Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)

draft-mglt-ipsecme-rfc7321bis-00

Migault, Mattsson, Nir, Wouters, Kivinen

19/07/2016- IETF96- Berlin

Motivations

- RFC7321 provides cryptographic implementation and usage guidance
- RFC7321bis only updates the implementation guidance part
- Most cryptographic algorithm had no implementation guidances
  - This is why we include them all algorithm allocated by IANA

Legend:

- $[1]$ - This requirement level is for 128-bit keys. 256-bit keys are at SHOULD. 192-bit keys can safely be ignored.
- $[IoT]$ - This requirement is for interoperability with IoT.

ESP Encryption

Name	Status	AEAD	Comment
ENCR_DES_IV64	MUST NOT	No	UNSPECIFIED
ENCR_DES	MUST NOT	No	$[RFC2405]$
ENCR_3DES	SHOULD NOT	No	$[RFC2451]$
ENCR_RC5	MUST NOT	No	$[RFC2451]$
ENCR_IDEA	MUST NOT	No	$[RFC2451]$
ENCR_CAST	MUST NOT	No	$[RFC2451]$
ENCR_BLOWFISH	MUST NOT	No	$[RFC2451]$
ENCR_3IDEA	MUST NOT	No	UNSPECIFIED
ENCR_DES_IV32	MUST NOT	No	UNSPECIFIED

ESP Encryption

Name	Status	AEAD	Comment
ENCR_NULL	MUST	No	$[RFC2410]$
ENCR_AES_CBC	MUST -	No	$[RFC3602]$ [1]
ENCR_AES_CTR	MAY	No	$[RFC3686]$
ENCR_AES_CCM_8	SHOULD	Yes	$[RFC4309]$ [1] $[IoT]$
ENCR_AES_CCM_12	MAY	Yes	$[RFC4309]$
ENCR_AES_CCM_16	SHOULD	Yes	$[RFC4309]$ [1]
AES-GCM with a 8 octet ICV	MAY	Yes	$[RFC4106]$
AES-GCM with a 12 octet ICV	MAY	Yes	$[RFC4106]$
AES-GCM with a 16 octet ICV	MUST	Yes	$[RFC4106]$ [1]
ENCR_NULL_AUTH_AES_GMAC	MAY	No	$[RFC4543]$
Reserved for IEEE P1619 XTS-AES	MAY	No	$[Matt\_Ball]$

ESP Encryption

Name	Status	AEAD	Comment
ENCR_CAMELLIA_CBC	MAY	No	$[RFC5529]$
ENCR_CAMELLIA_CTR	MAY	No	$[RFC5529]$
ENCR_CAMELLIA_CCM with an 8-octet ICV	MAY	No	$[RFC5529]$
ENCR_CAMELLIA_CCM with a 12-octet ICV	MAY	No	$[RFC5529]$
ENCR_CAMELLIA_CCM with a 16-octet ICV	MAY	No	$[RFC5529]$
ENCR_CHACHA20_POLY1305	MAY+	Yes	$[RFC7634]$

ESP-AH Authentication

Name	Status	Comment
NONE	MUST	$[RFC7296]$ AEAD
AUTH_HMAC_MD5_96	MUST NOT	$[RFC2403]$ $[RFC7296]$
AUTH_HMAC_SHA1_96	MUST-	$[RFC2404]$ $[RFC7296]$
AUTH_DES_MAC	MUST NOT	$[UNSPECIFIED]$
AUTH_KPDK_MD5	MUST NOT	$[UNSPECIFIED]$
AUTH_AES_XCBC_96	SHOULD	$[RFC3566]$ $[RFC7296]$ $[IoT]$
AUTH_HMAC_MD5_128	MUST NOT	$[RFC4595]$
AUTH_HMAC_SHA1_160	MAY	$[RFC4595]$

ESP-AH Authentication

Name	Status	Comment
AUTH_AES_CMAC_96	MAY	$[RFC4494]$
AUTH_AES_128_GMAC	MAY	$[RFC4543]$
AUTH_AES_192_GMAC	MAY	$[RFC4543]$
AUTH_AES_256_GMAC	MAY	$[RFC4543]$
AUTH_HMAC_SHA2_256_128	MUST	$[RFC4868]$
AUTH_HMAC_SHA2_384_192	MAY	$[RFC4868]$
AUTH_HMAC_SHA2_512_256	SHOULD	$[RFC4868]$

ESP-AH Compression

Name	Status	Comment
IPCOMP_OUI	MUST NOT	$[UNSPECIFIED]$
IPCOMP_DEFLATE	MAY	$[RFC2393]$
IPCOMP_LZS	MAY	$[RFC2395]$
IPCOMP_LZJH	MAY	$[RFC3051]$

Thank you for your attention