# ANSI X9.F.1 Cryptographic Standards

Don B. Johnson
Director of Standards, Certicom

October 1997

# What is ANSI X9.F.1?

- ANSI - American National Standards Institute
- X9 - American Bankers Association
- F - Financial Institution Security
- 1 - Tools
- Open meetings 4 times a year
- ANSI X9.F goes to ISO TC68 twice a year

CERTICOM

# ANSI X9.F.1 Requirements

- Bankers have perhaps the highest security requirements
- Billions of dollars are transferred electronically daily
- Single transactions can easily total millions of dollars
- Others: “If it’s good enough for bankers, it’s good enough for me.”

CERTICOM

# Why X9 standards?

- Mitigate risk of doing business
- Increase assurance of high level of security via open discussion
- Aid interoperability by encouraging vendor convergence
- Help determine prudent practice
- Aid assurance of correct implementation via conformance testing

# ANSI X9.F.1 Members

- Bankers - Citibank, Chase, First Union, FRB, Zions Bank, etc.
- Auditors - Accounting firms (KPMG, C&L)
- Vendors - IBM, DEC, Certicom, SDTI, Entrust, Verisign, Motorola, GTE, Spyrus, Polaroid, Pitney Bowes, IRE, etc.
- Government - NSA, NIST, CSE

# ANSI X9 Process

- Submission of proposal with 5 supporters (adopt/adapt ISO, IEEE, IETF, FIPS, etc.)
- New work item ballot
- Draft submission
- Line by line review
- Ballot final draft
- Standard

CERTICOM

# Symmetric Key

- X9.9 Message Authentication Code - Wholesale
- X9.19 Message Authentication Code - Retail
- X9.23 Message Encryption
- X9.52 Triple DES (ballot)

CERTICOM

# Digital Signatures

- X9.30 DSA - Digital Signature Algorithm (based on FIPS 186)
- X9.31 rDSA - reversible Digital Signature Algorithm (RSA and Rabin-Williams) (ballot)
- X9.62 ECDSA - Elliptic Curve Digital Signature Algorithm (ballot)

CERTICOM

# X9.31 rDSA

- Adapted from ISO 9796-2, encodes hash method inside signature
- Input to IEEE P1363 & ISO 14888-3.
- Key size: 1024 + 256s bits, s = 0, 1, 2, ...
- Mandates strong prime criteria generated via a seeded canonical hash-based method
- Seed can be used as evidence of correct key pair generation

# X9.62 ECDSA

- Elliptic Curve analog of DSA
- Adapted from IEEE P1363
- Key size: >= 161 bits, Vaudenay's attack on DSA is not possible (160-bit ECC is roughly equivalent to 1024-bit RSA in terms of MIPS years to break using best attacks)
- Optional seeded hash method of generating arbitrary system parameters

# X9.62 Subroutines

1. System Parameter Generation
2. (Optional) System Parameter Validation
3. Key Pair Generation
4. (Optional) Public-Key Validation
5. Signature Generation
6. Signature Verification

These aid in system conformance testing & user confidence.

# Key Establishment

- X9.17 - Symmetric Key Encryption
- X9.42 - Diffie-Hellman Key Agreement (Unified Model and MQV) (ballot, ideas input to IEEE)
- X9.44 - RSA Key Transport (in process)
- X9.63 - Elliptic Curve Key Establishment (in process)

# Certificates

- X9.57 Certificate Management
- X9.55 Certificate Extensions
- X9.45 Attribute Certificates (ballot)

# Conformance Testing

- X9.66 - Security Requirements for Cryptographic Modules (draft based on FIPS 140-1)
- X9 TG - Guidelines for Validating Implementations (proposal) - SHA-1, DSA, rDSA, ECDSA, DH, T-DES, etc.

# ANSI X9.F.1 Summary

- X9.F.1 is evolving a comprehensive suite of high security cryptographic standards for use by the financial industry
- Can be used by others with high security requirements
- We try to coordinate with ISO, IEEE, IETF and others

# X9.F.1 Contacts

- Chairman - Blake Greenlee, 203-762-8580 (blake.greenlee@greenlee.com)
- ABA Web Site - http://www.x9.org
- No mailing list: to obtain drafts, one can attend an open meeting
- To order an X9 standard - 800-338-0626 or 202-663-5087