Summary of the Workshop
On
Cryptographic Key Management Systems (CKMS)

National Institute of Standards and Technology

September 10-11, 2012

Background

Cryptographic Key Management (CKM) is a fundamental part of cryptographic technology and is considered one of the most difficult aspects associated with its use. Of particular concern are the scalability of the methods used to distribute keys and the usability of these methods. NIST has undertaken an effort to improve the overall key management strategies used by the public and private sectors in order to enhance the usability of cryptographic technology, provide scalability across cryptographic technologies, and support a global cryptographic key management infrastructure.

As part of the effort to improve key management, NIST has been developing a Framework for designing Cryptographic Key Management Systems (CKMS), which will be published as NIST Special Publication (SP) 800-130. To date, two versions of the document have been posted for public comment, followed by public workshops to discuss the draft document and the comments received during the public comment period. In addition, a Profile of the Framework document is being developed to customize the requirements in the Framework for the Federal government, and to provide guidelines for procuring, installing, configuring, operating and using a CKMS. When complete, the Profile document will be published as SP 800-152.

This document is a summary of the workshop held on September 10-11, 2012 to discuss the version of SP 130 that was provided for public comment in April of 2012, and to begin discussions on the requirements that should be included in the Federal Profile document (i.e., SP 800-152). A table containing an initial list of requirements for SP 800-152 was posted in August 2012 for public comment and for discussion at the workshop.

Workshop Summary

This summary was prepared by the CKMS team from notes taken during the workshop. A total of 51 participants were registered for the workshop, with another 106 viewing the web cast on September 10th, and 89 viewing on September 11th. The agenda and the slides used by each presenter are available at http://www.nist.gov/itl/csd/ct/ckm_workshop_2012.cfm. These presentations provided the workshop participants with the current status of key management issues, as well as possible solutions for the future. Please contact the presenter for further details

of their presentation. The summary of each presentation below includes a link to the specific slides used during the presentation.

Monday, September 10th

A. Welcome: Elaine Barker, NIST Cryptographic Technology Group, CKMS Team Leader. Ms. Barker welcomed the workshop participants and stated that the first day of the workshop would be devoted to the CKMS Framework and Profile, and the second day would be devoted to hard problems in Key Management.

B. Key Management in Historical Perspective: Whitfield Diffie, Internet Corporation for Assigned Names and Numbers.
Dr. Diffie provided his historical perspective of selected cryptographic systems and cryptographic key management, discussing the various phases of key management (from production through destruction), examining how these have been done in real systems, how they are affected by changing technology, and what have been the consequences of key-management failures. He also presented his views on the current problems in cryptographic key management, and what advances in cryptographic key management will be needed in the future. Some interesting points were:

1. Cryptography is an amplifier. Protecting a key is amplified to protecting the data.
2. Components of key management include production, shipping, storage, use, accounting, and destruction.
3. A good key must not be predictable when produced by a Key Management System. The randomness of keys is important, but non-predictability is more important.
4. His desiderata of keys: They should never be seen by humans, and must be easy to use, hard to copy, and easy to destroy.
5. Key distribution depends on key types, applications, and environments. Physical key distribution is expensive because humans and transportation are often involved. Electronic key production is generally less expensive, and electronic keys are easier to distribute.
6. Key Destruction methods have included dropping weighted code books into deep water from a ship, cutting wires on rotor cryptographic machines, burning paper tapes of keys, shredding codebooks, physically destroying memory modules that had contained keys, and overwriting with random bit patterns.
7. Changing keys immediately after their cryptoperiod expires is important. Users must change their passwords, PINs, and keys, as required. Key updating is easy, but has some problems (e.g., when a new key is based on an old key).
8. Key production (the current trend): Decentralization of key production means that less distribution required.
9. Future Key Management Issues:

- Who should pay for certificates? Should the certificate management systems be vendor driven or customer driven?
- Distributed Key Manufacture is a current theme. Is this more cost effective than central key manufacturing?
- Quantum Computing may someday ruin some current public key systems.
- What about using McEliece systems, knapsack systems and lattice-reduction-based systems in a post-quantum world?

C. Review of NIST SP 800-130: *Miles Smid, NIST Guest Researcher and CKMS Team Member.*

Mr. Smid provided an overview of the CKMS Framework provided in the latest draft of SP 800-130. Some salient points were:

1. The CKMS Design Framework lists the primary topics relating to a CKMS and specifies a large number of specification requirements that a CKMS designer must satisfy in the design documentation of a CKMS product.
2. The Framework does not specify what must be in a CKMS product, but only requires that the designer must describe, in the design documentation, what features are included in the product and how they are implemented and operated.
3. The Framework is not judgmental. It supports applications, but does not include applications. It uses the word "shall," but this may be changed in the final publication because it has caused some confusion among reviewers.
4. Framework advantages: The Framework provides a roadmap for designers to consider all factors of a comprehensive CKMS. The Framework is also a basis for the Federal Sector CKMS Profile; it is a foundation for Profiles of Requirements for a CKMS for various sectors, such as the Federal government and contractors, the health care industry, the financial industry, etc.
5. The Framework differs from Profile in several ways, including its scope, audience, use, requirements, etc.
6. Question: How should conformance of a product design be tested against the Framework? It is up to the product vendor and implementer to claim and assert conformance. NIST does not plan to establish such tests.
7. A CKMS designer must specify in the product design documentation what features are included in the product and how each feature operates. However, it is acceptable to state that a product does NOT implement some topic feature.
8. Procurement personnel can also determine if a product's design documentation conforms to the Framework because they will know that this product does not have this feature, while a competing product may have it. Every requirement on every topic must be addressed in the design, but it is up to the designer if a feature is not included in the CKMS design.

9. Question: How will government organizations be organized into security domains? Answer: Organizations may select which security domain (e.g., Health, Finance, Federal) they are in or choose to be in. They can create their own domain by defining a security policy for a group of users, computer applications, etc. Some organizations have several domains within their own organization already. For example, the legal department may have to label and protect its data differently than the technical department. Thus, the issue of the domain scope and specification depends strictly on which entities are following the security policy of that domain.
10. A primary benefit of a CKMS design complying with the Framework requirements is that organizations can more easily compare the capabilities of several CKMS products by comparing their designs using the Framework as a comparison template.
11. Final thoughts: CKMS security is very similar to the security of a typical computer system – the data of a CKMS are just keys and metadata, but these represent the data that must be given equivalent protection in the computer system.
12. Question: Is the Framework requiring too much documentation? There was no response from the participants.
13. Discussion question: Is the Basic Input/output System (BIOS) of a CKMS included in the components needing specification and testing? The BIOS should be included because it is part of a CKMS, and its security affects the security provided by the CKMS.
14. Participant comment: The Framework introduction should clearly differentiate between Framework conformance and Profile conformance.
15. Participant comment: Disaster recovery is a part of anomaly management. An operator needs to know what should be done in many situations, including emergencies. A CKMS designer should evaluate various anomalies of CKMS operation and provide guidance on what to do in each situation. A CKMS design document should state what potential anomalies have been studied and what avoidance mechanisms are included in the CKMS design.

D. Discussion of comments received on NIST SP 800-130: *Miles Smid, NIST Guest Researcher and CKMS Team Member.*
Mr. Smid discussed the comments that were received on the latest draft of the Framework publication. This presentation included the following points:

1. Submitted comment: The requirements are confusing about what is required in the CKMS product. Response: The requirements in the Framework are not intended to specify a CKMS design, but are intended to document what the designer chooses to design the CKMS. Any actual requirements for the CKMS design would be specified in a profile for a particular user sector.

2. Submitted comment: The Framework should state clearly that no conformance tests will be available or required to claim conformance with the Framework. Response: Such a statement is not appropriate for the Framework. Testing requirements for a given user sector may be specified in a profile intended for that sector.
3. Comments and questions from the workshop participants:
   - Provide more information on how the Framework differs from the Profile.
   - Does a CKMS have the capability to list what went wrong?
   - Is the PKI Certificte Policy (CP) and Certificate Practices Statement (CPS) considered as sufficient for the Framework or Profile?

E. Using NIST SP 800-130 to Evaluate Existing Systems: *Anthony J. Stieber.*
Mr. Stieber discussed his personal experiences with using NIST SP 800-130 as a framework for evaluating existing off-the-shelf cryptographic systems and products. This included using SP 800-130 as starting point to communicate with cryptographic product vendors and the successes and failures thereof. SP 800-130 was not written for this purpose, so the advantages and shortcomings of this approach will be discussed.

1. Security Domain Incompatibility is common within an organization and across organizations.
2. Public Key Cryptographic System (PKCS) #11 does work, but does not work completely as an interoperability standard. The Key Management Interoperability Protocol (KMIP) should do better.
3. End-to-end protection of data is rare; data is often encrypted and decrypted in hop-by-hop modes.
4. Policy in some technical development organizations: a product designer must not be the product implementer. The separation of skills and dual control of a product are more important than having one person both design and implement the product.
5. Cryptographic evaluation of CKMS products is mandatory for successful procurement. Having written, explicit security policies, is very important for successful evaluations. Not having an explicit security policy for a CKMS means that the procurer, administrator, operator, and user does not know what the CKMS is supposed to do to protect keys and metadata.
6. While the comprehensive, definitive Framework is useful, it was too much to use effectively as an evaluation tool. Instead, he created a short evaluation document to use as a tool.
7. His managers often wanted to know how many "bits of security" is needed for an organization's CKMS and how many are provided by the CKMS? This metric makes no direct sense for answering this, since it is a metric used for evaluating the security provided by a cryptographic algorithm. Measuring security in bits for systems and

equipment other than cryptographic algorithms is difficult to impossible. Other metrics are needed to measure their security.

8. NIST should broaden the possible uses of the Framework, such as using it as an evaluation tool. Editor's note: the Profile would be more appropriate as the basis for an evaluation tool.

F. Review of NIST SP 800-152 – *Elaine Barker,* NIST Cryptographic Technology Group, CKMS Team Leader.

Ms. Barker provided an overview of the purpose of the Profile for U.S. Federal Cryptographic Key Management Systems (CKSMs) to be published as SP 800-152, and introduced the table of requirements provided for public comment at http://csrc.nist.gov/publications/PubsSPs.html. The following points were made:

1. The CKMS Framework requires specific design documentation, while the Federal Profile requires specific features to be in the design and implementation of a CKMS product. The Profile also has many requirements for Federal agencies and their contractors for procuring, installing, configuring, administering, operating, maintaining and using CKMSs.
2. The Profile should be used by CKMS managers and users so they know how the CKMS should be managed and used following procurement and installation.
3. After the requirements table is finalized, the requirements will be integrated into the SP 800-152 document and issued for public comment.

G. Discussion of NIST SP 800-152 requirements with Workshop Participants: *Elaine Barker, Miles Smid, Dennis Branstad, CKMS Team.*

Ms. Barker discussed the initial requirements for SP 800-152 using a set of linked slides. Each area of requirements has been proposed with base requirements and augmented requirements for higher levels of security. In some cases, requirements have been listed that would be nice to have in the future. A number of both general and specific items were discussed.

1. Question from the audience: Will the Profile be restrictive or accepting of additional algorithms and features? Response: It is anticipated that the profile will allow other algorithms and mechanisms to be in a CKMS. However, their use may be restricted for Federal government use.
2. Question from the audience: Will there be tiers of Profiles? Response: It is anticipated that different sectors (e. g., health sector, financial sector) will have different Profiles and security domains. Additional security requirements may be placed on the CKMS by different Federal agencies when procuring a CKMS and on its users and administrators when operating the CKMS.

3. Question from the audience: Why would the classified community want to use the Profile when it has its own electronic key management systems? Response: This community has historically produced their own cryptographic equipment and rules for usage of keys. However, the classified and unclassified communities both prefer to use or augment commercial products because of cost considerations. The scope of the Federal profile is for the unclassified community because the authority of NIST is restricted to this. However, NSA personnel interact with NIST personnel on a regular basis to share technology that is appropriate to both communities.
4. Question from the audience: Will keys and metadata sensitivity be defined in the Profile? Response: The sensitivity of keys and metadata depends on the security policy of the using organization. The sensitivity of keys should be equal to, but sometimes greater than, the sensitivity of the data they are protecting.
5. A profile sector is composed of organizations having similar security requirements (e.g., Federal government; health care industry; financial industry) and will generally create their own CKMS Profile. Since there will generally be several layers of Profile requirements within each sector, it is expected that each sector will have a hierarchy of security policies, requirements, and CKMS specifications.
6. A Key designated as having a high sensitivity rating for confidentiality should never be used or stored in an area designated for moderate protection unless contained in another highly protected area, just like data marked highly sensitive to disclosure should never be processed in an area intended to protect and process only moderately sensitive data.
7. Requirements for accountability and anonymity are difficult to satisfy simultaneously. Sometimes personal accountability is required for users within the CKMS, but personal anonymity can be provided to users inside the CKMS protection boundary against observers outside the boundary.
8. Question from the audience: Is upgrading and downgrading within the scope of the Framework and Profile? Response: The keys for protecting the data that may be upgraded or downgraded are within the scope, but further consideration needs to be given to this topic.
9. The labeling of keys with a level implies that there exists a policy for what that level means and what type and level of protection this equates to.
10. An integrity code for a key and metadata (when used) must bind the key to its metadata so that a receiver can verify that the key and metadata have not been replaced or modified.
11. A security domain is logical; a cryptographic module is physical. Keys inside a cryptomodule are protected with a different policy than when they are outside the module.

12. A domain has a logical boundary, which is different than a physical boundary. A logical boundary depends on policy, among other things, while a physical boundary depends on the physical environment.
13. Recommendation from the audience: A desirable future feature for key storage would be to archive a key so that, if technology changes occur, the key could be recovered from one storage media and then re-archived in the new storage media.
14. The scope of key protection should depend on the type of keys.
15. The separation of duties and multi-party control should be required in high-risk CKMS environments.
16. Comment from the audience: The Profile should clarify the conditions for which a key and the application data can use the same cryptomodule or must use a different crypto module.
17. Discussion by the audience: Some wanted to allow FIPS 140 level 1, while others did not. Response: This will be considered and coordinated with the federal agencies.
18. Comment from the audience: Interoperable defaults should be defined and clarified. More specification of the details of interoperability would be useful.
19. Comment from the audience: For key agreement, the base interoperability default is not useful for store-and-forward situations. Response: This will be revised.
20. Comment from the audience: Auditing logs may need confidentiality protection. Protection against the modification of logs is required.
21. Question from the audience: Will the Framework be modified if there is a Profile requirement not covered? Response: It depends on the requirement, but it would be done in a future revision of the Framework.
22. Comment from the audience: Anomaly analysis of the CKMS should be described; it should be required/recommended in the Profile.
23. Comment from the audience: The Profile should differentiate among the requirements for designers, vendors, and government people. Response: This will be attempted.
24. Question from the audience: Who should be responsible for doing these tests? Who pays for it? Response: Needs to be explored.

Tuesday, September 11

A. Welcome and Leap-ahead Inspirational Talk: *Tim Polk, NIST Cryptographic Technology Group Leader.*

Mr. Polk provided the audience with his views on what is currently possible and what the hard problems are for a leap-ahead in key management.

1. Key Management forces the organization of data protection problems. One problem in one area of key management can compromise the security of the entire data security system.

2. Questions regarding hard problems: What is needed? What do we have? What is missing? Framework and Profile completion are important. Bringing research issues to the forefront is also very important. Leap ahead is the goal – not just moving forward incrementally.
3. Goals in this area: Interoperability across domains. Also, Federal PKI experience tells us that cross certification of certificates was too difficult early on. The PKI is the poster child for lack of easy algorithm agility; for example, the transition of signatures from SHA-1 to SHA-256 for digital signatures was very difficult. PKI was a single-algorithm system and not designed for transitions.
4. Cryptography for very constrained devices that cannot be easily replaced is a real problem.
5. Anonymity: A CKMS goal is to get the right key to the right person or people; a unique identity is usually required for identity verification.
6. Kerberos is designed for cross-domain interoperability, but is not appropriate for all applications.
7. Question from the audience: What is your definition of cost?" What is the cost of having multiple CKMS products? Response: Cost is not the products and the system only, but also the personnel costs to support and use the system.
8. There may be advantages to keeping CKMSs separate. It could reduce security risks. We usually need different CKMSs for different applications.
9. The scalability of a CKMS is another hard problem.

B. Security Policies as a Foundation for Cryptographic Key Management: *Dennis Branstad, NIST Guest Researcher and CKMS Team Member.*
Dr. Branstad provided his views on the requirements for security policies and his vision for the future.

1. A layered set of policies were described, starting at the highest level of an organization's Information Management Policy, down to a detailed level of the Cryptographic Key Management Systems Policy for managing the keys and their associated metadata for the organization.
2. Some of policies of the Department of Commerce/National Institute of Standards and Technology on information management were described, down to the detailed level of encrypting Personally Identifiable Information (PII) using a FIPS 140-2 Cryptographic Module before storing the PII on a flash drive before removing it from the NIST facility.
3. A simple CKMS implements an information security policy through the set of key management services, data security services, levels of protection provided to keys and data, key storage facilities, and CKMS backup processing capability available to a user.

4. A number of security policy-related questions were posed, and policy implementation tradeoffs were discussed.
5. Dr. Branstad encouraged the use of a formal security policy specification language, an automated security policy language processor, and an automated security policy enforcement system in which an organization can unambiguously specify the security that it requires to be provided for its electronic data and the keys used to protect it. A simple example of a security policy syntax meta-language and the semantics, or meaning, of the policy specifications written in the policy language that could be automatically enforced by a CKMS in the future was provided.
6. Policies relating to sharing of information between different security domains and obtaining security assurances were discussed, as well as the use of multi-level security domains.
7. Dr. Branstad identified possible Profile requirements that would be nice to have in future CKMSs – beyond the base and augmented levels specified in the tables for the Profile document.
8. CKMS Policies should be configurable and automated to manage keys that protect sensitive applications and data.
9. Automated security policy specification, negotiation, and enforcement are desirable for sensitive applications among mutually suspicious but cooperating organizations. Key management based on an automated dynamic Domain Security Policy will help meet this goal. This enforcement system in one CKMS in one security domain in one country could negotiate an acceptable temporary security policy to protect a transaction involving one or more other organizations in other countries working jointly on a sensitive global project.

C. How to Balance Privacy and Key Management in User Authentication: *Anna Lysyanskaya, Brown University.*

Dr. Lysyanskaya addressed the perceived conflict between Personal Privacy and Personal Accountability in computing and communications.

1. The basis of personal accountability is unique personal identity verification. She suggested that an appropriate organization should establish personal privacy standards, guidelines and policies.
2. There is an urgent need for a means to articulate a policy for granting access to data and to the keys used to protect them.
3. Cryptography can provide both accountability and privacy, when needed, and claimed that there is little contradiction between anonymity and privacy that could not be resolved.
4. Dr. David Chaum has published papers on anonymous credentials for anonymous identity.

5. There can be an emergency override for anonymity and true identity.
6. Dr. Lysyanskaya introduced an approach to link someone's actions together without knowing the person's identity.
7. A Zero-knowledge proof involves proving a statement to be true without disclosing information as to why it is true.
8. Misconception: if all transactions are private, you can't detect and prevent identity fraud.
9. Revoking Anonymous Credentials: in both non-anonymous and anonymous worlds
10. We could refresh valid credentials daily, but not revoked ones;
11. We could maintain revocation lists to keep unauthorized entities out.
12. Dynamic accumulators can be used to hash membership certificates. A user can efficiently prove he is in the accumulator. Revocation means "removing" a user from the accumulator; non-revoked users can still prove that they are in the new accumulator;
13. Reference LibertPetersYung12: A user can efficiently prove that he is not in the revocation list efficiently.
14. Question from the audience: Anonymous systems are hard to manage. How do we assure law-enforcement authority in this area?

D. Key Centric Identity and Privilege Management: *Paul Lambert, Marvell.*

There is a need to improve the foundational mechanisms we use in communication protocols to establish security relationship. New mechanisms are required to efficiently authenticate devices and determine "who can do what". Public key cryptography, X.509 certificates and XML security mechanisms are supposed to provide some solutions to this problem area, but are not always adequate when complex relationships need to be managed. A key centric framework for cryptographic authentication and authorization was described that is being developed within the IEEE's ICSG Privilege Management Working Group. The "key centric" framework uses hashes of public keys as the primary unique identifiers for devices and builds on these identifiers to create and sign statements used for authorization.

The following points were made during the presentation:

1. Real names need not be used for identity.
2. Wireless peer-to-peer authentication exchange needs strong authentication, and key establishment.
3. For Smart Grid: each device should have an identity and requires access control.
4. Requirements for any security system: protocols, representations, and syntax that is mapped to semantics (semantics are actions to be taken for each correct "sentence" of a programming or policy specification language).

5. Policies need to be expressed about real managed objects.
6. Device-to-device authentication is needed for many applications.
7. Policy must state how attributes are managed.
8. Tracking of mobile devices is easy with a fixed ID for the device; however, the owner loses the privacy of his location because of the device being carried.

E. Wireless/Mobile Applications: *Lily Chen, NIST.*

Dr. Chen discussed the key management challenges in mobility applications. The traditional cellular network relies on a dedicated infrastructure to "handover" keys such that when a mobile phone switches its connection from one base station to another, a protected link can be established immediately. As mobility is introduced in wireless heterogeneous networks, a mobile node may switch its connection between different security domains and/or between networks with different radio technologies. Furthermore, some of the newly emerged wireless networks may not be facilitated with a security infrastructure. The talk focused mainly on challenges in trust models, key hierarchies, key updates, distributions, and revocations for mobility applications in heterogeneous networks. Dr. Chen also explored key management approaches for mobility in inter-domain and/or inter-technology scenarios.

1. Mobile secure links are set up and then handed over hop-by-hop (i.e., link by link). Links include the mobile device to a local tower; a tower to a local controller; and a controller to an authentication server. The handover from one base station to another is called a handoff. A handover requires no break in speech and no break in security. A secure link handover means a handover of a subscriber's keys.
2. Service areas may have different service providers.
3. The 3G network solution is different than the 4G solution.
4. Challenges:
   - The lack of an infrastructure – IEEE 802.11 (WLAN) was not designed to support mobility.
   - The trust/threat model – different wireless technologies use different trust models.
   - Access authentication – a roaming agreement between mobile service providers may not cover the authentication going from one service domain to another.
   - Different authentication protocols will end up with different key hierarchies.
   - KASUMI VS AES CCM involves different algorithms; the policy is that the same key shall not be used in different algorithms.
5. Approaches
   - Fast authentication and session key establishment, pre-authentication using the existing link and re-authentication after the new link is established.
   - Key Separation
   - Use the same credentials for different access networks.

- Use a media-independent handover service for key distribution. Media and service-independent key management is the moving in the right direction, but will take a long time to launch.

F. Securely Managing Cryptographic Keys used within a Cloud Environment: *Sarbari Gupta, Electrosoft.*

Dr. Gupta discussed the special issues and challenges that arise in managing keys that protect data in the cloud, the approaches that are currently being used for managing such keys, and the areas where there are significant opportunities for improvement.

1. The Federal government is being pushed to cloud computing and storage (by OMB).
2. Cryptography is essential to secure cloud operations, but key management is hard.
3. FedRAMP (Federal Risk Analysis and Management Program): The analysis of security is based on NIST SP 800-53.
4. Cloud Service Models differ by the use of software or platform or infrastructure. Cloud deployment is public, private, community, or a hybrid. The user (organization or individual) must acquire a Cloud Service Provider (CSP) (via a contract for service). A browser for the Cloud is now a complex service or a software package and often suffers inherent weaknesses.
5. Cryptography should be integral to cloud operations. Requirements include a strong authentication of users and administrators, strong communication protection, and partitions and protections for user data in shared environments. Cryptography should provide data confidentiality, even against a service provider, and should provide and assure data integrity.
6. Security in the cloud is often a management control issue: who selects the protection and then who provides it? Should it be a user or a service provider, or should it be shared?
7. FISMA FIPS 199 stipulates Security Categorization for the Federal government: Low, Moderate, and High.
8. SC-13 Use of Cryptography (a security control in the National Vulnerability Database associated with SP 800-53A): FIPS-validated cryptography is required, plus other security policy protections.
9. There are no explicit requirements for a Key Management Policy (KMP), although a PKI certificate policy exists.
10. FedRAMP weaknesses regarding Key Management: there are no requirements for a Key Management Policy or Key Management Practices.
12. Dr. Gupta recommends mandatory 3rd Party Auditing of Security.

G. Random Bit Generation Using SP 800-90: Elaine Barker, NIST Cryptographic Technology Group, and CKMS Team Leader.
Ms. Barker provided a high-level overview of the SP 800-90 series of publications on random bit generation (RBG) that have been under development since 1998. The first of these documents was published in 2007 and revised in 2012. SP 800-90B on entropy sources and SP 800-90C on RBG constructions have now been provided for public comment. These documents and instructions for providing comments are available at http://csrc.nist.gov/publications/PubsSPs.html.

H. Secure Key Storage and True Random Number Generation – An Overview; René Struik, Struik Security Consultancy.

With the proliferation of more and more cheap, consumer-style devices, one cannot assume a secure computing platform to be available, thus potentially jeopardizing implementation security and, thereby, the security of the cryptographic system. These attacks could target secure and authentic key storage or seeds for random number generation, by targeting their storage location. This talk provided an overview of some relatively new techniques that could assist in thwarting these attacks that are based on exploiting the variability of silicon production processes ("physically unclonable functions"). These techniques can also be used to derive truly random seeds for a deterministic random number generator. Thus, both secure key storage and secure random number generation can be realized at the same time.

The main observation underlying these techniques is that one does not actually need to store a key on a device in the power-down state, as long as one can reliably reconstruct this once the device is powered-up. Standard semiconductor components can be used to realize this "intrinsic key", which is unique on a per-device basis and has all the properties one expects of a key: randomness and reliability. Some of the salient points were highlighted, including details on the reliability of key reconstruction and the randomness of the resulting keys. Also discussed were the potential use of these techniques to facilitate key lifecycle management and to thwart invasive implementation attacks.

1. A key can stay in a device when the power is off, or can be recreated from the characteristics of the device itself when the power is turned on, in which case, one does not need permanent key storage. A key can be derived, depending on unique characteristics of the device.
2. Physically Unclonable Functions (PUFs), which react in unpredictable, device-specific ways to stimuli, can be used for this purpose. They tend to be reliable and behave randomly. Their reliability depends on the use of error-control codes so as to

remove the measurement errors of subsequent PUF read-outs. Errors may be due to the PUF technology, chip process technology, temperature, voltage and the aging of the device, and are typically up to 15%. PUF read-outs between different devices should be unpredictable (approximately 50%), thereby realizing their uniqueness.

3. A device key is derived from a reference PUF value and depends on "device characteristics" that cannot be determined outside the device.
4. The device can be zeroized when the device has power (e.g., when under attack), but cannot be zeroized when the power is off. In some devices, a key is stored in the permanent memory of the device, and can be attacked in power-off mode. However, since device keys derived using PUF techniques are not stored on the device itself, these cannot be attacked, in that case.
5. Device characteristics upon which the key is based cannot change too much over time, since otherwise reliable key reconstruction is not possible. Practical implementations of SRAM-based PUFs and PUFs based on ring oscillators suggest that these can be reliably implemented with relatively low implementation cost and using standard semiconductor components..
6. The errors in subsequent PUF measurements can be used as entropy source for random bit generation.

I. Designing Key Management with Usability in Mind: *Mary Theofanos, NIST.*

Ms. Theofanos presented her view of the usability considerations required for a CKMS. They included the following:

1. Usability is defined as the extent to which a product can be used by specified **users** to achieve specified goals with **effectiveness, efficiency, and satisfaction** in a specified **context of use**."
2. Metrics available are concerned with quality, time to complete task, and the level of satisfaction in performing a task.
3. Usability is very important; the steps must be easy, and the number of steps must be minimized.
4. Complexity is the enemy of security if it affects ease-of-use, since users will avoid using a system or will use it incorrectly. A user's perception of a new system is strongly correlated with their initial ease-of-use experiences. Users have a wide variance in wants and needs. A usability evaluation must involve iterative testing throughout the design and implementation of the system; an ease-of-use evaluator must know the users – work with them and then do tests. Designers need to make it easy for a user to do the right thing and difficult to do the wrong thing; reduce complexity to increase "ease of use."
5. Multi-factor identity verification concept (i.e., something known + something possessed), is not understood by many users.

6. A security product has to provide other benefits to a user for it to be used.
7. "Measuring the User Experience" by Tullis and Albert, was cited as a good reference for practical information to enable usability professionals and product developers to measure the usability of a product.
8. ISO 9241-210:2010 (another reference) provides requirements and recommendations for human-centered design principles and activities throughout the life cycle of computer-based interactive systems.

J. Panel: Cross-Domain Interactions: Scenarios and Solutions: *Bob Griffin, RSA; John Leiseboer, Quintessence Labs; and Saikat Saha, SafeNet.*

Though significant progress has been made in achieving key management interoperability within an enterprise, interactions across security domains with different policies and objectives remain a difficult problem. In the interaction between a cloud service provider and its tenant enterprises, for example, issues such as ownership of keys, requirements for visibility and governance, isolation of tenant environments and segregation of duties greatly increase the difficulty of key distribution. Complex enterprise environments create new requirements for key management for core elements of the infrastructure, such as hardware security modules. New cryptographic models such as quantum key distribution require thinking about key distribution in new ways.

The panelists in this session explored several critical scenarios that must be addressed in these and other interactions related to using cryptographic objects across security domains, and the implications of these scenarios for protocols supporting interoperability across these domains, including trust establishment, entity credentials and tenant identification.

1. The panel members are KMIP Committee members.
2. Cross-Domain security issues: Trust establishment, ownership of keys, protection for keys at rest, protection of keys in transit, propagating key policy, negotiating key policy, managing access to keys, managing key life-cycle, visibility of key-related services, and proof of possession.
3. A policy object must be supported in the protocol; a client must make a decision on trusting transaction participants and the other parties' policies for sharing keys.
4. Managing access to keys includes verifying that the correct key is in the cloud.
5. An HSM (Hardware Security Module) is a dedicated crypto processor that is designed for the protection of the crypto key lifecycle. It is validated for security by third parties and can be used to provide a Trust anchor.
6. A key policy may need to be propagated across domains. Cross-domain negotiation is very important.

7. Quantum Key Distribution (QKD): A quantum channel is a one-way channel; an authenticated "classical" channel is two-way; the goal is to create a final key to be used.
8. Some applications need the ability to operate a One-Time Pad (OTP) Cipher (a classical simple enciphering system in which a random source of bits is Exclusive-ORed with the data bits by the transmitter and transmitted.
9. The KMIP can be used as a transmission system for keys; however, cross-domain issues are significant.
10. QKD technology is not mature, but is deployed and may be mass deployed within 5 years (in the opinion of the panelist). QKD is a valid technology in which any loss of information in the channel is attributed to an eavesdropper. QKD has a range of 50-150 kilometers, but there have been several experiments with "space" channels, as well as other channels; the band width for keys is small now, but can go up to terabits per second in the future.

K. Key Management Challenges of Derived Credentials and Techniques for Addressing Them: *Francisco Corella, Pomcor.*

Derived credentials on mobile devices raise new challenges. One challenge arises from the costs associated with verification of a certificate chain: retrieving CRLs, CRL updates or OCSP assertions incurs bandwidth costs and may add to latency if performed synchronously with authentication, while verifying the signatures on the certificates in the chain and on the CRLs, CRL updates or OCSP assertions reduce battery life and further increase latency. Another challenge is the lack of tamper-resistant storage for credentials and biometrics in mobile devices. Yet another challenge is key management complexity, which stands in the way of agile development of mobile apps.

Three techniques were proposed that addressed those challenges. The first technique dispenses with certificates by obtaining the user's identity from a directory. The mobile device demonstrates knowledge of a private key to an app (a web-based app or a back-end of a native app), and the app uses a hash of the associated public key to find (in the directory) a device record and a user record referenced by the device record, obtaining user identifiers and/or attributes from the latter. The second technique obviates the need for tamper resistance by using a PIN and/or a biometric key to efficiently regenerate (rather than decrypt) a key pair. An attacker who reads the file system of the device cannot mount an offline guessing attack against the PIN and/or biometric key because validation of the key pair requires online authentication. The third technique uses inter-app communication facilities currently available in iOS and Android platforms to outsource authentication to a prover: a black box and a verifier: another black box, insulating developers from cryptographic complexities.

1. Goal/Motivation: to store a credential in a mobile device, such as a cell phone, rather than yet another device (e.g., smart card).
2. Techniques for Addressing Challenges: Public key cryptography without certificates, key pair regeneration as an alternative to tamper resistance, and encapsulation of cryptographic and biometric processing in black boxes.
3. Current mobile devices do not have tamper-resistant storage; they can encrypt a key with a PIN, but this is not acceptable because an encrypted key can be obtained and decrypted with trial and error in an off-line attack.
4. Beyond Derived Credentials: Password elimination on the web without sacrificing privacy and social logins without passwords.
5. Dr. Corella claims that his techniques eliminate passwords and preserve privacy (anonymity, unlinkability, and unobservability).
6. Data protection in an iPhone is locked by a PIN: Data is encrypted using a key in a key hierarchy, including a key derived from private information and a "hardware key" that cannot be extracted by a casual user.
7. Three PINs are involved in process: a short PIV PIN, a long PIN and another short PIN. Their use must be kept separate.

L. Workshop Wrap-Up: *Tim Polk, NIST Cryptographic Technology Group Leader.*

1. Send in comments on SP 800-152, even if after October 10th.
2. Recordings of the workshop will NOT be available on the web.

Next Steps

The comments received during the workshop and during the public comment period on the Framework document (SP 800-130) will be incorporated into a final version of that document. Completion is expected in early 2013.

Discussions on the initial requirements for the Profile document (SP 800-152) will be incorporated into the list of initial requirements, and additional Profile requirements will be identified. These requirements will be coordinated with the Federal government agencies for feasibility prior to formalizing them in a complete draft of the Profile. In addition, the Profile requirements will be analyzed against a current key management system used by the Federal government to determine how well the system would conform to the Profile, and to determine if there are additional requirements that may need to be included in the Profile. Following these activities, the Profile document will be coordinated further with the Federal government agencies and provided for public comment. It is anticipated that the initial draft of SP 800-152 will be available by early 2014.