Tech-invite

http://www.tech-invite.com

IPSec Guide

IKE Exchanges (Phase 1 and Phase 2)

V1.0 – March 2, 2005

This document shows detailed time diagrams for Phase 1 and Phase 2 IKE exchanges.

Phase 1 is where two IKE peers establish the ISAKMP Security Association, a secure and authenticated channel. The four authentication methods defined in RFC2409 are illustrated, in "main" mode only.

Phase 2 is where Security Associations are negotiated on behalf of IPSec. The "Quick" mode exchanges are detailed with and without PFS (perfect forward secrecy) service.

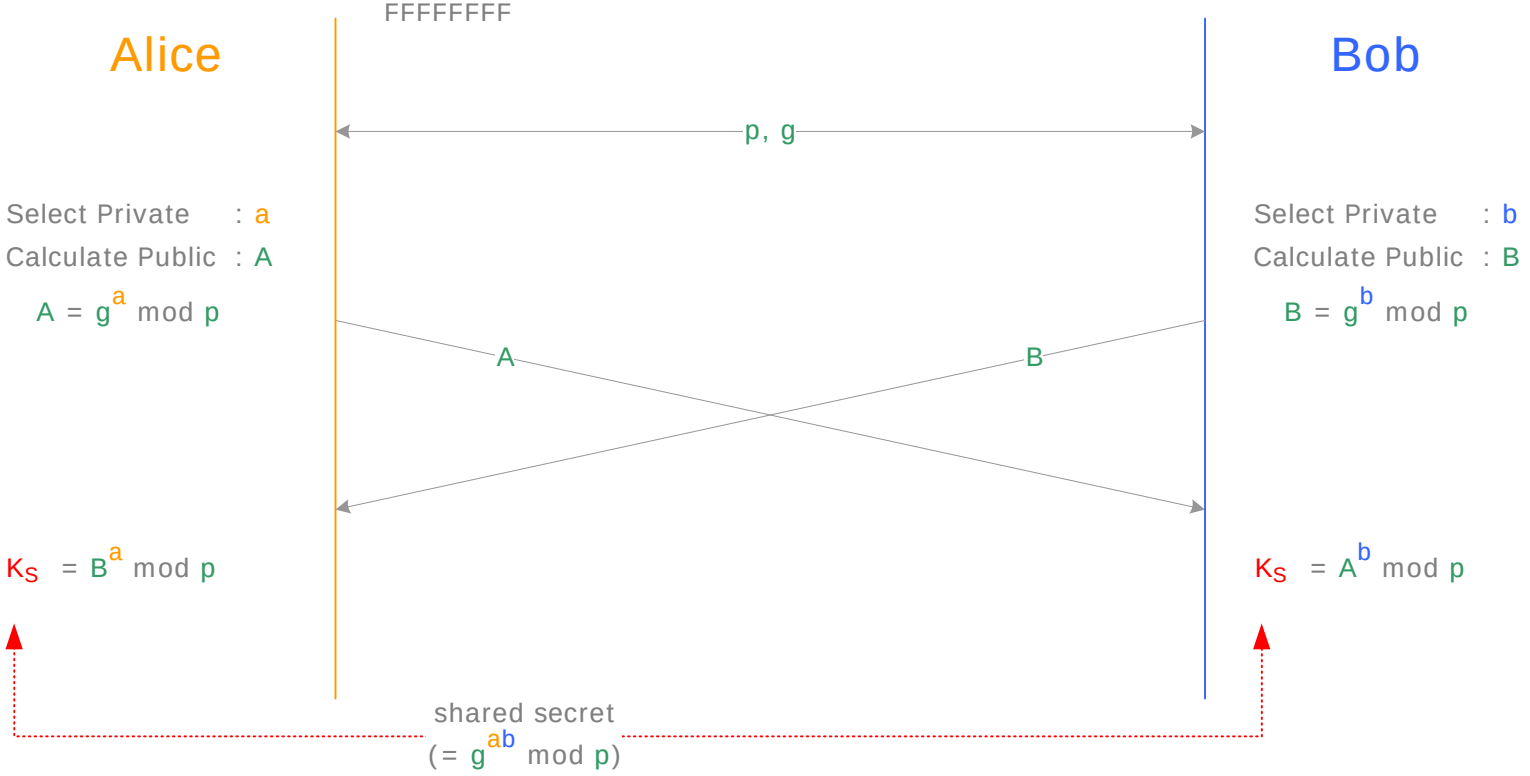
26 pages

Diffie-Hellman Key Exchange – Principles

"We now suggest a new public key distribution system which has several advantages..."
Whitfield Diffie and Martin E. Hellman
("New Directions in Cryptography" 1976)

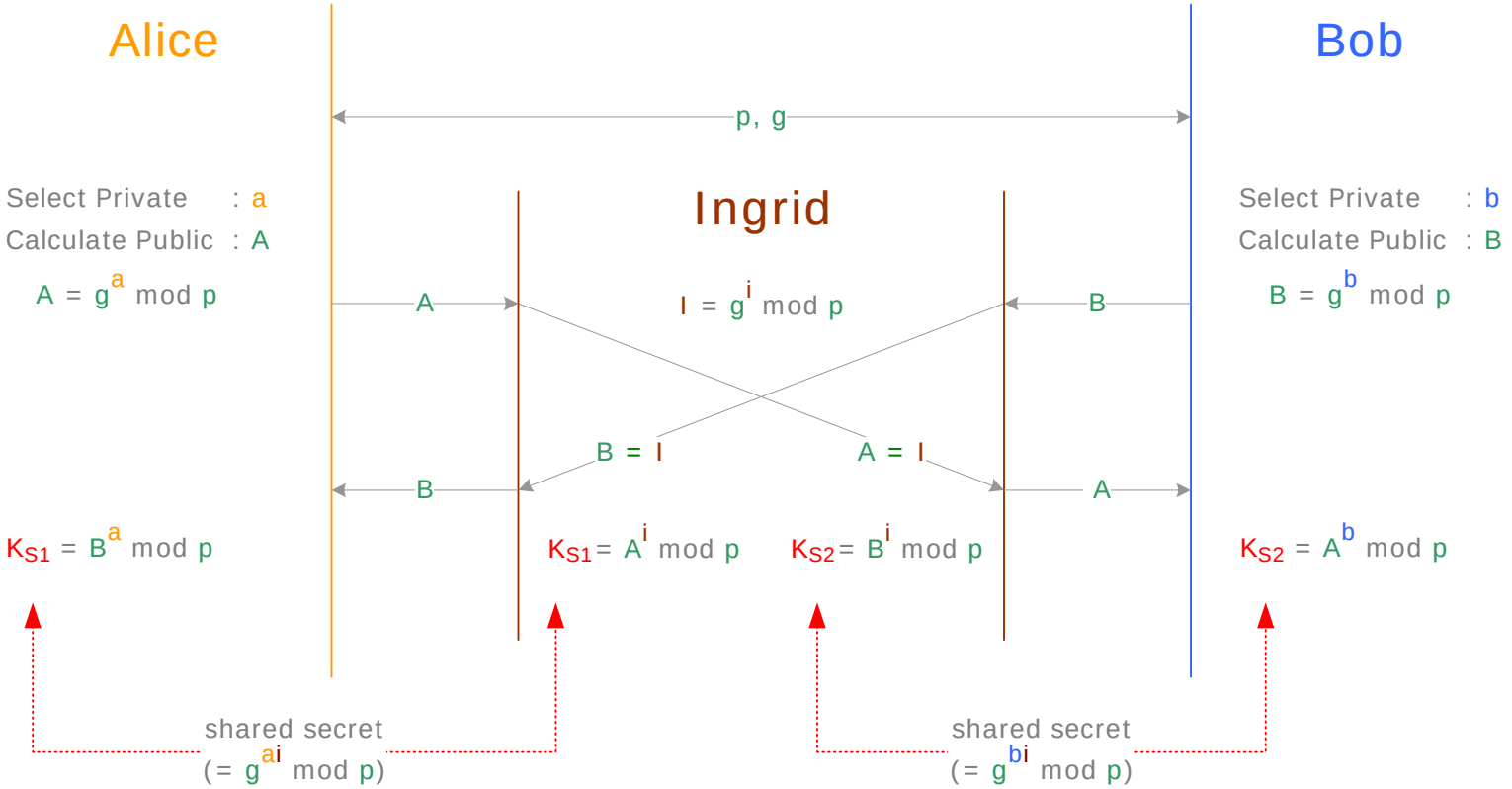
p (prime) and g (generator) public values, with IPSec, are documented in RFC 2409 and other RFCs. For example, with the first Oakley default group, g = 2 and p 's hexadecimal value, on 768 bits, is:

```
FFFFFFFF FFFFFFFF C90FDAA2 2168C234 C4C6628B
80DC1CD1
29024E08 8A67CC74 020BBEA6 3B139B22 514A0879
8E3404DD
EF9519B3 CD3A431B 302B0A6D F25F1437 4FE1356D
6D51C245
E485B576 625E7EC6 F44C42E9 A63A3620 FFFFFFFF
FFFFFFFF
```



Diffie-Hellman Key Exchange – Man-in-the-middle Attack

To prevent this "man-in-the-middle" attack, DH public values exchanged between peers have to be authenticated.



IPSec / IKE Exchanges – RFC 2409 (IKE) Notation

HDR	ISAKMP header
HDR*	ISAKMP header with encrypted payload
SA	SA negotiation payload with one or more proposals
<P>_b	Body of payload P (generic payload header not included)
CKI-I CKI-R	Initiator's cookie and Responder's cookie, respectively
g^xi g^xr	Diffie-Hellman (DH) public values of the initiator and responder respectively
g^xy	Diffie-Hellman shared secret
KE	Key Exchange payload
Nx	Nonce payload; x can be: i or r for the ISAKMP initiator and responder respectively
IDx	Identification payload for "x". x can be: "ii" or "ir" for the ISAKMP initiator and responder respectively during phase one negotiation; or "ui" or "ur" for the user initiator and responder respectively during phase two.

SIG	Signature payload. The data to sign is exchange-specific.
CERT	Certificate payload
HASH, HASH_I, ...	Hash payload. The contents of the hash are specific to the authentication method.
prf (key, msg)	Keyed pseudo-random function --often a keyed hash function-- used to generate a deterministic output that appears pseudo-random. prf's are used both for key derivations and for authentication (i.e. as a keyed MAC).
SKEYID	String derived from secret material known only to the active players in the exchange
SKEYID_e	Keying material used by the ISAKMP SA to protect the confidentiality of its messages
SKEYID_a	Keying material used by the ISAKMP SA to authenticate its messages
SKEYID_d	Keying material used to derive keys for non-ISAKMP security associations
<x>y	Indicates that "x" is encrypted with the key "y"
|	Concatenation of information- e.g. X | Y is the concatentation of X with Y

IKE Phase 1

Exchanges

IPSec / IKE Exchanges Phase 1 – Synopsis

Main Mode, Authenticated with Pre-Shared Key

HDR, SA →
← HDR, SA
HDR, KE, Ni →
← HDR, KE, Nr
HDR*, IDii, HASH_I →
← HDR*, IDir, HASH_R

Main Mode, Authenticated with Signatures

HDR, SA →
← HDR, SA
HDR, KE, Ni →
← HDR, KE, Nr
HDR*, IDii, [CERT,] SIG_I →
← HDR*, IDir, [CERT,] SIG_R

Main Mode, Authenticated with Public Key Encryption

HDR, SA →
← HDR, SA
HDR, KE, [HASH(1),] <IDii_b>Pubkey_r, <Ni_b>Pubkey_r →
← HDR, KE, IDir_b>Pubkey_i, <Nr_b>Pubkey_i
HDR*, HASH_I →
← HDR*, HASH_R

Main Mode, Authenticated with Revised Public Key Encryption

HDR, SA →
← HDR, SA
HDR, [HASH(1),] <Ni_b>Pubkey_r, <KE_b>Ke_i, <IDii_b>Ke_i [, <Cert-I_b>Ke_i] →
← HDR, <Nr_b>Pubkey_i, <KE_b>Ke_r, <IDir_b>Ke_r
HDR*, HASH_I →
← HDR*, HASH_R

Aggressive Mode, Authenticated with Pre-Shared Key

HDR, SA, KE, Ni, IDii →
← HDR, SA, KE, Nr, IDir, HASH_R
HDR, HASH_I →

Aggressive Mode, Authenticated with Signatures

HDR, SA, KE, Ni, IDii →
← HDR, SA, KE, Nr, IDir, [CERT,] SIG_R
HDR, [CERT,] SIG_I →

Aggressive Mode, Authenticated with Public Key Encryption

HDR, SA, [HASH(1),] KE, <IDii_b>Pubkey_r, <Ni_b>Pubkey_r →
← HDR, SA, KE, IDir_b>Pubkey_i, <Nr_b>Pubkey_i, HASH_R
HDR, HASH_I →

Aggressive Mode, Authenticated with Revised Public Key Encryption

HDR, SA, [HASH(1),] <Ni_b>Pubkey_r, <KE_b>Ke_i, <IDii_b>Ke_i [, <Cert-I_b>Ke_i] →
← HDR, SA, <Nr_b>Pubkey_i, <KE_b>Ke_r, <IDir_b>Ke_r, HASH_R
HDR, HASH_I →

IKE Main Mode – Authentication with a Pre-Shared Key

1) Negotiation of Protection Mechanisms

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : -
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 1 (ISAKMP)
  - # of Transforms : 2
  - T Payload
    - Next Payload : 3 (T)
    - Transform # : 0
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : SHA
      - Authentication Method : Pre-Shared Key
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600
  - T Payload
    - Next Payload : 0
    - Transform # : 1
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : MD5
      - Authentication Method : Pre-Shared Key
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600

HDR, SA →

← HDR, SA

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 1 (ISAKMP)
  - # of Transforms : 1
  - T Payload
    - Next Payload : 0
    - Transform # : 0
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : SHA
      - Authentication Method : Pre-Shared Key
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600

IKE Main Mode – Authentication with a Pre-Shared Key

2) Diffie-Hellman Exchange

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 4 (KE)
- Exchange Type : 2 (Main Mode)
- Flags : -

KE Payload
- Next Payload : 10 (NONCE)
- Key Exchange Data : g^xi (DH Public Value)

NONCE Payload (Ni)
- Next Payload : 0
- Nonce Data : nonce_i

HDR, KE, Ni →

SKEYID = prf (pre-shared-key, Ni_b | Nr_b)

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY_R
- Next Payload : 4 (KE)
- Exchange Type : 2 (Main Mode)
- Flags : -

KE Payload
- Next Payload : 10 (NONCE)
- Key Exchange Data : g^xr (DH Public Value)

NONCE Payload (Nr)
- Next Payload : 0
- Nonce Data : nonce_r

← HDR, KE, Nr

SKEYID = prf (pre-shared-key, Ni_b | Nr_b)

SKEYID_d = prf (SKEYID, g^xy | CKY-I | CKY-R | 0)
SKEYID_a = prf (SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
SKEYID_e = prf (SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)

Note: Encryption keys are generated from SKEYID_e in a manner that is defined for each algorithm

IKE Main Mode – Authentication with a Pre-Shared Key

3) Authentication

Initiator Peer

hash_i = prf (SKEYID,
g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b)

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

ID Payload (IDii)

Next Payload	: 8 (HASH)
ID Type	: 1 (ID_IPV4_ADDR)
Protocol ID	: -
Port	: -
Identification Data	: id_isakmp_i

HASH Payload (HASH_I)

Next Payload	: 0
Hash Data	: hash_i

HDR*, IDii, HASH_I →

Responder Peer

hash_r = prf (SKEYID,
g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b)

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

ID Payload (IDir)

Next Payload	: 8 (HASH)
ID Type	: 1 (ID_IPV4_ADDR)
Protocol ID	: -
Port	: -
Identification Data	: id_isakmp_r

HASH Payload (HASH-R)

Next Payload	: 0
Hash Data	: hash_r

← HDR*, IDir, HASH_R

IKE Main Mode – Authentication with Signatures

1) Negotiation of Protection Mechanisms

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : -
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 1 (ISAKMP)
  - # of Transforms : 2
  - T Payload
    - Next Payload : 3 (T)
    - Transform # : 0
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : SHA
      - Authentication Method : RSA signatures
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600
  - T Payload
    - Next Payload : 0
    - Transform # : 1
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : MD5
      - Authentication Method : RSA signatures
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600

HDR, SA →

← HDR, SA

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 1 (ISAKMP)
  - # of Transforms : 1
  - T Payload
    - Next Payload : 0
    - Transform # : 0
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : SHA
      - Authentication Method : RSA signatures
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600

IKE Main Mode – Authentication with Signatures

2) Diffie-Hellman Exchange

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 4 (KE)
- Exchange Type : 2 (Main Mode)
- Flags : -

KE Payload
- Next Payload : 10 (NONCE)
- Key Exchange Data : g^xi (DH Public Value)

NONCE Payload (Ni)
- Next Payload : 0
- Nonce Data : nonce_i

HDR, KE, Ni →

SKEYID = prf (Ni_b | Nr_b, g^xy)

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY_R
- Next Payload : 4 (KE)
- Exchange Type : 2 (Main Mode)
- Flags : -

KE Payload
- Next Payload : 10 (NONCE)
- Key Exchange Data : g^xr (DH Public Value)

NONCE Payload (Nr)
- Next Payload : 0
- Nonce Data : nonce_r

← HDR, KE, Nr

SKEYID = prf (Ni_b | Nr_b, g^xy)

SKEYID_d = prf (SKEYID, g^xy | CKY-I | CKY-R | 0)
SKEYID_a = prf (SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
SKEYID_e = prf (SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)

Note: Encryption keys are generated from SKEYID_e in a manner that is defined for each algorithm

IKE Main Mode – Authentication with Signatures

3) Authentication

Initiator Peer

hash_i = prf (SKEYID,
  g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b)

sig_i = E^{RSA}_{KRi} (hash_i)

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

ID Payload (IDii)

Next Payload	: 6 (CERT)
ID Type	: 1 (ID_IPV4_ADDR)
Protocol ID	: -
Port	: -
Identification Data	: id_isakmp_i

CERT Payload

Next Payload	: 9 (SIG)
Cert Encoding	: 4 (X.509 signature)
Certificate Data	: KUi 's certificate

Signature Payload (SIG_I)

Next Payload	: 0
Signature Data	: sig_i

HDR*, IDii, [CERT], SIG_I →

← HDR*, IDir, [CERT], SIG_R

Responder Peer

hash_r = prf (SKEYID,
  g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b)

sig_r = E^{RSA}_{KRr} (hash_r)

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

ID Payload (IDir)

Next Payload	: 6 (CERT)
ID Type	: 1 (ID_IPV4_ADDR)
Protocol ID	: -
Port	: -
Identification Data	: id_isakmp_r

CERT Payload

Next Payload	: 9 (SIG)
Cert Encoding	: 4 (X.509 signature)
Certificate Data	: KUr 's certificate

Signature Payload (SIG_R)

Next Payload	: 0
Signature Data	: sig_r

IKE Main Mode – Authentication with Public Key Encryption

1) Negotiation of Protection Mechanisms

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : -
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 1 (ISAKMP)
  - # of Transforms : 2
  - T Payload
    - Next Payload : 3 (T)
    - Transform # : 0
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : SHA
      - Authentication Method : Encryption with RSA
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600
  - T Payload
    - Next Payload : 0
    - Transform # : 1
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : MD5
      - Authentication Method : Encryption with RSA
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600

HDR, SA →

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 1 (ISAKMP)
  - # of Transforms : 1
  - T Payload
    - Next Payload : 0
    - Transform # : 0
    - Transform-Id : KEY_IKE
    - Attributes
      - Encryption Algorithm : 3DES-CBC
      - Hash Algorithm : SHA
      - Authentication Method : Encryption with RSA
      - DH Group : 1024-bit MODP
      - Life Type : Seconds
      - Life Duration : 3600

← HDR, SA

IKE Main Mode – Authentication with Public Key Encryption

2) Diffie-Hellman Exchange

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 4 (KE)
- Exchange Type : 2 (Main Mode)
- Flags : -

KE Payload
- Next Payload : 8 (HASH)
- Key Exchange Data : g^xi (DH Public Value)

HASH Payload [HASH(1)]
- Next Payload : 5 (ID)
- Hash Data : hash(cert_pubkey_r)

ID Payload (IDii)
- Next Payload : 10 (NONCE)
- ID Type : 1 (ID_IPV4_ADDR)
- Protocol ID : -
- Port : -
- Identification Data : id_isakmp_i

NONCE Payload (Ni)
- Next Payload : 0
- Nonce Data : nonce_i

SKEYID = prf (hash(Ni_b | Nr_b), CKY-I | CKY-R)

HDR,
KE,
[HASH(1),]
<IDii_b>Pubkey_r,
<Ni_b>Pubkey_r

HDR
,KE
,<IDir_b>Pubkey_i
,<Nr_b>Pubkey_i

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 4 (KE)
- Exchange Type : 2 (Main Mode)
- Flags : -

KE Payload
- Next Payload : 8 (HASH)
- Key Exchange Data : g^xr (DH Public Value)

ID Payload (IDir)
- Next Payload : 10 (NONCE)
- ID Type : 1 (ID_IPV4_ADDR)
- Protocol ID : -
- Port : -
- Identification Data : id_isakmp_r

NONCE Payload (Nr)
- Next Payload : 0
- Nonce Data : nonce_r

SKEYID = prf (hash(Ni_b | Nr_b), CKY-I | CKY-R)

SKEYID_d = prf (SKEYID, g^xy | CKY-I | CKY-R | 0)
SKEYID_a = prf (SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
SKEYID_e = prf (SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)

Note: Encryption keys are generated from SKEYID_e in a manner that is defined for each algorithm

IKE Main Mode – Authentication with Public Key Encryption

3) Authentication

Initiator Peer

```
hash_i = prf (SKEYID,
  g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b )
```

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

HASH Payload (HASH_I)

Next Payload	: 0
Hash Data	: hash_i

HDR*, HASH_I →

← HDR*, HASH_R

Responder Peer

```
hash_r = prf (SKEYID,
  g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b )
```

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

HASH Payload (HASH-R)

Next Payload	: 0
Hash Data	: hash_r

IKE Main Mode – Authentication with Revised Public Key Encryption

1) Negotiation of Protection Mechanisms

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : -
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)

P Payload
- Next Payload : 0
- Proposal # : 0
- Protocol ID : 1 (ISAKMP)
- # of Transforms : 2

T Payload
- Next Payload : 3 (T)
- Transform # : 0
- Transform-Id : KEY_IKE
- Attributes
  - Encryption Algorithm : 3DES-CBC
  - Hash Algorithm : SHA
  - Authentication Method : Revised Encryption with RSA
  - DH Group : 1024-bit MODP
  - Life Type : Seconds
  - Life Duration : 3600

T Payload
- Next Payload : 0
- Transform # : 1
- Transform-Id : KEY_IKE
- Attributes
  - Encryption Algorithm : 3DES-CBC
  - Hash Algorithm : MD5
  - Authentication Method : Revised Encryption with RSA
  - DH Group : 1024-bit MODP
  - Life Type : Seconds
  - Life Duration : 3600

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 1 (SA)
- Exchange Type : 2 (Main Mode)
- Flags : -

SA Payload
- Next Payload : 0
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)

P Payload
- Next Payload : 0
- Proposal # : 0
- Protocol ID : 1 (ISAKMP)
- # of Transforms : 1

T Payload
- Next Payload : 0
- Transform # : 0
- Transform-Id : KEY_IKE
- Attributes
  - Encryption Algorithm : 3DES-CBC
  - Hash Algorithm : SHA
  - Authentication Method : RevisedEncryption with RSA
  - DH Group : 1024-bit MODP
  - Life Type : Seconds
  - Life Duration : 3600

IKE Main Mode – Authentication with Revised Public Key Encryption

2) Diffie-Hellman Exchange

Initiator Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 8 (HASH)
- Exchange Type : 2 (Main Mode)
- Flags : -

HASH Payload [HASH(1)]
- Next Payload : 10 (NONCE)
- Hash Data : hash (cert_pubkey_r)

NONCE Payload (Ni)
- Next Payload : 4 (KE)
- Nonce Data : nonce_i

KE Payload
- Next Payload : 5 (ID)
- Key Exchange Data : g^xi (DH Public Value)

ID Payload (IDii)
- Next Payload : 6 (CERT)
- ID Type : 1 (ID_IPV4_ADDR)
- Protocol ID : -
- Port : -
- Identification Data : ID_isakmp_i

CERT Payload (Cert-I)
- Next Payload : 0
- Cert Encoding : 4 (X.509 signature)
- Certificate Data : KUi 's certificate

SKEYID = prf (hash(Ni_b | Nr_b), CKY-I | CKY-R)

HDR,
[HASH(1),]
<Ni_b>Pubkey_r,
<KE_b>Ke_i,
<IDii_b>Ke_i
[,<CertI_b>Ke_i]

HDR
,<Nr_b>Pubkey_i
,<KE_b>Ke_r
,<IDir_b>Ke_r

Responder Peer

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 10 (NONCE)
- Exchange Type : 2 (Main Mode)
- Flags : -

NONCE Payload (Nr)
- Next Payload : 4 (KE)
- Nonce Data : nonce_r

KE Payload
- Next Payload : 5 (ID)
- Key Exchange Data : g^xr (DH Public Value)

ID Payload (IDir)
- Next Payload : 0
- ID Type : 1 (ID_IPV4_ADDR)
- Protocol ID : -
- Port : -
- Identification Data : ID_isakmp_r

SKEYID = prf (hash(Ni_b | Nr_b), CKY-I | CKY-R)

SKEYID_d = prf (SKEYID, g^xy | CKY-I | CKY-R | 0)
SKEYID_a = prf (SKEYID, SKEYID_d | g^xy | CKY-I | CKY-R | 1)
SKEYID_e = prf (SKEYID, SKEYID_a | g^xy | CKY-I | CKY-R | 2)

Note: Encryption keys are generated from SKEYID_e in a manner that is defined for each algorithm

IKE Main Mode – Authentication with Revised Public Key Encryption

3) Authentication

Initiator Peer

```
hash_i = prf (SKEYID,
  g^xi | g^xr | CKY-I | CKY-R | SAi_b | IDii_b )
```

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

HASH Payload (HASH_I)

Next Payload	: 0
Hash Data	: hash_i

HDR*, HASH_I →

Responder Peer

```
hash_r = prf (SKEYID,
  g^xr | g^xi | CKY-R | CKY-I | SAi_b | IDir_b )
```

ISAKMP HDR

Initiator Cookie	: CKY-I
Responder Cookie	: CKY-R
Next Payload	: 5 (ID)
Exchange Type	: 2 (Main Mode)
Flags	: Encrypted

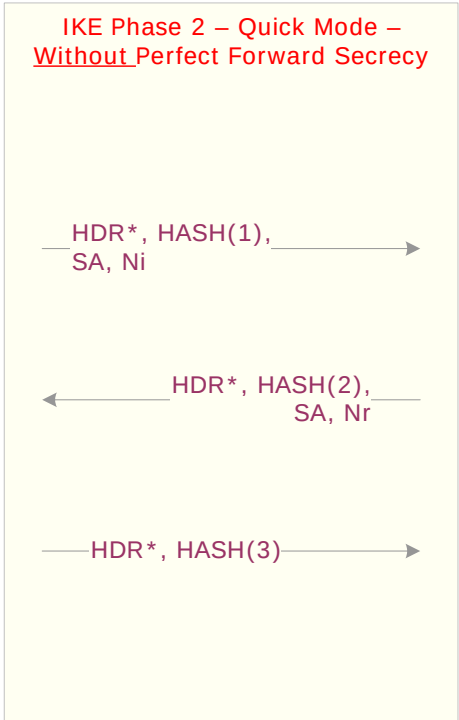
HASH Payload (HASH-R)

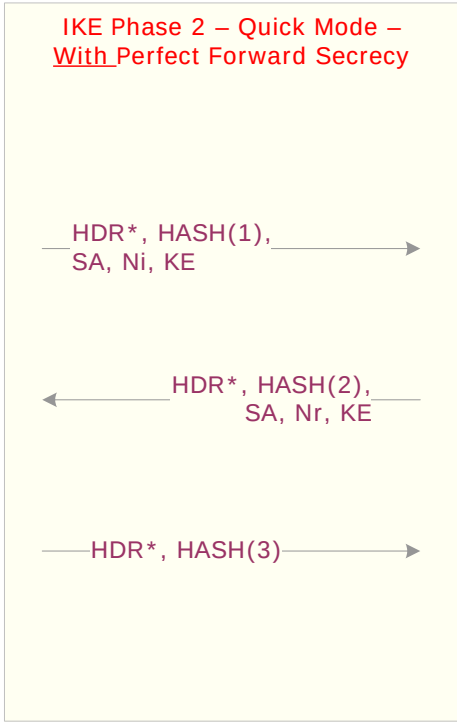
Next Payload	: 0
Hash Data	: hash_r

← HDR*, HASH_R

IKE Phase 2

Exchanges





IKE Quick Mode – Without Perfect Forward Secrecy (1)

Initiator Peer

hash_1 = prf (SKEYID_a, M-ID | SA | Ni)

```
ISAKMP HDR
  Initiator Cookie            : CKY-I
  Responder Cookie            : CKY-R
  Next Payload                : 8 (HASH)
  Exchange Type               : 32 (Quick Mode)
  Flags                       : Encrypted
  Message ID                  : M-ID
HASH Payload [HASH(1)]
  Next Payload                : 1 (SA)
  Hash Data                   : hash _1
SA Payload
  Next Payload                : 10 (NONCE)
  Domain of Interpretation    : 1 (IPSEC)
  Situation                   : 1 (IDENTITY)
  P Payload
    Next Payload              : 0
    Proposal #                : 0
    Protocol ID               : 3 (ESP)
    # of Transforms           : 2
    SPI                       : spi_i
    T Payload
      Next Payload            : 3 (T)
      Transform #             : 0
      Transform-Id            : 3 (ESP_3DES)
      Attributes
        Encapsulation Mode          : 2 (Transport)
        Authentication Algorithm    : 2 (HMAC-SHA)
    T Payload
      Next Payload            : 0
      Transform #             : 1
      Transform-Id            : 2 (ESP_3DES)
      Attributes
        Encapsulation Mode          : 2 (Transport)
        Authentication Algorithm    : 1 (HMAC-MD5)
NONCE Payload (Ni)
  Next Payload                : 0
  Nonce Data                  : nonce_i
```

HDR*, HASH(1), SA, Ni →

Responder Peer

IKE Quick Mode – Without Perfect Forward Secrecy (2)

Initiator Peer		Responder Peer

hash_2 = prf (SKEYID_a, M-ID | Ni_b | SA | Nr)

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 8 (HASH)
- Exchange Type : 32 (Quick Mode)
- Flags : Encrypted
- Message ID : M-ID

HASH Payload [HASH(2)]
- Next Payload : 1 (SA)
- Hash Data : hash _2

SA Payload
- Next Payload : 10 (NONCE)
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 3 (ESP)
  - # of Transforms : 1
  - SPI : spi_r
  - T Payload
    - Next Payload : 0
    - Transform # : 0
    - Transform-Id : 3 (ESP_3DES)
    - Attributes
      - Encapsulation Mode : 2 (Transport)
      - Authentication Algorithm : 2 (HMAC-SHA)

NONCE Payload (Ni)
- Next Payload : 0
- Nonce Data : nonce_r

← HDR*, HASH(2), SA, Nr

IKE Quick Mode – Without Perfect Forward Secrecy (3)

Initiator Peer		Responder Peer
hash_3 = prf (SKEYID_a, 0 | M-ID | Ni_b | Nr_b)		
ISAKMP HDR Initiator Cookie : CKY-I Responder Cookie : CKY-R Next Payload : 8 (HASH) Exchange Type : 32 (Quick Mode) Flags : Encrypted Message ID : M-ID HASH Payload [HASH(3)] Next Payload : 1 (SA) Hash Data : hash _3	HDR*, HASH(3) →	

IKE Quick Mode – With Perfect Forward Secrecy (1)

Initiator Peer

hash_1 = prf (SKEYID_a, M-ID | SA | Ni | KE)

```
ISAKMP HDR
  Initiator Cookie            : CKY-I
  Responder Cookie            : CKY-R
  Next Payload                : 8 (HASH)
  Exchange Type               : 32 (Quick Mode)
  Flags                       : Encrypted
  Message ID                  : M-ID
HASH Payload [HASH(1)]
  Next Payload                : 1 (SA)
  Hash Data                   : hash _1
SA Payload
  Next Payload                : 10 (NONCE)
  Domain of Interpretation    : 1 (IPSEC)
  Situation                   : 1 (IDENTITY)
  P Payload
    Next Payload              : 0
    Proposal #                : 0
    Protocol ID               : 3 (ESP)
    # of Transforms          : 2
    SPI                       : spi_i
    T Payload
      Next Payload            : 3 (T)
      Transform #             : 0
      Transform-Id            : 3 (ESP_3DES)
      Attributes
        Encapsulation Mode          : 2 (Transport)
        Authentication Algorithm    : 2 (HMAC-SHA)
    T Payload
      Next Payload            : 0
      Transform #             : 1
      Transform-Id            : 2 (ESP_3DES)
      Attributes
        Encapsulation Mode          : 2 (Transport)
        Authentication Algorithm    : 1 (HMAC-MD5)
NONCE Payload (Ni)
  Next Payload                : 4 (KE)
  Nonce Data                  : nonce_i
KE Payload (KE)
  Next Payload                : 0
  Key Exchange Data           : g^xi (DH Public Value)
```

HDR*, HASH(1), SA, Ni, KE →

Responder Peer

IKE Quick Mode – With Perfect Forward Secrecy (2)

Initiator Peer		Responder Peer

hash_2 =
prf (SKEYID_a, M-ID | Ni_b | SA | Nr | KE)

ISAKMP HDR
- Initiator Cookie : CKY-I
- Responder Cookie : CKY-R
- Next Payload : 8 (HASH)
- Exchange Type : 32 (Quick Mode)
- Flags : Encrypted
- Message ID : M-ID

HASH Payload [HASH(2)]
- Next Payload : 1 (SA)
- Hash Data : hash _2

SA Payload
- Next Payload : 10 (NONCE)
- Domain of Interpretation : 1 (IPSEC)
- Situation : 1 (IDENTITY)
- P Payload
  - Next Payload : 0
  - Proposal # : 0
  - Protocol ID : 3 (ESP)
  - # of Transforms : 1
  - SPI : spi_r
  - T Payload
    - Next Payload : 0
    - Transform # : 0
    - Transform-Id : 3 (ESP_3DES)
    - Attributes
      - Encapsulation Mode : 2 (Transport)
      - Authentication Algorithm : 2 (HMAC-SHA)

NONCE Payload (Ni)
- Next Payload : 4 (KE)
- Nonce Data : nonce_r

KE Payload (KE)
- Next Payload : 0
- Key Exchange Data : g^xr (DH Public Value)

← HDR*, HASH(2), SA, Nr, KE

IKE Quick Mode – With Perfect Forward Secrecy (3)

Initiator Peer		Responder Peer
hash_3 = prf (SKEYID_a, 0 | M-ID | Ni_b | Nr_b)		
ISAKMP HDR Initiator Cookie : CKY-I Responder Cookie : CKY-R Next Payload : 8 (HASH) Exchange Type : 32 (Quick Mode) Flags : Encrypted Message ID : M-ID HASH Payload [HASH(3)] Next Payload : 1 (SA) Hash Data : hash _3	HDR*, HASH(3) →	