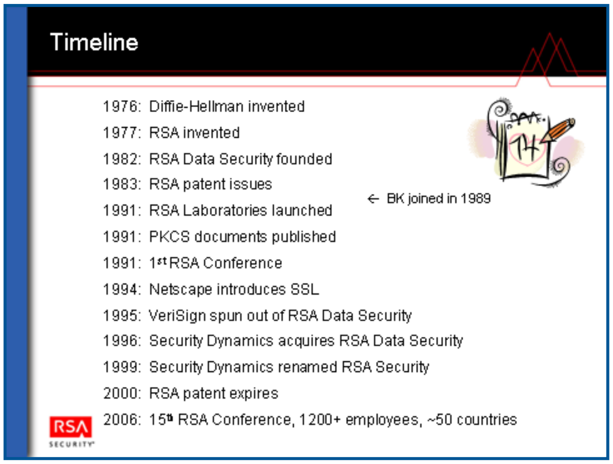
The Convergence of Key Management and Information Management

Burt Kaliski
Director, EMC Innovation Network
Founding Scientist, RSA Laboratories

NIST Key Management Workshop
June 9, 2009

Growing Up with Alice and Bob



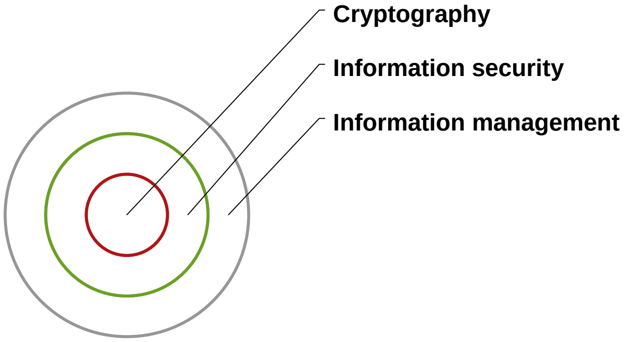
Timeline

1976: Diffie-Hellman invented
1977: RSA invented
1982: RSA Data Security founded
1983: RSA patent issues
1991: RSA Laboratories launched ← BK joined in 1989
1991: PKCS documents published
1991: 1st RSA Conference
1994: Netscape introduces SSL
1995: VeriSign spun out of RSA Data Security
1996: Security Dynamics acquires RSA Data Security
1999: Security Dynamics renamed RSA Security
2000: RSA patent expires
2006: 15th RSA Conference, 1200+ employees, ~50 countries

← 1983: BK interns at National Bureau of Standards

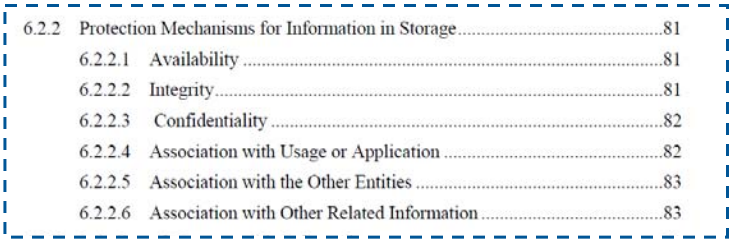
Source: B. Kaliski, “Growing Up with Alice and Bob: Three Decades with the RSA Cryptosystem,” presented at Singapore Management University, April 2006

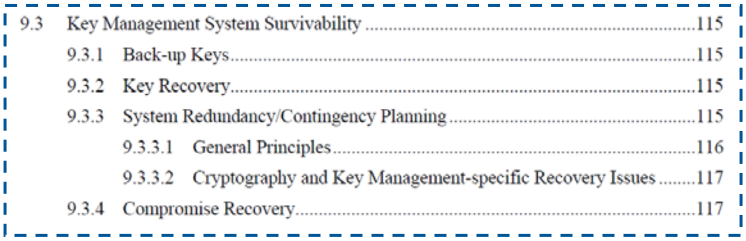
Cryptography in Context



What's the "use case"?

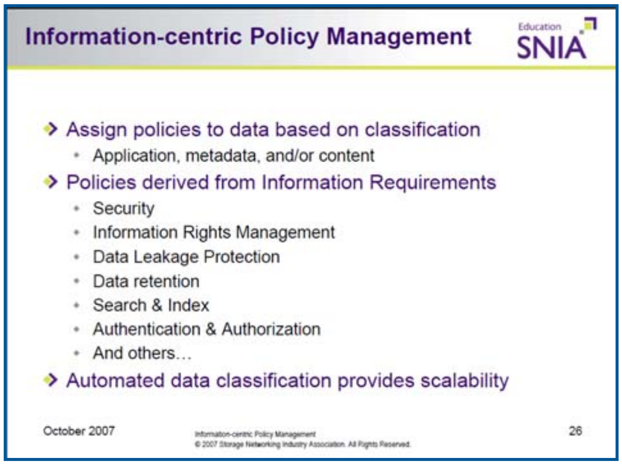
Is It Key Management …





Source: NIST Special Publication 800-57, "Recommendation for Key Management – Part 1: General (Revised)," March 2007

… Or Information Management?



Information-centric Policy Management

Education SNIA

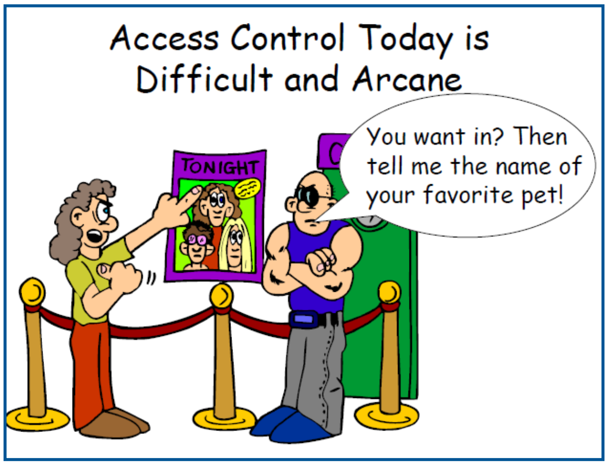
- Assign policies to data based on classification
  - Application, metadata, and/or content
- Policies derived from Information Requirements
  - Security
  - Information Rights Management
  - Data Leakage Protection
  - Data retention
  - Search & Index
  - Authentication & Authorization
  - And others…
- Automated data classification provides scalability

October 2007 Information-centric Policy Management © 2007 Storage Networking Industry Association. All Rights Reserved. 26

What's the difference between data and keys?

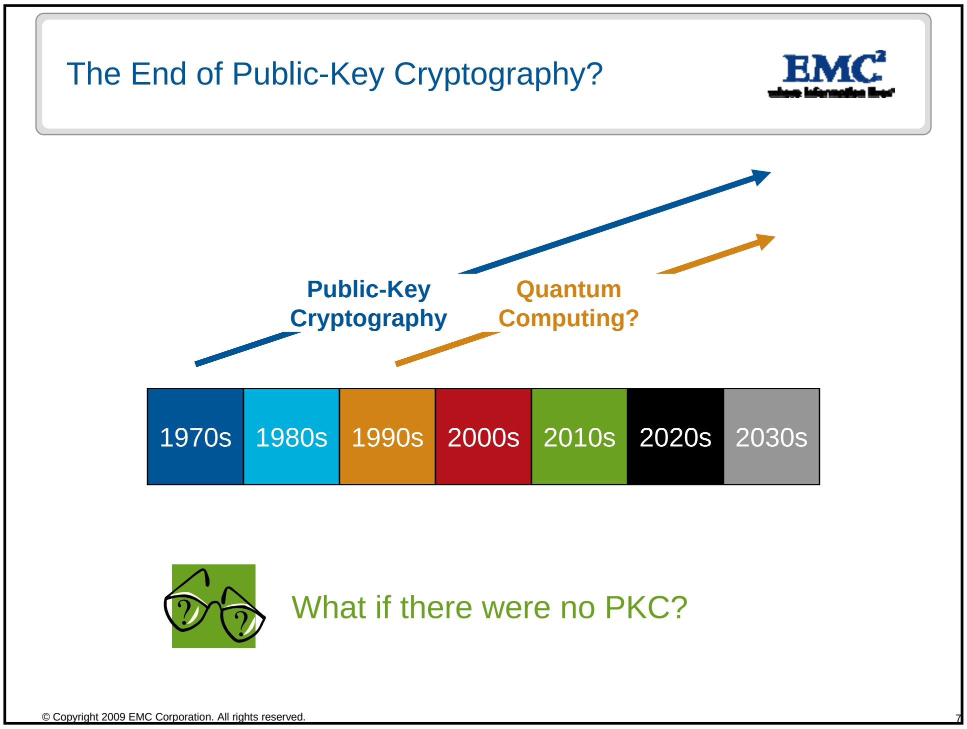
Source: E. StPierre, "Information-Centric Policy Management," Storage Networking Industry Association, 2007

More Than Just Keys


Access Control Today is Difficult and Arcane
TONIGHT
You want in? Then tell me the name of your favorite pet!

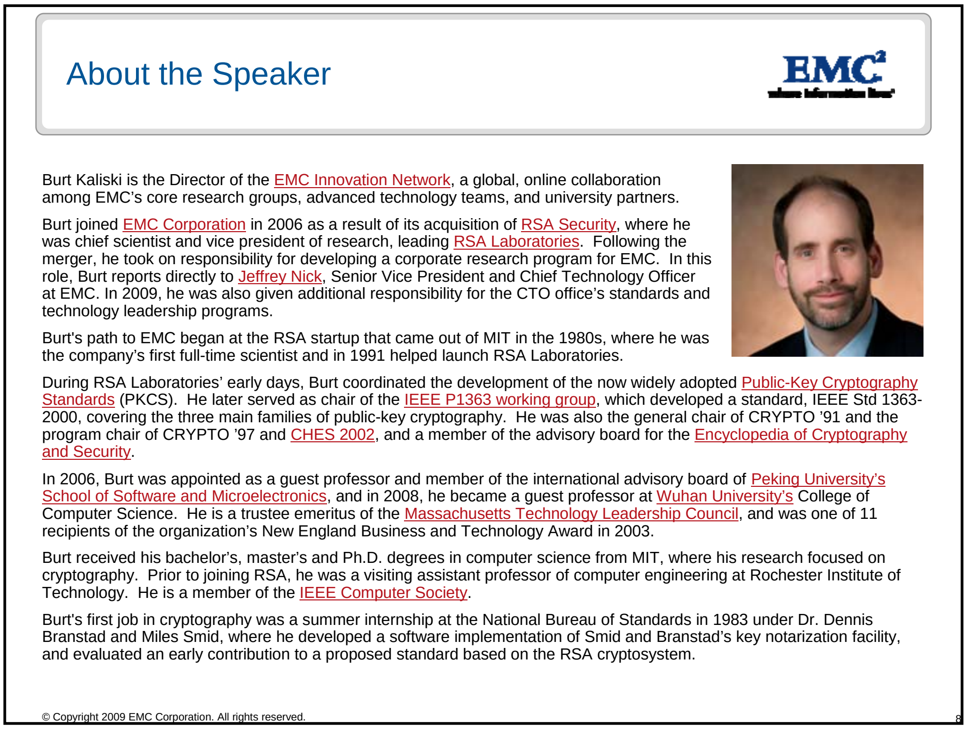
What's the difference between keys and data?

Source: A. Juels, "Next Generation Access Control: The Bouncer Turned Doorman," EMC Innovation Network Lecture Series, November 2008



The End of Public-Key Cryptography?

What if there were no PKC?



About the Speaker

Burt Kaliski is the Director of the EMC Innovation Network, a global, online collaboration among EMC's core research groups, advanced technology teams, and university partners.

Burt joined EMC Corporation in 2006 as a result of its acquisition of RSA Security, where he was chief scientist and vice president of research, leading RSA Laboratories. Following the merger, he took on responsibility for developing a corporate research program for EMC. In this role, Burt reports directly to Jeffrey Nick, Senior Vice President and Chief Technology Officer at EMC. In 2009, he was also given additional responsibility for the CTO office's standards and technology leadership programs.

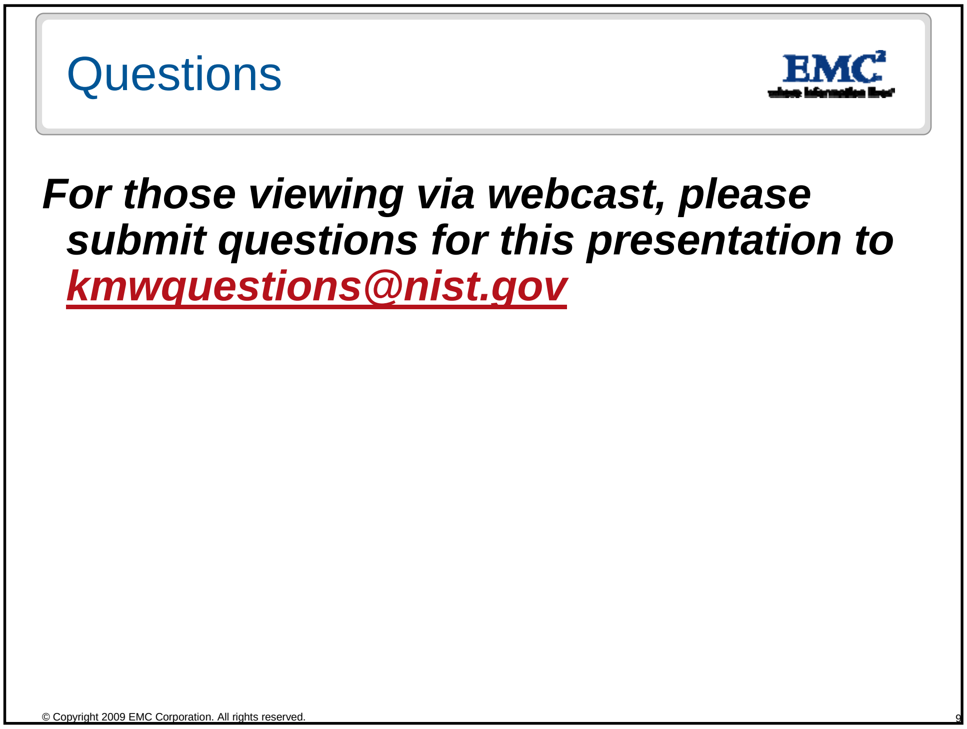
Burt's path to EMC began at the RSA startup that came out of MIT in the 1980s, where he was the company's first full-time scientist and in 1991 helped launch RSA Laboratories.

During RSA Laboratories' early days, Burt coordinated the development of the now widely adopted Public-Key Cryptography Standards (PKCS). He later served as chair of the IEEE P1363 working group, which developed a standard, IEEE Std 1363-2000, covering the three main families of public-key cryptography. He was also the general chair of CRYPTO '91 and the program chair of CRYPTO '97 and CHES 2002, and a member of the advisory board for the Encyclopedia of Cryptography and Security.

In 2006, Burt was appointed as a guest professor and member of the international advisory board of Peking University's School of Software and Microelectronics, and in 2008, he became a guest professor at Wuhan University's College of Computer Science. He is a trustee emeritus of the Massachusetts Technology Leadership Council, and was one of 11 recipients of the organization's New England Business and Technology Award in 2003.

Burt received his bachelor's, master's and Ph.D. degrees in computer science from MIT, where his research focused on cryptography. Prior to joining RSA, he was a visiting assistant professor of computer engineering at Rochester Institute of Technology. He is a member of the IEEE Computer Society.

Burt's first job in cryptography was a summer internship at the National Bureau of Standards in 1983 under Dr. Dennis Branstad and Miles Smid, where he developed a software implementation of Smid and Branstad's key notarization facility, and evaluated an early contribution to a proposed standard based on the RSA cryptosystem.



Questions

For those viewing via webcast, please submit questions for this presentation to kmwquestions@nist.gov