e-Government recommended ciphers list

February 20, 2003

The Ministry of Internal Affairs and Communication

The Ministry of Economy, Trade and Industry

Category of technique		Name
Public-key cryptographic techniques	Signature	DSA
		ECDSA
		RSASSA-PKCS1-v1_5
		RSA-PSS
	Confidentiality	RSA-OAEP
		RSAES-PKCS1-v1_5(Note 1)
	Key agreement	DH
		ECDH
		PSEC-KEM(Note 2)
Symmetric-key cryptographic techniques	64-bit block ciphers(Note 3)	CIPHERUNICORN-E
		Hierocrypt-L1
		MISTY1
		3-key Triple DES(Note 4)
	128-bit block ciphers	AES
		Camellia
		CIPHERUNICORN-A
		Hierocrypt-3
		SC2000
	Stream ciphers	MUGI
		MULTI-S01
		128-bit RC4(Note 5)
Other techniques	Hash functions	RIPEMD-160(Note 6)
		SHA-1(Note 6)
		SHA-256
		SHA-384
		SHA-512
	Pseudo-random number generators(Note 7)	PRNG based on SHA-1 in ANSI X9.42-2001 Annex C.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) Appendix 3.1
		PRNG based on SHA-1 for general purpose in FIPS 186-2 (+ change notice 1) revised Appendix 3.1

Notes:

(Note 1) This is permitted to be used for the time being because it was used in SSL3.0/TLS1.0.

(Note 2) This is permitted to be used only in the KEM (Key Encapsulation Mechanism) -DEM(Data Encapsulation Mechanism) construction.

(Note 3) When constructing a new system for e-Government, 128-bit block ciphers are preferable if possible.

(Note 4) The 3-key Triple DES is permitted to be used for the time being under the following conditions:

1) It is specified as FIPS 46-3
2) It is positioned as the de facto standard

(Note 5) It is assumed that 128-bit RC4 will be used only in SSL3.0/TLS (1.0 or later). If any other cipher listed above is available, it should be used instead.

(Note 6) If a longer hash value is available when constructing a new system for e-Government, it is preferable to select a 256-bit (or more) hash function. However, this does not apply to the case where the hash function is designated to be used in the public-key cryptographic specifications.

(Note 7) Since pseudo-random number generators do not require interoperability due to their usage characteristics, no problems will occur from the use of a cryptographically secure pseudo-random number generating algorithm. These algorithms are listed as examples.

Annex

Information table for the e-Government Recommended Ciphers List

Date	Location	Before	After	Reason
October 12, 2005	Notes: 1) in (Note4)	It is specified as FIPS 46-3	It is specified as SP 800-67	Change of a pointer to the spec document.