

IEEE KEY MANAGEMENT SUMMIT 2008

**Welcome to KMS 2008!**

Matt Ball, Program Chair

---

IEEE KEY MANAGEMENT SUMMIT 2008

**IEEE KMS 2008 is Sponsored by**



**IEEE Mass Storage Systems  
Technical Committee (MSSTC)**

# KMS 2008 is Supported by



IEEE KEY MANAGEMENT SUMMIT 2008

# KMS 2008 Program Committee

- Jack Cole, US Army
- Bob Griffin, RSA Security (EMC)
- Eric Hibbard, Hitachi Data Systems
- Larry Hofer, Emulex
- Walt Hubis, LSI Logic
- Jim Hughes, Sun Microsystems
- Bob Lockhart, nCipher
- Fabio Maino, Cisco Systems
- Michael Marcil, Vormetric
- Luther Martin, Voltage
- Landon Noll, Cisco Systems
- Arshad Noor, StrongAuth
- Subhash Sankuratripati, NetApp
- Hannes Tschofenig, Nokia/Siemens Networks

# Logistics

- Please turn cell phones to silent!
- Sessions will be recorded, so please use microphones for questions
- When asking a question, please state your name and optionally title and company.
- Get to the question! Don't pontificate

# Tuesday Program

- 8:00am: Introduction and Importance of Key Management (Matt Ball)
- 8:30am: Overview of Key Management and Key Management Standards (Landon Noll)
- 9:00am: Overview of IEEE P1619.3 Key Management (Walt Hubis)
- 9:30am: OASIS Enterprise Key Management Infrastructure (Arshad Noor)
- 10:00am: --- Break ---
- 10:30am: ANSI X9 Key Management Overview (Jim Randall)
- 11:00am: Key Management for Government Mobile Computers (Bill Burr)
- 11:30am: Cryptographic Interoperability Strategy for the U.S. DoD (Sandi Roddy)
- 12:00pm: --- Lunch ---
- 1:30pm: Overview of the TPM Key Management Standard (Greg Kazmierczak)
- 2:00pm: Key Management for Fabric Based Data At Rest Encryption (Scott Kipp)
- 2:30pm: The RSA Perspective on Encryption Key Management (Bob Griffin)
- 3:00pm: --- Break ---
- 3:30pm: Provisioning System for Enterprise Key Management and Distribution (Lockhart)
- 4:00pm: Key Management Challenges around Distributed File System Namespaces (Kavuri)
- 4:30pm: Financial Industry Panel (Jon Oltsik)
- 5:30pm: Reception

# Wednesday Program

- 8:00am: Overview of IETF KEYPROV (Phillip Hallam-Baker)
- 8:30am: DMTF Credential Management Data Model and Interface Technologies (Jon Hass)
- 9:00am: Cryptography Everywhere - a Security Administrator's Nightmare (Tim Hahn)
- 9:30am: Password-based Encryption Using Hidden Computational Delay (Xavier Boyen)
- 10:00am: --- Break ---
- 10:30am: Key Management Using StrongKey (Arshad Noor)
- 11:00am: Sun Key Management System 2.0 using Web Services (Sandy Stewart)
- 11:30am: The Voltage Key Management System (Terence Spies)
- 12:00pm: --- Lunch ---
- 1:30pm: Key Management for Full Disk Encryption (FDE) (Garry McCracken)
- 2:00pm: HP Key Management Overview (Mark Schiller)
- 2:30pm: Take a More Holistic Approach to Key Lifecycle Management (Paul Turner)
- 3:00pm: --- Break ---
- 3:30pm: Compliance Panel (Ramon Krikken)
- 4:15pm: Standards Groups Panel (Ramon Krikken)
- 5:00pm: Wrap-Up (Matt Ball)
- 5:30pm: Dinner

# Goals of KMS 2008

- Understand the current key management standards
- Understand current vendor key management solutions
- Understand the needs of the customer