



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

Elaine Barker and Allen Roginsky

# 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
  - 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
- 1<sup>st</sup> comment period ended on March 15<sup>th</sup>
- Soon to be posted for 2<sup>nd</sup> 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?

# Summary of Changes in Draft 2

- Now discusses use; validation will be part of the FIPS 140 IG
- 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 alg. or find the key
  - Approved: specified in a FIPS or NIST SP
  - (New) Acceptable: safe to use (as far as we know)
  - (New) Allowed: Users must accept some risk

# Encryption and Decryption:

- Encryption:
  - 2-key TDES
    - **Acceptable** through 2010
    - **Allowed** from 2011 through 2015, but with  $\leq 2^{20}$  blocks per key max (**new**)
  - SKIPJACK
    - **Acceptable** through 2010
  - AES and 3-key TDES
    - **Acceptable**

# Encryption and Decryption (contd.)

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

# Digital Signatures:

- Signature generation:
  - 80 bits of strength **acceptable** through 2010 (DSA and RSA:1024-bit keys; ECDSA:160 to 223-bit keys)
  - 80 bits of strength **allowed** from 2011 through 2013 (**new**)
  - $\geq 112$  bits of strength **acceptable** (DSA and RSA: 2048 and 3072-bit keys; ECDSA: keys  $\geq 224$  bits)
- Signature verification:
  - $\geq 80$  bits of strength **acceptable**

# Random Number Generation:

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

# DH and MQV Key Agreement:

- 80 bits of strength **acceptable** through 2010 (FF: 1024-bit keys; EC: 160 to 223-bit keys)
- 80 bits of strength **allowed** from 2011 through 2013 (**new**)
- $\geq 112$  bits of strength **acceptable** (FF: 2048-bit keys; EC: keys  $\geq 224$ -bits)

# Key Agreement and Key Transport using RSA:

- 1024-bit keys **acceptable** through 2010
- 1024-bit keys **allowed** from 2011 through 2013 (**new**)
- 1024-bit keys **allowed** for decryption only thereafter
- 2048-bit keys **acceptable**

# Key Wrapping (Mode):

- 2-key TDES
  - Wrapping **acceptable** through 2010
  - Wrapping **allowed** from 2011 through 2015 (**new**)
  - Unwrapping **acceptable** through 2010
  - Unwrapping **allowed** 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 **allowed** from 2011 through 2015  
(**new**)
  - AES and 3-key TDES: **Acceptable**

# Hash Functions (FIPS 180-3):

- SHA-1:
  - **Acceptable** for signature generation through 2010
  - **Allowed** for signature generation from 2011 through 2013 (**new**)
  - **Acceptable** 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 **allowed** through 2013 (**new**)
  - Keys  $\geq 112$  bits **acceptable**
- CMAC (SP 800-38B):
  - 2-key TDES **acceptable** through 2010
  - 2-key TDES **allowed** 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](mailto:CryptoTransitions@nist.gov) **ASAP**.
- FIPS are available at <http://csrc.nist.gov/publications/PubsFIPS.html>.
- Contacts:
  - Elaine Barker ([ebarker@nist.gov](mailto:ebarker@nist.gov))
  - Allen Roginsky ([Allen.Roginsky@nist.gov](mailto:Allen.Roginsky@nist.gov))



**Additional  
Discussion?**