CRYPTOGRAPHIC KEY MANAGEMENT WORKSHOP
Focus Paper
Computer Security Division, NIST
June 8-9, 2009

Key management has been identified as a major component of various national cyber security initiatives that address the protection of information processing applications. Numerous issues have been identified in the current key management methodologies that need to be addressed, including the lack of guidance, the scalability of the methods used to distribute keys and the usability of these methods. This workshop is intended to identify the inadequacies of the current key management methodologies, and to plan for a transition to more useful and appropriate key management methods.

The Cryptographic Key Management (CKM) workshop will be conducted by the Computer Security Division of NIST to identify and develop technologies that will allow organizations, both Federal and domestic, to leap ahead of normal development life-cycles in order to vastly improve the security of sensitive and valuable computer applications. The workshop is the first step in a five year process to develop a key management framework and begin its implementation.

This paper describes the focus of the CKM workshop to be conducted at NIST on June 8-9, 2009. Participants must electronically register with NIST to either attend the workshop in the Administration Building on the NIST campus in Gaithersburg, Maryland, or participate in the workshop from remote locations via Web Cast connections. Remote participants will be able to view and listen to all proceedings of the workshop, submit questions in real-time to speakers via e-mail, and post comments following the workshop on an edited workshop bulletin board. For those unable to attend the workshop in person or participate remotely, an electronic copy of the workshop audio and video will be available on the NIST workshop website for thirty days following the workshop.

A question-answer format was selected for this focus paper to facilitate adding new questions submitted by the public prior to the workshop. All submitted questions will be reviewed, edited, answered, and possibly incorporated in future versions of the focus paper.

What is the purpose for the CKM workshop?

NIST is conducting the workshop in order to 1) identify future environments, the international enterprises likely to utilize them, the applications being performed in them, and a seamless array of key management mechanisms and protocols; 2) create a key management framework that will support the use of the cryptographic mechanisms used to provide security for these environments and applications, and 3) lay a foundation for a comprehensive plan in developing, standardizing, and adopting scalable, usable and secure key management practices.

The workshop will cover a broad spectrum of cryptography-based security mechanisms that are: 1) currently available, but under-utilized because they lack user-friendly automated key management services; 2) under development, but not reaching the marketplace because of financial, logistical, and support service problems; and 3) needed to support future computing environments, such as: "cloud" computing, integrated international applications, and dynamic personal and organizational relationships among people, governments, and global applications.

What is a key management framework?

A key management framework is a basic conceptual structure that is used to specify the high-level issues and requirements for secure key management and will be the initial product of the CKM workshop. The framework will provide a structure for defining key management architectures from which key management systems can be built.

The CKM framework is intended to define the components of a seamless set of technologies that will automatically create, establish, supply, store, protect, manage, update, replace, verify, lock, unlock, authenticate, audit, backup, destroy, and oversee all cryptographic keys needed for applications in the computing and communicating environments of the future. The framework will define the requirements for secure key management; the topics to be addressed include security policies, trust issues, cryptographic algorithms and key sizes for generating, distributing, storing, and protecting keys, key distribution, interoperable protocols, archiving, key recovery, key lifecycles, transparent user interfaces, etc.

What are some applications specifically to be addressed by the workshop?

Some large-scale applications to be addressed include the protection of critical infrastructure information, uniform (if not universal) health care, international finance, real-time national voting systems, integrated electronic commerce, international multi-media communications, long term information archives, Federal and State social services, and automatic data conversion conforming to technology changes, etc. New processing paradigms include Cloud/Web 2.0 and secure electronic personal data assistants capable of easily interfacing to personally private domains, such as family, finances, health, politics, religion, education, and professions. Special considerations include provisioning (i.e., providing needed parameters whenever and wherever needed) and maintenance of cryptographic keys for cryptography-based security mechanisms, and the long term integrity, availability, and confidentiality assurance of the keys used to protect data-at-rest (in short and long term storage).

What is involved in key management?

Cryptography is often an integral component in protecting information. Cryptographic technology includes data encryption algorithms, digital signature algorithms, data authentication algorithms, communication protocols to utilize and support the above, and

cryptographic key management. CKM includes policies for selecting appropriate key generation/establishment algorithms and key sizes, protocols to utilize and support the distribution of keys, protection and maintenance of keys and related data, and integration of key management with cryptographic technology to provide the required type and level of protection specified by the overall security policy and specifications.

Why is NIST leading this effort?

NIST is responsible for developing standards for Federal use and assisting national or international standards bodies in producing a range of standards, including those for protecting information and its processing. NIST has a long history of developing and standardizing cryptographic technology and its associated key management provisions. In fulfilling its responsibilities, NIST has established working relationships with security system developers, academic researchers, commercial vendors, government and public sector computer users, and network operators in developing and utilizing effective information security standards. As a result, NIST is in a unique position to facilitate discussions of the problems associated with the current key management methodologies and, in cooperation with the aforementioned sectors, to develop improved methods for current and future environments and applications.

Will the CKM workshop focus only on the framework?

The workshop agenda is broader than just defining the framework. Keynote speakers are being invited to present their perspective of the present and their predictions for the future in several areas: computing, communications, and cryptography. These will be broader than just security. The focus of these presentations will be: Where are we now? Where should we go? How can we get there? The speakers are being selected based on their outstanding contributions to these fields, so they are also asked to recall lessons learned from their experiences. All participants are invited to submit written statements on these broad topics. They should specifically address how seamless cryptographic protection could be integrated into future applications and how cryptographic keys could be automatically provided whenever and wherever required with whatever type and level of protection is desired.

What are some specific topics that should be discussed during the CKM workshop?
(Note to prospective participants: recommendations for specific additions to the following list may be made by email to the workshop organizers. Please check the CKM workshop website. These recommendations will be reviewed and may be integrated in the list, but without attribution.)

Specific topics might include:

- Computing, communications, and cryptography in the future;
- Pre-determined (known and selected by the application initiator) and undetermined “cloud” computing environments;
- Non-specified, but acceptable attributes of data sources and computing resources of an application;

- Establishing and assuring trust in future processing environments;
- Pointers to, and short descriptions of, on-going CKM development projects targeted for the next few years;
- Migration from "trusted, closed" environments to unknown, dynamic environments;
- CKM key generation, establishment, distribution algorithms and protocols;
- User and vendor acceptance of the NIST specified CKM.

Alternatives to cryptography for protecting the communications of future applications could be explored. The submission of suggestions for forward-thinking, alternative key management solutions for future applications is encouraged.

What are some future directions of the CKM project?

Research and development must be conducted to complete the comprehensive security perimeter around all sensitive data and critical services available in the "cyber-cloud" of the future. Technology and procedures must be developed, standardized, and automatically instantiated, based on a dynamic risk environment monitored by the network, the provider, and the user.

How can I participate and what might be the results?

Interested parties can participate in the CKM workshop, either locally or remotely, or view the workshop recordings that will be available for a period of 30 days after the workshop. There will be a 30 day period following the workshop during which comments and contributions may be submitted to the CKM activity.

NIST intends to post a draft CKM framework for public comment in the fall of 2009. NIST will use the framework to develop key management guidance and to prepare possible workshops to discuss CKM-related activities. Comments on this draft framework will be solicited from the public.