

# 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 Cyber Security 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.