NIST Interagency Report 7609

National Institute of
Standards and Technology
U.S. Department of Commerce

Cryptographic Key Management Workshop Summary – June 8-9, 2009

Elaine Barker
Dennis Branstad
Santosh Chokhani
Miles Smid

NIST Interagency Report 7609

Cryptographic Key Management Workshop Summary – June 8-9, 2009

Elaine Barker
Dennis Branstad
Santosh Chokhani
Miles Smid

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

January 2010

U.S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report 7609
59 pages (January 2010)

Commercial Disclaimer

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

Acknowledgments

The authors wish to acknowledge the significant time and effort that the workshop speakers contributed to make the workshop a success. The workshop was organized within a short timeframe but resulted in a set of excellent presentations concerning problems with current key management systems and approaches for improving them. Significant experience and expertise were represented in the keynote presenters and the technical participants. NIST wishes to thank all those that participated in the workshop, both on-site and via the webcast, and plans to incorporate contributions of the participants in future publications and projects.

Abstract

On June 8 and 9, 2009, NIST held a Cryptographic Key Management (CKM) Workshop at its Gaithersburg, Maryland, campus that attracted approximately 80 people attending the workshop in person, with another 75 participating through video conferencing, and an additional 36 participating via audio teleconferencing. A total of 36 speakers, including technical experts, security standards leaders, and experienced managers gave presentations on various aspects of CKM during the workshop. Two presentations were made remotely via audio teleconferencing facilities. This summary provides the highlights of workshop presentations organized both by major CKM topics and also by presenter. Electronic access to the slides used for the presentations will be available for at least one year following the Workshop at http://csrc.nist.gov/groups/ST/key_mgmt. Additional information regarding the CKM project will be made available through the NIST website at http://csrc.nist.gov/groups/ST/key_mgmt.

Audience

The intended audience of this document includes individuals and organizations seeking to better understand cryptographic key management, with an emphasis on those planning to design, procure, or use a secure CKM system. A CKM System Design Framework is under development that will describe, in a logical structure, the components of a CKM system and the characteristics that make them easier to describe, design and operate.

Disclaimer

This is a summary of the CKM Workshop sponsored by, and held at, NIST. The authors have attempted to capture the primary concepts and contributions of the presenters and participants in this summary. Clarification and context information has been provided by the authors to enhance readability, but no signficant effort was made to verify the accuracy and completeness of the information presented. In addition, the noise interference in the transcripts of the presentations that were used to prepare this report and the limitations of the automation processes involved in preparing the transcript may have resulted in errors and omissions that affect the utility of the information in the report. Readers are encouraged to contact the presenters and

quoted participants to verify or clarify the summaries herein when using this information in designing or implementing security products and services.

Executive Summary

The Cryptographic Key Management (CKM) workshop was initiated by the NIST Information Technology Laboratory's Computer Security Division to identify technologies that need to be developed that would allow organizations to "leap ahead" of normal development lifecycles to vastly improve the security of future sensitive and valuable computer applications. The workshop was the first step in developing a CKM System Design Framework that will address issues discussed during the workshop.

This summary provides the highlights of the presentations, organized both by topic and by presenter, in a bulleted format for rapid scanning. A definition of acronyms used in this report is provided in Appendix A. Copies of the slides used by the presenters are available at http://csrc.nist.gov/groups/ST/key_mgmt, and should be reviewed if more details of the presentations are desired.

Key management has been identified as a major component of national cybersecurity initiatives that address the protection of information processing applications. Numerous problems have been identified in current key management methodologies, including the lack of guidance, inadequate scalability of the methods used to distribute keys, and user dissatisfaction because of the "unfriendliness" of these methods. The workshop sought to identify the inadequacies of current key management methodologies and to plan for a transition to more useful and appropriate key management methods.

NIST conducted the workshop in order to: 1) identify future computing environments, the international enterprises likely to utilize them, the applications that will be performed in them, and an array of key management mechanisms and protocols that will be needed to provide appropriate security for the applications; 2) discuss the creation of a key management system design framework that will support the use of effective cryptographic mechanisms required 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.

Presentations covered a broad spectrum of cryptography-based security issues, including CKM systems that are currently available but under-utilized because they lack user-friendly automated key management services; CKM systems that are under development but not reaching the marketplace because of financial, logistical, and support service problems; and new security mechanisms needed to support future computing environments, such as: "cloud" computing, integrated international applications, and secure management of dynamic relationships among people, international organizations, and global applications.

A CKM System Design Framework specifies key management components that should be considered when developing a secure CKM system and provides requirements for design specifications. The Framework is intended to define the components of a seamless set of technologies that, to the greatest extent feasible, 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 computing and communicating environments. The CKM System Design Framework will help to specify security policies, key establishment methods, key archiving, key recovery, and key protection requirements and mechanisms, and to identify and resolve usability, scalability and trust issues.

Workshop presentations touched on cloud computing and secure electronic personal data assistants capable of interfacing to private domains. Automatic provisioning (i.e., providing needed security parameters whenever and wherever needed) and maintenance of cryptographic keys, as well as assuring the integrity, availability, and confidentiality of the keys used to protect information in long term storage, were stressed during the presentations.

Table of Contents

Contents

1. CKM Workshop Program

Cryptographic Key Management Workshop Program
June 8-9, 2009

Monday, June 8, 2009

8:00am - 9:00am **Registration**

Morning Moderator: Elaine Barker, NIST

9:00am - 9:15am **Administrative Remarks and Purpose of Workshop**
Curt Barker, Chief Cybersecurity Advisor, NIST

NIST Welcome (no slides)
Patrick Gallagher, Deputy Director, NIST

9:15am – 10:15 **Morning Keynotes: Innovative Future Computing Applications**
Vice Admiral J. Mike McConnell (USN Ret), Senior Vice President, Booz Allen Hamilton (no slides)

The Future of IT Security and Privacy: Dreams of an IT Practitioner
George Strawn, Chief Information Officer, National Science Foundation

10:15am - 11:15am **Key Management Today: Status and Issues**

Key Management in Internet Security Protocols
Russ Housley, Vigil Security, LLC

NSA Key Management Experience
Petrina Gillman and Jonathan Booth, NSA

11:15am -11:30am **Break**

11:30am - 12:00pm **Key Management: Lessons Learned**
Vijay Bharadwaj, Microsoft

12:00pm - 12:30pm **Future Key Management Methods**
David McGrew, Cisco

12:30pm - 1:00pm **2010 Transitions**
Elaine Barker, NIST

1:00pm - 2:00pm **Lunch**

Monday, June 8, 2009

Afternoon Moderator: Tim Polk, NIST

2:00pm - 2:30pm	**Security and Ease of Use** *Marinus Struik, Certicom NL*
2:30pm - 3:00pm	**Afternoon Keynote: Advances in Telecommunications** **Towards Improving the Security of the Internet** *Vint Cerf, Vice President & Chief Internet Evangelist, Google*
3:00pm - 3:30pm	**Usability and Key Management** *Mary Theofanos, NIST*
3:30pm - 3:45pm	**Break**
3:45pm - 4:15pm	**Key Management Lifecycle** *Joe Skehan, Venafi*
4:15pm - 4:45pm	**Cloud Computing: Some Implications for Key Management** *Lee Badger, NIST*
4:45pm - 5:15pm	**Five-Minute Presentations** IEEE Key Management Summit 2010, *Matt Ball, Sun Microsystems* *Stephen Ranzini* (no slides)
5:15pm	**Adjourn for the Day**

Tuesday, June 9, 2009

Morning Moderator: Bill Burr, NIST

8:45am - 9:45am	**Morning Keynotes: The Future of Key Management**
	Key Management and Electronic Fair Exchange *Silvio Micali, Dugald C. Jackson Professor of Computer Science, MIT*
	The Convergence of Key Management and Information Management *Burt Kaliski, Director, EMC Innovation Network* (Audio Presentation)
9:45am – 10:45am	**Enterprise Key Management Panel** *Panel Chair: Robert Griffin, RSA* *Matt Ball, Sun* *Matt Fanto, Aegis Data Security* *Chii-Ren Tsai, Citigroup* *Steven Wierenga, Hewlett Packard* (Audio Participant)
10:45am - 11:00am	**Break**
11:00am - 11:30am	**Identity-Based Key Management** *Terence Spies, Voltage*
11:30am -12:00pm	**Scalability and Control Realized with a Centralized Key Management Approach** *John Marchioni, ARX*
12:00pm - 12:30pm	**Approaches to Globally Scalable Key Distribution** *Jeffrey Opper, BAE*
12:30pm - 1:00pm	**The Use of Group Key Management in Internet Standards** *Brian Weis, Cisco*
1:00pm - 2:00pm	**Lunch**

Tuesday, June 9, 2009

Afternoon Moderator: Elaine Barker, NIST

2:00pm - 2:30pm **Key Management for Symmetric Keys**
Sarbari Gupta, Electrosoft

2:30pm - 3:00pm **StrongKey, Open Source Symmetric Key Management**
Arshad Noor, StrongAuth, Inc.

3:00pm - 3:30pm **Essentials of a Cryptographic Key Management Framework**
Miles Smid, Orion Security Solutions

3:30pm - 3:45pm **Break**

3:45pm - 4:15pm **Leap-Ahead Technologies**
Miles Smid, Orion Security Solutions

4:15pm - 4:45pm **Five-Minute Presentation**

Speed-ups of Elliptic Curve-Based Schemes, *Rene Struik, Certicom*

The Compliance Hangover, *Brian Tokuyoshi, PGP Corporation*

PKI Lessons Learned, *Santosh Chokhani, CygnaCom Solutions*

History of KM as I Know It, *Lawrence Himes* (no slides)

4:45pm - 5:00pm **Summary and Closing Remarks**
Elaine Barker, NIST

Due to severe weather in the Gaithersburg area on the afternoon of June 9, the meeting ended prior to this session due to technical difficulties.

2. CKM Workshop Presentation Highlights organized by Presenter

This section provides highlights of the presentations, comments, and questions of the CKM Workshop organized by Presenter.

2.1 June 8, Morning Session: Elaine Barker, NIST, Moderator

2.1.1 Introduction to the Workshop: William C. "Curt" Barker, NIST

Mr. Barker is the NIST Computer Security Division Chief and NIST Cybersecurity Advisor[1]

- This Cryptographic Key Management Workshop is the kickoff activity in a "leap-ahead" effort that we are undertaking as a part of the National Cybersecurity Initiative. The President recently announced the results of a cybersecurity policy review. Cybersecurity is a critical element in our national security posture. Our reliance on the internet is becoming nearly total.
- When the financial crisis hit Lehman Brothers, no one was paying close attention to the fact that most of the international fund transfers were going through that institution. Suddenly that capability was lost and what was a very serious situation turned into a real crisis.
- The role of key management in cybersecurity is critical. We have cryptographic functions that are used for identification and authentication, both from the standpoint of protecting privacy, but more importantly, for integrity and authentication mechanisms.
- Even when we look at biometric methods for identification and authentication to control access to critical functions, we're still dependent on cryptographic functions for protecting the integrity of the biometrics.
- The methods for distributing keys efficiently are different from the methods of being able to revoke and replace keys efficiently on a large scale.
- We have institutional issues, including getting the mechanisms into place. We're told that many of our technical problems are more or less solved. Where can I buy the solution? Who's implementing it?
- We need to understand the requirements of the Federal government. We have to be working hand-in-hand with industries. What are our resources and what are our practical constraints?
- We're hoping this workshop will identify many new security requirements and propose a way to satisfy them.
- The President's policy review has brought home to a large community the nature of the threats that we're facing. It also demonstrates the urgency of having policies and technologies available and in place for mitigating those threats.
- We have to come up with solutions for the next generation. From a standards point of view, we must have practical, adequately precise standards that will integrate effectively

[1] Subsequent to this CKM Workshop, Mr. Barker was assigned to the U.S. Department of Commerce's Office of Policy and Strategic Plans. He is currently the DOC Cybersecurity and Privacy Coordinator of DOC participation in the Executive Branch's Cybersecurity Initiatives.

into government operations and industry business practices and product development cycles.

- We need to understand the potential impediments to satisfying those requirements in technical, social, and institutional contexts. We have to evaluate alternative approaches, and then we need to analyze the benefits versus the costs.
- We're going to accept very high risks in our research because we're going for very high payoffs. We're not going to accept high risks in the future Internet, because we don't want the adversaries to have high payoffs.
- In the end, we want to establish actions and roles that are not simply limited to the government. There are roles for government, roles for the academic community, and roles for industry.
- One requirement is to have scalable solutions in very large applications. While we know how to handle key management reasonably effectively for up to a million people, we need to go a couple of orders of magnitude beyond that in the relatively near future.
- Privacy concerns and security concerns are sometimes conflicting. The organizations that use security mechanisms and key management methods are very diverse.
- We don't have just a national security environment and a non-national security environment today; we have a collective community.
- Some impediments to vastly improving CKM include: organizational requirements that are often conflicting, funding issues, using the funds effectively, and intellectual property interests.
- Creating a standard that is widely used is difficult if the standard infringes on someone's intellectual property. Standards can only succeed if they may be used satisfactorily within existing intellectual property constraints.
- The whole concept of the internet is based not on a single system, but a set of standard protocols that allow independent systems to interoperate with each other. We have to support this interoperability among future systems.
- Standards must not only be technically correct and precise, but they must be understandable to, and easily used by, the general public. We need to be able to communicate what we're doing and why we're doing it to the people who make policies, procurement regulations, and user instructions.
- When protecting stored data, good information management methods must be able to discover three years from now what algorithm and what key were used to encrypt the information. Often, the result of poor CKM for stored data is absolute security; no one, including ourselves, can use the data if the key used to decrypt the data cannot be retrieved.
- Our present role is to get folks to work together in a manner that will create useful CKM standards in the future. We rely on other Federal agencies to state their specific requirements so we can come up with CKM standards that satisfy their requirements and are user-friendly, cost effective, and secure.

- Executive and legislative oversight and resource allocation must be in the proper context. Expectations must be consistent with technical reality. We must work with industry, not just from the standpoint of innovation and technical expertise, but making sure the standards that result will be implemented, not just can be implemented.
- We need to work with academia because we get many creative inputs from its members, who are not constrained by short-term corporate goals. We rely on obtaining innovative ideas from our colleagues overseas.
- We need to develop CKM techniques for the future. We need to analyze them for security and ease of implementation and use.
- We need to create standards that are testable. Ideally, they should be tested automatically so we can minimize the effort of conducting manual product assurance.
- We need to have procedures for qualifying products as meeting our standards so that they may be easily procured by the government and others. The procurement qualification process needs to be efficient and strongly coupled with our technical specifications.
- We must first identify key players in the CKM program. We then must establish appropriate roles and partnerships among the players. We need to coordinate our actions to produce widely acceptable solutions. We need to be able to demonstrate and test our solutions in actual applications.
- We need to have standards that institutionalize acceptable CKM solutions in a manner that provides compatible products in the real world that are easily implemented and are efficiently used and maintained.

2.1.2 Welcome to NIST: Dr. Patrick Gallagher, Acting Director[2], NIST

Dr. Gallagher welcomed the CKM Workshop participants to NIST. He stated that key management is critical for all sensitive information processing applications, and that economic prosperity is a major goal and needs information security.

2.1.3 Future Computing Applications: Vice Adm. J. Mike McConnell, BAH

Keynote Speaker: Vice Admiral J. Mike McConnell (USN Ret.) is a Senior Vice President of Booz Allen Hamilton (BAH) and a former Director of National Intelligence. He previously served as Director of the National Security Agency. President Obama has asked McConnell to continue to serve on his President's Intelligence Advisory Board (PIAB) which advises the President on all matters related to intelligence.

- The Internet has changed the world. It has increased global productivity, manufacturing, and communications. It has changed the United States. It has increased our standard of living and is very wonderful device that we all enjoy.
- The Internet has introduced a level of vulnerability that is unprecedented. We are worried about spies who might be invading our privacy and our sensitive or critical information systems, but mostly about attacks against our information systems that steal or destroy our data. Money is just data in some computer, and the whole system is based on confidence. A bank in Tokyo must be able to send $100 million in a couple of seconds

[2] Dr. Gallagher has since been confirmed as the Director of NIST.

with high confidence that the transaction will be receipted and reconciled, that the books will be brought up to date, and the transaction was completed correctly. If something interferes with that confidence, the banking system could fail.

- The nation is at strategic risk. While nineteen terrorists destroyed the two world trade centers, they could have been even more successful had they done nothing more than destroy our vital national and economic data. This would have had an order of magnitude greater impact on the globe and the United States.
- I was in a group that had an opportunity to brief then-candidate Barack Obama on security on the 2nd of September, 2008. We described lots of national problems: Iranian nuclear weapons, al Qaeda, Taliban, and Pakistan. He asked what else was out there that he needed to worry about. I said, "Senator, you know what the Chinese did to your personal computer system in terms of background papers and your speeches." He said, "Yes, they accessed my data." I told him that this was true, but if their intent was to destroy or modify his data and disrupt critical infrastructure control and information processing services, he and the country would be in big trouble.
- The current Internet attacks are mostly to collect and exploit. Where someone may access privately sensitive data to get an information advantage, large stable organizations and countries are not likely to destroy another country's highly valuable or sensitive data because of the consequences of world instability.
- President Obama is now addressing cybersecurity at the most senior level. The Cyberspace Policy Review that was just issued attests to that. However, the Cybersecurity Initiative is primarily to protect .mil and .gov information. Somebody should worry about .com. Ninety eight percent of the world is .com or .edu or .org or a foreign segment of the global internet.
- Now that we're so dependent on the Internet, it is proposed that a public-private partnership be formed to focus on protecting the Internet. That group would focus on what we need to do as a nation, even in a global partnership, to solve these problems. Panels would be set up to address strategy, technology, and operations.
- My prediction is that we're going to have a catastrophic event, and then we're going to be screaming. We have an opportunity to address and solve Internet problems before we have that anticipated catastrophic event. We now have the attention of the new President.
- Curt Barker showed a slide stating what needs to be done. What I hope is that the nation will come together in a partnership that collaborates and cooperates to do those things.
- Ultimately, we need to re-engineer the Internet for the globe. We must design and build security into the new Internet. We must include countries such as Russia and China in creating the design. We have to do this because the globe could be so advantaged by this secure Internet capability and is currently so vulnerable. Something big must be done now.

2.1.4 The Future of IT Security and Privacy, Dr. George O. Strawn, NSF

Keynote Speaker: Dr. George Strawn is the National Science Foundation's Chief Information Officer (CIO), where he guides the agency in the development and design of innovative information technology. Since joining the NSF in 1991, Dr. Strawn has served as the Executive

Officer of Computer and Information Science and Engineering (CISE) and as the Director of the CISE Division of Advanced Networking Infrastructure and Research. He was the Program Director of the NSFNET, which became the first national DS-3 Internet backbone network.

- In computer technology we keep moving faster and faster. We have seen an improvement of price-performance in computer technology by a factor of nearly one million in the past 30 years.
- Many NSF Internet applications need security, including email, project funds management, travel, proposal submission and proposal evaluation.
- If true security is required on today's Internet, a user must follow one of three laws: Don't buy a computer, Don't turn it on, or Don't attach it to a network.
- NSF needs better integrated cryptography in its sensitive applications. Currently, NSF doesn't use PKI because of cost and complexity, but does use identity management, including identifying users and visitors, additional authentication of NSF users, and authorization of NSF users to systems and data.
- NSF security policy has been continually modified in accordance with new problems: we encrypt in https, we seldom do anything that requires un-proven methodologies for the first time, we follow all government rules, and we want to be told that something new is mandatory in order to justify a new budget item.
- NSF now combines information management with security management. It has a strict security awareness program. Its visitor network was separated from its internal NSF user network, and all social security numbers in the system are encrypted.
- In the next decade, we foresee more OMB/NIST mandates; more programs for protecting the Internet, rather than protecting users from the Internet; and more security designed-into commercially available acceptable products.
- We would truly like to be able to create secure systems from insecure components.

2.1.5 Internet Key Management Security: Russ Housley, IETF Chair, Vigil Sec.

This talk focused on the use of key management in today's internet.

- Nearly all internet security protocols use cryptography for authentication, integrity and/or confidentiality, and hence, require key management (KM).
- KM brings expense to the Internet because of the complexity, required infrastructure, and the computation power needed to perform cryptographic protection.
- The Internet security protocols use various KM approaches, including: pre-shared keys (e.g., manually initialized, communicating parties mutually derive a new key for data protection), PK cryptography (key agreement, key transport) , and Key Distribution Centers (the KDC has a secret key for every subscriber; the KDC generates and distributes a subscriber-subscriber data protection key using the KDC-subscriber keys).
- Public key certificates bind a subscriber's identity to a public key; a certificate contains: the subject's name, the subject's public key, the key's validity period and the issuer's name.

- The initial enrollment of a subscriber is the most expensive and hardest part of key management, because it takes human interaction with a subscriber in a trusted environment.
- IETF protocol efforts include: IKEv1 and IKEv2, TLS, Secure Shell, EAP; CMS and Kerberos.
- The Extensible Authentication Protocol (EAP) provides authentication for people and devices.
- IETF enrollment efforts include: KeyProv and a dynamic symmetric key provisioning protocol.
- There is a clear need for standards in certificate enrollment, but previous attempts have failed.
- There is a clear need for cryptographic algorithm agility. Negotiation among competing algorithms increases complexity, but also allows transition more easily when an algorithm gets old or broken.
- There have been a lot of transitions from one algorithm to another in encryption and secure hashing. The Internet community sees a need to respond to these changes in algorithms, especially when a security flaw is found, but seldom in other circumstances. A transition takes 5 to 15 years, and the cost of implementation, testing and deployment are high because it causes a loss of interoperability in some circumstances.

2.1.6 Key Management Experience at NSA, Petrina Gillman and Jonathon Booth, NSA

Presenter: Petrina Gillman:

- The NSA Key Management lifecycle model has arisen from over 50 years of experience in designing and managing cryptographic systems.
- Key management starts with identifying user needs and requirements in a KM planning document (e.g., limiting those who can request keys – usually one or two special people for requesting a set of keys for a specific time period).
- Cryptography is required in cyberspace and can provide more information assurance capabilities.
- There is an expressed preference for key distribution using public key cryptography.
- NSA requires strict accounting for keys, multi-person (between 2 and *N* people) control on plaintext keys, secure key storage, and three layer key management, including transport, packaging, and key format.
- There are few standards for key generation, ordering, distribution, accounting, destruction, commercial implementation, and key format.
- CKM is growing in complexity; point-to-point communications security is old technology. It is desirable to have interoperability with existing legacy systems.
- NSA is helping to define standards packages and key formats in the IETF and PKIX for the Suite B cryptographic algorithms (i.e., those used to protect classified data up to SECRET).

- NSA has a goal of working with industry to define a common set of cryptographic algorithms that can be used in creating products that meet a wide range of U.S. Government needs.
- NSA would like to have some interoperability among high-assurance government devices and commercial off-the-shelf devices, especially for emergency situations, such as 9/11 and hurricane Katrina.
- NSA would support defining key formats as a parameter that could be imported to an algorithm for interoperability among government and commercial devices. Everyone likes to do their own key format now; there is a key formatting explosion.

Presenter: Jonathan Booth, NSA

- NSA is now more open in its interactions with public groups, e.g., cryptographic message syntax in RFC 3852, trust anchor format and protocol standard, an asymmetric private key format, and symmetric and asymmetric key management packages.
- NSA does not intend to recreate existing standards, but rather work with open groups to establish standards that also satisfy NSA's requirements.
- NSA wants to support wider audiences of users, including FEMA, allies, charities, State governments, and emergency first-responders.
- A nested security approach protects a red key (i.e., unencrypted data encrypting key) with integrity, authenticity and secrecy provisions.
- There is a tradeoff between security and simplicity. Good security requires complexity in certain security components, layers of protection, layers of metadata in security packages, and a robust metadata system to support security provisions. Some cryptographic key metadata can be hidden. Security packages will be as complex or simple as the user wants within a procured KM system.

2.1.7 Vijay Bharadwaj, Microsoft

- The presentation was about lessons learned from Microsoft's extensive use of cryptography within their product line (e.g., a crypto API in Windows since 1996 and CNG in Windows VISTA since 2006/2007). He emphasized the need to look at the entire system and that the biggest issues in crypto-based security were with scalability, federated systems, and the customer's specific domain.
- He described the Microsoft use of a security development lifecycle (SDL) that is used for all security developments in the company. All components of the system are developed simultaneously and then laid out on paper so that the system flow can be analyzed for ANYTHING AND EVERYTHING that can go wrong in the total system, not in individual components in isolation. Evaluators must think of how an entire system can be broken.
- He emphasized the differences between hardware and software challenges: hardware has different failure modes and different update capabilities than software.
- Microsoft systems are designed using a tool kit of mechanisms (subsystems) and best practices. There is a great need for a key management tool kit of generic building blocks

from which individually chosen subsystems can be integrated into the total system. Key management is an application that must be form-fit to the user requirement. We need methods to analyze the resulting system end-to-end.

- He emphasized 1) that KM is a major requirement that is difficult and complex, 2) the need to analyze the entire system for both security and reliability, and 3) that an **e**nterprise KM is an un-trusted client in a trusted server, versus a trusted client in an un-trusted server, as the case when a consumer uses cloud computing.
- He stressed 1) that users don't care about keys, 2) that users don't like to worry about details, but need to be guided, 3) that humans tend to be the weak link, and 4) that there needs to be a crypto administrator in charge of cryptography who controls a user's identification and authentication.
- He believes 1) that a CKM framework was needed, 2) that SP 800-57 is a good start, 3) that security has to be built into applications and systems, 4) that security best practices had to be supported by security toolkits, 5) that algorithm agility was necessary, and 6) that there is a need to know what system state is expected by a user and that the user can determine the security state of an application.
- Keys are used to achieve security, but real-life security objectives are defined in human terms. Systems are broken by exploiting this difference.
- He stated that KM systems are very big, comprehensive and application-specific, and that security analysis must encompass all the players in a dynamic information system and network.
- He stated that ceremonies are useful for analyzing the end-to-end security of processes and can detect "out of band' attacks, such as social engineering; a ceremony is a structured diagram of specific transactions among a set of entities to determine weaknesses in an entity or process flow.
- A key management platform for composability with existing subsystems, such as identity verification and authentication, is needed; a collection of generic building blocks of security that can be integrated into a system and methods to analyze the resulting system are needed in creating a good key management platform.

2.1.8 Future Key Management Methods: David McGrew, Cisco

- The focus of the talk was from a manufacturer's perspective and included the challenges of the equipment distribution problem and creating a manufacturer's device certificates. A manufacturer often ships devices to customers with a hardwired private key, device certificate, and device identifier. This would give the capability for devices to authenticate each other from a distance, but would not solve the authorization problem.
- Threshold cryptography was discussed (i.e., *M* out of *N* keys must be available to perform an operation), as well as manufacturing certificates, automating manual key distribution, and a symmetric key generation system.
- Threshold cryptography is useful for encrypted data storage access (e.g., a minimum number of people must cooperate in order to retrieve sensitive, stored information.

- There is a problem with replacing the keys and updating revocation lists. We need to be able to streamline the distribution process and replace manual key distribution with a minimal impact process.
- We need an automated CKM system that can be implemented in existing systems.
- Requirements include: the authenticated/authorized distribution of keys, keys must persist over a long term, a system that replaces/updates keys when needed, key creation should not be centralized, minimal operational impact, and the CKM should be interoperable with Multipoint Key Distribution (MKD). Candidates for this type of KM system would be Kerberos (for session keys), OASIS (for storage keys) or GDOI (for group key management).

2.1.9 2010 Transitions: Elaine Barker, NIST

- The talk described NIST recommendations to transition from algorithms and key sizes that are believed to be too weak (i.e., no longer secure) to a stronger set of algorithms and key sizes, including deadlines for transition from the old set to the new set.
- A security strength (AKA "bits of security") is a number associated with the expected amount of work (often measured in binary operations) that is required to obtain any given key used by an application by testing all possible keys. The security strength is specified in bits and is currently a value from the set {80, 112, 128, 192, 256}. 80 bits of security are good through December 31, 2010. Thereafter, NIST recommends 112 bits as the minimum.
- Material was provided from NIST SP 800-57, Part 1 (for algorithms, key sizes, security strengths, and recommended transition times), FIPS 186-3 (for digital signatures), and FIPS 180-3 (hash functions). See the presentation slides or referenced documents for details and comparisons among algorithms and parameters.

2.2 June 8, 2008, Afternoon Session; Tim Polk, NIST, Moderator

2.2.1 Security and Ease of Use: Marinus Struik, Certicom Research, NL

- The talk focused on the assertion that security can be a justification for making a system easy to use. A good system should have a configuration that is easy to understand. Understanding a secure system must be attained. Security must be designed into the system and then be fully used in order to be understood.
- Security technology can make trust lifecycle management intuitive and hidden from the user.
- Challenge: Bridge the gap between state-of-the-art security that is known and security that is actually being used.
- Education gap: Conventional wisdom is that "computer security systems can't be effective unless they are complex and difficult to use." While this may once have been true, the security profession has witnessed dramatic improvements over the last ten years.
- Perception gap: Conventional wisdom is that security technologies are too expensive to implement with sensor and control networks, due to energy constraints, and

computational and storage constraints. There is also a gap between security perceived by the user and actual security provided to the user.

- Affordability gap: Conventional wisdom is that the licensing cost of security technologies may present a hurdle. Licensing models, such as those used with the consumer electronics industry, may have some merit for ubiquitous computing as well, since both are concerned with mass-scale deployment of networked devices ("the internet of things") and enforcement of compliance.
- The Open Systems Interconnect (OSI) architecture was used to discuss various layer-layer issues, both between peers and between upper layers and lower layers in a network.
- The presentation addressed problems with setting up secure links; devices and device IDs; reusing a key at different layers; a multi-application device in which various applications could have different security requirements; certificate generation; communication encapsulated in one protected part of a device that can be trusted; idealized provisioning, where there is no security perimeter, versus where there is a security perimeter with specified trust inside; various network technologies; little human involvement in secure system operations; and having many root keys permanently in a device that are seldom used except in accordance with security policy. Trusted modules are possible, but he would like to minimize trust dependencies.
- A Security Policy Engine was mentioned, but not dwelt on. It is surmised that this is an automaton that implements a user's data security policy by creating or selecting an appropriate cryptographic policy and supporting key management policy that achieves the data security policy. This has been a topic of research proposals and projects, but little advancement has been achieved in implementation and use.
- He asserted that virtually no additional training is required for a user in order to effectively use cryptography if CKM is properly designed.

2.2.2 Improving the Security of the Internet, Dr. Vint Cerf, Google

Keynote Speaker: Dr. Cerf is a Vice President and the Chief Internet Evangelist of Google. He served as a senior vice president of MCI from 1994-2005, as VP of the Corporation for National Research Initiatives from 1986-1994, and as Principal Scientist for the U.S. Defense Advanced Research Projects Agency. Known as one of the "Fathers of the Internet," Dr. Cerf is the co-designer of the architecture of the Internet and was founding president of the Internet Society.

- Stronger authentication is needed for smart Internet "edge devices" (e.g., routers, routing switches, integrated access devices) that provide authenticated access to the backbone network, as well as stronger authentication for active processes, users, and digital objects, with the implication that we need better access controls and two-part authenticators for devices.
- More vulnerabilities will be found in browsers, operating systems, routers, domain name resolution processes, DPI-based attacks (e.g., against TCP) and MANETs (auto configuration and overrun conditions).
- Attacks include zombies, botnets, drive-by downloads, and zero day attacks.

- A bright prospect of solving these problems was not presented. A list of protective measures that "sort of work,", "hair brained ideas" and "obvious responses" was provided.
- An extortion threat was described for getting money by threatening to take specific networks down, but not the Internet itself.
- If hosts and routers must authenticate themselves, the overhead will be too high.
- A certificate for every person in the general population is somewhat problematic. It is difficult to really verify the initial identifier without context.
- The Trusted Computing Base is a three-decades-old concept ("Orange Book efforts").
- Verifying that the object code in a computer is the "same as" the source code is a difficult problem.
- Google has started to "crawl" the WWW looking for malware. Malware is flagged, and users are warned about visiting a flagged website.
- Computer configurations that have gone "bad" are difficult to detect.
- Trust levels were discussed, with communicating parties going to increased levels of trust, based on their common security policy.
- We may need to consider trust models similar to those used by banks for guaranteed signatures and risk limits on credit card transactions.
- Multiple identities with multiple identifiers for an individual are a must. Attribute certificates stating the authorizations of differing identities must be supported.
- Individual activities must not be confused with organizational activities.
- The roles for an individual must be supported, and role-based authentication is needed (i.e., the authentication of a person will depend on the role that the person is attempting to fill). Roles for processes must be similarly supported.

2.2.3 Usability and Key Management: Mary Theofanos, NIST

- The presenter provided a commentary on the difficulty of using cryptographic security systems, which have little regard for the convenience of the user. We need to take the user's perspective into account when designing cryptographic systems if we want the security to be actually used, as opposed to being circumvented.
- It is not acceptable to only have a choice between usability with little security and security with little usability. A CKM system designer has to know the prospective user and to understand that security is not the primary task of the user. A system must be efficient, effective and understandable. There is no complex system that is secure.
- Users will bypass security when it gets in the way. Users feel that timeliness and efficiency are more important than security; A LOAD-AND-GO security service must be provided to users.
- An experiment was described about how easy or hard it was to use the PKI for the security of a wireless network at the Palo Alto Research Center. The objective was to

give 200 users an X.509 certificate and to use the Extensible Authentication Protocol in TLS mode to authenticate to the wireless network. The user was asked to request and retrieve certificates through a web-based interface. Eight computer science Ph.D. students volunteered for the experiment; 38 distinct steps were involved in obtaining and using a certificate; the average time to request, receive a certificate, and configure a secure environment was 140 minutes. Many of the students described PKI enrollment as the most difficult computer task they had ever been asked to perform. All had little idea of what they had done to their computer systems. Establishing security had reduced their ability to configure and maintain their own machines. The conclusion of the experiment was that usability is more than just the user interface.

- CKM designers have to adopt the mantra of making it easy for users to do the right thing. Designers have to align the design to the user's conceptual model of a security system. The interface has to use terminology that is intuitively obvious to the general computer user. The complexity of the CKM system has to be minimized for the user if it is to be used effectively.
- Certificate pop-ups have to be minimized, because users have become accustomed to ignoring pop-ups. Factors that inhibit the adoption of new technologies have to be eliminated, and those that promote the adoption of effective security technologies have to be encouraged.

2.2.4 A Holistic Approach to Key Management Lifecycle: Joe Skehan, Venafi

- Pressure from many sides drives the use of encryption: regulation compliance, outside auditors, the Board of Directors, policy compliance, protection of critical data, etc. The question is: Who owns encryption? IT operations, auditors, Infosec, or business units? The answer is everyone. There are many competing sets of rules and people who have a stake.
- Encryption challenges include: data security, key security, enforceability, operational efficiency, system availability, reputational risk, business continuity, disaster recovery, and privacy.
- A security analysis should start with risk management, including an inventory of keys, certificates, and applications. An application must be configured for enterprise-wide encryption, which includes client protection, servers, networks and archival data storage.
- Security, cryptography, and cryptographic keys can be managed using a cryptography management platform that can track everything throughout the life cycle of provisioning, enrollment, monitoring, and discovery. Included would be the processes involving keys and certificates, cryptography and CKM policies, secure implementation validation, audit, and security notifications (must notify customers affected by a security breach).
- Major design issues include: What should be done when a certificate expires? Who should administrator a CKM system? When information is lost, was it in encrypted form? When should certificates expire? Should key management be automated or manual? What cryptographic algorithms, protocols, and interfaces are being used?
- The reality of lifecycle key management is that policy and workflow must be continuous, and all the components must be integrated properly. Enterprise encryption policies must

be comprehensive and cover a wide range of components, including certificates, keys, algorithms, validity periods, and multiple person control. Policy is the overarching guidance and requirement that must be achieved.

- Enterprise encryption policies must cover data, discovery, keys, certificates, key storage, applications, disaster recovery, validation and monitoring, reporting of workflow and process, personnel roles and assignments.
- Encryption management and distribution models cover a broad range, from manual to automated management involving several types of agents and protocols.
- Requirements and constraints driving encryption management models include levels of automation, automated agents, remote access decisions, duplication of keys, centralized monitoring and alerting.

2.2.5 Cloud Computing: Implications for Key Management, Lee Badger, NIST

- This presentation described a future technology that may bring the biggest challenge to effective key management and security in general.
- Cloud computing will provide convenient, remote, on-demand utilization (e.g., rental) of computing power and applications that the user cannot afford to maintain locally, but may need from time to time. This capability will provide ubiquitous network access, on-demand self-service of computing power, metered-use (rent by the hour), elasticity of the capability meeting real-time requirements, and resource pooling.
- The result is that there will be software, hardware, and infrastructures as services to be obtained at will. The question that must be asked is where and how will security in general, and CKM specifically, take place? Who or what is responsible for security while data is being processed within the cloud: by the cloud itself, or by the application?
- How can applications be secured in a cloud-computing environment? Can virtual machines maintain separate security policies?
- Cloud capability may be deployed by various cloud providers to a multitude of cloud customers in various ways, including: software as a service, platform as a service, and infrastructure as a service.
- Delivery models of service providers include: internal, community, public, and hybrid. Each has benefits and some controversy.
- Two basic kinds of clouds include storage clouds and processing clouds; both require extremely fast, reliable, secure and low-cost networking.
- Clouds are a good fit for very large-scale applications involving huge quantities of data and vast computing power that is often highly variable in quantity over time.
- Cloud computing already has a wide array of interested participants, both providers and consumers.
- API's are being defined and implemented for cloud computing, including a means for: configuring storage, managing key-pairs, configuring IP addresses, and managing instances of control, such as run, reboot, terminate, and query.

- CKM in a cloud environment must provide the usual capability of generating, using, storing, distributing, revoking, verifying, and destroying keys. Two scenarios of CKM are emerging: key management by the cloud infrastructure, or key management by specific applications that have been entrusted to run in the cloud infrastructure.
- A cloud infrastructure CKM model was described that has a centralized cloud security center for multiple data storage and computation centers.
- Hardware configurations were described, including virtual machines to be used for security. It was noted that having fully trusted virtual machines is not as simple as it looks, because virtual machines can be suspended, copied, moved, or lost.
- A Virtual Machine Manager (VMM) implementation was tested for quality, and all systems failed the tests; device emulation was particularly vulnerable.
- Conclusions: Cloud infrastructures can help in some key management areas. Clouds are designed to separate users. Users may be able to leverage the cloud infrastructure as a trusted third party
- One workshop participant asserted that cloud computing is the most insecure technology to come along and cannot be secured.

2.2.6 CKM Workshop Five Minute Presentations: June 8, 2009

Workshop participants could register to give five minute presentations at the end of each day. Two were given at the end of the first day:

Steven Ranzini, University Bank:

- He gave a description of a Southeast Michigan pilot program within a health provider community that will utilize Federated Identity Management systems to manage health databases.
- He asserted that small, distributed databases are inherently safer than very large, centralized ones for several reasons. He stated that some approaches used health care "silos" to manage health care information, and discussed first-responder emergency access to patient data (i.e., the EMT doesn't know where the emergency victim's healthcare data are located when the responder first starts to look for it) in unplanned circumstances, which caused special security provisions to be needed.

Matt Ball, SUN Systems:

- He announced an IEEE key management summit meeting to be held on May 4-5, 2010, in Lake Tahoe, Nevada; the website URL is http://www.keymanagementsummit.org.

2.3 June 9, 2009, Morning Session: Bill Burr, NIST, Moderator

2.3.1 Key Management and Fair Electronic Exchange, Dr. Silvio Micali, MIT

Keynote speaker: Dr. Silvio Micali is a professor of computer science in the Department of Electrical Engineering and Computer Science at MIT. He received his Ph.D. in Computer Science from the University of California at Berkeley. He has over 80 publications and over 40 foreign and domestic patents, primarily in the field of cryptography.

- The presentation focused on key management as an enabler of other cryptographic technologies, including fair electronic exchange (fair exchange is where both communicating parties obtain exactly the information and assurance they need). Non-repudiation of a transaction is needed, even with digital signature. A virtual trusted party is needed to complete transactions, even if a receiver does not want to use non-repudiation.
- Fair Electronic Exchange is defined so that both parties of an electronic transaction get what they need, or neither gets anything. One party gets the message only if the other party gets a receipt for the message. This is crucial to electronic commerce, but not easy, even with digital signatures.
- An online trusted third party (TTP) is not acceptable because of connectivity overhead. An offline Trusted Post Office model is acceptable. Certified email was used as an example.
- Example: the TTP is off-line; the TTP is unaware that S (the sender) and R (the receiver) are transacting. If S and R are both trusted, no additional security is needed; otherwise, a trusted, offline "electronic post office" is needed to provide additional security. Details of the mathematical transformations needed for a transaction are contained in the presentation slides.
- One laptop computer can handle the role of the Trusted Electronic Post Office for an entire country.
- An economic justification for a Fair Electronic Exchange system was provided.
- Fair Contract Signing between two un-trusted parties was the next example; group keying[3] is necessary in many electronic transactions, because not all parties are available, but the availability of a subset is acceptable.
- Conclusion: Mathematical foundation + concrete wisdom = good key management
- The presenter holds patents that cover the topics of the presentation.

2.3.2 Key Management and Information Management, Burt Kaliski, EMC

Keynote Speaker: Dr. Burt Kaliski is the Director of the EMC Innovation Network, which purchased RSA Security, where he was chief scientist and vice president of research. Dr. Kaliski was a primary developer of the Public-Key Cryptography Standards (PKCS). He received three degrees from MIT, where his research focused on cryptography.

- Good key management (KM) must be used to support good cryptography, which must be used to support good information security, which must be used to support good information management.
- The talk surveyed the history and future of Public Key Management (PKM); PKM is based on the original invention of the Diffie-Hellman public key cryptographic algorithm in 1976, and the RSA algorithm in 1977, along with many improvements up to the

[3] In this context, group keying is normally implemented as follows: The key K is formed by combining at least M key components out of a total of N key components, where $M \leq N$. Each of the N key components is held by a different entity. Any M or more key components can be combined using a mathematical process to form the key K.

present. The focus within EMC is on the convergence of cryptographic key management (CKM) with information management.

- They are now looking at the bigger, system-wide picture, not just cryptography, which is a component of security, and not just security, which is a service of information management. This broader picture will shape the future of cryptography.
- Information policy will be derived in the future from information requirements, which include security, information rights, data leakage protection, data retention, data search and index, authentication and authorization. Policies will be assigned to data, based on classification, and automated data classification will make scalability feasible.
- Data security using cryptography trades the problem of protecting lots of data with the identical, but smaller, problem of protecting the key(s) that protect the data.
- The security system that implements and supports cryptography is more important than the specific cryptographic algorithms, in many circumstances. Security needs a trusted system that enforces access control. Physical security needs a system that can be virtualized.
- Data managers must be able to assign information management policies and, subsequently, information security policies to data, based on some classification schema, including the application, metadata, and/or content of the data. Policies are derived from information requirements and include: information rights management, data leakage protection, data retention, data search and index, authentication and authorization.
- Automated data classification provides scalability. Information policy must be primary and must be able to drive security policy, which can be called information-centric policy management.
- Information management must be based on a service-oriented architecture, with multiple levels of display of information to the manager. A cryptographic key is just another piece of information in a database; if wrapped, a key is really just data needing the same protection as normal data.
- Policy for managing personal identity information is just another extension of information management.
- The presentation ended with the question: What if there was no Public Key Cryptography? His response: quantum computing threats are real, but have not been mounted. Second question: Could symmetric key management, trusted hardware, etc. fill in the need? No answer was provided.

2.3.3 Enterprise Key Management Panel, Chair: Robert Griffin, RSA

Chii-Ren Tsai, Citigroup

- His presentation focused on Citigroup's security program that utilizes Key Management (KM) in combination with a security program based on risk analysis. The most prevalent problems with KM today include: weak pseudo-random number generators for key generation; cryptographic keys that are hard-coded into the application; approved Certificate Authorities, cryptographic algorithms and key lengths that are not used;

cryptographic keys that are not renewed periodically; and cryptographic keys and passwords that are not encrypted/protected in storage or in transit.

- Future directions include: central KM solutions for managing keys in Hardware Security Modules (HSM's) or software; a cryptographic key management framework to simplify KM; segregating key management from key use; key attributes and KM policy, especially for symmetric keys; and KM policy mapping for interoperability.

Matt Ball, Sun Microsystems

- Sun's perspective on enterprise KM was presented. The mission is to ensure that a user does not lose or destroy the key! Enterprise KM includes: the secure creation of keys, auto replication of keys, KM policy, audit logging, role-based management, scalability across an enterprise (good availability and a large number of keys and applications), interoperability, and standards compliance (e.g., IEEE P1619.3, OASIS KM interoperability protocol) and secure key export to trusted partners.

Matt Fanto, Aegis

- The focus of the talk was on KM in the auto industry. Cryptography is being, or will be, used in all aspects of the automotive business, including within the car itself. They are concerned with (1) a single point of failure, where systems are without support for redundancy, so that KM systems or backups are at the risk of a BIG loss (catastrophic); (2) immediate needs versus costs, and a more flexible credentialing system – many manufacturers are locked into the current system with no way to change – Electronic Key Management (EKM) is needed that can leverage existing policies and authentication methods to lower cost and give faster deployment; and (3) an offline availability of keys.

Steven Wierenga, Hewlett Packard

- HP has a long history of KM for the financial debit/payment network. The drivers for cryptography are recent legislation on notification of breaches, the Payment Card Industry Data Security Standard (PCI-DSS) that provides mandates for all credit card companies, plus large-scale hacks, fines, and remediation. HP would like to see interoperable KM systems that support cryptography.

Panel Discussion:

- Response to audience questions about what is wanted/needed:

- Citigroup would like to see split responsibility for KM implementation and operation;
- SUN Microsystems would like to see a single industry standard;
- The auto industry is just starting to use enterprise KM. Interoperability will be a problem because keys are burned into devices during vehicle manufacture;
- RSA: Standards must be extensible/flexible enough to take into account new user groups and new technologies;
- HP: The OASIS KMIP (Key Management Interoperability Protocol) and Client Software Development Kit (SDK) with a no-cost license.

- Comments made by the audience:

- Enterprise Key Management: Counter measures are needed. Simplify key functions, and improve ease of use. Public key management is difficult, but doable; certificates make it doable. Symmetric key management is good, but cumbersome – a wedding of public key and symmetric key management must be supported.
- PKCS: The 1995 standard must be able to evolve to keep up with new technology and applications.
- Criminals will go after the highest value target. Security managers must mitigate the risk and protect valuable and sensitive data.

2.3.4 Identity-Based Key Management (IBKM): Terence Spies, Voltage Security

- The scope of the presentation was enterprise-level key management for encryption in sensitive applications. The intended consumer of this presentation is an enterprise developer that needs to encrypt data.
- It is important to know for whom the CKM system is being developed.
- For many of you, crypto is a lot of fun. However, designers must make cryptography easy to use and friendly. Currently, anti-spam tools are understood and desired by users, but cryptography is not.
- Premise: Whenever data is in the clear, it can be hacked. We must keep data encrypted as much as possible.
- One security solution is data link protection, whereby device keys are used in communication devices at every end of every link to protect data. However, there will still be vulnerabilities in applications.
- We need to be able to turn an access control policy into an encryption key, and the access control policy plus a credential into a decryption key.
- Three different key management scenarios were described, satisfying very different customer needs: (1) Intranet portal document sharing; (2) customer communications; and (3) partner-to-partner data sharing. Examples of Identity-Based Key Management (IBKM) architectures and requirements were provided for each.
- The advantages of IBKM are: authentication is done at decryption time, which matches a user's expectations of the authentication needed to get information; keys are short lived, making a new public key is nearly free; and the time between identity binding and key issuance is short, as opposed to bind-first systems. IBKM provides a model for thinking about application-level key management.
- Because of application vulnerabilities, some data must be encapsulated no matter where processed, stored, or transferred. Applications must be able to process ciphertext when given a security policy and the necessary credentials.
- Access policy must be definable as some function or algorithm that enforces the policy via a cryptographic key (e.g., encipher, decipher, sign, verify, authenticate).
- Credential Policy must be definable as a function or algorithm that processes ciphertext and yields plaintext.

- Taxonomy of keys: signature creation, signature verification, communication privacy, stored data privacy, authentication.
- The Chief Information Security Officer must be able to communicate with enterprise security developers. Access control data must be the basis of cryptographic mechanism control. Failures in many KM services often force users to get a key outside of the KM system with disastrous results.
- IBKM looks like access control. Your Name@domain is a natural identifier and can be used effectively as such, with appropriate authentication and verification. This identifier is simply a Directory object for a user. RFC 822 identifiers are as universal as they come.
- Benefits: IBKM yields automatic identity authentication at decryption time. Users are used to providing their ID and authenticator to access data. Identity Based Encryption (IBE) can also be used for binding to groups, i.e., ID = group or role. The key server authenticates the identity for access authorization.
- Information management policy and security policy can be implemented and enforced by the key server.

2.3.5 Scalability using Centralized Key Management, John Marchioni, ARX

- The talk focused on scalability and the need for using a centralized key management approach. Specifically, cost-efficient, scalable, secure and easy-to-use PKI applications are needed by industry.
- From the vendor's perspective, the user is the problem! There are major problems with distributing keys in terms of scalability when the user gets involved. The process of key revocation often breaks down because users do not maintain updated revocation lists. It's difficult to audit key usage and key actions remotely.
- With a centralized key distribution system, actions do not get lost and revocation and certificate control are easier. An audit of actions is much easier if the user has to go through a central facility to use the key.
- A PKI should be a business customer enabler. Customers don't want to be involved in KM. They just want to get their job done!
- Centralized key management provides a lower administration burden. An enterprise cannot rely on end users for security, especially managing keys. Centralized KM minimizes the involvement of the user; it provides scalability with control. Organizations of all sizes can benefit from centralized key management strategies; they will find centralized KM both affordable and durable.
- In many customers' environments, users need to digitally sign for a transaction very infrequently. Non-repudiation services are also seldom required; authentication is often a local matter. One-time password tokens are often used, and an identity-challenge oftentimes suffices for a signature if it is done whenever a signature is needed.

2.3.6 Globally Scalable Key Distribution: Jeffrey Opper, BAE Systems

- DARPA supported some work on globally scalable key distribution for military applications, including very large groups of users. Examples include sensors remotely deployed in very large numbers (sometimes called sensor dust); millions of micro, unmanned aviation vehicles; and global support of secure wireless delivery systems, such as radios, telephones, and GPS.
- The revocation of potentially compromised keys must be completed in seconds, not minutes. Very large subsets of keys need to be revoked upon command. The revocation of keys must scale according to the number of end points revoked, not to the total number of keys. It is permissible to miss a rekey, but not a revocation (i.e., fail-secure). A binary-tree approach is used. A key distribution algorithm must guarantee that only a specific subset of good nodes has good keys for a period.
- Key management requirements of the presenter's customers include: secure global key distribution; responsive key revocation; customized "last mile" delivery for special environments, such as the military; scalable key encryption algorithms must support secure wireless delivery; a near-zero vulnerability of disclosure of a key must be maintained; and an override of policy must be available when a commander demands it.
- The Certificate Authority deals with keys globally, while the end user deals with them locally. The KMS must be more dynamic as the number of customers scale upwards. Key Management requirements include secure global key distribution; responsive key revocation: a near-zero vulnerability window, due to compromise; revocation within seconds, not minutes; delegation to remote management with an override capability; and KM must be mission and context driven.
- Summary: Our global presence requires globally-scalable key management. Deterring the cyber threat requires nearly-instantaneous revocation. Operational requirements mandate flexible last-mile deployment strategies. Fundamental technologies exist that provide the needed scale, weighted key assignment, batched transmission, permutation trees; and augmented broadcast encryption.

2.3.7 Use of Group Key Management in Internet Standards: Brian Weis, Cisco

- The presentation focused on group key management (GKM), where a group consists of three or more entities sharing the same key material.
- GKM methods can be broadly classified as either: contributory (e.g., CLIQUES), where group members use the Group Diffie-Hellman algorithm to independently derive group keying material; or centralized (e.g., RFC 3547 (GDOI)), where group members register with a trusted third party (group controller/key server) and are given group keying material.
- Standards groups have concentrated on centralized GKM, because such methods best meet the needs of Internet group applications. Authorization is straightforward; revocation of group members is relatively easy; centralized methods typically use existing KM framework components.

- General authenticated encryption methods can be used for key transport. It is recommended that key derivation methods described in NIST SP 800-108 should be explicitly noted as updates in newer NIST recommendations.
- Specific standards were discussed, such as IEEE 802.1 frame encryption, IEEE 802.11i, and Internet RFC 3740 as examples undergoing review regarding GKM.

2.4 June 9, Afternoon Session, Elaine Barker, NIST, Moderator

2.4.1 Authentication using PIV Symmetric Keys, Sarbari Gupta, Electrosoft

- The presentation focused on experience with the government FIPS 201 standard Personal Identity Verification (PIV) card and its use of symmetric keys.
- The PIV standard presents a rapid (and potentially two-factor) authentication scheme using PIV symmetric keys. The benefits of the symmetric Card Authentication Key (CAK) use are: strong authentication, compared to the use of a Card Holder Unique Identifier (CHUID); fast; doesn't need a PIN to activate; and can be performed over a contactless interface.
- The cons of symmetric (CAK) authentication: typical symmetric key challenge-response schemes require the CAK to be known by the verifier, and a cross-agency verifier will not know the CAK.
- In the FIPS 201-1 standard, the CAK is optional; it may be a symmetric or asymmetric Card Authentication Key.
- NIST SP 800-116 strongly recommends that a CAK be included in a PIV card. The PIV card uses single factor of authentication. The holder of the card cannot be verified; in a PACS (Physical Access Control System). One agency can use a symmetric CAK for accessing another agency in a PACS.
- A Federal Agency Smart Credential Number (FASC-N) is an index to a large data base. A nonce is special data in a PACS data base. An agency can grant or deny user access based on an authenticated FASC-N.
- Challenge-response access control is possible via a PIV card. PKI authentication-at-enrollment establishes a basis of trust. Improvement in security is obtained via a multi-factor authentication and dynamic challenge-response pair.
- One issue in physical access control is the handling of local PIV cards versus the handling of visitor PIV cards.
- The PIV system must get the FASC-N from the PIV authentication certificate, and then prompt the user for a PIN challenge-response. The key is not entered into the PIV card by the user.
- A question was asked regarding PIV card expense: The questioner wanted the cost of a PIV card to be reduced by an order of magnitude. The response was that it is hoped that within two years the PIV card may have reduced cost.

- Bill McGregor, NIST PIV project leader, responded to the question regarding the cost of the PIV card. He said there is now an imigration to the PIV card, and 3 million PIV cards have been issued. Costs are expected to come down as volume and competition increase.

2.4.2 Open Source Symmetric Key Management: Arshad Noor, StrongAuth, Inc.

- StrongKey is an open source electronic symmetric key management system. An EKMS is a collection of technology, policies and procedures for managing the life-cycle of all cryptographic keys – both symmetric and asymmetric – in an enterprise. It provides a graphic user interface (GUI), and supports RSA, ECDSA public keys and symmetric keys.
- StrongKey allows an administrator to define a CKM security policy; to generate, encrypt, decrypt, escrow, authorize, recover, destroy, and audit operations regarding cryptographic keys; and to manage keys for applications, such as phones, cash registers, laptop computers, cell phones, and desktop computers.
- The Public Key Infrastructure (PKI) is a concept. A Secure Key Management System (SKMS) is what the typical customer wants and uses.
- In a Global SKMS, every request/response is digitally signed. The symmetric key in a response is always encrypted. Every object in the SKMS data base is digitally signed, including the audit trail. Every symmetric key is encrypted and digitally signed. The key cache is in the client. Customers must be able to continue processing if a key fails to be authenticated. A customer security policy decision is whether to fail safe or to fail soft.
- Encryption takes place in the application layer. While the application layer can be exploited, data at all lower layers is encrypted. Who encrypts at Layer 7? Application vendors, POS terminals , Payment Application Best Practices (PABP) applications, e-commerce, healthcare, VoIP service companies, and application development teams that do not control lower layers of the network architecture tend to encrypt at the application layer.
- The payment card industry encrypts the card data and uses an appropriate CKM system. An example was provided of a $16M lawsuit against an auditor that approved the security of another bank performing card services for that bank.
- An SKMS will do for symmetric key management what the DNS did for name-service management, and DBMS did for data management.

2.4.3 Cryptographic Key Management Framework: Miles Smid, Orion Security

- NIST initiated this CKM workshop, in part, to solicit information on what constituted a Cryptographic Key Management (CKM) Framework; I hope that the ideas expressed in this talk will stimulate further input.
- There are many potential CKM solutions; the value of each solution usually depends upon the particular application that it is trying to satisfy. At a workshop like this, the attendee is presented with a bewildering array of possible solutions, and even when the reference documents are examined, there is a lack of consistency that prevents comparison.

- A CKM Framework might provide organization and consistency to the collection of CKM system designs by specifying the essential components of a CKM system in a structured framework and present a logical order in which they might be addressed. In addition, the framework could specify key management standards that should be followed or at least considered when developing a CKM solution. The framework may also lay a foundation for future standards that need to be developed in order to have more complete, secure, and interoperable solutions. Such a framework may bring order to disorder and thus, lead to the increased use of cryptography for information security applications. In order to benefit from the economies of scale, NIST would like the framework to be used by both the U.S. Government and the private sector.
- The CKM System Design Framework could be thought of as a comprehensive list of the essential policies, components, activities, processes, and assurances that compose a CKM solution. If you come up with a different definition or have some additional components to suggest, please let us know.
- There is a simple analogy between a CKM System Design Framework and the process involved in the building trade, and more specifically, a custom home. The materials required to construct a home could be thought of as the components required to build the home according to the design illustrated in the blueprints. Similarly, CKM policies and components could be selected from a CKM System Design Framework in order to develop a CKM solution that, in turn, supports an information management application. Thus, the CKM System Design Framework is an essential element in a CKM solution. Assurances of quality in the custom home are provided in building standards, local building codes, and standards of best practices of the building trade. When the CKM policies, components, and recommended security practices are properly selected from the System Design Framework and combined properly in a CKM system design, we have a well-defined CKM solution.
- The System Design Framework defines and provides general information about the policies, components and assurances available, but does not dictate the specifics of the policies, components and procedures to be used in a CKM implementation. If the System Design Framework tried to specify all the requirements for all possible CKM implementations, there would be too many frameworks. Rather, the framework provides a structure for insertion of the specific policies, components and procedures that are used to satisfy a particular application.
- Organizational policies for data availability, confidentiality, integrity, and access control are very important inputs when using the framework to design a CKM solution. In addition, the key management policies for all key types and related keying material over the key management lifecycle need to be consistent with the overall data protection policies.
- In order to ensure that the CKM solution provides adequate support for the application, the framework needs to define necessary inputs regarding the unique requirements or constraints that are imposed by the application or the organization performing it. For example, input should include the desired target security strength for the managed information, the assurances that the CKM solution must meet to achieve the target

security strength, and how conformance of the implementation to the CKM solution is to be verified.

- CKM components from the framework must be selected to support the specified organizational and application policies, requirements and constraints. CKM components include keys, algorithms, primitives, and protocols. Components may also include modules, products, and even the combination or composition of other components in an innovative manner to provide a secure CKM solution.
- For interoperability, certain interfaces will need to be specified. Possible interfaces include: the cryptographic algorithm interface, the key management interface, the cryptographic module interface, the product interface, and the application interface. In general, only the interfaces that are used by entities outside the application need to be specified.
- Finally, the framework should encourage a CKM solution developer to think about future transitions. When will the CKM solution need maintenance, when will it need to be replaced, and how might it best be phased out? These questions are usually overlooked by today's CKM solutions. As a result, it is often considered preferable to live with an insecure CKM solution, than to suffer the pain of replacing it.
- Frameworks can be strong supporting structures. We will try to define a single CKM Framework that is a useful foundation for, and relevant to, all potential CKM solutions and information management applications.

Comments from the audience

- The Common Data Security Architecture (CDSA) has goals that are similar to those in the CKM Framework.
- There are other elements that need to be in the Framework.

2.4.4 Leap-Ahead Technologies: Miles Smid, Orion Security Solutions

- There are several problems with today's Cryptographic Key Management (CKM) solutions. They are expensive, hard to implement, difficult to maintain, perhaps insecure, and user unfriendly. Wouldn't it be nice if we could find a new technology that would permit us to leap over these problems in order to attain our goal of secure, cost effective, transparent, information management systems?
- Consider what makes a leap-ahead technology in cryptographic key management. There are at least four types of leaps that we could make: a leap in base technology, a leap in security, a leap in the ease of management or use, or a leap in some combination of these items.
- Leap in base technology: This usually involves a major change in a base technology that eliminates the old technology, and many of the problems along with it. Computer networking technologies have made such dramatic advances that today we no longer have to worry about how many days it will take to get information from one party to another. Unfortunately, this technology significantly increased the need for communications security that uses cryptography, which in turn leads to our need for effective

cryptographic key management solutions. Quantum cryptography may someday provide us with the leap that we seek, but for now.

- Leap in security: Ideally, we would like network security at no extra cost. Recall the days when we were told that the cost of safety was not justifiable in automobiles. We were told that the public would never pay for seat belts. Today, not only do we have seat belts, but we have front and rear air bags, side air bags, and someday soon perhaps upper and lower air bags. Yes, we pay more for our cars, but we expect safety to be built in.

  There may also be smaller leaps in security that could help solve our cryptographic key management problems. What if we had the capability to automatically validate key establishment protocols or even use provably-secure protocols? Quantum cryptography could also improve security by permitting us to easily distribute secret values in a secure manner. But, there is more to key management than key establishment. Many key management problems involve the secure generation, storage, access and recovery of the keys, either before or after they are distributed.

- Leaps in ease of implementation, management, and use: We have already made significant progress in this area. Electronic distribution of wrapped keys led to an improvement over manually distributed keys, and public key-based key distribution led to an improvement over key wrapping. Today, PKI, even with all of its problems, provides a major leap ahead over previously used systems.

  But, we still seem to be repeating some of the mistakes of the past. We build systems, we implement them, and then we find out that the users consider them unacceptable. We must not wait until the last minute to get the user's opinion. We need to build prototypes of a system and test them with real users before we extensively field the final product.

- We need to explore the advantages of alternative approaches like identity-based key management.

- What if we had cloud key management? By that I mean that I could go to some trusted part of the cloud and say, "Please give me a key to communicate securely with jsmith@verizon.net." Better yet would be if I could go to the trusted part of the cloud and say, "Please give me a secure channel to jsmith@verizon.net." Best of all would probably be if the security was provided by the cloud for all my communications.

- I like a holistic approach to enterprise key management. Perhaps this effort will lead to a standard set of key management capabilities for information protection.

- After considering the possibilities for a leap-ahead in cryptographic key management, I feel that I should mention the advantages of just walking. We always like to find the easy way out, but sometimes old fashioned work is the best route to progress. So I would hope that we continue to improve on what we have and let the leaps come where they may.

- Comment: Customers want to defer to authorities to tell them what is good, better, or best. There is a need for a public-private partnership that allows the new CKM technologies to incubate and be evaluated so that consumers will accept the solutions when they become available. RSA had to be vetted for some time before it became accepted.

- Comment: In Michigan, there are trusted CKM test-beds planned for development under President Obama's bailout financial plan that will be used to verify the utility and security of various solutions.
- Comment: We must have a uniform solution to a uniform family of problems. We should have a glossary of security to minimize undefined buzzwords that are used to sell commercial products. You may be creating the same problems but in different clothes. A lexicon is needed in security.
- Comment/question: Generating a key by a CA and associating it with you. Is this key management?

2.4.5 CKM Workshop Five-Minute Presentations, June 9, 2009

- **Rene Struik, Certicom Research**: The Elliptic Curve Digital Signature Algorithm (ECDSA) signature scheme can be made into a Fast ECDSA signature scheme (40% faster). It can also achieve fast digital signature verification. We should transition from ECDSA to Fast ECDSA. The details are available in the presentation slides.
- **Larry Himes:** He spoke of his many years of experience in security technology, including validation of cryptographic devices to FIPS 140-1 and 140-2, which were difficult tasks.
- **Santosh Chokhani, CygnaCom Solutions:** What is good about PKI? E-business growth is supported by a PKI. Most people know about Public Key certificates. PKI has created some wealth for many people. One of the biggest problems with the PKI is enrollment. Some lessons learned regarding PKI usage are that the PKI should be put behind a screen, and the user should not know anything about it. Sometimes one needs 40 keys to use a secure information system; too many keys are the problem; one key per person should be sufficient. It is hard to implement shades of gray in trust. Do not use the word policy unless you have to and mean it.
- **Brian Tokuyoshi, PGP Corporation:** The emphasis should be on the goal, rather than on the path for getting there. Compliance is a motivator for reluctant users. Protection from data breaches should be, but often is not, the prime motivator.
- A major problem is often that there are too many keys, rather than too few. Data on laptops should be encrypted.
- Definitions of the words secure, key management, etc. are important. E-discovery is finding out how long it takes to encrypt and decrypt data. Key management is often done poorly: there is no overall strategy, and handling data-at-rest can be expensive. We need a plan to manage keys BEFORE encryption is mandated and used.
- There are six steps to encryption, but people often start at step 5. In technical innovation, there are often peaks of expectations, followed by troughs of disillusionments. Applications tend to make poor key management systems. For a lot of end user organizations, it's going to get worse before it gets better.
- Customers need to start thinking about processes for security, not just the technology. Compliance initiatives should emphasize getting the administration done right. Best practices include a plan for your long term encryption requirements**.**

- An organization must develop an enterprise policy on managing keys. It must survey and catalog existing data, its sensitivities, and its security requirements. It must develop and deploy a plan for managing encryption keys, and it must deploy the data protection solution, and then tackle the next project.

2.4.6 Overall Summary of the CKM Workshop: Elaine Barker, NIST

(Note: Weather conditions caused the workshop to close early. This presentation was prepared but never presented. A summary of the presentation slides is included for completeness.)

- Cryptographic Key Management: There is a major need to undertake key management as part of the national cybersecurity initiative. The CKM workshop is a first step towards a comprehensive and interoperable CKM. A joint government-industry partnership is the best approach.
- Key Organizations to be involved: NIST and other government agencies, standards groups, IETF, IEEE, OASIS, industry and academia, etc.
- Key Management is needed for e-Commerce, banking, air traffic control, the aerospace industry, defense, emergency first responders, the health care industry, the Internet (Routing, DNSSEC, etc.), citizens and consumers.
- Considerations for future key management systems: Design systems for high availability and survivability. Prepare for emergency access to keys; worry about unintended consequences – both good and bad. In light of quantum computing, look at means other than using public keys. Look at quantum-resistant algorithms and schemes.
- Requirements for CKM: Must be user-friendly; easy to use – plug and play; must be a user-driven capability; must be secure, cost-effective, fault-tolerant, and highly available; must provide protection against destructive attacks and be interoperable; must be designed to be used enterprise-wide, by multi-partners that use multi-vendor products, and be usable by multi-applications; must be scalable and enhance interoperability in time of emergency. Metadata must be defined, as well as defining the security to protect it. We also need key inventory control, accountability/auditing of the keys, policies for managing the keys and metadata, and safety requirements for certain applications.
- Challenges: Cost, enrollment, complexity, unclear future computing paradigms are (e.g., cloud computing), user-friendliness, security analysis, and competing solutions that do not interoperate.
- Applicable Models: One can model CKM systems in different ways, including the complete life cycle. Do a security analysis on all the keys in the system. Model all system administrators and their actions, and have information management models of all keys protecting data in the computer.
- Users of a CKM System: Humans, devices, applications, programmers, administrators, and others.
- Design Considerations: We need a mix of long-term symmetric and asymmetric keys for some applications. We also need algorithm and security parameter agility and to keep the design simple and cheap.

- Technologies and Standards to be considered: Identity-based encryption; Enterprise enterprise key management; OASIS KMIP; Computer Mediated Communications (CMC), which is any communication based transaction that occurs between two or more networked computers; factory-generated device keys for enterprise enrollment and registration; identity-based symmetric keys that may reduce the scale of the symmetric key distribution problem; cloud computing; subset-difference revocation; and group key management.
- Next Steps: A workshop summary (i.e., this NIST IR) will be posted in the fall of 2009, and a draft Cryptographic Key Management System Design Framework will be posted for comment in the Fall of 2009; an IEEE Key Management Summit Workshop will be held in the Spring of 2010; NIST research results will be posted on its web page when available.

3. CKM Workshop Presentation Highlights Organized by Topic

This section presents highlights of the presentations organized by selected topics for Cryptographic Key Management (CKM). These CKM topic highlights have been extracted from the highlights of the Workshop presentations. Explanatory information was added when clarification was required.

A subset of these topics will provide a foundation for the CKM System Design Framework (herein sometimes called the CKM Framework) being developed by NIST. Other topics are included here to present auxiliary information that is needed to understand CKM systems and their major issues, but not needed to design them. The acronym CIA is often used in security where C is Confidentiality Assurance; I is Integrity Assurance; and A is Availability Assurance of data.

3.1 Policy

A policy is a specification of the objectives, constraints, responsibilities, and actions concerning a specific subject. A Data Security policy (e.g., CIA assurance) specifies the sensitivity of data to disclosure, modification, and destruction, and specifies what actions are to be performed in protecting the data's confidentiality, integrity, and availability. A Cryptographic Key policy is similar to and derived from the security policy for the data protected by the keys. The protection of the key from disclosure and modification must be assured in order to protect the data from disclosure and undetected modification. To assure data availability, both the encrypted data and the key needed to decrypt that data must be available when and where needed. Policy negotiation involves two or more entities (users, processes, computers) attempting to combine data having different policies.

The following are highlights of presentations from the workshop related to policy considerations.

- Most of the international fund transfers had been going through a single financial institution. When that capability was lost, a very serious situation turned into a real crisis.
- The President's policy review has brought home to a large community the nature of the threats that we're facing. It also demonstrates the urgency of having policies and technologies available and in place for mitigating those threats.
- We should not accept high risks in the future Internet because we don't want the adversaries to have high payoffs.
- We want to establish actions and roles that are not limited only to the government. There are roles for government, roles for the academic community, and roles for industry.
- Privacy concerns and security concerns are sometimes conflicting. The organizations that use security mechanisms and key management methods are very diverse in policy.
- We don't have just a national security environment and a non-national security environment today; we have a collective community.

- We must first identify key players in the CKM program. We then must establish appropriate roles and partnerships among the players. We need to coordinate our actions to produce widely acceptable solutions.
- The current Federal Cybersecurity initiatives are primarily to protect .mil and .gov information on the Internet. However, ninety eight percent of the world is .com or .edu or .org or a foreign segment of the global Internet.
- A public-private partnership should be formed to focus on protecting the Internet. That group would focus on what we need to do as a nation, even as a global partnership, to solve the problems with the Internet. Panels would be set up to address policy, strategy, technology, and operations.
- We need to address and solve Internet problems before we have a catastrophic event.
- The nation should come together in a partnership that collaborates and cooperates to solve the widespread information-security problem.
- Ultimately, we need to re-engineer the Internet for the globe. We must design and build security into the new Internet. We must include countries such as Russia and China in creating the design.
- NSF security policy has been continually modified in accordance with new problems. We (NSF) seldom do anything that requires un-proven methodologies, we follow all government rules, and we want to be told that something new is mandatory.
- NSF now combines information management with security management. It has a strict security awareness program; its visitor information network was separated from its internal NSF user network, and all Social Security Numbers in the system are encrypted.
- In the next decade, we foresee more OMB/NIST mandates and more programs for protecting the Internet from the users, rather than protecting users from the Internet.
- We need solutions that support wider audiences of users, including FEMA, allies, charities, State governments, and emergency first-responders.
- Pressure from many sides drives the use of encryption: regulation compliance, outside auditors, the Board of Directors, policy compliance, the protection of critical data, etc. There are many competing sets of rules and people who have a stake.
- The reality of lifecycle key management is that policy and workflow must be continuous, and all the components must be integrated properly. Enterprise encryption policies must be comprehensive and cover a wide range of components, including certificates, keys, algorithms, validity periods, and multi-person control. Policy is the overarching guidance and requirement that must be achieved.
- Enterprise encryption policies must cover data, discovery, keys, certificates, key storage, applications, disaster recovery, validation and monitoring, reporting of workflow and process, personnel roles and assignments.
- Information policy will be derived in the future from information requirements, including security, information rights, data leakage protection, data retention, data search, data

index, authentication, and authorization. Policies will be assigned to data, based on classification, and automated data classification will make scalability feasible.

- Data managers must be able to assign information management policies and information security policies to data, based on the application, application metadata, and/or content of the data. Policies must be derived from information requirements and include: information rights management, data leakage protection, data retention, data search and index, authentication and authorization.
- Automated data classification supports a level of scalability. Information policy must be primary and must be able to drive security policy, which can be called information centric policy management. Cryptographic key management policy is derived from these policies.
- The policy for managing personal identity information is just another extension of information management and information protection policy.
- We need to be able to turn: 1) an access control policy into an encryption key, and 2) the access control policy plus a credential into a decryption key.
- Access policy must be definable as some function or algorithm that enforces the policy via a cryptographic key (e.g., encipher, decipher, sign, verify, authenticate).
- A credential policy must be definable as a function or algorithm that processes ciphertext after encryption and yields plaintext after decryption.
- Information management policy and security policy can be implemented and enforced by a key server.
- A good CKM system allows an administrator to define a CKM security policy, which is then enforced by the system.
- CKM policies and components should be created and selected based on a CKM System Design Framework in order to develop a CKM solution that, in turn, supports an information management application. Thus, the CKM System Design Framework is an essential element in creating a CKM solution.
- A CKM framework defines and provides general information about the policies, components and assurances available, but does not dictate the specifics of the policies, components and procedures to be used in a CKM implementation.
- Organizational policies for data availability, confidentiality, integrity, and access control are very important inputs when using the framework to design a CKM solution. In addition, the key management policies for all key types and related keying material over the key management lifecycle need to be consistent with the overall data protection policies.
- CKM components from the System Design Framework must be selected to support the specified organizational and application policies, requirements and constraints.

3.2 Trust

Trust is a quality assigned to an entity concerning the de facto level of assurance provided by the entity in a specific area. If an entity has a high level of trust, fewer security provisions are required for it. Entities requiring some level of trust include users, PKI services, servers, devices, and software, as well as the communications channel itself.

The following are highlights of presentations from the workshop related to trust considerations.

- The Internet has introduced a level of vulnerability that is unprecedented. We are worried about spies who might be invading our privacy and our sensitive or critical information systems, but mostly about attacks against our information systems that steal or destroy our data.
- The nation is at strategic risk.
- Unauthorized destruction of data may be a more significant problem than disclosure of the data.
- The current Internet attacks are intended mostly to collect information and exploit it. Destruction of highly valuable or sensitive data is unlikely because of the consequences of world instability.
- All components of a system should be laid out so that the system flow can be analyzed for ANYTHING AND EVERYTHING that can go wrong in the total system, not in individual components in isolation. Evaluators must think of how an entire system can be broken. Total systems design solutions are needed.
- Certificates for the general public are somewhat problematic; it is difficult to really verify the initial identifier (e.g., of the person associated with a certificate) without context.
- Verifying that the object code in a computer is the "same as" the source code is a difficult problem.
- We should look and flag websites containing malware and warn users about visiting a flagged website.
- Communicating parties should seek and use increased levels of trust, based on having a common security policy.
- A security analysis should start with a risk analysis, including an inventory of keys, certificates, and applications. An application must be configured for enterprise-wide encryption, which includes client protection, servers, networks and archival data storage.
- Fair exchange is where both communicating parties obtain exactly the information and assurance they need. Non-repudiation of a transaction is needed, even with digital signatures. A virtual trusted party is needed to complete transactions, even if the receiver does not want to use non-repudiation.
- An online trusted third party (TTP) is not acceptable because of the required communication connectivity overhead. An offline Trusted Post Office (TPO) model is acceptable; certified email was used as an example.

- Example: A TTP is offline. The TTP is unaware that (the Sender) S and (the Receiver) R are transacting. If S and R are both trusted, no additional security is needed; otherwise, a trusted offline "electronic post office" is needed to provide additional security. Details of the mathematical transformations needed for a transaction are contained in Silvio Micali's slides.
- One laptop computer can handle the role of a Trusted Electronic Post Office for the entire country.
- Economic justification for a Fair Electronic Exchange system was provided by the Silvio Micali.
- Fair Contract Signing between two un-trusted parties was the next example; group keying[4] is necessary in many electronic transactions, because not all parties are available, but a predetermined subset of all the parties is acceptable.
- The security system that implements and supports cryptography is more important than specific cryptographic algorithms in many circumstances. A trusted system that enforces access control is needed for security. A system that can be virtualized is needed for physical security.

3.3 Impediments

Impediments are barriers that must be circumvented or overcome in order to achieve a goal. Impediments to designing, implementing, and using a CKM system include: patents owned by others that cover parts of the system, competition by others in a closed market, no standards for the product that might enlarge the market, and too many standards that confuse the customer and reduce the market.

The following are highlights of presentations from the workshop that discuss impediments.

- We have institutional issues, including getting the useful security mechanisms into place.
- We need to understand the requirements of the Federal government. We have to be working hand-in-hand with industries. What are our resources and what are our practical constraints?
- We need to understand the potential impediments to satisfying requirements in technical, social, and institutional contexts. We have to evaluate alternative approaches, and then we need to analyze the benefits versus the costs.
- Some impediments to vastly improving CKM include: organizational requirements that are often conflicting, funding issues, using the funds effectively, and intellectual property interests.
- Creating a standard that is widely used is difficult if the standard infringes on someone's intellectual property. Standards can only succeed if they may be used satisfactorily within existing intellectual property constraints.

[4] In this context, group keying is normally implemented as follows: The key K is formed by combining at least M key components out of a total of N key components, where $M \leq N$. Each of the N key components is held by a different entity. Any M or more key components can be combined using a mathematical process to form the key K.

- KM brings expense to the Internet because of the complexity, required infrastructure, and computation power needed to perform cryptographic protection.
- The initial enrollment of a subscriber is the most expensive and hardest part of key management, because it takes human interaction with a subscriber in a trusted environment.
- KM is a major requirement that is difficult and complex. There is a need to analyze an entire system for both security and reliability. An enterprise KM is an untrusted client in a trusted server, rather than a trusted client in an un-trusted server, as is the case when a consumer uses cloud computing .
- Users don't care about keys. Users don't like to worry about details, but need to be guided. Humans tend to be the weak link. There needs to be a crypto administrator in charge of cryptography and who controls user identification and authentication.
- The biggest problem is manual key distribution. There is a problem with replacing the keys and updating revocation lists. We need to be able to streamline the distribution process and replace manual key distribution with a minimal impact process.
- There is an education gap. The conventional wisdom is that "computer security systems can't be effective unless they are complex and difficult to use." While this may once have been true, the security profession has witnessed dramatic improvements over the last ten years.
- There is a perception gap. The conventional wisdom is that security technologies are too expensive to implement with sensor and control networks, due to energy constraints, and computational and storage constraints. There is also a gap between security perceived by the user and actual security provided to the user.
- There is an affordability gap. The conventional wisdom is that the licensing cost of security technologies may present a hurdle. Licensing models, such as those used with the consumer electronics industry, may have some merit for ubiquitous computing as well, since both are concerned with mass-scale deployment of networked devices ("the internet of things") and enforcement of compliance.
- Issues that need further work: problems with setting up secure links; devices and device IDs; reusing a key at different layers (e.g., of a network); a multi-application device in which various applications could have different security requirements; certificate generation; communication encapsulated in one protected part of a device that can be trusted; idealized provisioning where there is no security perimeter versus where there is a security perimeter with specified trust inside; trusted modules are possible, but we would like to minimize trust dependencies; various network technologies; little human involvement in secure system operations; having many root keys permanently in a device that are seldom used, except in accordance with security policy.
- More vulnerabilities will be found in browsers, operating systems, routers, domain name resolution processes, DPI-based attacks (e.g., Against TCP) and MANETs (auto configuration and overrun conditions).
- Vulnerabilities include zombies, botnets, drive-by downloads, and zero day attacks.

- Attackers could threaten to bring parts of the Internet down if not paid a ransom.
- If hosts and routers must authenticate themselves, the overhead will be too high.
- Computer configurations that have gone "bad" are difficult to detect.
- Encryption challenges include: data security, key security, enforceability, operational efficiency, system availability, reputational risk, business continuity, disaster recovery, and privacy.
- How can applications be secured in a cloud-computing environment? Can virtual machines maintain separate security policies?
- Challenges (i.e., what makes CKM hard)? Cost; user enrollment; system complexity; future computing paradigms that are unclear (e.g., Cloud Computing); user-friendly requirements; accurate security analyses; and competing solutions that do not interoperate.

3.4 Usability

Usability is a metric for measuring the ease of correct use of a system by a human user the satisfaction of a person that is using a system. A CKM system requires several user-performed operations, ranging from easy to very difficult, depending on the design. CKM operations include: user registration, key initialization, certificate creation, KM service responses, and KM-User interfaces.

The following are highlights of presentations from the workshop related to usability.

- Standards must not only be technically correct and precise, but they must be understandable to, and easily used by, the general public. We need to be able to communicate what we're doing and why we're doing it to the people who make policies, procurement regulations, and user instructions.
- When protecting stored data, good information management methods must be able to discover three years from now what algorithm and what key were used to encrypt the information.
- We rely on other Federal agencies to state their specific requirements so that we can come up with CKM standards that satisfy their requirements and are user-friendly, cost effective, and secure.
- Key management starts with identifying user needs and requirements in a KM planning document.
- Virtually no additional training should be required for a user in order to effectively use cryptography if CKM is properly designed.
- We need to take the user's perspective into account when designing cryptographic systems if we want the security to be actually used, as opposed to being circumvented.
- It is not acceptable to only have a choice between usability with little security and security with little usability. A CKM system designer has to know the prospective user and to understand that security is not the primary task of the user. A system must be efficient, effective and understandable; there is no complex system that is secure.

- Conventional wisdom is that "computer security systems can't be effective unless they are complex and difficult to use."
- PKI enrollment is often the most difficult computer task to perform. Usability is more than just the user interface. CKM designers have to adopt the mantra of making it easy for users to do the right thing. Designers have to align the design to the user's conceptual model of a security system. The interface has to use terminology that is intuitively obvious to the general computer user. The complexity of the CKM system has to be minimized for the user if it is to be used effectively.
- Certificate pop-ups have to be minimized, because users have become accustomed to ignoring pop-ups. Factors that inhibit the adoption of new technologies have to be eliminated, and those that promote the adoption of effective security technologies have to be encouraged.
- Applicable Models: Cryptographic key life cycle (key birth to death management); security analysis; model all system actors and their actions; information management models must be the foundation of key management.
- Users of a CKM System are humans, devices, applications, programmers, and administrators.
- Design Considerations must include a mix of long-term symmetric and asymmetric keys for some applications, algorithm agility, security parameters, and a desire to keep it simple and keep it cheap.
- When the CKM policies, components, and recommended security practices are properly selected from the CKM System Design Framework and combined properly in a CKM system design, we have a well-defined CKM solution.
- We would like to see a leap in ease of implementation, management, and use; we have already made significant progress in this area. Electronic distribution of wrapped keys led to an improvement over manually distributed keys, and public key based key distribution led to an improvement over key wrapping. PKI has been a major leap ahead over previously-used manual keying or point-to-point symmetrically keyed systems.
- We build systems, we implement them, and then we find out that the users consider them unacceptable. We must not wait until the last minute to get the user's opinion. We need to build prototypes of a system and test them with real users before we extensively field the final product.
- We need to explore the advantages of alternative approaches, e.g., identity-based key management.

3.5 Scalability

Scalability is a metric for a CKM system that is used to measure and describe the ease of enlarging the number of entities it supports. This metric depends on the amount of personal use, organizational use, inter-organization use, and global use of the system.

The following are highlights of presentations from the workshop that are related to scalability.

- One requirement is to have scalable solutions in very large applications. While we know how to handle key management reasonably effectively for up to a million people, we need to go a couple of orders of magnitude beyond that in the relatively near future.
- We don't have just a national security environment and a non-national security environment today; we have a collective community.
- Define a key format as a parameter that could be imported to an algorithm for interoperability among government and commercial devices.
- Enterprise encryption policies must cover data, discovery, keys, certificates, key storage, applications, disaster recovery, validation and monitoring, reporting of workflow and process, personnel roles and assignments.
- Delivery models of service providers include: internal, community, public, and hybrid. Each has benefits and some controversy.
- Clouds are a good fit for very large-scale applications involving huge quantities of data and vast computing power that is often highly variable in quantity over time.
- Scalability is a metric of a CKM system that depicts the ease by which the number of supported users (people, devices, applications) can be greatly increased; there is a great need for a scalable, centralized key management approach. Specifically, cost-efficient, scalable, secure and easy-to-use PKI applications are needed by industry.
- From the vendor's perspective, the user is the problem. There are major problems with distributing keys in terms of scalability when the user gets involved; the process of key revocation often breaks down because users do not maintain updated revocation lists. It is difficult to audit key usage and key actions remotely.
- With a centralized key distribution system, actions do not get lost, and revocation and certificate control are easier. The audit of actions is much easier if a user has to go through a central facility to use the key.

3.6 Interfaces

An interfaces is the point of interaction between two entities (e.g., the point where information is exchanged between entities). Interfaces in a CKM system include: the KM-organization, the KM-manager, the KM-user, the KM-communication channel, KM-storage, and the KM-application.

The following are highlights of presentations from the workshop that are related to interfaces.

- API's are being defined and implemented for cloud computing, including configuring storage, managing key-pairs, configuring IP addresses, and managing instances of control, such as run, reboot, terminate, and query.
- The advantages of Identity-based Key Management (IDKM) are: the authentication of a user's ID is done at decryption time, which matches a user's expectations that authentication is needed to retrieve information; keys are short lived; making a new public key is nearly free; the time between identity binding and key issuance is short, as opposed to bind-first and issuer-later systems; and IDKM provides a model for thinking about application level key management.

- Because of application vulnerabilities, some data must be encapsulated no matter where processed, stored, or transferred. Applications must be able to process ciphertext when given a security policy and the necessary credentials.
- Encryption takes place in the application layer. Even though the application layer can be exploited, all data will be encrypted in the lower layers. Applications supporting encryption at the application layer (layer 7) include application vendors, POS providers, PABP, e-commerce, healthcare, VoIP service companies, and application development teams that do not control lower layers of the network architecture.
- Key Management is required for the applications and consumers, including: e-Commerce, banking, air traffic control, the aerospace industry, defense, emergency first responders, the health care industry, the Internet (Routing, DNSSEC, etc.), citizens and consumers.
- In order to insure that the CKM solution provides adequate support for the application, the CKM System Design Framework needs to define methods for specifying the unique requirements or constraints that are imposed by the application or the organization performing it. For example, one input should be the desired target security strength for the managed information, the assurances that the CKM solution must meet to achieve the target security strength, and how conformance of the implementation to the CKM solution is to be verified.
- CKM components include keys, algorithms, primitives, and protocols. Components may also include modules, products, and even the combination or composition of other components in an innovative manner to provide a secure CKM solution.
- For interoperability, certain interfaces will need to be specified. Possible interfaces include: the cryptographic algorithm interface, the key management interface, the cryptographic module interface, the product interface, and the application interface. In general, only the interfaces that are used by entities outside the application need to be specified.

3.7 Algorithms

An algorithm is a set of rules for performing a specific operation. Cryptographic algorithms specify the operations of encrypting, decrypting, authenticating, digitally signing, and verifying digital signatures or authentication codes. Algorithms are defined in a cryptographic system and a supporting CKM system for data protection (C, I), key protection (C, I, A), key generation, key establishment (exchange, agreement, distribution), key update, key destruction, etc.

The following are highlights of presentations from the workshop that are related to algorithms.

- There have been a lot of transitions from one algorithm to another in encryption and secure hashing. Transitions take 5 to 15 years because of the high cost of implementation, testing, and deployment, and a possible loss of interoperability.
- There is an expressed preference for key distribution using public key cryptography.
- Define a common set of cryptographic algorithms that can be used in creating products that meet a wide range of US Government needs.

- Threshold cryptography[5] is useful for encrypted data storage access (e.g., a minimum number of people must cooperate in order to retrieve sensitive, stored information).
- The most prevalent problems with KM today include: weak pseudo-random generators for key generation, cryptographic keys that are hard-coded into the application, approving Certificate Authorities, cryptographic algorithms and key lengths that are not used, cryptographic keys that are not renewed periodically, and cryptographic keys and passwords that are not encrypted/protected in storage or in transit.

3.8 Key Types

There are several types of cryptographic keys that may be used in a CKM system: symmetric keys (e.g., one key used for both encryption and decryption), asymmetric-public keys (the public component of a public key pair), and asymmetric-private keys (the private component of a public key pair). Keys are further classified by their life-time: ephemeral keys, which have a short life-time and are usually used only once; and static or long-term keys, which have a longer lifetime and are usually used multiple times.

The following are highlights of presentations from the workshop that are related to key types.

- The Internet security protocols use various KM approaches, including: pre-shared keys (e.g., manually initialized, or communicating parties mutually derive a new key for data protection), PK cryptography (key agreement, key transport), and Key Distribution Centers (the KDC has a secret key for every subscriber, and generates and distributes a subscriber-subscriber data protection key using the KDC-subscriber keys).
- A manufacturer often ships devices to customers with a hardwired private key, device certificate, and device identifier. This would give the capability to devices to authenticate other devices with which it will communicate.
- Taxonomy of keys: This includes signature creation, signature verification, communication privacy, stored data privacy, authentication.

3.9 CK Lifecycle

A CK lifecycle includes all the phases associated with a cryptographic key between the time it is generated and it is destroyed. These include: generation, distribution, storage, usage, replacement, revocation, deletion/zero-ing, expiry, update, etc.

The following are highlights of presentations from the workshop that are related to the CK lifecycle.

- The methods for distributing keys efficiently are different from the methods of being able to revoke and replace keys efficiently on a large scale.
- NSA requires strict accounting for keys, multi-person (between 2 and *N* people) control on plaintext keys, secure key storage, and three-layer key management, including transport, packaging, and key format.
- A security strength: (AKA “bits of security”) is a number associated with the expected amount of work (often measured in binary operations) that is required to obtain any

[5] See the previous footnote on group keying and *M* of *N* keying.

single key used by an application by testing all possible keys. The security strength is specified in bits and is currently a value from the set {80, 112, 128, 192, 256}. 80 bits of security are good through December 31, 2010. Thereafter, NIST recommends 112 bits as the minimum.

- For details and comparisons of algorithms, key sizes, security strengths, and recommended transition times, see NIST SP 800-57, Part 1 (for general key management), FIPS 186-3 (for digital signatures), and FIPS 180-3 (hash functions).
- Security, cryptography, and cryptographic keys can be managed using a cryptography management platform that can track everything throughout the life cycle of provisioning, enrollment, monitoring, and discovery. Included would be the processes involving keys and certificates, cryptography and CKM policies, secure implementation validation, audit, and security notifications (must notify customers affected by security breach).
- The reality of lifecycle key management is that policy and workflow must be continuous, and all the components must be integrated properly. Enterprise encryption policies must be comprehensive and cover a wide range of components, including certificates, keys, algorithms, validity periods, and multiple person control. Policy is the overarching guidance and requirement that must be achieved.
- Encryption management and distribution models cover a broad range, from manual to automated key management involving several types of agents and protocols.
- Requirements and constraints driving encryption management models include the levels of automation, automated agents, remote access decisions, duplication of keys, centralized monitoring and alerting.
- CKM in a cloud environment must provide the usual capability of generating, using, storing, distributing, revoking, verifying, and destroying keys. Two scenarios of CKM in a cloud are emerging: key management by the cloud infrastructure, or key management by specific applications that have been entrusted to run in the cloud infrastructure.
- Applicable Models must consider key life cycles; a birth to death management of keys; security analysis; model all actors and actions; and information management models.

3.10 CK Metadata

Metadata is the information used to specify the uses and characteristics of cryptographic keys in a CKM system. Metadata may include: the key owner, the PKI service, key usage, the validity period, key parameters, etc.

The following are highlights of presentations from the workshop that are related to metadata.

- Public key certificates bind a subscriber's identity to a public key. A certificate contains: the subject's name, the subject's public key, the validity period, and the issuer's name.
- There is a tradeoff between security and simplicity. Good security requires complexity in certain security components, layers of protection, layers of metadata in security packages, and a robust metadata system to support security provisions. Some cryptographic key metadata can be hidden. Security packages will be as complex or simple as the user wants within a procured KM system.

- Major design issues include: What should be done when a certificate expires? Who should administrator a CKM system? When information is lost, was it in encrypted form? When should certificates expire? Should key management be automated or manual? What cryptographic algorithms, protocols, and interfaces are being used?

3.11 Standards

Standards are accepted specifications and practices in a topic that may provide interoperability among various implementations, a minimum level of performance, a maximum level of risk, etc. Standards in the CKM area are developed by a number of organizations, including: NIST, IETF, ANSI, ISO, and OASIS.

The following are highlights of presentations from the workshop that are related to standards.

- We have to come up with solutions for the next generation. From a standards point-of-view, we must have practical, adequately precise standards that will integrate effectively into government operations and industry business practices and product development cycles.
- The whole concept of the Internet is based not on a single system, but a set of standard protocols that allow independent systems to interoperate with each other. We have to support this interoperability among future systems.
- Standards must not only be technically correct and precise, but they must be understandable to, and easily used by, the general public. We need to be able to communicate what we're doing and why we're doing it to the people who make policies, procurement regulations, and user instructions.
- We need to create standards that are testable. Ideally, they should be tested automatically so we can minimize the effort of conducting manual product assurance.
- Executive and legislative oversight and resource allocation must be in the proper context. Expectations must be consistent with technical reality. We must work with industry, not just from the standpoint of innovation and technical expertise, but making sure that the standards that result will be implemented, not just can be implemented.
- We need to work with academia because we get many creative inputs from its members, who are not constrained by short-term corporate goals. We also rely on obtaining innovative ideas from our colleagues overseas.
- IETF protocol efforts include: IKEv1 and IKEv2, TLS, Secure Shell, EAP, CMS, and Kerberos.
- The Extensible Authentication Protocol (EAP) provides authentication for people and devices.
- The IETF enrollment efforts include: KeyProv and a dynamic symmetric key provisioning protocol.
- There is a clear need for standards in certificate enrollment, but previous attempts have failed.

- There are few standards for: key generation, ordering, distribution, accounting, destruction, commercial implementation, and formats for keys.
- NSA is helping to define standards packages and key formats in the IETF and PKIX for the Suite B cryptographic algorithms (i.e., those used to protect classified data up to SECRET).
- NSA is now more open in its interactions with public groups, e.g., the cryptographic message syntax in RFC 3852, a trust anchor format and protocol, standard asymmetric private key formats, and symmetric and asymmetric key management packages.
- NSA does not intend to recreate existing standards, but rather work with open groups to establish standards that also satisfy NSA's requirements.
- Matt Ball announced an IEEE key management summit meeting in Lake Tahoe, Nevada that will be held on May 4-5, 2010; the website url is http://www.keymanagementsummit.org.
- Standards for cryptography are often based on legislation regarding notification of security breaches; the Payment Card Industry Data Security Standard (PCI-DSS) mandates security for all credit card companies, fines for non-compliance, and remediation.
- Public Key Cryptography Standard (PKCS): this 1995 standard must evolve to keep up with new technology and applications.
- Group Key Management (GKM) provides key management for groups consisting of three or more entities sharing the same key material; GKM methods can be broadly classified as either contributory (e.g., CLIQUES), where group members use the Group Diffie-Hellman Algorithm to independently derive group keying material, or centralized (e.g., RFC 3547 (GDOI)), where group members register with a trusted third party (group controller/key server) and are given group keying material.
- Standards groups have concentrated on centralized GKM, because such methods best meet the needs of internet group applications. Authorization is straightforward, revocation of group members is relatively easy, and centralized methods typically use the existing CKM System Design Framework components.
- General authenticated encryption methods can be used for key transport. It is recommended that the key derivation methods described in NIST SP 800-108 should be explicitly noted as updates in newer NIST recommendations.
- Specific standards, such as IEEE 802.1 frame encryption, IEEE 802.11i, and Internet RFC 3740, are undergoing review regarding GKM.
- The FIPS 201 Personal Identity Verification (PIV) standard card is an example of an authentication scheme that uses symmetric keys. The benefits of using a symmetric card authentication key (CAK) are: strong authentication compared to using the Card Holder Unique Identifier (CHUID), activation without a PIN, and the authentication can be performed over a contactless interface. The bad side of symmetric (CAK) authentication is that the symmetric key challenge-response schemes require the verifier to know the CAK, but the cross-agency verifier will not know the CAK.

- In the FIPS 201-1 standard, the CAK is optional; it may be a symmetric or asymmetric card authentication key. NIST SP 800-116 strongly recommends that the CAK be included in a PIV card. Single-factor authentication is not as robust as two-factor authentication. In a PACS (Physical Access Control System), one agency can use a symmetric CAK for accessing another agency in a PACS.
- PKI authentication at enrollment establishes a basis of trust. Improvement in security is obtained via a multi-factor authentication and dynamic challenge-response pair.
- The CKM System Design Framework may provide a foundation for future standards that needs to be developed in order to have more complete, secure, and interoperable solutions.

3.12 Requirements and Recommendations

Requirements are specifications that must be satisfied in a topic area, and recommendations are specifications that should be satisfied.

The following are highlights of presentations from the workshop that are related to requirements and recommendations.

- We need to understand the requirements of the Federal government. We have to be working hand-in-hand with industry. What are our resources, and what are our practical constraints?
- We need to develop CKM techniques for the future. We need to analyze them for security and ease of implementation and use.
- We need to have procedures for qualifying products as meeting our standards, so that they may be easily procured by the government and others. The procurement qualification process needs to be efficient and strongly-coupled with our technical specifications.
- We need to be able to demonstrate and test our solutions in actual applications.
- We would truly like to be able to create secure systems from insecure components.
- Many NSF Internet applications need security, including email, project funds management, travel, proposal submission and proposal evaluation.
- NSF needs better integrated cryptography in its sensitive applications. Currently, NSF doesn't use PKI because of cost and complexity, but does use identity management, including identifying users and visitors, additional authentication of NSF users, and authorization of NSF users to systems and data.
- Cryptography is required in cyberspace and can provide more information assurance capabilities.
- CKM is growing in complexity. Point to point communications security is old technology. It is desirable to have interoperability with existing legacy systems.
- NSA would like to have some interoperability among high-assurance government devices and commercial off-the-shelf devices, especially for emergency situations, such as 9/11 and hurricane Katrina.

- A nested security approach protects a red key (e.g., an unencrypted data encrypting key) with integrity, authenticity and secrecy provisions.
- We need to look at the entire system; the biggest issues in crypto-based security are with scalability, federated systems, and the customer's specific domain.
- Hardware has different failure modes and different update capabilities than software.
- Microsoft systems are designed using a tool kit of mechanisms (subsystems) and best practices. There is a great need for a key management tool kit of generic building blocks from which individually-chosen subsystems can be integrated into the total system. Key management is an application that must be form-fitted to the user requirement. We need methods to analyze the resulting system end-to-end.
- A key management platform for composability with existing subsystems, such as identity verification and authentication, is needed. A collection of generic building blocks of security that can be integrated into a system and methods to analyze the resulting system are needed in creating a good key management platform.
- We need an automated CKM system that can be implemented in existing systems. Requirements include: 1) the authenticated/authorized distribution of keys, 2) keys must persist over a long term, 3) a system that replaces/updates keys when needed, 4) key creation should not be centralized, and 5) minimal operational impact. Candidates for this type of KM system would be Kerberos (for session keys), OASIS (for storage keys) or GDOI (for group key management).
- Security can be a justification for making a system easy to use. A good system should have a configuration that is easy to understand. Understanding a secure system must be attained. Security must be designed into the system and then be fully used in order to be understood. Security technology can make trust lifecycle management intuitive and hidden from the user.
- We need to bridge the gap between state-of-the-art security that is known and security that is actually being used.
- A security policy engine is needed that implements a user's data security policy by creating or selecting an appropriate cryptographic policy and a supporting key management policy that achieves the data security policy.
- Stronger authentication is needed for smart Internet "edge devices" (e.g., routers, routing switches, integrated access devices) that provide authenticated access to the backbone network, as well as stronger authentication for active processes, users, and digital objects, with the implication that we need better access controls and two-part authenticators for devices.
- Multiple identities with multiple identifiers for an individual are a must. Attribute certificates stating the authorizations of differing identities must be supported. Individual activities must not be confused with organizational activities.
- Roles for an individual must be supported, and role-based authentication is needed (i.e., the authentication of a person will depend on the role that person is attempting to fill). Roles for processes must similarly be supported.

- Enterprise KM requires: the secure creation of keys; automatic replication of keys; an enterprise-wide KM policy, as well as application-specific KM policies; audit logging; role-based management; scalability across the enterprise (good availability and a large number of keys and applications); interoperability; standards compliance (e.g., IEEE P1619.3, OASIS KM interoperability protocol); and secure key export to trusted partners.
- Automakers are concerned with: (1) a single point of failure in systems without sufficient redundancy so that KM systems are at risk of a BIG loss (catastrophe); (2) immediate security needs versus higher costs; (3) the need for a more flexible credentialing system (many are locked into the current system with no way to change.
- Electronic Key Management (EKM) is needed that can leverage existing policies and authentication methods to lower cost and give faster deployment;
- Designers must make cryptography easy to use and friendly. Currently, anti-spam tools are understood and desired by users, but cryptography is not.
- A Chief Information Security Officer must be able to communicate with enterprise security developers. Access control data must be the basis of cryptographic mechanism control. Failures in many KM services often force users to get a key outside of the KM system, with disastrous results.
- Centralized Key management provides a lower administration burden. An enterprise cannot rely on end users for security, especially managing keys. Centralized KM minimizes the involvement of the user and provides scalability with control. Organizations of all sizes can benefit from centralized key management strategies; they will find centralized KM both affordable and durable.
- In many customers' environments, users need to digitally sign a transaction very infrequently. Non-repudiation services are also seldom required. Authentication is often a local matter. One-time password tokens are often used, and an identity-challenge oftentimes suffices for a signature if it is done whenever a signature is needed.
- Military applications must support very large groups of users. Examples include sensors remotely deployed in very large numbers (sometimes called sensor dust). Future key management systems must efficiently support millions of micro, unmanned aviation vehicles. Global support of secure wireless delivery systems, such as radios, telephones, and GPS, is required.
- Revocation of potentially compromised keys must be completed in seconds, not minutes. Very large subsets of keys must be revoked upon command. In many applications, revocation of keys must scale according to the number of end points revoked, not to the total number of keys. It is permissible to miss a rekey, but not a revocation (i.e., a system must fail-secure). A binary-tree approach is used to design an efficient key revocation system. A key distribution algorithm must guarantee that only a specific subset of good nodes has good keys for a period.
- Key management requirements of military applications include: secure global key distribution; responsive key revocation; and customized "last mile" delivery for special environments, such as the military. Scalable key encryption algorithms must support

secure wireless delivery. A near-zero vulnerability of the disclosure of a key must be maintained. An override of policy must be available when a commander demands it.

- The Certificate Authority must deal with keys globally, while the end user must deal with them locally. The KMS must be more dynamic as the number of customers scale upwards.
- Global presence requires globally-scalable key management.
- Deterring the cyber threat requires nearly-instantaneous revocation. Operational requirements mandate flexible last-mile deployment strategies. Fundamental technologies exist that provide the needed scale, including: weighted key assignment, batched transmission, permutation trees, and augmented broadcast encryption.
- Compliance enforcement is a motivator for reluctant users. Protection from data breaches should be, but often is not, the prime motivator.
- There is a major need to support key management technology as part of the national cybersecurity initiative. The CKM project is designed to develop a comprehensive and interoperable CKM.
- Requirements: user-friendly; easy to use, i.e., system components must "Plug and Play"; user-driven capability; secure; cost-effective; fault-tolerant and highly available; provide protection against destructive attacks; interoperable; enterprise-wide; multi-partner; multi-vendor; multi-application; scalable; and enhanced interoperability in time of emergency.
- We would like network security at no extra cost (not at no cost).
- Key management requires more than key establishment. Key management systems must provide for the secure generation, storage, access and recovery of the keys, either before or after they are distributed.
- We must have a "leap" in ease of implementation, management, and use (recall that the electronic distribution of wrapped keys led to an improvement over manually distributed keys, and public key-based key distribution led to an improvement over key wrapping).
- A holistic approach to enterprise key management is needed, where a complete standard set of key management capabilities would be widely available for information protection.
- Customers want to defer to authorities to tell them what key management system is good, better, and best. There is a need for a public-private partnership that allows the new CKM technologies to incubate and be evaluated, so that consumers will accept the solutions when they become available. The RSA algorithm had to be vetted for some time before it became accepted.
- We must have a uniform solution to a uniform family of problems. We need a glossary of security to minimize undefined buzzwords that are used to sell commercial products. A well-understood standard lexicon is needed in security.

3.13 New Technologies

New CKM technologies are needed to keep up with the increased demand for security, due to significant increases in computer capability, applications, and usage. New or greatly improved technologies are needed in: quantum cryptographic algorithms/computing, cloud computing, identity-based cryptography, security improvements, speed improvements, usability improvements, and cost reductions.

The following are highlights of presentations from the workshop that are related to new technologies.

- In computer technology, we keep moving faster and faster. We have seen an improvement of price-performance in computer technology by a factor of nearly one million in the past 30 years.
- Cloud computing will provide convenient, remote, on-demand utilization (e.g., rental) of computing power and applications that the user cannot afford to maintain locally, but may need from time to time. This capability will provide ubiquitous network access, on-demand self-service of computing power, metered-use (rent by the hour), elasticity of capability meeting real-time requirements, and resource pooling.
- There will be software, hardware, and infrastructures as services to be obtained at will. The question that must be asked is where and how will security in general, and CKM specifically, take place? Who or what is responsible for security while data is being processed within the cloud: by the cloud itself or by the application?
- A cloud capability may be deployed by various cloud providers to a multitude of cloud customers in various ways, including: software as a service, platform as a service, and infrastructure as a service.
- Cloud computing already has a wide array of interested participants, both providers and consumers.
- A cloud infrastructure CKM model might have a centralized cloud security center for multiple data storage and computation centers.
- In cloud computing, virtual machines may be used for security. Having fully trusted virtual machines is not as simple as it looks, because virtual machines can be suspended, copied, moved, or lost. A Virtual Machine Manager implementation was tested for quality, and all systems failed the tests; device emulation was particularly vulnerable.
- Cloud infrastructures can help in some key management areas. Clouds are designed to separate users. Users may be able to leverage the cloud infrastructure as a trusted third party.
- One workshop participant asserted that cloud computing is the most insecure technology to come along and cannot be secured.
- Fair Electronic Exchange is defined so that both parties of an electronic transaction get what they need or neither party gets anything. One party gets the message only if the other party gets a receipt for the message. Fair exchange is crucial to electronic commerce, but not easy, even with digital signatures.

- Future directions of key management include: central KM solutions for managing keys in Hardware Security Modules (HSM's); a cryptographic key management framework is needed to simplify the understanding of KM; key management should be isolated from a key users; guidance on the use of key attributes; KM policy must be easily defined and enforced, especially for symmetric keys; and KM policy negotiation/mapping is required for effective interoperability among applications.
- Identity Based Key Management (IBKM) must yield automatic identity authentication at decryption time. Users must provide their ID and authenticator to access data. Identity Based Encryption (IBE) is required for binding users into groups (i.e., ID = group or role). The key server must authenticate identity for access authorization.
- An Elliptic Curve Digital Signature Algorithm (ECDSA) signature scheme must be made into a Fast ECDSA signature scheme (40% faster) so that it can achieve fast digital signature verification. There should be a transition from ECDSA to Fast ECDSA.
- Considerations for future key management systems must include: a design of CKM systems for high availability, survivable CKM Systems, emergency access to keys, and worry about unintended consequences, both good and bad.
- In light of quantum computing, CKM system designers must look at means other than public key-based key management systems; they must look at quantum computing-resistant algorithms and schemes.
- Technologies and Standards must support identity-based encryption, enterprise key management, OASIS KMIP, CMC, and factory-generated device keys for enterprise enrollment and registration.
- Identity based symmetric keys should be used to reduce the scale of the symmetric key distribution problem.
- The CKM System Design Framework should encourage a CKM solution developer to think about future transitions and address when the CKM solution will need maintenance, when it will need to be replaced, and how it might best be phased out
- Quantum cryptography should be reviewed as a candidate for providing us with the leap in key management capabilities that we seek.
- A Cloud Cryptographic Key Management system is needed. There should be a trusted part of the cloud to provide a key to communicate securely with anyone else on the network or any service provider in the cloud. There should be a way to go to the trusted part of the cloud to establish a secure connection to any service or other user in the "cloud." Security should be automatically provided by the cloud for all communications.

3.14 Framework

A framework is a basic structure consisting of a set of components that can be combined in a variety of designs within a set of defined architectures. The components are described in detail in a framework, but are not restricted on how they must be combined or used when designing a system or other functional entity. A System Design Framework may describe the characteristics of each component, which standards the components comply with, and provide examples of how

they may be used. A framework is not intended to suffice as an architecture, a design, blueprints, or specifications of an entity that may be created from the described components.

The following are highlights of presentations from the workshop that are related to the future Cryptographic Key Management Framework.

- A CKM framework is needed; SP 800-57 is a good start. Security has to be built into applications and systems, security best practices have to be supported by security toolkits, and algorithm agility is necessary. We need to know what system state is expected by a user, and the user must be able to determine the security state of an application.

3.15 Applications

An application in information processing is program that is designed to perform one or more tasks using a set of data. Security needs to be considered for applications to protect the data during communication or while in storage, to authenticate the users performing the applications, and to assure that performance of the tasks is authorized for the users. Cryptography is often used to provide or support one or more of the tasks. Key management is required when using cryptography to assure that one or more cryptographic keys are properly generated, that they are distributed where they are needed for cryptographic processing, and that they are stored securely so they are available when needed and not disclosed to unauthorized users or processes.

The following are highlights of presentations from the workshop that are related to applications.

- The role of key management in cybersecurity is critical. We have cryptographic functions that are used for identification and authentication, both from the standpoint of protecting privacy, but more importantly, for integrity and authentication mechanisms.
- Even when we look at biometric methods for identification and authentication to control access to critical functions, we're still dependent on cryptographic functions for protecting the integrity of the biometrics.
- Key management is critical for all sensitive information processing applications. Economic prosperity is a major goal and needs information security.
- The Internet has changed the world. It has increased global productivity, manufacturing, and communications. It has changed the United States. It has increased our standard of living and is a very wonderful device that we all enjoy. These are all due to the innovative applications created for the Internet and its users.
- Nearly all Internet security protocols use cryptography for authentication, integrity and/or confidentiality, and hence, require key management (KM).
- A Southeast Michigan pilot program within a health provider community utilizes Federated Identity Management systems to manage health data bases.
- A workshop participant asserted that small, distributed databases are inherently safer than very large, centralized ones for several reasons. He stated that some approaches used health care “silos” to manage health care information. He discussed first-responder emergency access to patient data (i.e., the EMT doesn’t know where the emergency

victim's healthcare data is located when the responder first starts to look for it) in unplanned circumstances, which caused special security provisions to be needed

4. Summary of Comments Received Subsequent to Workshop

NIST created an Email address and a WebLog[6] (Blog) to facilitate discussion among participants regarding cryptographic key management subsequent to the workshop and to disseminate new information to the workshop participants and other interested parties. Five initial questions (A through E) were posted on the blog in order to initiate discussion. Each question had multiple sub-questions. This is a summary of the comments or responses received from the public.

Question A dealt with leap-ahead technologies. A comment was received from Stephen Lange Ranzini who thought that an on-demand Federated Identity Management System, based on the Liberty Alliance's Identity Assurance Framework, would enable a leap-ahead in securing cyberspace. He believes that this would be a major improvement in both security and ease of use over the existing user name and password systems. The Federated system would not require multiple one-time password tokens. Mr. Ranzini feels that banks are best equipped to provide this single sign-on service, and notes that strong security across the Internet for users is identified in various Federal Government cybersecurity strategy documents as one of the top hard problems that need to be addressed.

Question B asked "What constitutes a key management framework? Mike Markowitz responded to a comment by Santosh Chokhani who stated that the security of keys "can be ensured using standards, such as FIPS 140-2." Mr. Markowitz quoted a portion of FIPS 140-2 that states that "conformance to this standard is not sufficient to ensure that a particular module is secure." He feels that there is a perception that standards accomplish much more than they actually do. Mr. Markowitz proposed that a Question F be posted that asks "What can we expect to accomplish with a KM standard?" As a result, Question F was posted.

Question C asked "Do you see new applications requiring key management?" Stephen Lange Ranzini responded that "If a Federated Identity Management system were widely deployed, new industries would be created" (see response to Question A).

Question E asked "What R&D activities should be undertaken to advance the key management technology?" Larry Hofer stated that a Certificate Revocation List (CRL) may be problematic for implementations with limited memory. He then wondered "What do we see happening to resolve this technical issue?"

Mike Markowitz responded to Larry Hofer by pointing out that the OCSP and SCVP efforts are intended as CRL alternatives.

Stephen Lange Ranzini felt that a permanent test bed in the healthcare industry would yield rapid progress in creating a trusted computing environment and assist in the nationwide deployment of an identity assurance Federation.

Comments received through email: The following comments were sent directly to NIST.

Steven Wierenga, HP Distinguished Technologist, appreciated the opportunity to participate in the workshop and would do so in the future. However, he stated that the technical arrangements for the workshop's remote presenters and panelists were extremely difficult because of interference in the sound systems. He hopes that these problems will be resolved for future workshops (Note: see summary following this section.)

[6] May no longer be available.

Chii-Ren Tsai, Senior Vice President of Citigroup O&T Risk Management, felt that the workshop was very successful. He fully supports the directions that NIST has taken to improve key management. Trusted insiders are the major threat. We need more awareness of the threat and the importance of sound key management. Mr. Tsai will be happy to contribute to the Framework discussions as much as he can. Citigroup has been conveying its key management requirements to product vendors with some nice results. He looks forward to a comprehensive framework and the products to make secure solutions.

Chii-Ren Tsai, Senior Vice President of Citigroup O&T Risk Management, provided some thoughts for consideration.

1. Each key management system is supposed to have a secure key store where asymmetric and private keys are kept in encrypted form. The master key used to encrypt the keys may need to be protected in a HSM (hardware security module).
2. Cryptographic keys should be managed via a key management interface that is separate from the key use interface.
3. Security administrators who manage keys via the key management interface are not authorized to browse keys in the clear, nor access the key use interface.
4. Dual control should be embedded in key management functions that must be performed manually, such as key export, key injection, key deletion, etc.
5. Cryptographic keys that will be centrally managed may need to be defined like a key object, with attributes to simplify key management. For example, the following attributes may be useful if they are coupled with keys, especially symmetric keys:
    a. Key Label
    b. Cryptographic Algorithm
    c. Key length
    d. Key type
    e. Key renewal policy (e.g., renewal frequency, renewal method, etc.)
    f. Creation date
    g. Application
    h. Owner
    i. Exportable
6. The KM framework should allow key management policies to be created so that each organization can define its own policies to comply with its standards. The syntax of KM policy definition can be standardized for interoperability.
7. A KM protocol (e.g., KMIP) is required to allow central management of keys in various platforms and products. Such a protocol should be able to carry key attributes, as well as policy mapping, and support mutual authentication with access control.
8. It (a key management system) must be implemented with sufficient security features, such as strong authentication, audit/logging, access control, data confidentiality and integrity.

9. Each key management system should allow additional key management protocols or APIs to be plugged-in to automate certain KM functions in business applications.
10. Ideally, newly developed applications based on such a KM framework can be seamlessly managed by a KM tool, built out of the same framework.

In a separate email, Chii-Ren Tsai, Senior Vice President of Citigroup O&T Risk Management, provided additional comments:

1. What I previously described does not cover (apply to) KM domains that are application specific. Some of them can be generalized or will benefit from the general purpose framework if re-engineered, but quite a few are narrowly focused and tightly coupled with the application architecture.
2. Public key-enabled applications, such as secure email, IPSec, and certified document signing, have key management that is synonymous with certificate management, even if their certificates are populated with slightly different attributes.
3. With secure tape archiving, key generation protection, retention, and recovery are critical.
4. Hardware security modules tend to have different flavors and architectures (e.g., network-based versus locally attached).

Summary: Email responses seemed better at dealing with significant issues than the workshop Blog. The Citigroup participant's interest in CKM is quite apparent, and his follow-up ideas on the essential elements of a cryptographic key management framework are very much worth considering. The Computer Security Division normally conducts small workshops of technical experts who are divided into working groups to discuss specific topics. Remotely provided participation is mostly one-way communication to the individual watching the real-time video, and few questions or comments were received by email. As an experiment and to save two presenters time and travel costs, they gave their presentations remotely using the audio facilities that were shared with many other participants. This turned out to be unacceptable because the background audio noise from the non-presenters was louder than the presentation. The experiment resulted in a strong recommendation that more audio facilities should be used in the future to assure that the presenter had an exclusive audio connection with the workshop.

Appendix A: Acronyms

Acronym	Definition
AKA	Also Known As
ANSI	American National Standards Institute
API	Application Programming Interface
CAK	Card Authentication Key
CDSA	Common Data Security Architecture
CHUID	Card Holder Unique Identifier
CIA	C = Confidentiality assurance, I = Integrity assurance, A = Availability assurance
CIO	Chief Information Officer
CISE	Computer and Information Science and Engineering
CK	Cryptographic Key
CKM	Cryptographic Key Management
CKMS	Cryptographic Key Management System
CMS	Cryptographic Message Syntax
CRL	Certificate Revocation List
DAR	Data-At-Rest
DBMS	DataBase Management System
DNS	Domain Name System
EAP	Extensible Access Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
EKM	Electronic Key Management
EKMS	Electronic Key Management System
EMT	Emergency Medical Technician
FEMA	Federal Emergency Management Agency
GDOI	Group Domain of Interpretation
GKM	Group Key Management
GUI	Graphical User Interface
HSM	Hardware Security Module
IBE	Identity=Based Encryption
IBKM	Identity-Based Key Management
ID	Identity
IDKM	Identity-Based Key Management
IEEE	Institute of Electronic and Electrical Engineers
IETF	Internet Engineering Task Force
ISO	International Standards Organization
IT	Information Technology
KDC	Key Distribution Center
KM	Key Management
KMS	Key Management System
MKD	Multipoint Key Distribution
NIST	National Institute of Standards and Technology
NSA	National Security Agency

NSF	National Science Foundation
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
PABP	Payment Application Best Practices
PACS	Physical Access Control System
PIV	Personal Identity Verification
PK	Public Key
PKCS	Public Key Cryptography System
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509 Certificates
PKM	Public Key Management
POS	Point of Sale
R & D	Research and Development
RFC	Request For Comment
RSA	Rivest-Shamir-Adelman (algorithm)
SCVP	Server-based Certificate Validation Protocol
SDL	Security Development Lifecycle
SKMS	Secure Key Management System
TPO	Trusted Post Office
TTP	Trusted Third Party
VMM	Virtual Machine Manager
VOIP	Voice Over IP (Voice Over the Internet Protocol)
WWW	Word Wide Web