Interagency Advisory Board

Meeting Agenda, Wednesday, May 23, 2012

1. **Opening Remarks** *(Mr. Tim Baldridge, IAB Chair)*
2. **Revision of the Digital Signature Standard** *(Tim Polk, NIST)*
3. **Update on Content and Status of FIPS 201-2** *(Hildy Ferraiolo, NIST)*
4. **The Importance, Expectation, and Value of FPKIMA** *(Chris Louden)*
5. **Use of PIV/CAC as a Payment Token in Transit Applications** *(Greg Garback, WMATA)*
6. **Closing Remarks** *(Mr. Tim Baldridge, IAB Chair)*

Filling The Gaps: Changes and Additions to NIST Crypto Standards

Tim Polk

May 23, 2012

Overview

- Two relatively minor updates to current NIST specifications
  - Updates to the SHA-2 family (March 2012)
  - Updates to digital signature algorithms (Comment period closes May 25, 2012)
- A decade-long effort comes to fruition just in time
  - Random bit generation specifications (Part A published in January; drafts of B, C late FY12)

FIPS 180-4

- provides a general procedure for creating an initialization value
- adds two additional secure hash algorithms to the Standard: SHA-512/224 and SHA-512/256
  - More efficient alternatives on platforms that are optimized for 64-bit operations
- removes a restriction that padding must be done before hash computation begins
  - Increased flexibility and possibly efficiency in implementations for many applications

FIPS 186-3, Change Notice 1

- Allows the use of any random bit/number generator that is approved for use in FIPS-140-validated modules
- Corrects statements in FIPS 186-3 regarding the generation of the integer k
  - k is used as a “secret number” in the generation of DSA and ECDSA digital signatures
- Corrects a typographical error in the processing steps of secret number generation for ECDSA
- Relaxes restrictions on the retention and use of prime number generation seeds for generating RSA key pairs
- Corrects the wording of the criteria for generating RSA key pairs
- Use of a salt with RSASSA-PSS digital signatures scheme aligned with Public Key Cryptography Standard (PKCS) #1

Random Bit Generation (RBG) (SP 800-90A, B and C)

- Purpose: To provide approved RBGs with “tunable” security strengths (112, 128, 192, 256 bits).
- Collaborative effort by NIST and NSA.
- Based on work conducted with ANSI X9 (X9.82).
- Includes models, and requirements for validation and health testing.

RBGs: SP 800-90A

- SP 800-90A (DRBGs):
  - Contains four DRBG algorithms using approved hash functions and block ciphers.
  - Completed in 2006; revised in 2012.
  - DRBG algorithms currently being validated by the CAVP.

RBGs: SP 800-90B

- SP 800-90B (Entropy Sources):
  - The most difficult part to develop.
  - Available for public comment this summer.
  - Planning to meet with developers and CMVP labs to discuss validation issues.

RBGs: SP 800-90C

- SP 800-90C (RBG Constructions);
  - Contains constructions for DRBGs and NRBGs.
  - Combines SP 800-90A DRBGs with SP 800-90B entropy sources.
  - Available for public comment this summer.

Links

- http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf
- http://csrc.nist.gov/publications/drafts/fips186-3/change-notice_fips-186-3.pdf
- http://csrc.nist.gov/publications/nistpubs/800-90A/SP800-90A.pdf

Questions?