# NIST Cryptographic Key Management (CKM) Program
# Cryptographic Key Management System (CKMS) Project
# Frequently Asked Questions (FAQs)

1. **Why is Cryptographic Key Management (CKM) so important?** CKM 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 current key management methodologies that need to be addressed, including the lack of technical and operational CKM guidance, the poor scalability of the methods used to distribute cryptographic keys, and the general lack of user-friendliness of these methods. This project is intended to identify the inadequacies of the current key management methodologies, and to assist in making a transition to more useful and appropriate key management methods.
2. **What is involved in Cryptography, CKM, and CKMS?** Cryptography is a fundamental and integral component for protecting information during communications and in some data storage media. Cryptographic technology includes, but is not limited to, data encryption algorithms, digital signature algorithms, data authentication algorithms, communication protocols to utilize and support these algorithms, and cryptographic key management. CKM includes the policies for selecting appropriate key generation/establishment algorithms and key sizes, the key establishment schemes and protocols to utilize and support the distribution of keys, the protection and maintenance of keys and related data, and the integration of key management with cryptographic technology to provide the required type and level of protection specified by the overall security policy of an organization. Cryptographic Key Management Systems are the components of CKM that are automated to perform the services required in creating, distributing, and managing keys used in all cryptographic applications.
3. **What are the goals of the Project?** The NIST Cryptographic Key Management Systems (CKMS) Project is a set of tasks within the Federal Cyber Security Program that was created to greatly improve the security of information within National and International critical automated processing applications. The goals are to provide a CKMS Design Framework, a set of profiles, and a CKMS conformance testing program that will result in the availability of secure and interoperable cryptographic key management systems. Profiles for secure CKMS for both Federal and commercial information systems may be developed, and programs for testing conformance of the designs of the CKMS to both the Framework and the profiles are planned, subject to sufficient funding and user interest.
4. **What activities have been conducted to date on the Project?** NIST initiated the CKMS Project in early 2009 by assembling a team of experts in cryptography with extensive experience in technology and standards development; conducting a workshop in June 2009 to collect information on the current status and long term goals for improving CKMS; and drafting a Framework for Designing CKMS.

NIST is also currently planning a second, more technically-focused workshop to be conducted on September 20-21, 2010, at NIST.

5. **What was the purpose for the NIST CKM workshop held in June 2009?** NIST conducted the workshop to identify problems with the currently implemented key management systems, to identity future secure information processing environments, international enterprises likely to utilize key management systems, and applications potentially being performed in them, and to discuss the possibility of a seamless array of key management mechanisms and protocols. It was focused on how to create a key management framework to be used in designing a CKMS that will support the use of the cryptographic mechanisms used to provide security for these environments and applications in order to lay a foundation for developing, standardizing, and adopting scalable, usable and secure key management practices. The workshop covered a broad spectrum of cryptography-based security mechanisms that are: 1) currently available, but may be 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
6. **What are the goals of the 2010 NIST Workshop on CKMS Design?** This Workshop will focus on two objectives: to provide technical feedback to NIST on the contents of the Draft Framework for Designing a CKMS and to assist in defining requirements and constraints for a Profile of Secure CKMS for Federal Applications (Profile).
7. **What is a CKMS design framework?** A Cryptographic Key Management System design framework is a conceptual structure that is used to specify the high-level issues and basic design requirements for secure key management. Such a framework provides a structure for defining key management architectures from which key management systems can be built. The CKMS design framework defines the components for a CKMS that will 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 defines requirements for key management system design that cover 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.
8. **What is the status of the Framework?** The Draft Framework was posted for public comment by NIST as draft SP 800-130 on June 16, 2010 on its Website www.nist.gov. Written comments on the 88 page document may be submitted by sending email to ckmsdesignframework@nist.gov by August 17, 2010. The comments will be analyzed by the NIST CKMS Project team and subsequently discussed at the September CKMS Workshop. The final CKMS Design Framework publication (SP 800-130) will reflect these comments and discussions.

9. **What is the status of the Profile for?** An outline of this Profile has been created based on the CKMS Design Framework, but no draft of the Profile will be available until after the September CKMS Workshop. Detailed development work will then be initiated by the NIST CKMS Team.
10. **What are the differences between a standard, a framework, and a profile?** A standard is an established norm or a set of specifications on any specific topic that can or must be followed or "conformed to" by its intended audience. NIST creates Federal Information Processing Standards (FIPS), and Guidelines (e.g., NIST Recommendations) that are published as NIST Special Publications (SPs). Many other organizations (e.g., American National Standards Institute, Institute of Electrical and Electronic Engineers, and the Organization of International Standardization) also publish standards. A framework is a detailed description or specification of the components of a specific topic (e.g., houses, computers, cryptographic key management systems). A profile is a selection of a subset of possible components that can or must be selected from a Framework to achieve one or more specific goals (e.g., security, interoperability, compatibility).
11. **Will the CKMS Design Framework and the Profile be published as standards or guidelines?** NIST and many other organizations can and do develop standards and technical recommendations on various topics. FIPS are often published by NIST on special technical topics where compatibility, interoperability, or a predetermined level of security are required. Technical recommendations are sometimes published when a FIPS is not required, but specific technical information and guidance are needed to achieve specific goals. The CKMS Design Framework will be published as a NIST SP as a useful tool to design, specify and compare implementations of a CKMS. It will contain specific requirements that the CKMS designer must satisfy in order to claim conformance to, or conformance with, the Framework. It will not assure interoperability or security of conforming CKMS. However, the Profile is intended to assure defined levels of security and specify certain interfaces for interoperability. Its specifications and requirements are intended for Federal organizations implementing or procuring CKMS systems in the future. Comments on the Framework and Profile will be solicited and discussed during and subsequent to the September CKMS Workshop.
12. **Will there be other CKMS Profiles developed?** It is hoped that other organizations will use the Framework to develop profiles appropriate for their environments, thus improving key management globally. NIST has the responsibility for developing standards and guidelines for improving the security of U.S. Federal information processing systems handling valuable and sensitive, but unclassified, applications and information. NIST will work with organizations responsible for, or interested in, developing profiles in similar areas but outside its specific authorized areas.
13. **Will there be other CKMS Frameworks developed?** One goal of the CKMS Project was to develop a single comprehensive and extensible Framework that satisfied everyone's requirements in this area. The Framework is intended to accommodate all existing and future CKMS in general, but will not specify all the

embodiments and implementations of the fundamental components. If the Framework fails to satisfy this goal, it will be modified as needed.

14. **What tests, testing procedures, and testing facilities are planned for supporting the CKMS Project?** NIST has developed numerous specifications, procedures, and facilities for testing conformance to the standards and guidelines it is responsible for developing and supporting. The scope and content of the tests to support this Project are still under discussion and are subject to interest and available resources. The general CKMS structure, applicable architectures, and potentially useful tests will be subjects of discussion at the September Workshop.
15. **What "Leap Ahead" Security Technologies are needed for future cell phone, wireless Internet, personal digital assistant, cloud computing, and widely-dispersed safety and security monitoring applications?** It is a goal of the CKMS Project team to create a flexible, robust, and useful Framework for designing CKMS that are useful for a broad spectrum of future applications requiring dynamic security measures to satisfy their needs. Much like many of today's service industries and support infrastructures (such as the ubiquitous electrical system, the automobile industry with a competitive but widely-distributed gasoline supply system, and interoperable national and international telecommunication systems based on a variety of technologies), automated secure systems with closely-coupled key management support systems can also be created. Standards and guidelines are needed in secure key management to satisfy the requirements for cost-effective protection in future applications. Advanced technologies implementing and enforcing the formal specifications of security policies are also needed. Automated key distribution that provides keys whenever and wherever they are needed must be available. Digital rights management and protection will be required, and keys must be available whenever digital access is authorized. Other examples will be explored at the September CKMS Workshop.
16. **What CKMS areas may need to be further addressed in NIST SP 130?** Formal security specification languages were discussed, but the team reached no consensus on the use of formal languages. Automated keying in high-risk environments (such as widely distributed motion detection or other security monitoring environments) was not addressed. Cloud computing was discussed, but firm requirements have not been established for how computing associations would be monitored in the future. Critical infrastructures have been identified in other government security investigations, but were not factored into the initial draft Framework.
17. **What on-going research and development efforts exist in government, commercial, or international environments that should be reviewed and considered for incorporation in the CKMS Design Framework?** Ongoing research and development activities supportive of our tasks will be a topic of the September workshop. Major research support organizations in this area include DARPA, NSF, NSA, and consortia of industrial groups.
18. **What applications (e.g., financial, medical, publishing, communications, etc.) or enterprises (e.g., FDIC, NYSE, Life Insurance) should be considered in developing other profiles?** This topic will be discussed during the September workshop.

19. **Why is NIST leading this effort?** NIST is responsible for developing Standards and Guidelines for the protection of sensitive, but unclassified, U.S. Federal information and for 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 Standards and Guidelines in 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 and Guidelines. 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.
20. **How can I participate and what might be the results?** Interested parties can participate in the CKMS workshop, either locally or remotely. A WEBCAST will be available for the general sessions of the workshop for listening to the presentations and viewing visual material. Remote participants can send questions via email during these sessions. No published proceedings or summary of the workshop will be produced by NIST. Details for registering and participating in the Workshop will be posted at http://csrc.nist.gov/groups/ST/key_mgmt/.