

**Initial IANA registry contents
draft-ietf-ipsec-ikev2-iana-00.txt**

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on June 15, 2004.

Copyright Notice

Copyright (C) The Internet Society (2003). All Rights Reserved.

Abstract

This is a non-standards track document that tells IANA how to populate the initial IKEv2 registries.

Table of Contents

1.	List of Registries	3
2.	IKEv2 Exchange Types	4
3.	IKEv1 Payload Types	5
4.	IKEv2 Payload Types	6
5.	IKEv2 Transform Types	7
5.1	IKEv2 Transform Attribute Types	7
5.2	IKEv2 Encryption Transform Values	7
5.3	IKEv2 Pseudo-random Function Transform Values	8
5.4	IKEv2 Integrity Algorithm Transform Values	8
5.5	IKEv2 Diffie-Hellman, ECP and EC2N Transform Values	8
5.6	IKEv2 Extended Sequence Numbers Transform Values	9
6.	IKEv2 Identification Types	10
7.	IKEv2 Certification Payload Format	11
8.	IKEv2 Authentication Method	12
9.	IKEv2 Notification Payload Types	13
9.1	IKEv2 IPCOMP Algorithm Types	14
10.	IKEv2 Security Protocol Identifiers	15
11.	IKEv2 Traffic Selector Types	16
12.	IKEv2 Configuration (CFG) Payload Types	17
13.	IKEv2 Configuration Payload Attribute Types	18
	Normative references	19
	Author's Address	19
	Full Copyright Statement	20

1. List of Registries

The following registries should be created.

Note: when creating a new Transform Type, a new registry for it must be created.

- * IKEv2 Exchange Types
- IKEv2 Payload Types
- IKEv2 Transform Types
 - IKEv2 Transform Attribute Types
 - IKEv2 Encryption Transform Values
 - IKEv2 Pseudo-random Function Transform Values
 - IKEv2 Integrity Algorithm Transform Values
 - IKEv2 Diffie-Hellman, ECP and EC2N Transform Values
 - IKEv2 Extended Sequence Numbers Transform Values
- IKEv2 Identification Types
- IKEv2 Certification Payload Format
- IKEv2 Authentication Method
- IKEv2 Notification Payload Type
- IKEv2 IPComp Transform IDs
- IKEv2 Security Protocol ID
- IKEv2 Traffic Selector Types
- IKEv2 Configuration request types
- IKEv2 Configuration attribute types

2. IKEv2 Exchange Types

The exchange type occurs in the IKEv2 header.

Exchange Type	VALUE
=====	
RESERVED	0-33
IKE_SA_INIT	34
IKE_AUTH	35
CREATE_CHILD_SA	36
INFORMATIONAL	37
Reserved for IKEv2+	38-239
Reserved for private use	240-255

3. IKEv1 Payload Types

Add

RESERVED

33-63

4. IKEv2 Payload Types

NAME	ACRONYM	VALUE
=====		
No Next Payload		0
RESERVED		1-32
Security Association	SA	33
Key Exchange	KE	34
Identification - Initiator	IDi	35
Identification - Responder	IDr	36
Certificate	CERT	37
Certificate Request	CERTREQ	38
Authentication	AUTH	39
Nonce	Ni, Nr	40
Notify	N	41
Delete	D	42
Vendor ID	V	43
Traffic Selector - Initiator	TSi	44
Traffic Selector - Responder	TSr	45
Encrypted	E	46
Configuration	CP	47
Extended Authentication	EAP	48
RESERVED TO IANA		49-127
PRIVATE USE		128-255

5. IKEv2 Transform Types

Transform Type	NUMBER
=====	=====
Encryption Algorithm	1
Pseudo-random Function	2
Integrity Algorithm	3
Diffie-Hellman/ECC Group	4
Extended Sequence Numbers	5
RESERVED TO IANA	6-240
PRIVATE USE	241-255

5.1 IKEv2 Transform Attribute Types

Attribute Type	value	Attribute Format
-----		-----
RESERVED	0-13	
Key Length (in bits)	14	TV
RESERVED	15-17	
RESERVED TO IANA	18-16383	
PRIVATE USE	16384-32767	

5.2 IKEv2 Encryption Transform Values

For Transform Type 1 (Encryption Algorithm), defined Transform IDs are:

Name	Number	Defined In
=====	=====	=====
RESERVED	0	
ENCR_DES_IV64	1	(RFC1827)
ENCR_DES	2	(RFC2405)
ENCR_3DES	3	(RFC2451)
ENCR_RC5	4	(RFC2451)
ENCR_IDEA	5	(RFC2451)
ENCR_CAST	6	(RFC2451)
ENCR_BLOWFISH	7	(RFC2451)
ENCR_3IDEA	8	(RFC2451)
ENCR_DES_IV32	9	
ENCR_RC4	10	
ENCR_NULL	11	(RFC2410)
ENCR_AES_CBC	12	
ENCR_AES_CTR	13	
RESERVED TO IANA	14-1023	

PRIVATE USE

1024-65535

5.3 IKEv2 Pseudo-random Function Transform Values

For Transform Type 2 (Pseudo-random Function), defined Transform IDs are:

Name	Number	Defined In
=====	=====	=====
RESERVED	0	
PRF_HMAC_MD5	1	(RFC2104)
PRF_HMAC_SHA1	2	(RFC2104)
PRF_HMAC_TIGER	3	(RFC2104)
PRF_AES_CBC	4	
RESERVED TO IANA	5-1023	
PRIVATE USE	1024-65535	

5.4 IKEv2 Integrity Algorithm Transform Values

For Transform Type 3 (Integrity Algorithm), defined Transform IDs are:

Name	Number	Defined In
=====	=====	=====
NONE	0	
AUTH_HMAC_MD5_96	1	(RFC2403)
AUTH_HMAC_SHA1_96	2	(RFC2404)
AUTH_DES_MAC	3	
AUTH_KPDK_MD5	4	(RFC1826)
AUTH_AES_XCBC_96	5	
RESERVED TO IANA	6-1023	
PRIVATE USE	1024-65535	

5.5 IKEv2 Diffie-Hellman, ECP and EC2N Transform Values

For Transform Type 4 (Diffie-Hellman, ECP and EC2N Group), defined Transform IDs are: (see also [[1](#)])

Name	Number	Defined In
=====	=====	=====
NONE	0	
768-bit MODP group	1	(IKEv2 B.1)
1024-bit MODP group	2	(IKEv2 B.2)
155-bit EC2N	3	(IKEv2 B.3)
185-bit EC2n	4	(IKEv2 B.4)

1536-bit MODP group	5	(RFC3526 . sec.2)
RESERVED TO IANA	6-13	
2048-bit MODP group	14	(RFC3526 . sec 3)
3072-bit MODP group	15	(RFC3526 . sec 4)
4096-bit MODP group	16	(RFC3526 . sec 5)
6144-bit MODP group	17	(RFC3526 . sec 6)
8192-bit MODP group	18	(RFC3526 . sec 7)
RESERVED TO IANA	19-1023	
PRIVATE USE	1024-65535	

5.6 IKEv2 Extended Sequence Numbers Transform Values

For Transform Type 5 (Extended Sequence Numbers), defined Transform IDs are:

Name	Number	Defined In
=====	=====	=====
No Extended Sequence Numbers	0	(IKEv2)
Extended Sequence Numbers	1	
RESERVED TO IANA	2-65535	

6. IKEv2 Identification Types

Name	Number	Defined In
=====	=====	=====
RESERVED	0	(IKEv2. section 3.5)
ID_IPV4_ADDR	1	(IKEv2. section 3.5)
ID_FQDN	2	(IKEv2. section 3.5)
ID_RFC822_ADDR	3	(IKEv2. section 3.5)
RESERVED	4	(IKEv2. section 3.5)
ID_IPV6_ADDR	5	(IKEv2. section 3.5)
RESERVED	6	(IKEv2. section 3.5)
RESERVED	7	(IKEv2. section 3.5)
RESERVED	8	(IKEv2. section 3.5)
ID_DER_ASN1_DN	9	(IKEv2. section 3.5)
ID_DER_ASN1_GN	10	(IKEv2. section 3.5)
ID_KEY_ID	11	(IKEv2. section 3.5)
RESERVED TO IANA	12-255	

7. IKEv2 Certification Payload Format

Name	Number	Defined In
=====	=====	=====
RESERVED	0	(IKEv2. section 3.6)
PKCS #7 wrapped X.509 certificate	1	(IKEv2. section 3.6)
PGP Certificate	2	(IKEv2. section 3.6)
DNS Signed Key	3	(IKEv2. section 3.6)
X.509 Certificate - Signature	4	(IKEv2. section 3.6)
Kerberos Token	6	(IKEv2. section 3.6)
Certificate Revocation List (CRL)	7	(IKEv2. section 3.6)
Authority Revocation List (ARL)	8	(IKEv2. section 3.6)
SPKI Certificate	9	(IKEv2. section 3.6)
X.509 Certificate - Attribute	10	(IKEv2. section 3.6)
Raw RSA Key	11	(IKEv2. section 3.6)
Hash and URL of PKIX certificate	12	(IKEv2. section 3.6)
Hash and URL of PKIX bundle	13	(IKEv2. section 3.6)
RESERVED TO IANA	14 - 200	
PRIVATE USE	201 - 255	

8. IKEv2 Authentication Method

The authentication method occurs in the Authentication Payload in IKEv2 [section 3.8](#).

Name	Number	Defined In
=====	=====	=====
RESERVED	0	(IKEv2)
RSA Digital Signature	1	(IKEv2 section 2.15)
Shared Key Message Integrity Code	2	(IKEv2 section 2.15)
DSS Digital Signature	3	(IKEv2 section 2.15)
RESERVED TO IANA	4-200	
PRIVATE USE	201-255	

9. IKEv2 Notification Payload Types

The authentication method occurs in the Notification Payload in IKEv2 [section 3.10.1](#). Errors types are 0-16383. Status types are 16384-65535.

Name =====	Number =====	Defined In =====
Error Types		
RESERVED	0	
UNSUPPORTED_CRITICAL_PAYLOAD	1	(IKEv2 section 3.10.1)
RESERVED	2,3	
INVALID_IKE_SPI	4	(IKEv2 section 3.10.1)
INVALID_MAJOR_VERSION	5	(IKEv2 section 3.10.1)
RESERVED	6	
INVALID_SYNTAX	7	(IKEv2 section 3.10.1)
RESERVED	8	
INVALID_MESSAGE_ID	9	(IKEv2 section 3.10.1)
RESERVED	10	
INVALID_SPI	11	(IKEv2 section 3.10.1)
RESERVED	12,13	
NO_PROPOSAL_CHOSEN	14	(IKEv2 section 3.10.1)
RESERVED	15,16	
INVALID_KEY_PAYLOAD	17	(IKEv2 section 3.10.1)
RESERVED	18-23	
AUTHENTICATION_FAILED	24	(IKEv2 section 3.10.1)
RESERVED	25-33	
SINGLE_PAIR_REQUIRED	34	(IKEv2 section 3.10.1)
NO_ADDITIONAL_SAS	35	(IKEv2 section 3.10.1)
INTERNAL_ADDRESS_FAILURE	36	(IKEv2 section 3.10.1)
FAILED_CP_REQUIRED	37	(IKEv2 section 3.10.1)
TS_UNACCEPTABLE	38	(IKEv2 section 3.10.1)
RESERVED TO IANA - Error types	39 - 8191	
Private Use - Errors	8192 - 16383	
Status Types		
INITIAL_CONTACT	16384	(IKEv2 section 3.10.1)
SET_WINDOW_SIZE	16385	(IKEv2 section 3.10.1)
ADDITIONAL_TS_POSSIBLE	16386	(IKEv2 section 3.10.1)
IPCOMP_SUPPORTED	16387	(IKEv2 section 3.10.1)
NAT_DETECTION_SOURCE_IP	16388	(IKEv2 section 3.10.1)
NAT_DETECTION_DESTINATION_IP	16389	(IKEv2 section 3.10.1)

3.10.1)	COOKIE	16390	(IKEv2 section
3.10.1)	USE_TRANSPORT_MODE	16391	(IKEv2 section
3.10.1)	HTTP_CERT_LOOKUP_SUPPORTED	16392	(IKEv2 section
3.10.1)	REKEY_SA	16393	(IKEv2 section
	RESERVED TO IANA - STATUS TYPES	16394 - 40959	
	Private Use - STATUS TYPES	40960 - 65535	

9.1 IKEv2 IPCOMP Algorithm Types

The IPCOMP notification type occurs in a Notification Payload of type IPCOMP_SUPPORTED (16387). The transform IDs currently defined are:

NAME	NUMBER	DEFINED IN
-----	-----	-----
RESERVED	0	
IPCOMP_OUI	1	
IPCOMP_DEFLATE	2	RFC 2394
IPCOMP_LZS	3	RFC 2395
IPCOMP_LZJH	4	RFC 3051
RESERVED TO IANA	5-240	
PRIVATE USE	241-255	

10. IKEv2 Security Protocol Identifiers

The security protocol ID occurs in the Delete Payload, in IKEv2 [section 3.11](#).

Name	Number	Defined In
=====	=====	=====
RESERVED	0	(IKEv2)
IKE_SA	1	(IKEv2 section 3.11)
AH - authentication header	2	(IKEv2 section 3.11)
ESP - encapsulated security payload	3	(IKEv2 section 3.11)
RESERVED TO IANA	4-200	
PRIVATE USE	201-255	

11. IKEv2 Traffic Selector Types

The traffic selector type Traffic Selector Payloads, defined in IKEv2 [section 3.13](#).

Name	Number	Defined In
=====	=====	=====
RESERVED	0-6	
TS_IPV4_ADDR_RANGE	7	(IKEv2 section 3.13.1)
TS_IPV6_ADDR_RANGE	8	(IKEv2 section 3.13.1)
RESERVED TO IANA	9-255	

12. IKEv2 Configuration (CFG) Payload Types

The CFG type occurs in the Configuration Payload, defined in IKEv2 [section 3.15](#).

CFG Type	Value
=====	=====
RESERVED	0
CFG_REQUEST	1
CFG_REPLY	2
CFG_SET	3
CFG_ACK	4
RESERVED TO IANA	5-127
PRIVATE USE	128-255

13. IKEv2 Configuration Payload Attribute Types

The CFG attribute type occurs in the Configuration Payload, defined in IKEv2 [section 3.15](#). Note this is a 15 bit field.

Attribute Type	Value	Multi-Valued	Length
=====	=====	=====	=====
RESERVED	0		
INTERNAL_IP4_ADDRESS	1	YES*	0 or 4 octets
INTERNAL_IP4_NETMASK	2	NO	0 or 4 octets
INTERNAL_IP4_DNS	3	YES	0 or 4 octets
INTERNAL_IP4_NBNS	4	YES	0 or 4 octets
INTERNAL_ADDRESS_EXPIRY	5	NO	0 or 4 octets
INTERNAL_IP4_DHCP	6	YES	0 or 4 octets
APPLICATION_VERSION	7	NO	0 or more
INTERNAL_IP6_ADDRESS	8	YES*	0 or 16 octets
INTERNAL_IP6_NETMASK	9	NO	0 or 16 octets
INTERNAL_IP6_DNS	10	YES	0 or 16 octets
INTERNAL_IP6_NBNS	11	YES	0 or 16 octets
INTERNAL_IP6_DHCP	12	YES	0 or 16 octets
INTERNAL_IP4_SUBNET	13	NO	0 or 8 octets
SUPPORTED_ATTRIBUTES	14	NO	Multiple of 2
INTERNAL_IP6_SUBNET	15	NO	17 octets
RESERVED TO IANA	16-16383		
PRIVATE USE	16384-32767		

* These attributes may be multi-valued on return only if multiple values were requested.

Normative references

- [1] Kivinen, T. and M. Kojo, "More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)", [RFC 3526](#), May 2003.

Author's Address

Michael C. Richardson
Sandelman Software Works
470 Dawson Avenue
Ottawa, ON K1Z 5V7
CA

EMail: mcr@sandelman.ottawa.on.ca

URI: <http://www.sandelman.ottawa.on.ca/>

Full Copyright Statement

Copyright (C) The Internet Society (2003). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

