

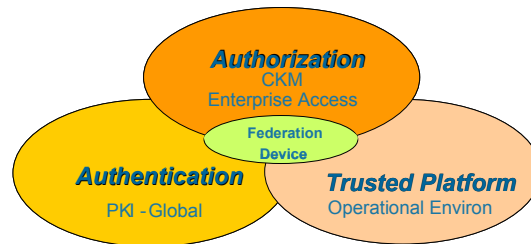
# Technologies Juxtaposed: PKI & CKM<sup>®</sup> - A Winning Combination

## 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 hardware 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.

## PKI Interoperability with CKM<sup>®1</sup>

<i>Interoperable with CKM Desktop / RTE</i>	<i>CKM Cryptographic Service Provider (1024 bit keys)</i>	<i>Revocation Checking: CRL DP<sup>2</sup></i>	<i>Revocation Checking: OCSP<sup>3</sup></i>	<i>Client Authentication (bilateral SSL)</i>	<i>S/MIME<sup>4</sup></i>
<b>ACES (issued by DST)</b>	Yes	Yes	Yes	Yes	Yes
<b>Alacris</b>	n/a	Yes	Yes	Yes	Yes
<b>Baltimore UniCERT v3.5.3</b>	Yes	Yes	n/a	Yes	Yes
<b>beTRUSTed</b>	Yes	Yes	Yes	Yes	Yes
<b>CertCo CertValidator</b>	n/a	No, Next Update field is not present in CRL	Yes	n/a - no private key	n/a - no private key
<b>Comodo</b>	Yes	Yes	n/a	unknown	n/a
<b>Comtrust</b>	Yes	No	n/a	Yes	Yes
<b>Digital Signature Trust (DST)</b>	Yes	Yes	Yes	Yes	Yes
<b>DoD IECA (issued by DST)</b>	Yes	Yes	n/a	Yes	Yes
<b>e-Certify</b>	Yes	Yes	n/a	Yes	Yes

<sup>1</sup> Internal testing with the exception of RSA Security. RSA Security also performed testing of CKM products and certified them as RSA Secured Keon Ready.

<sup>2</sup> Certificate must have *CRL Distribution Points* field (with a URL)

<sup>3</sup> Certificate must have *Authority Information Access* field.

<sup>4</sup> Tested using Microsoft Outlook 2000 to send a signed message with the certificate and key pair stored on a CKM Token.

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

<b>Entrust PKI v6.0</b>	Yes	Yes	n/a	Yes	Yes
<b>GeoTrust</b>	Yes	Yes	n/a	Yes	Yes
<b>Global Sign</b>	Yes	No, cert does not have CRL DP field	n/a	Yes	Yes
<b>iPlanet Certificate Management System v4.2 SP2</b>	Yes	Yes	Yes	Yes	Yes
<b>Ksign PKI 2.0</b>	n/a	Yes	Yes	Yes	Yes
<b>Microsoft Windows 2000 PKI</b>	Yes	Yes	n/a	Yes	Yes
<b>Microsoft Windows Server 2003</b>	Yes	Yes	n/a	Yes	Yes
<b>OpenValidation</b>	n/a	No, cert does not have CRL DP field	Yes	Yes	Yes
<b>QuoVadis</b>	n/a	Yes	No - only supports https	Yes	Yes
<b>RSA Security Keon CA v6.0.2</b>	Yes	Yes	Yes	Yes	Yes
<b>SafeScrip</b>	Yes	Yes	n/a	Yes	Yes
<b>SmartTrust</b>	n/a	No, Next Update field is not present in CRL	n/a	Yes	n/a - no email address in cert
<b>SSH Communications Security</b>	Yes	Yes	Yes	Yes	Yes
<b>Sun ONE Certificate Server v4.7</b>	Yes	Yes	Yes	Yes	Yes
<b>SwissSign</b>	Yes	No, cert does not have CRL DP field	n/a	Yes	Yes
<b>SyntheSys idSure</b>	Yes	No, cert does not have CRL DP field	n/a	unknown	Yes
<b>TC Trust Center</b>	Yes	No, cert does not have CRL DP field	n/a	Yes	Yes
<b>Tumbleweed Valicert Validation Authority</b>	n/a	Yes	Yes	Yes	Yes

<b>VeriSign Managed PKI v5.0</b>	Yes	Yes	Yes	Yes	Yes
<b>Wild ID</b>	n/a	Yes	n/a	Yes	Yes
<b>WISeKey</b>	Yes	Yes	n/a	Yes	Yes