The 2017 NIST Transition to Stronger Cryptographic Algorithms

Allen Roginsky

CMVP, NIST

May 17, 2017

The upcoming SP 800-131A Transition

History 101

- The original publication of SP 800-131A (in 2011)
- The 2013 Transition
  - Skipjack
  - 80-bit-strong key establishment schemes
  - The legacy use of various algorithms

History 102

- The 2015 Transition (same version of SP 800-131A)
  - The non-SP-800-90A-compliant RNGs are no longer approved
  - No more two-key Triple-DES encryption
  - The two-key Triple-DES decryption for legacy use only

The Next Stage

- SP 800-131A Rev1 published in November, 2015

Affected Algorithms and Schemes

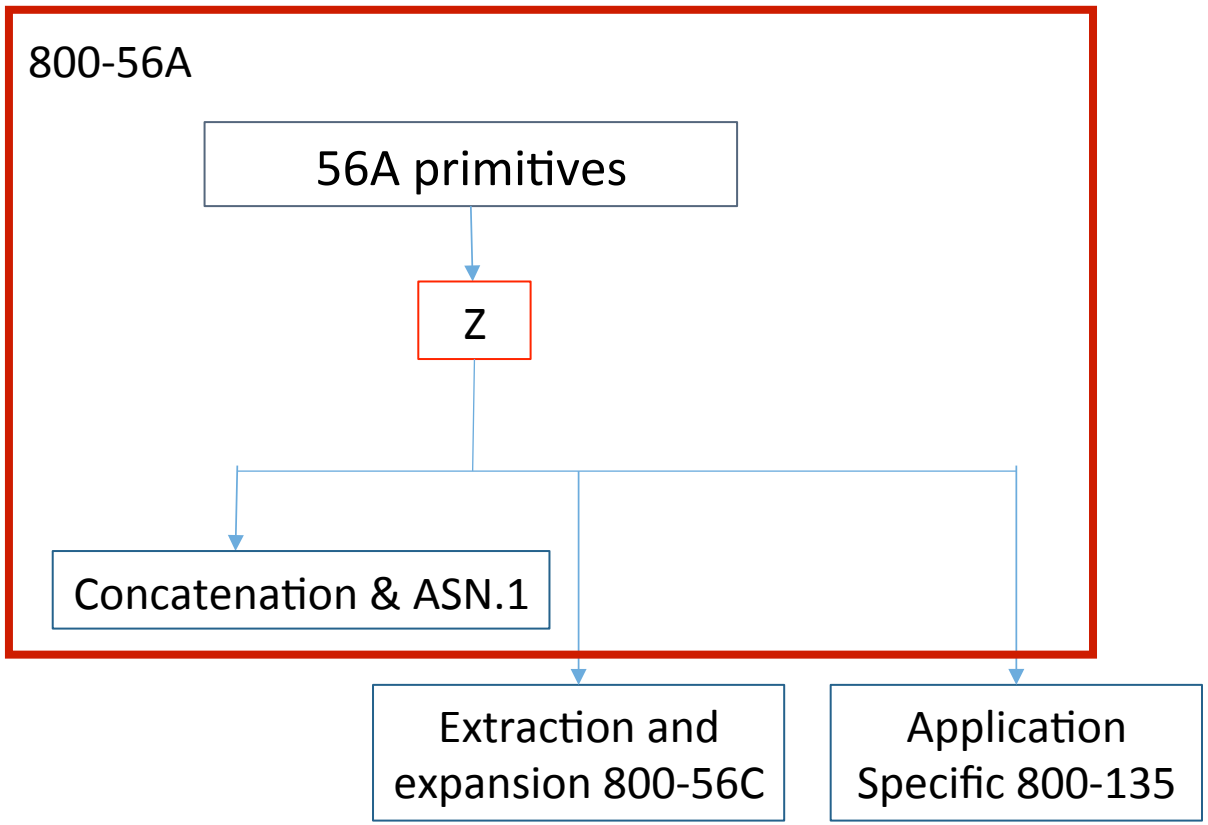
- Key Agreement
- Key Transport
    - Key Encapsulation
    - Key Wrapping

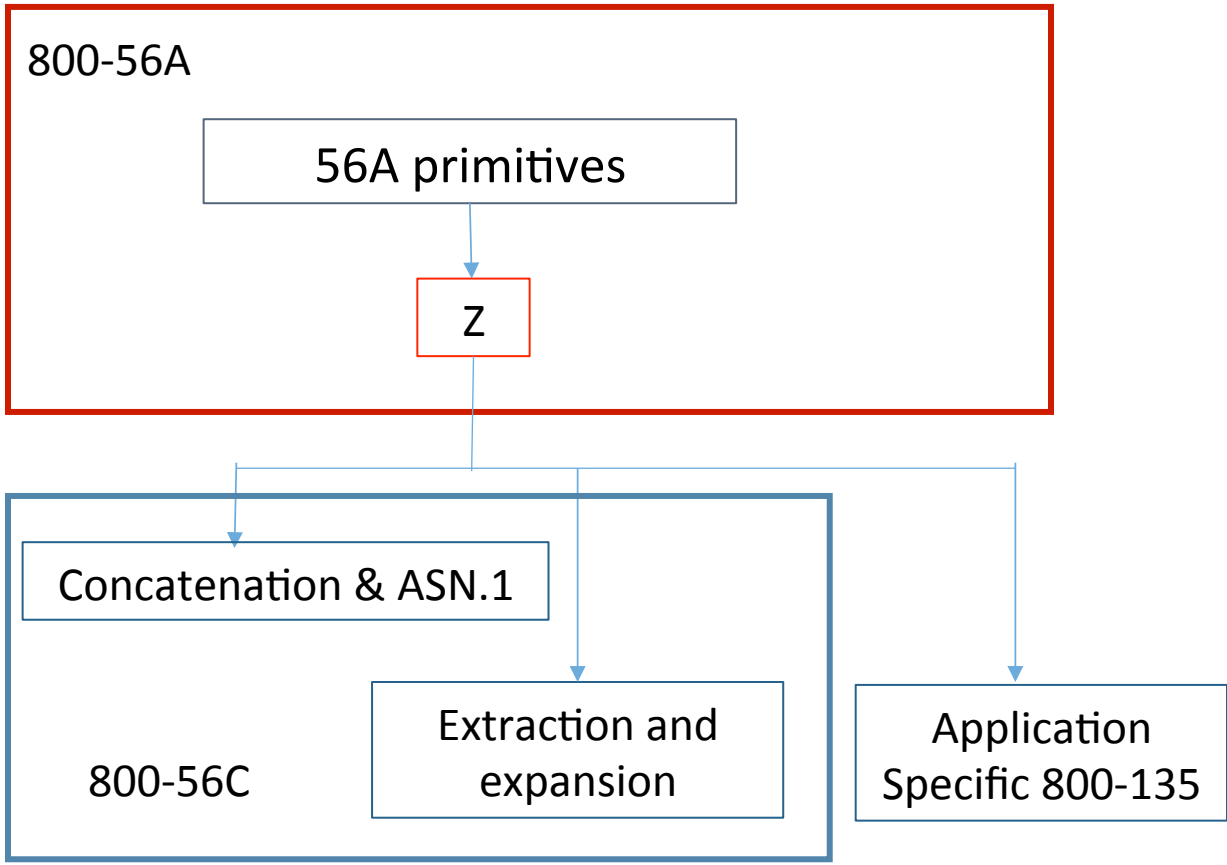
Key agreement

- The SP 800-56A Rev2 – compliant DH and MQV schemes are approved
  - Primes p, q: computed from a random seed, $|p| \geq 2048$, $|q| \geq 224$, q divides p-1
- The SP 800-56A Rev3 – compliant DH and MQV schemes will be approved when the new standard is announced
  - Will include the “safe” primes thus accommodating many industry protocols
  - Safe primes: pre-selected sets of (p, q) pairs, $p = 2q + 1$
- Schemes that are not compliant with SP 800-56A Rev2 or SP 800-56A Rev3
  - Allowed now, if the strength is at least 112 bits
  - Will become non-compliant on January 1, 2018
- The CMVP and the CT group may issue a guidance to accommodate a possible short delay in the publication of SP 800-56A Rev3

Major revisions on SP 800-56A and SP 800-56C **(presented by Dr. Lily Chen)**

- Structure change: moved key derivation methods to 56C





Key-Agreement Key Sizes

- The FFC key-size restriction: $|p| \geq 2048$ bits, $|q| \geq 224$ bits. The *goal* is to move exclusively to the $p = 2q + 1$ prime pairs
- ECC: The NIST-Recommended Elliptic Curves will be listed in SP 800-186
- ECC: New submissions using non-NIST-Recommended curves will not be accepted N months after the publication of SP 800-56A Rev3 (N is small)

RSA-based Key Encapsulation

- The SP 800-56B Rev1 – compliant schemes are approved
- The SP 800-56B Rev2 – compliant schemes will be approved when the new standard is announced
- No major transition issues are expected
- Schemes that are not compliant with SP 800-56B Rev1 or SP 800-56B Rev2
  - Allowed now, if the strength is at least 112 bits
  - Will become non-compliant on January 1, 2018 or at the time a draft of SP 800-56B Rev2 is published
- The CMVP and the CT group may issue a guidance to accommodate a possible delay in the publication of SP 800-56B Rev2

Key Encapsulation Key Sizes

- The RSA modulus of 2048 or 3072 are currently approved
- All RSA modulus sizes greater than or equal to 2048 bits are allowed
- It is expected that SP 800-56B Rev2 will have the greater than 2048 bit lengths approved

Key Wrapping Using AES and Triple-DES

- Today:
  - All SP 800-38F compliant implementations are approved
  - Key wrapping/unwrapping using an approved mode of AES or three-key Triple-DES is allowed
  - Key unwrapping using two-key Triple-DES is allowed
- The new submissions after December 31, 2017:
  - Key wrapping shall be compliant with SP 800-38F
  - Key unwrapping using the compliant block ciphers will be allowed (legacy-use). The length of this transition is to be announced.