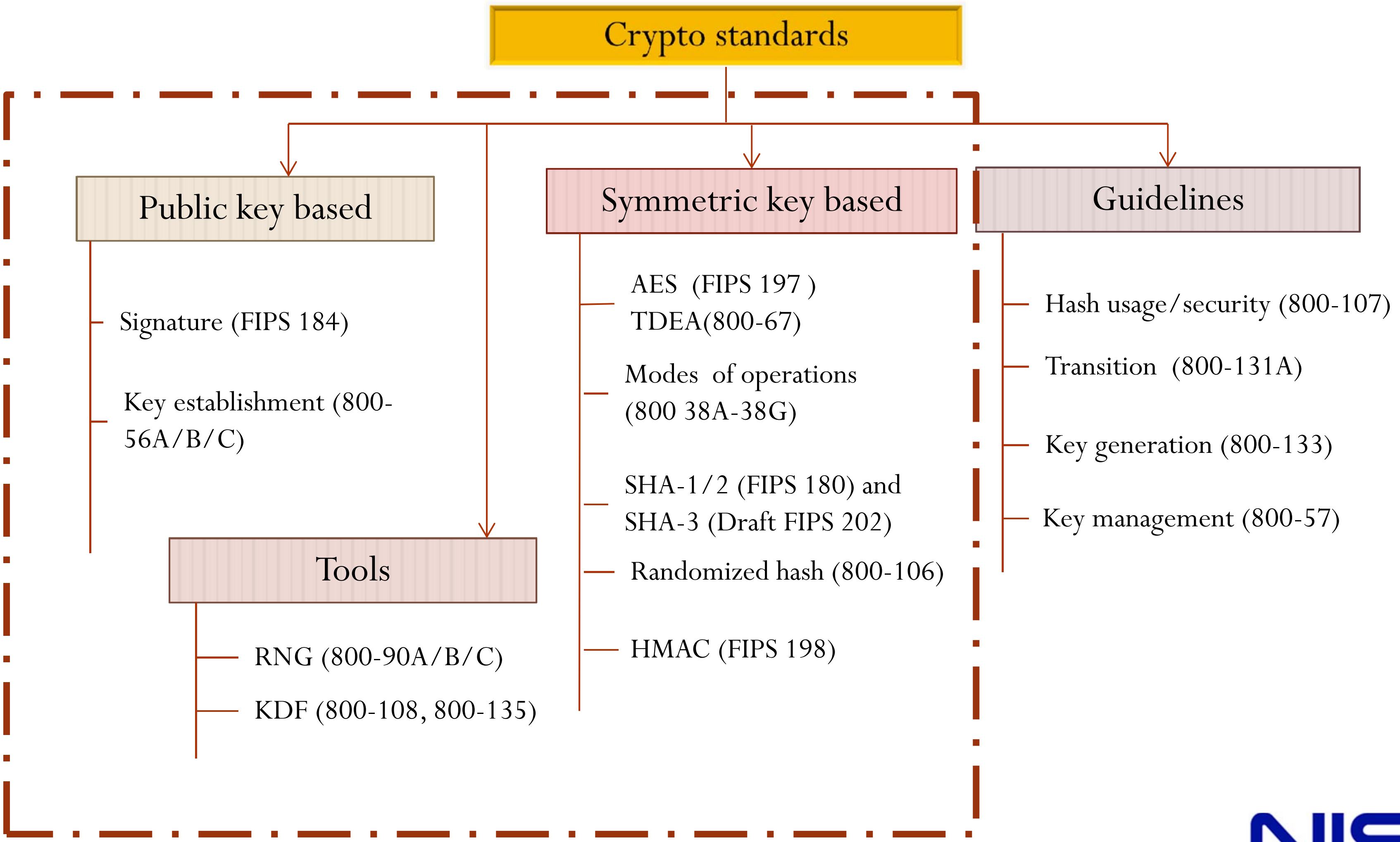
Outline

- Overview of NIST cryptography standards
- Adoptions in ISO/IEC
- Adoptions in IETF
- Adoptions in IEEE 802 wireless standards
- Remarks

NIST Crypto Standards - Overview



Crypto standards

Public key based

- Signature (FIPS 184)
- Key establishment (800-56A/B/C)

Tools

- RNG (800-90A/B/C)
- KDF (800-108, 800-135)

Symmetric key based

- AES (FIPS 197)
  TDEA(800-67)
- Modes of operations (800 38A-38G)
- SHA-1/2 (FIPS 180) and SHA-3 (Draft FIPS 202)
- Randomized hash (800-106)
- HMAC (FIPS 198)

Guidelines

- Hash usage/security (800-107)
- Transition (800-131A)
- Key generation (800-133)
- Key management (800-57)

NIST Crypto Standards
Major development methods

- Cryptographic algorithm competitions
  - Advanced Encryption Standard (AES)
  - Secure Hash Algorithm – 3 (SHA-3)
- Adoption of standards developed in other standards organizations (e.g. SP 800-56A, SP 800-56B)
- Develop new standards
  - In-house development based on well accepted research results (e.g. SP 800-56C)
  - Selected among submissions (e.g. modes of operations in 38 series)

Symmetric Key-Based Cryptography

- Block Ciphers
  - FIPS 197 Advanced Encryption Standard (AES)
  - SP 800-67 Triple DES
  - Modes of operations
    - NIST SP 800-38 series (A/B/C/D/E/F/G)
- Hash Functions
  - FIPS 180-4 SHA-1 and SHA-2
  - Draft FIPS 202 SHA-3
- Message authentication codes
  - FIPS 198 HMAC (hash function-based)
  - NIST SP 800-38B CMAC (block cipher-based)

Public (Asymmetric) Key Cryptography

- Digital Signatures
  - FIPS 186-4
    - Discrete log-based: DSA and ECDSA
    - Factorization-based: RSA
- Key Establishment Schemes
  - NIST SP 800-56A Discrete Logarithm-Based
    - DHs, MQVs
  - NIST SP 800-56B Factorization-Based
    - RSA based key transport and key agreement

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (General)

- ISO/IEC JTC 1/SC 27 IT Security techniques
  - SC27 WG2
    - Cryptography and security mechanisms
- SC27 WG2 covers a much larger scope in standardizing cryptography and security mechanisms, compared with NIST standards
  - More than 20 active working items/projects
  - Multiple algorithms and schemes are standardized or studied in each working item/project

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (Block Ciphers)

- AES (in FIPS 197) and TDEA (in SP 800-67) are adopted in
  - ISO/IEC 18033-3:2010
    - Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers
      - 64-bit block ciphers: TDEA, MISTY1, CAST-128, HIGHT
      - 128-bit block ciphers: AES, Camellia, SEED
- Modes of operations (in SP 800-38A) are adopted in
  - ISO/IEC 10116:2006
    - Information technology -- Security techniques -- Modes of operation for an n-bit block cipher
      - Electronic Codebook (ECB)
      - Cipher Block Chaining (CBC), with optional interleaving
      - Cipher Feedback (CFB)
      - Output Feedback (OFB); and
      - Counter (CTR)

NIST

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (Authenticated encryption)

- Modes of operation for authenticated encryption
  - CCM (in SP 800-38C)
  - GCM (in SP 800-38D)
  - Key wrapping (in SP 800-38E)

  are adopted in

  - ISO/IEC 19772:2009
    - Information technology -- Security techniques -- Authenticated encryption
      - OCB 2.0, Key wrap, CCM, EAX, Encrypt-then-MAC, GCM

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (Hash Functions)

- SHA-1 and SHA-2 (in FIPS 180-4) families are adopted in
  - ISO/IEC 10118-3:2004
    - Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions
      - RIPEMD-160, RIPEMD-128, SHA-1, SHA-256, SHA-224, SHA-512, SHA-384, WHIRLPOOL
- Truncated version: SHA-512/224, SHA-512/256 (in FIPS 180-4), and SHA-3 functions will be adopted in the current revision of ISO/IEC 10118-3

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (HMAC and CMAC)

- HMAC (in FIPS 198-1) is adopted in
  - ISO/IEC 9797-2:2011
    - Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function
      - MDx-MAC
      - HMAC
- CMAC (in SP 800-38B) is adopted in
  - ISO/IEC 9797-1:2011
    - Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher
      - MAC Algorithm 5 (compatible with CMAC)

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (Key derivations)

- Key derivation functions: counter mode and feedback mode (in 800-108) are adopted in
  - ISO/IEC CD 11770-6
    - Information technology -- Security techniques -- Key management -- Part 6: Key derivation
- Two step key derivation methods – extraction and expansion (in 800-56C) are adopted in
  - ISO/IEC CD 11770-6
    - Information technology -- Security techniques -- Key management -- Part 6: Key derivation

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (Digital Signatures)

- DSA (in FIPS 186-4) is adopted in
    - ISO/IEC CD 14888-3
        - Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms
- RSA signature (in FIPS 186-4) is adopted in
    - ISO/IEC 14888-2:2008
        - Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (Key Establishment)

- ISO/IEC 11770-3:2008
  - Information technology -- Security techniques -- Key management -- Part 3: Mechanisms using asymmetric techniques
    - 11 key agreement mechanisms and 6 key transport mechanisms using generalized notations/equations without being specific about the mathematics structures
  - Mechanisms specified in ISO/IEC 1177-3:2008 can be instantiated by the schemes specified in SP 800-56A (DHs and MQVs) and SP 800-56B (RSA)

NIST Crypto Standards Adoptions in ISO/IEC JTC SC 27 (Summary)

- The major NIST symmetric key-based crypto standards have been adopted in standards developed by ISO/IEC SC27
  - The standards developed by ISO/IEC SC 27 are more general with multiple options in each category
- The NIST signature standards are adopted in standards developed by ISO/IEC SC27
- ISO/IEC SC27 specifies key establishment mechanisms using general models that can be instantiated by the schemes in SP 800-56A and SP 800-56B

NIST Crypto Standards Adoptions in IETF (Symmetric key algorithms)

- NIST symmetric key-based cryptography standards are generally adopted by IETF to protect protocols, e.g.
  - Transport Layer Security (TLS) 1.2 (RFC 5246)
    - AES, TDEA, SHA-1, SHA-2, HMAC are adopted in TLS cipher-suites, e.g.
      - TLS_RSA_WITH_AES_128_CBC_SHA
      - TLS_RSA_WITH_AES_256_CBC_SHA
      - TLS_RSA_WITH_AES_128_CBC_SHA256
      - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
      - TLS_DH_DSS_WITH_AES_128_CBC_SHA
  - Internet Key Exchange Protocol Version 2 (IKEv2) (RFC 7296)
    - AES, TDES, SHA-1, SHA-2 and HMAC*
  - IP Encapsulating Security Payload (ESP) (RFC 4303)
    - Encryption: Must support AES –CBC, if it is not NULL (RFC 4835)
    - Integrity: Must support HMAC* (RFC 4835)
  - IP Authentication Header (AH) (RFC 4302)
    - Integrity: Must support HMAC-SHA1-96 (RFC 4835)

* HMAC was adopted from IETF RFC 2104

NIST Crypto Standards Adoptions in IETF (Asymmetric key algorithms)

- Digital signatures specified in FIPS 186-4 have been adopted in many IETF standards, e.g. TLS, IKE, etc. for authentication
- Some key establishment schemes specified in SP 800-56A are used* by TLS and IKE
  - TLS provides three options for key establishment
    - RSA key transport, e.g.
      - TLS_RSA_WITH_AES_128_CBC_SHA
    - Ephemeral-static Diffie-Hellman key agreement, e.g.
      - TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
    - Ephemeral-ephemeral Diffie-Hellman key agreement, e.g.
      - TLS_DH_DSS_WITH_AES_128_CBC_SHA
  - IKE uses ephemeral-ephemeral Diffie-Hellman key agreement to establish keys

* NIST SP 800-56A and SP 800-56B specify schemes, not protocols.

NIST Crypto Standards Adoptions in IETF (Summary)

- NIST symmetric key-based crypto standards are adopted to protect protocols specified in IETF
- NIST digital signature standards are adopted for authentication
- IETF uses crypto primitives specified in NIST SP 800-56A and SP 800-56B for key establishment
- Some NIST crypto standards adopted IETF standards, e.g.
  - HMAC (in FIPS 198)
  - Application-specific key derivation functions (in SP 800-135)

NIST Crypto Standards Adoptions in IEEE 802 Wireless Standards

- In IEEE 802 wireless standards, NIST symmetric key based cryptography standards are adopted to apply protections, e.g.
  - AES in CCM, GCM modes
  - CMAC
  - HMAC
- Some of IEEE 802 wireless standards assume that key establishment is implemented at a higher layer (higher than MAC and physical layer)
  - That is the reason why schemes in 56A and 56B are not referred to in the IEEE 802 wireless standards
  - EAP-TLS can be used to establish keys at a higher layer for lower layer protection, which uses TLS (see IETF section of this presentation)
- Digital signatures specified in FIPS 186-4 are used for authentication, e.g.
  - IEEE 802.16 uses RSA signatures
  - IEEE 802.21 uses ECDSA

NIST Standards Adopted from Other Standard Bodies

- X9F1 (X9: financial industry standards)
  - SP 800-56A: based on X9.42 and X9.63
  - SP 800- 56B: based on X9.44
  - SP 800-90A: based on X9.82 part 3
  - FIPS 186-4 (RSA signature portion): X9.31
- IEEE 802.11 (wireless)
  - SP 800-38C CCM mode
- IEEE 1619-2007 (storage)
  - SP 800-38E XTS mode
- IETF RFC 2104
  - HMAC: Keyed-Hashing for Message Authentication

Remarks

- The presentation selected three major international/industry standards, ISO/IEC JCT SC27, IETF, and IEEE 802 to study adoptions of NIST crypto standards
  - NIST crypto standards are also adopted by other industry standards, such as Trusted Computing Group (TCG), Bluetooth, etc.
- Some of NIST public key cryptography standards (RSA signature in FIPS 186, DHs, and MQVs in SP 800-56A) were developed based on X9 standards developed in subcommittee X9F, working group X9F1
  - IEEE P1363 developed public key cryptography standards, including RSA, DHs, and MQVs, in almost the same timeframe as X9F1 development activities