



Transitioning of Cryptographic Algorithms and Key Sizes (SP 800-131- Draft 2)

Elaine Barker and Allen Roginsky

NIST

June 29, 2010

Background:

- Cryptography is used to protect sensitive information
- Attackers are becoming smarter, and computers are becoming more powerful
- Many commonly used crypto algorithms are “broken” (e.g., DES broken about 1998, and SHA-1 weakened by attacks in 2005)
- Defensive measures? Use other algorithms and larger key sizes

Background (contd.):

- Problem: How to transition
- Solution: Be flexible and plan ahead
 - Strategy originally proposed in Draft SP 800-57, Part 1 in 2003
 - SP 800-57, Part 1 completed in 2005; revisions in 2006 and 2007
 - Original Goal: To transition from a security strength of 80 bits to 112 bits by 2011
 - Some algorithms need to be replaced
 - Larger key sizes required

Purpose of SP 800-131:

- To bring more specific transition details to the attention of the Federal government agencies and the public
- 1st comment period ended on March 15th
- A two-month-long comment period followed
- Significant changes were introduced
- The second draft was posted on June 16 for a one-month long comment period

Issues from Received Comments:

- Use 2-key TDEA decryption beyond 2010?
- Extend transition dates (e.g., with risk assessment)?
- Different transition dates for digital signatures used for authentication, rather than document signing?
- Extend SP 800-131 scope to include use, as well as CMVP validation?
- How should revalidations be handled, especially of RNG implementations?

Issues from Received Comments (continued):

- Some protocols have not been designed to work with larger key sizes
- Some protocols, such as GDOI, are not affected by the purported weakness of shorter keys, yet they were axed by the original transition plan

Summary of Changes in Draft 2

- Now discusses use; validation will be covered in a separate document
- Some dates extended, with risk warnings
 - Based on recent analysis
 - Extends 80-bit to 112-bit security strength transition completion through 2013

Summary of Changes (Contd.)

- Terms:
 - (Security) strength: how hard to break the algorithm or find the key
 - Approved: specified in a FIPS or NIST SP
 - (New) Acceptable: safe to use (as far as we know)
 - (New) Deprecated: Users must accept some risk
 - (New) Restricted: Deprecated with additional restrictions
 - (New) Legacy Use: Permitted to process already protected information (some risk)

Rationale for a Delay in Transition

- Seven years passed since the first draft of 800-57
- The first 768-bit integer was reported factored in December 2009. Factoring a 1024-bit modulus is “1000 times harder”.
- Since Federal applications are so diverse, allow data owners manage some risk. The risk is clearly marked.
- Cost vs Security considerations
- Public comment review

Encryption and Decryption:

- Encryption:
 - 2-key TDES
 - **Acceptable** through 2010
 - **Restricted** from 2011 through 2015 ($\leq 2^{20}$ blocks per key max) (**new**)
 - The true security strength is somewhat near 120-n bits, if 2^n pairs of (plaintext, ciphertext) are available to the attacker
 - SKIPJACK
 - **Acceptable** through 2010
 - AES and 3-key TDES
 - **Acceptable**

Encryption and Decryption (continued)

- Decryption (**sort of new**)
 - 2-key TDES and SKIPJACK:
 - **Acceptable** through 2010
 - **Legacy use** thereafter
 - AES and 3-key TDES:
 - **Acceptable**

Digital Signatures:

- Signature generation:
 - 80 bits of strength **acceptable** through 2010
 - 80 bits of strength **deprecated** from 2011 through 2013 (**new**)
 - ≥ 112 bits of strength **acceptable** when FIPS 186-3 compliant; **deprecated** after 2013, otherwise
- Signature verification:
 - 80 bits of strength allowed for **legacy use** after 2010
 - ≥ 112 bits of strength **acceptable**

Digital Signatures (details):

- Not all currently approved digital signatures are FIPS 186-3 compliant
- 80 bits of strength:
 - DSA:
 - ($|p| \geq 1024$ and $|q| \geq 160$) and
 - ($|p| < 2048$ or $|q| < 160$)
 - RSA: $1024 \leq |n| < 2048$
 - EC: $160 \leq |n| < 224$
- 112 bits of strength:
 - DSA:
 - $|p| \geq 2048$ and $|q| \geq 224$
 - RSA: $|n| \geq 2048$
 - EC: $|n| \geq 224$

Random Number Generation:

- RNGs specified in FIPS 186-2, ANS X9.31-1998 and ANS X9.62-2005:
 - **Acceptable** through 2010
 - **Deprecated** from 2011 through 2015
- RNGs specified in SP 800-90:
 - **Acceptable**

DH and MQV Key Agreement:

- 80 bits of strength **acceptable** through 2010
- 80 bits of strength **deprecated** from 2011 through 2013 (**new**), not allowed after 2013
- ≥ 112 bits of strength **acceptable**, if 800-56A compliant; **deprecated** after 2010, otherwise

DH and MQV Key Agreement (details):

- 80 bits of strength, SP 800-56A compliant:
 - FF: $|p| = 1024$, $|q| = 160$
 - EC: $160 \leq |n| < 224$, $|h| \leq 10$
- 112 bits of strength, SP 800-56A compliant:
 - FF: $|p| = 2048$, $|q| = 224$ or 256
 - EC: $|n| \geq 224$, h as in Table 2, SP 800-56A:
 - $224 \leq |n| < 256$, $|h| \leq 14$
 - $256 \leq |n| < 384$, $|h| \leq 16$
 - $384 \leq |n| < 512$, $|h| \leq 24$
 - $512 \leq |n|$, $|h| \leq 32$

DH and MQV Key Agreement (more):

- 80 bits of strength, SP 800-56A non-compliant:
 - FF: $|p| \geq 1024$, $|q| \geq 160$
 - EC: $|n| \geq 160$

- 112 bits of strength, SP 800-56A non-compliant:
 - FF: $|p| \geq 2048$, $|q| \geq 224$
 - EC: $|n| \geq 224$

Key Agreement and Key Transport using RSA:

- Key transport schemes were approved long before SP 800-56B; may need to be treated differently
- Key Transport Schemes:
 - $|n| = 1024$, if 800-56B-compliant and $1024 \leq |n| < 2048$, if non-800-56B-compliant:
 - **Acceptable** through 2010
 - **Deprecated** from 2011 through 2013
 - Not allowed even for the decryption of transported keys after 2013

Key Agreement and Key Transport using RSA (continued):

- Key Transport Schemes:
 - $|n| = 2048$, if 800-56B-compliant and $|n| \geq 2048$, if non-800-56B-compliant:
 - Compliant: **Acceptable**
 - Non-complaint: **Deprecated** after 2013
- Key Agreement Schemes (all compliant):
 - $|n| = 1024$:
 - **Acceptable** through 2010, **Deprecated** from 2011 through 2013
 - $|n| = 2048$: **Acceptable**

Key Wrapping (Mode):

- 2-key TDES
 - Wrapping **acceptable** through 2010
 - Wrapping **restricted** ($\leq 2^{20}$ blocks per key max) from 2011 through 2015
 - Unwrapping **acceptable** through 2010
 - Unwrapping allowed for **legacy use** thereafter (**new**)
- AES and 3-key TDES
 - **Acceptable**

Deriving Keys from a Key (SP 800-108):

- HMAC-based KDF (HMAC in FIPS 198-1):
 - **Acceptable** using any **approved** hash function
- CMAC-based KDF (CMAC in SP 800-38B):
 - 2-key TDES **acceptable** through 2010
 - 2-key TDES **deprecated** from 2011 through 2015 (**new**)
 - AES and 3-key TDES: **Acceptable**

Hash Functions (FIPS 180-3):

- SHA-1:
 - **Acceptable** for signature generation through 2010
 - **Deprecated** for signature generation from 2011 through 2013 (**new**)
 - Allowed for **legacy use** for signature verification
 - **Acceptable** for other applications (e.g., HMAC, RNGs, KDFs)
- SHA-224, SHA-256, SHA-384, SHA-512:
 - **Acceptable** for all applications (including signature generation)

Message Authentication Codes:

- HMAC (FIPS 198-1 and SP 800-107):
 - Any **approved** hash function
 - 80 to 111-bit keys **acceptable** through 2010
 - 80 to 111-bit keys **deprecated** from 2011 to 2013 (**new**)
 - Keys ≥ 112 bits **acceptable**
- CMAC (SP 800-38B):
- 2-key TDES **acceptable** through 2010
- 2-key TDES **deprecated** from 2011 through 2015 (**new**)
- AES and 3-key TDES **acceptable**

Important Information:

- SP 800-131 and other SPs are available at <http://csrc.nist.gov/publications/PubsSPs.html>.
- Send comments to CryptoTransitions@nist.gov
- FIPS are available at <http://csrc.nist.gov/publications/PubsFIPS.html>.
- Contacts:
 - Elaine Barker (ebarker@nist.gov)
 - Allen Roginsky (Allen.Roginsky@nist.gov)



Additional
Discussion?