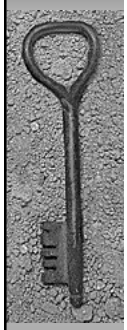
Key Management Workshop

November 1-2, 2001

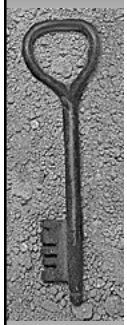


History

- Need for approved key establishment schemes for Federal applications to meet security and interoperability needs
- February 10-11, 2000 Workshop called for key management "framework" document specifying needed documents
  - Schemes including DH, RSA, and ECC from ANSI X9.42, 44, and 63 to be part of initial effort
  - At least one royalty-free scheme
  - Timeline

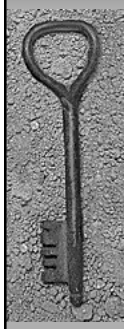
NIST Framework Approach

- Scheme Definition Document (Standard or Recommendation)
  - DH and MQV from ANSI X9.42
  - RSA from ANSI X9.44
  - ECC from ANSI X9.63
  - Key wrapping
  - Key derivation from a master key (?)



NIST Framework Approach (Contd.)

- Key Management Guidance Document (Recommendation or Guideline)
  - Key lifecycle
  - Cipher suite negotiation (selection)
  - Cryptoperiods
  - Assurance
  - Accountability
  - Key backup, archiving and recovery
  - PKI-related issues
  - Protocol issues
  - Implementation issues



Framework Timeline

- First draft for review (June 2001)
- Proposed key wrapping scheme (July 2001)
- Workshop on first draft (October 2001)
- Continued Development (Thereafter)

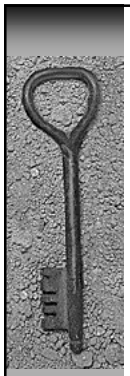
And here we are; just about back on schedule!

And so,we're here today

- Purpose of the workshop
  - This is not final!
  - We're all ears 
- Recording
- Report: http://www.nist.gov/kms
- Physical considerations

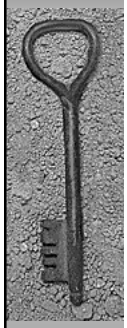
November 1: Morning Agenda

9:00-9:05	Welcome to the Workshop (Elaine Barker)
9:05-9:15	Overview of the History of the Key Management Project
	Goals and Purpose of Workshop
	Goals and Purpose of the Key Establishment Schemes Document (Elaine Barker)
9:15-10:15	Overview of the Key Establishment Schemes Document (Miles Smid)
10:15-10:30	Break
10:30-11:30	Issues and Discussions (Second Pass, Elaine Barker and Miles Smid)
11:30-12:30	Lunch



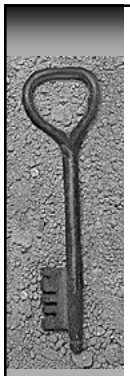
November 1: Afternoon Agenda

12:30-1:30	Issues and Discussion Continued (Second Pass, Elaine Barker and Miles Smid)
1:30-2:00	Final Discussion and New Items (Elaine Barker and Miles Smid)
2:00-2:15	Break
2:15-3:15	Status of Draft ANSI X9.44 (Burt Kaliski)
3:15-3:45	Future Plans (Elaine Barker)
3:45-4:00	Break
4:00-4:15	Overview of the Goals and Purpose of the Key Management Guideline (Elaine Barker)
4:15-4:45	Overview of the Key Management Guideline (Curt Barker)
4:45	Close for the day



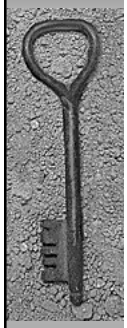
November 2: Morning Agenda

9:00-9:30	Introduction, Glossary, and Acronyms (Tim Polk)
9:30-10:30	Cryptographic Algorithms, Keys, and Other Keying Material (Miles Smid)
10:30-10:45	Break
10:45-11:45	Key Management Lifecycle (Curt Barker, Miles Smid)
11:45-12:45	Lunch



November 2: Afternoon Agenda

12:45-1:45	Key Management Lifecycle Continued (Curt Barker)
1:45-2:45	General Key Management Guidance (Elaine Barker)
2:45-3:00	Break
3:00-3:30	Key Management Guidance-Selected Infrastructures (Tim Polk)
3:30-4:30	Key Management Guidance-Selected Protocols and Applications (Bill Burr)
4:30-5:00	Final Discussion and New Items (Curt Barker, Elaine Barker, Bill Burr, Tim Polk, Miles Smid)
5:00-5:15	Future Plans (Elaine Barker)
5:15	Close



Key Establishment Schemes

- Document developers: Elaine Barker and Miles Smid
- Goals and Purpose
  - Secure schemes
  - Validation
  - Minimize number of schemes