

Internet Key Exchange Version 2 (IKEv2) Parameters

Created

2005-01-18

Last Updated

2018-08-21

Available Formats



XML



HTML



Plain text

Registries included below

- [IKEv2 Exchange Types](#)
- [IKEv2 Payload Types](#)
- [Transform Type Values](#)
 - [IKEv2 Transform Attribute Types](#)
 - [Transform Type 1 - Encryption Algorithm Transform IDs](#)
 - [Transform Type 2 - Pseudorandom Function Transform IDs](#)
 - [Transform Type 3 - Integrity Algorithm Transform IDs](#)
 - [Transform Type 4 - Diffie-Hellman Group Transform IDs](#)
 - [Transform Type 5 - Extended Sequence Numbers Transform IDs](#)
- [IKEv2 Identification Payload ID Types](#)
- [IKEv2 Certificate Encodings](#)
- [IKEv2 Authentication Method](#)
- [IKEv2 Notify Message Types - Error Types](#)
- [IKEv2 Notify Message Types - Status Types](#)
- [IKEv2 Notification IPCOMP Transform IDs \(Value 16387\)](#)
- [IKEv2 Security Protocol Identifiers](#)
- [IKEv2 Traffic Selector Types](#)
- [IKEv2 Configuration Payload CFG Types](#)
- [IKEv2 Configuration Payload Attribute Types](#)
- [IKEv2 Gateway Identity Types](#)
- [ROHC Attribute Types](#)
- [IKEv2 Secure Password Methods](#)
- [IKEv2 Hash Algorithms](#)

IKEv2 Exchange Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Value | Exchange Type | Reference |
|---------|--------------------|---------------------------------------|
| 0-33 | Reserved | [RFC7296] |
| 34 | IKE_SA_INIT | [RFC7296] |
| 35 | IKE_AUTH | [RFC7296] |
| 36 | CREATE_CHILD_SA | [RFC7296] |
| 37 | INFORMATIONAL | [RFC7296] |
| 38 | IKE_SESSION_RESUME | [RFC5723] |
| 39 | GSA_AUTH | [draft-yeung-g-ikev2] |
| 40 | GSA_REGISTRATION | [draft-yeung-g-ikev2] |
| 41 | GSA_REKEY | [draft-yeung-g-ikev2] |
| 42-239 | Unassigned | |
| 240-255 | Private use | [RFC7296] |

IKEv2 Payload Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference[\[RFC7296\]](#)**Available Formats**

CSV

| Value | Next Payload Type | Notation | Reference |
|---------|--------------------------------------|----------|---------------------------------------|
| 0 | No Next Payload | | [RFC7296] |
| 1-32 | Reserved | | [RFC7296] |
| 33 | Security Association | SA | [RFC7296] |
| 34 | Key Exchange | KE | [RFC7296] |
| 35 | Identification - Initiator | IDi | [RFC7296] |
| 36 | Identification - Responder | IDr | [RFC7296] |
| 37 | Certificate | CERT | [RFC7296] |
| 38 | Certificate Request | CERTREQ | [RFC7296] |
| 39 | Authentication | AUTH | [RFC7296] |
| 40 | Nonce | Ni, Nr | [RFC7296] |
| 41 | Notify | N | [RFC7296] |
| 42 | Delete | D | [RFC7296] |
| 43 | Vendor ID | V | [RFC7296] |
| 44 | Traffic Selector - Initiator | TSi | [RFC7296] |
| 45 | Traffic Selector - Responder | TSr | [RFC7296] |
| 46 | Encrypted and Authenticated | SK | [RFC7296] |
| 47 | Configuration | CP | [RFC7296] |
| 48 | Extensible Authentication | EAP | [RFC7296] |
| 49 | Generic Secure Password Method | GSPM | [RFC6467] |
| 50 | Group Identification | IDg | [draft-yeung-g-ikev2] |
| 51 | Group Security Association | GSA | [draft-yeung-g-ikev2] |
| 52 | Key Download | KD | [draft-yeung-g-ikev2] |
| 53 | Encrypted and Authenticated Fragment | SKF | [RFC7383] |
| 54 | Puzzle Solution | PS | [RFC8019] |
| 55-127 | Unassigned | | |
| 128-255 | Private use | | [RFC7296] |

Transform Type Values

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference[\[RFC7296\]](#)**Available Formats**

CSV

| Type | Description | Used In | Reference |
|---------|---------------------------------|-----------------------------|---------------------------|
| 0 | Reserved | | [RFC7296] |
| 1 | Encryption Algorithm (ENCR) | (IKE and ESP) | [RFC7296] |
| 2 | Pseudo-random Function (PRF) | (IKE) | [RFC7296] |
| 3 | Integrity Algorithm (INTEG) | (IKE, AH, optional in ESP) | [RFC7296] |
| 4 | Diffie-Hellman Group (D-H) | (IKE, optional in AH & ESP) | [RFC7296] |
| 5 | Extended Sequence Numbers (ESN) | (AH and ESP) | [RFC7296] |
| 6-240 | Unassigned | | |
| 241-255 | Private use | | [RFC7296] |

IKEv2 Transform Attribute Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference[\[RFC7296\]](#)**Available Formats**

CSV

| Value | Attribute Type | Format | Reference |
|-------------|----------------------|--------|---------------------------|
| 0-13 | Reserved | | [RFC7296] |
| 14 | Key Length (in bits) | TV | [RFC7296] |
| 15-17 | Reserved | | [RFC7296] |
| 18-16383 | Unassigned | | |
| 16384-32767 | Private use | | [RFC7296] |

Transform Type 1 - Encryption Algorithm Transform IDs**Registration Procedure(s)**

Expert Review

Expert(s)

Tero Kivinen

Reference[\[RFC7296\]](#)**Available Formats**

CSV

| Number | Name | ESP Reference | IKEv2 Reference |
|------------|---------------------------------|---|---|
| 0 | Reserved | [RFC7296] | - |
| 1 | ENCR_DES_IV64 | UNSPECIFIED | - |
| 2 | ENCR_DES | [RFC2405] | [RFC7296] |
| 3 | ENCR_3DES | [RFC2451] | [RFC7296] |
| 4 | ENCR_RC5 | [RFC2451] | [RFC7296] |
| 5 | ENCR_IDEA | [RFC2451] | [RFC7296] |
| 6 | ENCR_CAST | [RFC2451] | [RFC7296] |
| 7 | ENCR_BLOWFISH | [RFC2451] | [RFC7296] |
| 8 | ENCR_3IDEA | UNSPECIFIED | [RFC7296] |
| 9 | ENCR_DES_IV32 | UNSPECIFIED | - |
| 10 | Reserved | [RFC7296] | - |
| 11 | ENCR_NULL | [RFC2410] | Not allowed |
| 12 | ENCR_AES_CBC | [RFC3602] | [RFC7296] |
| 13 | ENCR_AES_CTR | [RFC3686] | [RFC5930] |
| 14 | ENCR_AES_CCM_8 | [RFC4309] | [RFC5282] |
| 15 | ENCR_AES_CCM_12 | [RFC4309] | [RFC5282] |
| 16 | ENCR_AES_CCM_16 | [RFC4309] | [RFC5282] |
| 17 | Unassigned | | |
| 18 | ENCR_AES_GCM_8 | [RFC4106] [RFC8247] | [RFC5282] [RFC8247] |
| 19 | ENCR_AES_GCM_12 | [RFC4106] [RFC8247] | [RFC5282] [RFC8247] |
| 20 | ENCR_AES_GCM_16 | [RFC4106] [RFC8247] | [RFC5282] [RFC8247] |
| 21 | ENCR_NULL_AUTH_AES_GMAC | [RFC4543] | Not allowed |
| 22 | Reserved for IEEE P1619 XTS-AES | [Matt Ball] | - |
| 23 | ENCR_CAMELLIA_CBC | [RFC5529] | [RFC7296] |
| 24 | ENCR_CAMELLIA_CTR | [RFC5529] | - |
| 25 | ENCR_CAMELLIA_CCM_8 | [RFC5529] [RFC8247] | - |
| 26 | ENCR_CAMELLIA_CCM_12 | [RFC5529] [RFC8247] | - |
| 27 | ENCR_CAMELLIA_CCM_16 | [RFC5529] [RFC8247] | - |
| 28 | ENCR_CHACHA20_POLY1305 | [RFC7634] | [RFC7634] |
| 29 | ENCR_AES_CCM_8_IIV | [draft-ietf-ipsecme-implicit-iv] | Not allowed |
| 30 | ENCR_AES_GCM_16_IIV | [draft-ietf-ipsecme-implicit-iv] | Not allowed |
| 31 | ENCR_CHACHA20_POLY1305_IIV | [draft-ietf-ipsecme-implicit-iv] | Not allowed |
| 32-1023 | Unassigned | | |
| 1024-65535 | Private use | [RFC7296] | [RFC7296] |

Transform Type 2 - Pseudorandom Function Transform IDs**Registration Procedure(s)**

Expert Review

Expert(s)

Tero Kivinen

Reference[\[RFC7296\]](#)**Available Formats**

CSV

| Number | Name | Reference |
|------------|-------------------|---------------------------|
| 0 | Reserved | [RFC7296] |
| 1 | PRF_HMAC_MD5 | [RFC2104] |
| 2 | PRF_HMAC_SHA1 | [RFC2104] |
| 3 | PRF_HMAC_TIGER | [UNSPECIFIED] |
| 4 | PRF_AES128_XCBC | [RFC4434] |
| 5 | PRF_HMAC_SHA2_256 | [RFC4868] |
| 6 | PRF_HMAC_SHA2_384 | [RFC4868] |
| 7 | PRF_HMAC_SHA2_512 | [RFC4868] |
| 8 | PRF_AES128_CMAC | [RFC4615] |
| 9-1023 | Unassigned | |
| 1024-65535 | Private use | [RFC7296] |

Transform Type 3 - Integrity Algorithm Transform IDs**Registration Procedure(s)**

Expert Review

Expert(s)

Tero Kivinen

Reference[\[RFC7296\]](#)**Available Formats**

CSV

| Number | Name | Reference |
|------------|------------------------|---|
| 0 | NONE | [RFC7296] |
| 1 | AUTH_HMAC_MD5_96 | [RFC2403] [RFC7296] |
| 2 | AUTH_HMAC_SHA1_96 | [RFC2404] [RFC7296] |
| 3 | AUTH_DES_MAC | [UNSPECIFIED] |
| 4 | AUTH_KPDK_MD5 | [UNSPECIFIED] |
| 5 | AUTH_AES_XCBC_96 | [RFC3566] [RFC7296] |
| 6 | AUTH_HMAC_MD5_128 | [RFC4595] |
| 7 | AUTH_HMAC_SHA1_160 | [RFC4595] |
| 8 | AUTH_AES_CMAC_96 | [RFC4494] |
| 9 | AUTH_AES_128_GMAC | [RFC4543] |
| 10 | AUTH_AES_192_GMAC | [RFC4543] |
| 11 | AUTH_AES_256_GMAC | [RFC4543] |
| 12 | AUTH_HMAC_SHA2_256_128 | [RFC4868] |
| 13 | AUTH_HMAC_SHA2_384_192 | [RFC4868] |
| 14 | AUTH_HMAC_SHA2_512_256 | [RFC4868] |
| 15-1023 | Unassigned | |
| 1024-65535 | Private use | [RFC7296] |

Transform Type 4 - Diffie-Hellman Group Transform IDs**Registration Procedure(s)**

Expert Review

Expert(s)

Tero Kivinen

Reference[\[RFC7296\]](#)[\[RFC6989\]](#)**Available Formats**

CSV

| Number | Name | Recipient Tests | Reference |
|--------|------|-----------------|---------------------------|
| 0 | NONE | | [RFC7296] |

| Number | Name | Recipient Tests | Reference |
|------------|---|---------------------|-----------|
| 1 | 768-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC7296] |
| 2 | 1024-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC7296] |
| 3-4 | Reserved | | [RFC7296] |
| 5 | 1536-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC3526] |
| 6-13 | Unassigned | | [RFC7296] |
| 14 | 2048-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC3526] |
| 15 | 3072-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC3526] |
| 16 | 4096-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC3526] |
| 17 | 6144-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC3526] |
| 18 | 8192-bit MODP Group | [RFC6989], Sec. 2.1 | [RFC3526] |
| 19 | 256-bit random ECP group | [RFC6989], Sec. 2.3 | [RFC5903] |
| 20 | 384-bit random ECP group | [RFC6989], Sec. 2.3 | [RFC5903] |
| 21 | 521-bit random ECP group | [RFC6989], Sec. 2.3 | [RFC5903] |
| 22 | 1024-bit MODP Group with 160-bit Prime Order Subgroup | [RFC6989], Sec. 2.2 | [RFC5114] |
| 23 | 2048-bit MODP Group with 224-bit Prime Order Subgroup | [RFC6989], Sec. 2.2 | [RFC5114] |
| 24 | 2048-bit MODP Group with 256-bit Prime Order Subgroup | [RFC6989], Sec. 2.2 | [RFC5114] |
| 25 | 192-bit Random ECP Group | [RFC6989], Sec. 2.3 | [RFC5114] |
| 26 | 224-bit Random ECP Group | [RFC6989], Sec. 2.3 | [RFC5114] |
| 27 | brainpoolP224r1 | [RFC6989], Sec. 2.3 | [RFC6954] |
| 28 | brainpoolP256r1 | [RFC6989], Sec. 2.3 | [RFC6954] |
| 29 | brainpoolP384r1 | [RFC6989], Sec. 2.3 | [RFC6954] |
| 30 | brainpoolP512r1 | [RFC6989], Sec. 2.3 | [RFC6954] |
| 31 | Curve25519 | [RFC8031], Sec. 3.2 | [RFC8031] |
| 32 | Curve448 | [RFC8031], Sec. 3.2 | [RFC8031] |
| 33-1023 | Unassigned | | |
| 1024-65535 | Reserved for Private Use | | [RFC7296] |

Transform Type 5 - Extended Sequence Numbers Transform IDs

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[RFC7296]

Available Formats



CSV

| Number | Name | Reference |
|---------|------------------------------|-----------|
| 0 | No Extended Sequence Numbers | [RFC7296] |
| 1 | Extended Sequence Numbers | [RFC7296] |
| 2-65535 | Reserved | [RFC7296] |

IKEv2 Identification Payload ID Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[RFC7296]

Available Formats



CSV

| Value | ID Type | Reference |
|-------|----------------|-----------|
| 0 | Reserved | [RFC7296] |
| 1 | ID_IPV4_ADDR | [RFC7296] |
| 2 | ID_FQDN | [RFC7296] |
| 3 | ID_RFC822_ADDR | [RFC7296] |
| 4 | Unassigned | [RFC7296] |
| 5 | ID_IPV6_ADDR | [RFC7296] |

| Value | ID Type | Reference |
|---------|----------------|---------------------------|
| 6-8 | Unassigned | [RFC7296] |
| 9 | ID_DER_ASN1_DN | [RFC7296] |
| 10 | ID_DER_ASN1_GN | [RFC7296] |
| 11 | ID_KEY_ID | [RFC7296] |
| 12 | ID_FC_NAME | [RFC4595] |
| 13 | ID_NULL | [RFC7619] |
| 14-200 | Unassigned | |
| 201-255 | Private use | [RFC7296] |

IKEv2 Certificate Encodings

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Value | Certificate Encoding | Reference |
|---------|-----------------------------------|---------------------------|
| 0 | Reserved | [RFC7296] |
| 1 | PKCS #7 wrapped X.509 certificate | [UNSPECIFIED] |
| 2 | PGP Certificate | [UNSPECIFIED] |
| 3 | DNS Signed Key | [UNSPECIFIED] |
| 4 | X.509 Certificate - Signature | [RFC7296] |
| 5 | Reserved | [RFC7296] |
| 6 | Kerberos Token | [UNSPECIFIED] |
| 7 | Certificate Revocation List (CRL) | [RFC7296] |
| 8 | Authority Revocation List (ARL) | [UNSPECIFIED] |
| 9 | SPKI Certificate | [UNSPECIFIED] |
| 10 | X.509 Certificate - Attribute | [UNSPECIFIED] |
| 11 | Raw RSA Key (DEPRECATED) | [RFC7296] |
| 12 | Hash and URL of X.509 certificate | [RFC7296] |
| 13 | Hash and URL of X.509 bundle | [RFC7296] |
| 14 | OCSP Content | [RFC4806] |
| 15 | Raw Public Key | [RFC7670] |
| 16-200 | Unassigned | |
| 201-255 | Private use | [RFC7296] |

IKEv2 Authentication Method

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Value | Authentication Method | Reference |
|-------|---------------------------------------|---------------------------|
| 0 | Reserved | [RFC7296] |
| 1 | RSA Digital Signature | [RFC7296] |
| 2 | Shared Key Message Integrity Code | [RFC7296] |
| 3 | DSS Digital Signature | [RFC7296] |
| 4-8 | Unassigned | [RFC7296] |
| 9 | ECDSA with SHA-256 on the P-256 curve | [RFC4754] |
| 10 | ECDSA with SHA-384 on the P-384 curve | [RFC4754] |
| 11 | ECDSA with SHA-512 on the P-521 curve | [RFC4754] |

| Value | Authentication Method | Reference |
|---------|---|---------------------------|
| 12 | Generic Secure Password Authentication Method | [RFC6467] |
| 13 | NULL Authentication | [RFC7619] |
| 14 | Digital Signature | [RFC7427] |
| 15-200 | Unassigned | |
| 201-255 | Private use | [RFC7296] |

IKEv2 Notify Message Types - Error Types

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Range | Registration Procedures |
|------------|-------------------------|
| 0-8191 | Expert Review |
| 8192-16383 | Private use |

| Value | NOTIFY MESSAGES - ERROR TYPES | Reference |
|------------|-------------------------------|---------------------------------------|
| 0 | Reserved | [RFC7296] |
| 1 | UNSUPPORTED_CRITICAL_PAYLOAD | [RFC7296] |
| 2-3 | Reserved | [RFC7296] |
| 4 | INVALID_IKE_SPI | [RFC7296] |
| 5 | INVALID_MAJOR_VERSION | [RFC7296] |
| 6 | Reserved | [RFC7296] |
| 7 | INVALID_SYNTAX | [RFC7296] |
| 8 | Reserved | [RFC7296] |
| 9 | INVALID_MESSAGE_ID | [RFC7296] |
| 10 | Reserved | [RFC7296] |
| 11 | INVALID_SPI | [RFC7296] |
| 12-13 | Reserved | [RFC7296] |
| 14 | NO_PROPOSAL_CHOSEN | [RFC7296] |
| 15-16 | Reserved | [RFC7296] |
| 17 | INVALID_KE_PAYLOAD | [RFC7296] |
| 18-23 | Reserved | [RFC7296] |
| 24 | AUTHENTICATION_FAILED | [RFC7296] |
| 25-33 | RESERVED | [RFC7296] |
| 34 | SINGLE_PAIR_REQUIRED | [RFC7296] |
| 35 | NO_ADDITIONAL_SAS | [RFC7296] |
| 36 | INTERNAL_ADDRESS_FAILURE | [RFC7296] |
| 37 | FAILED_CP_REQUIRED | [RFC7296] |
| 38 | TS_UNACCEPTABLE | [RFC7296] |
| 39 | INVALID_SELECTORS | [RFC7296] |
| 40 | UNACCEPTABLE_ADDRESSES | [RFC4555] |
| 41 | UNEXPECTED_NAT_DETECTED | [RFC4555] |
| 42 | USE_ASSIGNED_HoA | [RFC5026] |
| 43 | TEMPORARY_FAILURE | [RFC7296] |
| 44 | CHILD_SA_NOT_FOUND | [RFC7296] |
| 45 | INVALID_GROUP_ID | [draft-yeung-g-ikev2] |
| 46 | AUTHORIZATION_FAILED | [draft-yeung-g-ikev2] |
| 47-8191 | Unassigned | |
| 8192-16383 | Private use | [RFC7296] |

IKEv2 Notify Message Types - Status Types

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Range | Registration Procedures |
|-------------|-------------------------|
| 16384-40959 | Expert Review |
| 40960-65535 | Private use |

| Value | NOTIFY MESSAGES - STATUS TYPES | Reference |
|-------|-------------------------------------|---|
| 16384 | INITIAL_CONTACT | [RFC7296] |
| 16385 | SET_WINDOW_SIZE | [RFC7296] |
| 16386 | ADDITIONAL_TS_POSSIBLE | [RFC7296] |
| 16387 | IPCOMP_SUPPORTED | [RFC7296] |
| 16388 | NAT_DETECTION_SOURCE_IP | [RFC7296] |
| 16389 | NAT_DETECTION_DESTINATION_IP | [RFC7296] |
| 16390 | COOKIE | [RFC7296] |
| 16391 | USE_TRANSPORT_MODE | [RFC7296] |
| 16392 | HTTP_CERT_LOOKUP_SUPPORTED | [RFC7296] |
| 16393 | REKEY_SA | [RFC7296] |
| 16394 | ESP_TFC_PADDING_NOT_SUPPORTED | [RFC7296] |
| 16395 | NON_FIRST_FRAGMENTS_ALSO | [RFC7296] |
| 16396 | MOBIKE_SUPPORTED | [RFC4555] |
| 16397 | ADDITIONAL_IP4_ADDRESS | [RFC4555] |
| 16398 | ADDITIONAL_IP6_ADDRESS | [RFC4555] |
| 16399 | NO_ADDITIONAL_ADDRESSES | [RFC4555] |
| 16400 | UPDATE_SA_ADDRESSES | [RFC4555] |
| 16401 | COOKIE2 | [RFC4555] |
| 16402 | NO_NATS_ALLOWED | [RFC4555] |
| 16403 | AUTH_LIFETIME | [RFC4478] |
| 16404 | MULTIPLE_AUTH_SUPPORTED | [RFC4739] |
| 16405 | ANOTHER_AUTH_FOLLOWS | [RFC4739] |
| 16406 | REDIRECT_SUPPORTED | [RFC5685] |
| 16407 | REDIRECT | [RFC5685] |
| 16408 | REDIRECTED_FROM | [RFC5685] |
| 16409 | TICKET_LT_OPAQUE | [RFC5723] |
| 16410 | TICKET_REQUEST | [RFC5723] |
| 16411 | TICKET_ACK | [RFC5723] |
| 16412 | TICKET_NACK | [RFC5723] |
| 16413 | TICKET_OPAQUE | [RFC5723] |
| 16414 | LINK_ID | [RFC5739] |
| 16415 | USE_WESP_MODE | [RFC5840] |
| 16416 | ROHC_SUPPORTED | [RFC5857] |
| 16417 | EAP_ONLY_AUTHENTICATION | [RFC5998] |
| 16418 | CHILDLESS_IKEV2_SUPPORTED | [RFC6023] |
| 16419 | QUICK_CRASH_DETECTION | [RFC6290] |
| 16420 | IKEV2_MESSAGE_ID_SYNC_SUPPORTED | [RFC6311] |
| 16421 | IPSEC_REPLAY_COUNTER_SYNC_SUPPORTED | [RFC6311] |
| 16422 | IKEV2_MESSAGE_ID_SYNC | [RFC6311] |
| 16423 | IPSEC_REPLAY_COUNTER_SYNC | [RFC6311] |
| 16424 | SECURE_PASSWORD_METHODS | [RFC6467] |
| 16425 | PSK_PERSIST | [RFC6631] |
| 16426 | PSK_CONFIRM | [RFC6631] |
| 16427 | ERX_SUPPORTED | [RFC6867] |
| 16428 | IFOM_CAPABILITY | [Frederic_Firmin][3GPP TS 24.303 v10.6.0 annex B.2] |
| 16429 | SENDER_REQUEST_ID | [draft-yeung-g-ikev2] |
| 16430 | IKEV2_FRAGMENTATION_SUPPORTED | [RFC7383] |
| 16431 | SIGNATURE_HASH_ALGORITHMS | [RFC7427] |
| 16432 | CLONE_IKE_SA_SUPPORTED | [RFC7791] |
| 16433 | CLONE_IKE_SA | [RFC7791] |
| 16434 | PUZZLE | [RFC8019] |
| 16435 | USE_PPK | [draft-ietf-ipsecme-gr-ikev2] |
| 16436 | PPK_IDENTITY | [draft-ietf-ipsecme-gr-ikev2] |
| 16437 | NO_PPK_AUTH | [draft-ietf-ipsecme-gr-ikev2] |

| Value | NOTIFY MESSAGES - STATUS TYPES | Reference |
|-------------|--------------------------------|---------------------------|
| 16438-40959 | Unassigned | |
| 40960-65535 | Private use | [RFC7296] |

IKEv2 Notification IPCOMP Transform IDs (Value 16387)

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Value | Compression Type | Reference |
|---------|------------------|---------------------------|
| 0 | Reserved | [RFC7296] |
| 1 | IPCOMP_OUI | [UNSPECIFIED] |
| 2 | IPCOMP_DEFLATE | [RFC2394] |
| 3 | IPCOMP_LZS | [RFC2395] |
| 4 | IPCOMP_LZJH | [RFC3051] |
| 5-240 | Unassigned | |
| 241-255 | Private use | [RFC7296] |

IKEv2 Security Protocol Identifiers

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Protocol ID | Protocol | Reference |
|-------------|----------------------|---------------------------|
| 0 | Reserved | [RFC7296] |
| 1 | IKE | [RFC7296] |
| 2 | AH | [RFC7296] |
| 3 | ESP | [RFC7296] |
| 4 | FC_ESP_HEADER | [RFC4595] |
| 5 | FC_CT_AUTHENTICATION | [RFC4595] |
| 6-200 | Unassigned | |
| 201-255 | Private use | [RFC7296] |

IKEv2 Traffic Selector Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Value | TS Type | Reference |
|-------|----------|---------------------------|
| 0-6 | Reserved | [RFC7296] |

| Value | TS Type | Reference |
|---------|--------------------|---------------------------|
| 7 | TS_IPV4_ADDR_RANGE | [RFC7296] |
| 8 | TS_IPV6_ADDR_RANGE | [RFC7296] |
| 9 | TS_FC_ADDR_RANGE | [RFC4595] |
| 10-240 | Unassigned | |
| 241-255 | Private use | [RFC7296] |

IKEv2 Configuration Payload CFG Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Available Formats



CSV

| Value | CFG Type | Reference |
|---------|-------------|---------------------------|
| 0 | Reserved | [RFC7296] |
| 1 | CFG_REQUEST | [RFC7296] |
| 2 | CFG_REPLY | [RFC7296] |
| 3 | CFG_SET | [RFC7296] |
| 4 | CFG_ACK | [RFC7296] |
| 5-127 | Unassigned | |
| 128-255 | Private use | [RFC7296] |

IKEv2 Configuration Payload Attribute Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7296\]](#)

Note

Attribute Types with an "*" may be multi-valued on return only if multiple values were requested.

Available Formats



CSV

| Value | Attribute Type | Multi-Valued | Length | Reference |
|-------|----------------------|--------------|----------------|---------------------------|
| 0 | Reserved | | | [RFC7296] |
| 1 | INTERNAL_IP4_ADDRESS | YES* | 0 or 4 octets | [RFC7296] |
| 2 | INTERNAL_IP4_NETMASK | NO | 0 or 4 octets | [RFC7296] |
| 3 | INTERNAL_IP4_DNS | YES | 0 or 4 octets | [RFC7296] |
| 4 | INTERNAL_IP4_NBNS | YES | 0 or 4 octets | [RFC7296] |
| 5 | Reserved | | | [RFC7296] |
| 6 | INTERNAL_IP4_DHCP | YES | 0 or 4 octets | [RFC7296] |
| 7 | APPLICATION_VERSION | NO | 0 or more | [RFC7296] |
| 8 | INTERNAL_IP6_ADDRESS | YES* | 0 or 17 octets | [RFC7296] |
| 9 | Reserved | | | [RFC7296] |
| 10 | INTERNAL_IP6_DNS | YES | 0 or 16 octets | [RFC7296] |

| Value | Attribute Type | Multi-Valued | Length | Reference |
|-------------|-----------------------------------|--------------|----------------|---|
| 11 | Reserved | | | [RFC7296] |
| 12 | INTERNAL_IP6_DHCP | YES | 0 or 16 octets | [RFC7296] |
| 13 | INTERNAL_IP4_SUBNET | YES | 0 or 8 octets | [RFC7296] |
| 14 | SUPPORTED_ATTRIBUTES | NO | Multiple of 2 | [RFC7296] |
| 15 | INTERNAL_IP6_SUBNET | YES | 17 octets | [RFC7296] |
| 16 | MIP6_HOME_PREFIX | YES | 0 or 21 octets | [RFC5026] |
| 17 | INTERNAL_IP6_LINK | NO | 8 or more | [RFC5739] |
| 18 | INTERNAL_IP6_PREFIX | YES | 17 octets | [RFC5739] |
| 19 | HOME_AGENT_ADDRESS | NO | 16 or 20 | [http://www.3gpp.org/ftp/Specs/html-info/24302.htm] [John_Meredith] |
| 20 | P_CSCF_IP4_ADDRESS | YES | 0 or 4 octets | [RFC7651] |
| 21 | P_CSCF_IP6_ADDRESS | YES | 0 or 16 octets | [RFC7651] |
| 22 | FTT_KAT | NO | 2 octets | [TS 24.302 12.6.0] |
| 23 | EXTERNAL_SOURCE_IP4_NAT_INFO | NO | 0 or 6 | [TS 29.139] [Kimmo_Kymalainen] |
| 24 | TIMEOUT_PERIOD_FOR_LIVENESS_CHECK | NO | 0 or 4 octets | [TS 24.302 13.4.0] [Frederic_Firmin] |
| 25 | INTERNAL_DNS_DOMAIN | YES | 0 or more | [draft-pauly-ipsecme-split-dns] |
| 26 | INTERNAL_DNSSEC_TA | YES | 0 or more | [draft-ietf-ipsecme-split-dns] |
| 27-16383 | Unassigned | | | |
| 16384-32767 | Private Use | | | [RFC7296] |

IKEv2 Gateway Identity Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC5685\]](#)

Available Formats



CSV

| Value | Description | Reference |
|---------|---------------------------------|---------------------------|
| 0 | Reserved | [RFC5685] |
| 1 | IPv4 address of the VPN gateway | [RFC5685] |
| 2 | IPv6 address of the VPN gateway | [RFC5685] |
| 3 | FQDN of the VPN gateway | [RFC5685] |
| 4-240 | Unassigned | |
| 241-255 | Reserved for Private Use | [RFC5685] |

ROHC Attribute Types

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC5857\]](#)

Available Formats



CSV

| Value | ROHC Attribute Type | Format | Reference |
|-------------|---|--------|---------------------------|
| 0 | Reserved | | [RFC5857] |
| 1 | Maximum Context Identifier (MAX_CID) | TV | [RFC5857] |
| 2 | ROHC Profile (ROHC_PROFILE) | TV | [RFC5857] |
| 3 | ROHC Integrity Algorithm (ROHC_INTEG) | TV | [RFC5857] |
| 4 | ROHC ICV Length in bytes (ROHC_ICV_LEN) | TV | [RFC5857] |
| 5 | Maximum Reconstructed Reception Unit (MRRU) | TV | [RFC5857] |
| 6-16383 | Unassigned | | |
| 16384-32767 | Reserved for Private Use | | [RFC5857] |

IKEv2 Secure Password Methods

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[REC6467\]](#)

Available Formats



CSV

| Value | Description | Reference |
|------------|---------------------------|---------------------------|
| 0 | Reserved | [RFC6467] |
| 1 | PACE | [RFC6631] |
| 2 | AugPAKE | [RFC6628] |
| 3 | Secure PSK Authentication | [RFC6617] |
| 4-1023 | Unassigned | |
| 1024-65535 | Reserved for Private Use | [RFC6467] |

IKEv2 Hash Algorithms

Registration Procedure(s)

Expert Review

Expert(s)

Tero Kivinen

Reference

[\[RFC7427\]](#)

Available Formats



CSV

| Value | Hash Algorithm | Reference |
|------------|--------------------------|---------------------------|
| 0 | Reserved | [RFC7427] |
| 1 | SHA1 | [RFC7427] |
| 2 | SHA2-256 | [RFC7427] |
| 3 | SHA2-384 | [RFC7427] |
| 4 | SHA2-512 | [RFC7427] |
| 5 | Identity | [RFC8420] |
| 6-1023 | Unassigned | |
| 1024-65535 | Reserved for Private Use | [RFC7427] |

People

| ID | Name | Contact URI | Last Updated |
|-------------------|-----------------|---|--------------|
| [Frederic_Firmin] | Frederic Firmin | mailto:frederic.firmin@etsi.org | 2016-03-08 |

| ID | Name | Contact URI | Last Updated |
|--------------------|------------------|---|--------------|
| [John_Meredith] | John Meredith | mailto:john.meredith@etsi.org | 2010-05-17 |
| [Kimmo_Kymalainen] | Kimmo Kymalainen | mailto:kimmo.kymalainen@etsi.org | 2015-12-02 |
| [Matt_Ball] | Matt Ball | mailto:matt.ball@ieee.org | 2007-10-11 |