

KMI Key Management Infrastructure



"Information assurance enhances technology advantage."

### What KMI Means

A challenge ... A vision ... An architecture ... A roadmap ... A community effort ...

# The Challenge

### Information Assurance (IA) in a time of change.

The challenges and opportunities for achieving IA are different in the 21st Century. New technology has transformed the security environment. The web, high-powered personal computers, digital wireless communications, a thriving commercial information security industry — all have profound IA implications.

The same forces that gave birth to online retailing and computer banking will now impact how security solutions are delivered as well. Mere functional performance is no longer enough. Users want security products that deliver true technology advantage.

The power of information technology is no secret. As technology improvements accelerate, so too will demand for the benefits that such improvements bring. To unlock the power of technology, to keep pace with users' security demands, that is the challenge of the KMI.

We call this concept transparent security. It says that *information assurance enhances technology advantage*. It means that solution providers and users can achieve constantly improving information assurance as a matter of routine with minimum cost and distraction.

**The KMI** exploits the opportunity to use new technology for what it does best — remove barriers, including those imposed by traditional information assurance measures, such as:

- Labor-intensive methods to provision hardcopy cryptographic products
- Incompatible cryptographic products and systems
- Separate security infrastructures ("stovepipes") each with its own tools, methods, and training to obtain products and services
- © Closed security architectures with limited ability to incorporate upgraded technologies, new applications, additional user populations, or innovative deployment strategies and scenarios

It is to meet *both* the challenges and opportunities of the new environment that the National Security Agency has defined the KMI as the key to transparent security.

## Mere functional performance is no longer enough.

# Users want security products that deliver:

- Dramatic cost reductions, improved operating flexibility, greater mobility, and more advanced features
- Faster deployment of capabilities with solutions that are more specifically tailored to their particular situations
- Improved collaboration across geographic, organizational, and functional boundaries
- The convenience and flexibility of users serving and servicing themselves

### KMI CAPABILITIES WILL SUPPORT

Wireless and web-based distribution and management of keys 24x7

Direct "hands free" connection between security applications and the key management systems that support them

Ability to leverage and interoperate with commercial key and certificate management products and services

Use of common hardware and software across different user domains with different levels of assurance (trust) and sensitivity (classification)

Interoperability across user domains: geography, job function, affiliation, security class, etc.

*Users who exist within multiple domains simultaneously (e.g., may have multiple affiliations and multiple classifications)* 

In other words, the goal is to make the KMI a 21st Century key management infrastructure designed to achieve maximum usability, security, trust, performance, and availability for operators, users, and security applications.

# The Vision

#### Unified key management.

The NSA launched the Key Management Infrastructure (KMI) Strategic and Architectural Planning initiative in January 1999, supported by the CINCs, Services, Agencies, Joint Staff, and contractor personnel within the DoD. The initiative envisions an evolutionary migration from the current labor-intensive, fragmented, and closed infrastructure to one that is highly automated, unified, and extensible. The mission is sweeping: to define a single framework for modernizing and unifying the management of keys used to encode and decode information throughout the entire National Security Community. Over time, this initiative will touch every application and security measure used by members of this community.

These applications include messaging, file encryption, electronic commerce, file transfers, database transactions, access to web servers, and other applications, including command and control and combat support. Security measures comprise the various layers of a Defense in Depth strategy, including workstations, firewalls, routers, in-line network encryptors, software applications, and trusted database servers.

In all these areas, the KMI provides the framework with which to achieve the elements of information assurance:

- © Confidentiality —privacy of information
- Output Authentication restriction of access
- Integrity protection from tampering
- Non-repudiation proof of receipt

The goal is to realize an infrastructure that can embrace existing applications, networks, computing platforms and security measures while fully exploiting the capabilities of new technology as those appear over the horizon.

# The Architecture



#### Modular, distributed, standards based.

The fundamental advantage of the KMI versus previous code management approaches is the KMI architecture — consisting of three nodes: product source, management and client. This approach uses the fact that key management services typically call upon the same functions (e.g., registration, ordering, distribution) and that these can, therefore, be offered as a unified set of processes. They need not be redundantly "hardwired" into multiple products (e.g., cryptographic applications). In the KMI, multiple product sources and customers (clients) connect to the same management node via common interfaces. These standard interfaces are carefully optimized for building "plug and play" systems from many different components.

#### Benefits include:

- Best-of-breed" products that are available faster without retrofitting legacy systems
- Consistent policies and procedures easily established within and across product and user types
- Both new and existing products supported from one system
- Functions accessible from standard web browsers
- Management and product upgrades require no client upgrade
- Any deployment scenario easily accommodated from centralized to decentralized

### EXTEND AND ADAPT THE KMI WHERE NEEDED . . .

A small set of standard components (PSN, CSN, PRSN, clients) simply plug into each other over the Internet or private networks. KMI thus provides a framework for unified key management on a global scale yet is easily configured to satisfy virtually any set of local or regional requirements. KMI is equally suitable whether provisioning forward deployed protected enclaves or allowing "one button" distribution of sensitive but unclassified documents across domain boundaries.



## . . . TO DEPLOY FUNCTIONS AS NEEDED

Component	Function:
PSN	Product Source Node: Key generation Product production Cestificate creation
CSN	Central Services Node: Master store & replication Root certificate authority System management monitoring Long term archive KMI security management
PRSN	Primary Services Node: Registration Role & privilege assignment Order processing & distribution Tracking & control Directory Library Key recovery Help desk Local security management
Clients	KMI managers Requesting services Ordering Key distribution Key receipt Product/service use

# The Roadmap

# FROM STOVEPIPE NSA/DISA X.509 Commercial X.509 electronic applications Manual Systems NSA/DISA X.509 Commercial X.509 electronic Annual Systems Annual electronic Annual Systems Commercial X.509 electronic Annual Annual <

### The goal of KMI is security transparency -

to remove information assurance as an impediment to operational efficiency and effectiveness. Consistent with that goal is a transition to the KMI that is equally transparent. A major reason for the KMI architecture is, in fact, to allow for technology "encapsulation" — the use of external pieces of technology, including legacy components already in place and familiar to users. This will enable a smooth transition to new components, from multiple sources, as these components are introduced over time. Accordingly, the transition to the KMI will be guided by three principles:

- To support existing solutions until more compelling alternatives become available
- To build on parallel initiatives
- To employ a "phased iterative" approach to development

The KMI will be implemented as a series of capability increments, fielded every 18 to 24 months, that carefully build on components that already exist. This incremental strategy allows for the provisioning of urgently needed functional capabilities on a relatively short schedule without encountering the delays and requirements growth that can derail large programs. It also reduces developmental cost and schedule risk and takes advantage of new technology sooner. Each increment will add new and unifying functionality, platforms, products, or services, and may modify and integrate existing capabilities (including those defined in previous increments). Thus, the KMI roadmap allows for integrating requirements changes smoothly and indefinitely.

## THE TARGET KMI

An early milestone is to establish a baseline capability, or Target KMI, that offers the following services:

Registration - Identifying individuals or system elements to the KMI

**Enrollment** – Authenticating the establishment, modification, and deletion of privileges for individuals, organizations, and system elements

**Ordering** – Handling requests for cryptographic product (e.g., keying material, certificates, manuals, etc.) to support a security application.

Generation – Generating cryptographic products (e.g., symmetric key, asymmetric key and/or a public key certificate) by an infrastructure element

Distribution - Providing physical and electronic products to the user in a secure, authenticated manner

**Policy Management** -- Managing and enforcing policy and procedures for operating the KMI in a trusted and secure manner

Trust Extension ~ Reviewing and ruling on issues of cross certification and/or bridging with other key management infrastructures

**Archiving** – Providing for long time storage and retrieval of important data that may not be immediately accessible to on-line users of the system

Accounting – Tracking the location and status of cryptographic products.

Key Recovery – Supporting recovery of cryptographic keys that are needed to recover encrypted information when the intended decryption key is unavailable

**Compromise Management** – Providing notification of compromised keys and invalid certificates in a timely and authenticated manner

Audit Data Repository -- Supporting periodic security evaluation of KMI operations

Library – Providing access to key management reference documents and information

# The Community Effort

#### To engage the customer.

The goal is to create an infrastructure that adapts to the user's world, not the other way around. The NSA is actively working to involve a broad coalition of participants in the KMI effort: the military services, civil and DoD agencies, US partners, and technology providers — both government and commercial. Members of these constituencies participate throughout the KMI organizational structure, on the KMI Senior Steering Group, and within the various planning teams and operational committees. Across a variety of forums — both formal and informal constituencies are sincerely invited to contribute their views regarding the KMI's technical and operational requirements and capabilities. Opportunities for feedback include customer focus groups, a number of which have been hosted jointly by the NSA and the

Defense Information Security Agency (DISA). In these sessions, representatives of Commanders-In-Chief, military departments, and agencies are asked to participate in a collaborative environment to better understand the customer's requirements.

As KMI development moves forward, active community involvement will be key to the ultimate success of achieving truly transparent security and a successful evolution to that goal. To find out how you might become involved in the KMI effort, to receive periodic status updates, or to simply learn more about the KMI, please contact the KMI management team at the address listed on the back of this brochure.

