



The Security Division of EMC

Key Management in X9

Key Management Summit
September 23, 2008
James Randall

Key Management

- ▶ What is key management?
 - Key generation
 - Key distribution
 - Key life cycle Facility requirements
 - Modes
 - IVs
 - Message formats

Along came DES

- ▶ Standardized in X3.92 (single length keys) and
- ▶ X3.106 (modes)
- ▶ NIST issued FIPS 46

9.17 Key Management

- ▶ Encompassed:
 - Key generation
 - Key distribution
 - Key life cycle
 - Message formats
 - Facility requirements
 - Mandated FIPS 140-1
 - Required manually delivered keys
 - 2 and 3 layer architectures
- ▶ NIST – Key management using X9.17 (27 options)

Retail Key Management

- ▶ X9.24 Symmetric Key Management Part 1: Using Symmetric Techniques
- ▶ X9.65-2004 Triple Data Encryption Algorithm (TDEA) Implementation
- ▶ X9.69 Key Extensions
- ▶ X9.79 PKI Part 1 Framework

Public Key

- ▶ X9.42 Agreement of Symmetric Keys Using Diffie-Hellman
- ▶ X9.44 Key Establishment Using Integer Factorization Cryptography
- ▶ X9.62-2005 The Elliptic Curve Digital Signature Algorithm
- ▶ X9.63 Key Agreement and Key Transport Using Elliptic Curve Cryptography
- ▶ X9.70 Symmetric Key Distribution Using Public Key

Key Generation Extras

- ▶ X9.65 TDEA Implementation Standard
- ▶ X9.80 Prime Number Generation Primality Testing, and Primality Certificates
- ▶ X9.82 Parts 1 - 4 Random Number Generation

Authenticating Key Agreement and Key Transport

- ▶ X9.30-1&2 Public Key Cryptography Using Irreversible Algorithms
 - Part 1: The Digital Signature Algorithm (DSA)
 - Part 2: The Secure Hash Algorithm (SHA-1)
- ▶ X9.31 Digital Signatures Using Reversible Public Key Cryptography
- ▶ X9.92 Digital Signature Algorithms Giving Partial Message Recovery

Protocols for Key Management

- ▶ X9.69 Framework for Key Management Extensions
- ▶ X9.70 Symmetric Key Distribution Using Public Key
- ▶ X9.73 Cryptographic Message Syntax
- ▶ X9.77 Public Key Infrastructure Protocols

Other Protocols

- ▶ X9 45 Enhanced Controls
- ▶ X9 49 Secure Remote Access
- ▶ X9 55 Extensions
- ▶ X9 57 Certificate Management
- ▶ X9.68 Short Certificates
- ▶ X9.79 PKI Part 1 Framework
- ▶ X9 84 Biometric Security
- ▶ X9 88 Enhanced Digital Signatures
- ▶ X9 95 Trusted Time Stamp
- ▶ X9 96 XML CMS
- ▶ X9 111 Pen Test
- ▶ X9.112 Wireless - Part 1: General
- ▶ X9 113 Trusted Transaction



The Security Division of EMC

Thank you!