CMP Algorithms

draft-ietf-lamps-cmp-algorithms-07
Hendrik Brockhaus, Hans Aschauer, Mike Ounsworth, John Gray

Hendrik Brockhaus

IETF 112 – LAMPS Working Group

Activities since IETF 111 on CMP Algorithms

Changes since IETF 111:

- Provided final version ready for WGLC, fixing minor formatting nits
- WGLC was concluded in October
- Russ acts as document shepherd and submitted the draft to IESG for publication
- AD evaluation was performed by Roman

→Next step: update I-D, addressing AD feedback

→Specifically discussing introduction of Section 7

Structure of Section 7

Introduction:

- Provides general guidance for choosing sets of algorithms

Section 7.1:

- Updates RFC 4210 Appendix D.2 → CMP Updates, Section 2.28
- Uses algorithm identifier used in RFC 4210 Appendix D and E
- For backward compatibility, EncryptedValue is still used for transferring centrally generated keys → CMP Updates, Section 2.29
- Offers one mandatory set of algorithm, deprecates outdated algorithms

Section 7.2:

- Uses algorithm identifier used in Lightweight CMP Profile
- EnvelopedData is used for transferring centrally generated keys
- Does not specify any mandatory sets of algorithm

Deprecated algorithms from RFC 4210 D.2

It is planned to deprecate using the following algorithms specified in RFC 4210 Appendix D.2:

- MD5 and SHA-1
- DSA
- RC5, CAST-128, and 3-DES
- X9.9

DSA may still be good, but use is omitted to enhance interoperability in NIST SP 800-57 Part3 Rev. 1 Section 2.2.1.

3-DES is deprecated in NIST SP 800-131A.

PasswordBasedMac is not deprecated, but it is RECOMMENDED using PBMAC1.

Section 7 – updated introduction

The overall cryptographic strength of a CMP deployment will depend on several factors, including:

* Capabilities of the end entity: What kind of algorithms does the end entity support. The cryptographic strength of the system SHOULD be at least as strong as the algorithms and keys used for the certificate being managed.

* Algorithm profile: The overall strength of the profile will be the strength of the weakest algorithm it contains.

* Message protection: The overall strength of the CMC message protection

- MAC-based protection: The entropy of the shared secret information or password when MAC-based message protection is used (MSG_MAC_ALG).

- Signature-based protection: The strength of the key pair and signature algorithm when signature-based protection is used (MSG_SIG_ALG).

- Protection of centrally generated keys: The strength of the algorithms used for the key management technique (Section 7.1: PROT_ENC_ALG or Section 7.2: KM_KA_ALG, KM_KT_ALG, KM_KD_ALG) and the encryption of the content-encryption key and private key (Section 7.1: SYM_PENC_ALG, PROT_SYM_ALG or Section 7.2: KM_KW_ALG, PROT_SYM_ALG).

To avoid consuming too much computational resources it is recommended to choose a set of algorithms offering roughly the same level of security. Below are provided several algorithm profiles which are balanced, assuming the implementor chooses MAC secrets and / or certificate profiles of at least equivalent strength.

Algorithm use profiles – proposal sorted by algorithm usage

Bits of security	Recommended for managing keys up to	CMP protection	Key management technique	Key-wrap and symmetric encryption
		MSG_SIG_ALG, MSG_MAC_ALG	PROT_ENC_ALG or KM_KA_ALG, KM_KT_ALG, KM_KD_ALG	PROT_SYM_ALG, SYM_PENC_ALG or KM_KW_ALG
112	RSA2048 secp224r1	RSASSA-PSS (2048, SHA224 or SHAKE128) RSAEncryption (2048, SHA224) ECDSA (secp224r1, SHA224 or SHAKE128) PBMAC1 (HMAC, SHA224)	ESDH (2048) ECDH (secp224r1, SHA224) RSAEncryption (2048) PBKDF2 (HMAC, SHA224)	AES-128
128	RSA3072 secp2r1 Ed25519	RSASSA-PSS (3072, SHA256 or SHAKE128) RSAEncryption (3072, SHA256) ECDSA (secp256r1, SHA256 or SHAKE128) Ed25519 (SHA512) PBMAC1 (HMAC, SHA256)	ESDH (3072) ECDH (secp256r1, SHA256) X25519 RSAEncryption (3072) RSAES-OAEP (SHA256) PBKDF2 (HMAC, SHA256)	AES-128
192	secp384r1	ECDSA (secp384r1, SHA384) PBMAC1 (HMAC, SHA384)	ECDH (secp384r1, SHA384) PBKDF2 (HMAC, SHA384)	AES-192
224	Ed448	Ed448 (SHAKE256) PBMAC1 (HMAC, SHA512)	X448 PBKDF2 (HMAC, SHA512)	AES-256
256	secp521r1	ECDSA (secp521r1, SHA512) PBMAC1 (HMAC, SHA512)	ECDH (secp521r1, SHA512) PBKDF2 (HMAC, SHA512)	AES-256

Algorithm use profiles – alternative proposal sorted by algorithm

Bits of security	Recommended for managing keys up to	RSA	Elliptic curve	D-H	Hash function	Symmetric encryption
112	RSA2048 secp224r1	RSA2048	secp224r1	D-H (2048)	SHA224	AES-128
128	RSA3072 secp2r1 Ed25519	RSA3072	secp256r1 Ed25519/X25519	D-H (3072)	SHA256 SHAKE128	AES-128
192	secp384r1	-	secp384r1		SHA384	AES-192
224	Ed448	-	Ed448/X448	-	SHAKE256	AES-256
256	secp521r1	-	secp521r1	-	SHA512	AES-256