Cryptographic Key Management Workshop

March 4-5, 2014

Session 7: Interoperability and Transitioning

Elaine Barker,

Interoperability

- Definition: The ability of systems to communicate and work together.
- Interoperability is not required.
- At least one algorithm of each required type and a key length must be available as a default.
- Using other algorithms than the defaults and key lengths is OK if agreed upon.
- For an FCKMS, the defaults must be approved (PR: 2.1).

Interoperability Requirements

Purpose/alg. type	Low impact	Moderate impact	High impact	PR:
Block-cipher encryption	AES-128/CBC mode		AES-256/CBC mode	7.1
Block-cipher msg. authentication	AES-128/CMAC		AES-256/CMAC	7.2
Block-cipher auth. encryption	AES-128/GCM		AES-256/GCM	7.3
Key wrapping	AES-128/GCM		AES-256/GCM	7.4
Hash function	SHA-256		SHA-384	7.5
HMAC	HMAC-SHA-1	HMAC-SHA-256	HMAC-SHA-384	7.6
FF key agreement (interactive)	dhEphem/concatenation KDF			7.7
	SHA-256		SHA-384	

Interoperability Requirements

Purpose/alg. type	Low impact	Moderate impact	High impact	PR:
EC key agreement (interactive)	Ephemeral Unified Model/concatenation KDF			7.8
	SHA-256/P-256		SHA-384/P-384	
RSA key agreement/2 key pairs (interactive)	KAS2/concatenation KDF			7.9
	SHA-256		SHA-384	
FF key agreement (one-way)	dhOneFlow/concatenation KDF			7.10
	SHA-256		SHA-384	
EC key agreement (one-way)	One-Pass DH/concatenation KDF			7.11
	SHA-256/P-256		SHA-384/P-384	
RSA key agreement (one-way)	KAS1/concatenation KDF			7.12
	SHA-256		SHA-384	

Interoperability Requirements

Purpose/alg. type	Low impact	Moderate impact	High impact	PR:
RSA key transport	RSA-OAEP			7.13
Key derivation from a pre-shared secret	HMAC/counter mode			7.14
	SHA-256		SHA-384	
ECDSA digital signatures	SHA-256/P-256		SHA-384/P-384	7.15
RSA digital signatures	RSASSA-PSS			7.16

Interoperability Recommendations

Purpose/alg. type	Low impact	Moderate impact	High impact	PA:
Block-cipher encryption	AES-256/CBC			7.1
Block-cipher msg. authentication	AES-256/CMAC			7.2
Block-cipher auth. encryption	AES-256/GCM			7.3
Key wrapping	AES-256/GCM			7.4
Hash function	SHA-384			7.5
HMAC	HMAC-SHA-256 and HMAC-SHA-384			7.6
Key agreement	SHA-384			7.7
EC key agreement	P-384			7.8

Interoperability Recommendations

Purpose/alg. type	Low impact	Moderate impact	High impact	PA:
RSA key transport	RSA-KEM-KWS/KWP key wrapping			7.9
ECDSA digital signatures	P-384			7.10

Transitioning

- An FCKMS **shall:**
  - Use only cryptographic algorithms that cover the anticipated lifetime of the FCKMS, or have a transition strategy for migration (PR: 7.17), and
  - Have transition plans that select the algorithm(s) and key length(s) to be used during a transition period (PR: 7.18).
- An FCKMS **should:**
  - Support the update or replacement of cryptographic algorithms without disrupting operations (PA: 7.11).

Questions and Comments?