Yes	n/a	Yes	Yes
SmartTrust	n/a	No, next update field is not present in CRL	n/a	Yes	n/a -no email address in cert
SSH Communications Security	Yes	Yes	Yes	Yes	Yes
Sun ONE Certificate Server v4.7	Yes	Yes	Yes	Yes	Yes
SwissSign	Yes	No, cert does not have CRL DP field	n/a	Yes	Yes
SyntheSys idSure	Yes	No, cert does not have CRL DP field	n/a	unknown	Yes
TC Trust Center	Yes	No, cert does not have CRL DP field	n/a	Yes	Yes
Tumbleweed Valicert Validation Authority	n/a	Yes	Yes	Yes	Yes
VeriSign Managed PKI v5.0	Yes	Yes	Yes	Yes	Yes
Wild ID	n/a	Yes	n/a	Yes	Yes
WISeKey	Yes	Yes	n/a	Yes	Yes

Testing Environment: Dell Dimension machine (Pentium III, 866MHz, 256MB RAM), Microsoft Windows 2000 Professional OS, Office 2000

Please Note: n/a = product did not support this feature during testing; unknown = unable to test this feature