X9.82, Part 3
Differences from the Previous Version

October 20, 2004

Elaine Barker

General

- Title: DRBGs → DRBG Mechanisms
- Reorganization of Sections 8, 9 and 10

Section 8: Concepts and General Requirementrs

- Removed references to FIPS 140-2 cryptomodules
- Removed the 80-bit security level
- Entropy requirements for seeds:
  - Instantiation: security level + 64
  - Reseed: security level
  - Full entropy for cipher-based DRBGs
- More text on personalization strings

Section 9: Procedures

- Now specified at a higher level than before
  - Instantiate, reseed, generate, uninstantiate, test
  - Calls the algorithms
- Specifies different sources of input and output:
  - I/O from/to a consuming application
  - Other input (e.g., from an entropy source)
  - Output retained within the DRBG
- Block Cipher derivation function – NEW!

Section 9 (contd.)

- Self testing
  - Defined four configurations within DRBG boundaries
    * **Instantiate**, generate, uninstantiate & test
    * **Generate** and test
    * **Reseed**, generate and test
    * **Instantiate, generate, reseed**, uninstantiate and test

Section 9 (contd.)

- Self testing (contd.)

Health Testing Intervals and Levels of Testing

When to Test	Case 1	Case 2	Case 3
Prior to first instantiation	Non-Time-Critical	Time-Critical	Non-Time-Critical
Periodic	Time-Critical	Non-Time-Critical	Non-Time-Critical
On-demand	Non-Time-Critical	Non-Time-Critical	Non-Time-Critical

Section 9 (contd.)

- Self testing (contd.)
  - For each procedure, non-time-critical and time-critical testing is specified
  - For each configuration, the general testing process is specified

Section 9 (contd.)

- Self testing (contd.)
  - Example (Instantiate, Generate, Uninstantiate within a single DRBG boundary):
    * Select instantiate and generate parameters
    * Request instantiation
    * Request generation
    * Compare with expected results
    * Repeat as needed (if non-time-critical testing)
    * Test error handling
    * Uninstantiate

Section 10: DRBG Algorithm Specifications

- Six algorithms:
  - Hash-based: Hash_DRBG & HMAC_DRBG
  - Block-cipher-based: CTR_DRBG & OFB_DRBG (KHF_DRBG removed)
  - Number theoretic: Dual_EC_DRBG & MS_DRBG
- Tables of definitions (e.g., seed length, reseed_interval, etc.)

Section 10 (contd.)

- Internal state defined as working state and administrative information
- All DRBGs rewritten as "algorithms"
- Hash_DRBG: Instantiate and reseed use Hash_df.
- Diagrams provided for CTR_DRBG & OFB_DRBG

Section 11:Assurances

- Minimum documentation requirements: revised per functional requirements
- Operational/health testing: FIPS 140-2 (only) requirements removed

Annexes

- B: Four conversion routines
- D: Functional requirements per Part 1
- E: Revised number theoretic text
- F: Scenario examples for each DRBG

Attack on Hash_DRBG

- Explanation
  - Ignore?
  - Surgery?
  - Remove?

Schedule

- Written comments by Dec. 1
- Discuss comment resolution at January teleconference
- Stable document by March (tweaks only thereafter?)