

Transitions

Elaine Barker
National Institute of Standards and
Technology
June 8, 2009

Background Story

- DES was pretty good ... for a while
- DES (and others) now deemed insecure
 - Attacks developed by smart people
 - Computers became more powerful
- Failure to plan for changes
 - Incomplete education
 - Lack of alternative solutions
 - Installed base difficult to replace
 - Key management lacking

Addressing the Problem

- Educate the public
 - SP 800-57
 - General key management guidance
 - Security strength - Algorithm and key size strengths
 - Recommended transition time frames
- Provide alternative solutions
 - Triple DES, AES, DSA, RSA, ECDSA, DH, MQV, SHA-X, etc.
- Coordinate, publicize, encourage, discourage.....
- CMVP to “encourage/enforce” good practices by defining FIPS mode

Purpose of this Talk

- Bring transition issues to public's attention
- Obtain feedback
- Discussion paper

Security Strengths and Time Frames

(From SP 800-57, Part 1)

➤ Security strength

- Measure of the difficulty of defeating the cryptographic protection on data (e.g., encryption, digital signatures, etc.)
- Given in bits
- Security strengths of 80, 112, 128, 192 and 256 bits
- ≥ 80 bits until December 31, 2010
- ≥ 112 bits beginning in 2011

Algorithms, Key Sizes, and Security Strengths

(From SP 800-57, Part 1)

➤ ≤ 80 bits:

- Encryption: 2-key Triple DES and SKIPJACK
- Digital signatures: 1024-bit DSA and RSA, ECDSA ($f=160-223$)
- Key agreement: 1024-bit FF DH and MQV, EC DH & MQV ($f=160-223$), 1024-bit RSA
- Key transport: 1024-bit RSA
- Hash functions: SHA-1 for digital signatures and hash-only applications

Comparable Security Strengths

(Additional slide inserted from SP 800-57, Part 1 by request)

Bits of security	Symmetric key algorithms	FFC (e.g., DSA, D-H) ²	IFC (e.g., RSA) ³	ECC (e.g., ECDSA) ⁴
80	2-key TDEA ¹	$L = 1024$ $N = 160$	$k = 1024$	$f = 160-223$
112	3-key TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224-255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256-383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384-511$
256	AES-256	$L = 15360$ $N = 512$	$k = 15360$	$f = 512+$

¹ The assessment of at least 80-bits of security for 2TDEA is based on the assumption that an attacker has at most 2^{40} matched plaintext and ciphertext blocks.

² L = length of public key, N = length of private key.

³ k = length of the modulus ; commonly considered to be the key size.

⁴ f = the length of n (i.e., the order of the base point), commonly considered to be the key size.

Encryption Transitions

Encryption Algorithm	New Validations	Already Validated Implementations
Two-key Triple DES (SP 800-67)	Through 2010	Disallow after 2010
Three key Triple DES (SP 800-67)	OK	OK
SKIPJACK (FIPS 185)	Through 2010	Disallow after 2010
AES-128 (FIPS 197)	OK	OK
AES-192 (FIPS 197)	OK	OK
AES-256 (FIPS 197)	OK	OK

Digital Signature Transitions (FIPS 186-3)

Purpose	New Validations*	Already Validated Implementations*
Non-repudiation	≥ 80 bits through 2010	Disallow < 112 bits after 2010 ≥ 112 bits OK
Authentication (e.g., cards)	≥ 80 bits through 2013	Disallow < 112 bits after 2013 ≥ 112 bits OK
Integrity (e.g., software/firmware integrity)	≥ 80 bits through 2010	Validated implementations continue to be OK

* Given in bits of security (i.e., security strength)

RNG Transitions

Description	New Validations	Already Validated Implementations
SP 800 90 (HASH, HMAC, CTR, DUAL_EC)	OK	OK
SHA 1 (FIPS 186-2)*	OK through 2010	Disallow after 2015
Sym. Alg. (FIPS 186-2)*	OK through 2010	Disallow after 2015
ANS X9.31 ANS X9.17*	OK through 2010	Disallow after 2015

* Design or guidance does not support 112-bit security strength

Key Agreement (DH and MQV) Transitions

Scheme	New Validations	Already Validated Implementations
SP 800-56A primitives	OK ¹	OK
Non-tested DH and MQV primitives	OK through 2010	Test by 2014
KDFs:		
SP 800-56A	OK ²	OK
IKEv2, IKEv1, X9.42, X9.63, SSH, SRTP, TLS (1.0, 1.1, 1.2)	OK	OK

1 Currently, tested only when the KDF complies with SP 800-56A. Planned to test all DH and MQV implementations in the future.

2 Now tested.

Hash Function Transitions (FIPS 180-3)

Hash Function	New Validations	Already Validated Implementations
SHA-1	OK for all hash function applications through December 31, 2010	Digital signatures: see Table 2 Hash-only: Disallow after 2010 OK for all other applications
SHA-224		OK for all hash function applications
SHA-256		
SHA-384		
SHA-512		

Others

- Key Agreement and Key Transport Using RSA (SP 800-56B)
 - Currently in draft; will be completed soon
 - Should be similar to DH and MQV Key Agreement
- Deriving additional keys from a single key (SP 800-108)
 - Tests and Implementation guidance to be developed

Others (contd.)

- Key wrapping
 - No “official” pub yet developed
 - AES key wrapping spec. at http://csrc.nist.gov/groups/ST/toolkit/documents/kms/AES_key_wrap.pdf
 - FIPS 140-2 Implementation Guidance allows key wrapping using AES and Triple DES
 - 2-key Triple DES will be disallowed after December 31, 2010

Discussion paper will be available at:

http://csrc.nist.gov/groups/ST/key_mgmt/
and
[http://csrc.nist.gov/groups/STM/cmvp/
announcements.html](http://csrc.nist.gov/groups/STM/cmvp/announcements.html)

Please send comments to:

ebarker@nist.gov
with "Transition comment" in the subject line