IPsecME RFC4307bis

IETF 95
Buenos Aires, Argentina
2016-04-04

Tero Kivinen <kivinen@iki.fi>
Yoav Nir <ynir.ietf@gmail.com>
Paul Wouters <pwouters@redhat.com>
Daniel Migault <daniel.migault@ericsson.com>

What

- Updating the RFC4307
  - IKEv2 algorithms only, ESP and AH are in the separate document
  - Deprecate old algorithms
  - Mandate new algorithms
  - Add rationale for algorithm selection
  - Add IoT algorithms

IKEv2 Encryption Algorithms

Name	Status	Comment
ENCR_AES_CBC	MUST-	128-bit keys
ENCR_CHACHA20_POLY1305	SHOULD	Might be SHOULD+ on next version
AES-GCM with a 16 octet ICV	SHOULD	128-bit keys
ENCR_AES_CCM_8	SHOULD	Algorithm for IoT
ENCR_3DES	MAY	Too short block length
ENCR_DES	MUST NOT	Too weak

IKEv2 Pseudo-random Function Algorithms

Name	Status	Comment
PRF_HMAC_SHA2_256	MUST	
PRF_HMAC_SHA2_512	SHOULD+	
PRF_HMAC_SHA1	MUST-	There is industry wide movement to deprecate SHA1
PRF_AES128_XCBC	SHOULD	Algorithm for IoT
PRF_HMAC_MD5	MUST NOT	MD5 is already considered broken, so HMAC version might get broken soon too

IKEv2 Integrity Algorithms

Name	Status	Comment
AUTH_HMAC_SHA2_256_128	MUST	
AUTH_HMAC_SHA2_512_256	SHOULD	
AUTH_HMAC_SHA1_96	MUST-	There is industry wide movement to deprecate SHA1
AUTH_AES_XCBC_96	SHOULD	Algorithm for IoT
AUTH_HMAC_MD5_96	MUST NOT	MD5 is already considered broken, so HMAC version might get broken soon too
AUTH_DES_MAC	MUST NOT	Too weak
AUTH_KPDK_MD5	MUST NOT	Too weak

IKEv2 Diffie-Hellman Groups

Name	Status	Comment
14 – 2048-bit MODP Group	MUST	
19 – 256-bit random ECP Group	SHOULD	
5 – 1536-bit MODP Group	SHOULD NOT	Bit too weak
2 – 1024-bit MODP Group	SHOULD NOT	Too weak, but was MUST before, so kept as SHOULD NOT to maintain backward compatibility
1 – 768-bit MODP Group	MUST NOT	Too weak
22 – 1024-bit MODP Group with 160-bit Prime Order Subgroup	SHOULD NOT	Has small subgroups, slower
23 – 2048-bit MODP Group with 224-bit Prime Order Subgroup	SHOULD NOT	Has small subgroups, slower
24 – 2048-bit MODP Group with 256-bit Prime Order Subgroup	SHOULD NOT	Has small subgroups, slower

IKEv2 Authentication Methods

Name	Status	Comment
1 – RSA Digital Signature	MUST	
3 – DSA Digital Signature	SHOULD NOT	Uses SHA1
9 – ECDSA with SHA-256 on the P-256 curve	SHOULD	No hash agility, better use Digital Signatures
10 – ECDSA with SHA-384 on the P-384 curve	SHOULD	No hash agility, better use Digital Signatures
11 – ECDSA with SHA-512 on the P-512 curve	SHOULD	No hash agility, better use Digital Signatures
14 – Digital Signature	SHOULD	Not enough implementations to make MUST

IKEv2 RSA Key Lengths

Name	Status	Comment
2048	MUST	
3072 and 4096	SHOULD	
Between 2048 - 3071 and Between 3073 - 4095	MAY	
< 2048	SHOULD NOT	

IKEv2 Digital Signature Hash Algorithms

Name	Status	Comment
SHA1	SHOULD NOT	
SHA2-256	MUST	
SHA2-384	MAY	
SHA2-512	SHOULD	

IKEv2 Digital Signature OIDs

Name	Status	Comment
RSASSA-PSS with SHA-256	SHOULD	
ecdsa-with-sha256	SHOULD	
sha1WithRSAEncryption	SHOULD NOT	Uses SHA1
dsa-with-sha1	SHOULD NOT	Uses SHA1
ecdsa-with-sha1	SHOULD NOT	Uses SHA1
RSASSA-PSS with Empty Parameters	SHOULD NOT	Uses SHA1
RSASSA-PSS with Default Parameters	SHOULD NOT	Uses SHA1
Others	MAY	