# IPv6 Conformance

# Test Specification
# IKEv1
# End-Node using Aggressive Mode

**Technical Document**

Revision 1.0

IPv6 Forum
IPv6 Logo Committee

# Modification Record

Version 1.0  April 21,  2006

# Acknowledgement

IPv6 Forum would like to acknowledge the efforts of the following organizations in the development of this test specification.

- TAHI Project
- IRISA
- University of New Hampshire - Interoperability Laboratory (UNH-IOL)

# Introduction

The IPv6 forum plays a major role in bringing together industrial actors, to develop and deploy the next generation of IP protocols. Contrary to IPv4, which started with a small closed group of implementers, the universality of IPv6 leads to a huge number of implementations. Interoperability has always been considered as a critical feature in the Internet community.
Due to the large number of IPv6 implementations, it is important to provide the market a strong signal proving the level of interoperability across various products. To avoid confusion in the mind of customers, a globally unique logo program should be defined. The IPv6 logo will give confidence to users that IPv6 is currently operational. It will also be a clear indication that the technology will still be used in the future. To summarize, this logo program will contribute to the feeling that IPv6 is available and ready to be used.

The IPv6 Logo Program consists of three phases:

Phase 1 :
In a first stage, the Logo will indicate that the product includes IPv6 mandatory core protocols and can interoperate with other IPv6 implementations.

Phase 2 :
The "IPv6 ready" step implies a proper care, technical consensus and clear technical references. The IPv6 ready logo will indicate that a product has successfully satisfied strong requirements stated by the IPv6 Logo Committee (v6LC).

To avoid confusion, the logo "IPv6 Ready" will be generic. The v6LC will define the test profiles with associated requirements for specific functionalities.

Phase 3 :
Same as Phase 2 with IPsec mandated.

# Requirements

The Node Under Test (NUT) must satisfy following requirements.

| parameter | | | BASIC | ADVANCED |
|---|---|---|---|---|
| Exchange type | Phase-1 | | Main mode | Aggressive mode |
| | Phase-2 | | Quick mode | – |
| ISAKMP SA | Encryption Algorithm *1 | | 3DES-CBC | DES-CBC, AES-CBC (128bit) |
| | Hash Algorithm | | SHA1 | MD5 |
| | Authentication Method | | Pre-shared key | Digital Signature (RSA) |
| | Diffie-Hellman Group | | 2 | 1,5,14 |
| | Life Type | | Seconds | – |
| IPsec SA | Encapsulation mode | End-Node | Transport | Tunnel |
| | | SGW | Tunnel | – |
| | Security Protocol | | ESP with Authentication | ESP (without Authentication) |
| | Encryption Algorithm | | 3DES-CBC | DES-CBC, AES-CBC (128bit), ESP-NULL |
| | Hash Algorithm | | HMAC-SHA1 | HMAC-MD5 , AES-XCBC |
| | Life Type | | Seconds | – |
| IKE Phase-1 | Sending multiple proposal | | – | Support |
| IKE Phase-2 | PFS | | – | Support |
| | Commit bit | | – | Support |
| | Re-key | | Support | – |
| | Sending multiple proposal | | – | Support |

| | | | | |
|---|---|---|---|---|
| IPsec Transmission | Encapsulation mode | End-Node | Transport | Tunnel |
| | | SGW | Tunnel | - |
| | Security Protocol | | ESP with Authentication | ESP (without Authentication) |
| | Encryption Algorithm | | 3DES-CBC | DES-CBC, AES-CBC (128bit), ESP-NULL |
| | Hash Algorithm | | HMAC-SHA1 | HMAC-MD5 , AES-XCBC |
| | Anti-replay | | Sender | Receiver |

**Equipment Type:**

We define two possibilities for equipment types, they are as follows:

End-Node:

A node who can use IKE(IPsec) only for itself. Host and Router can be an End-Node.

SGW (Security Gateway):

A node who can provide IKE(IPsec tunnel mode) for nodes behind it. Router can be a SGW.

**Category:**

All NUTs are required to support BASIC. ADVANCED is required for all NUTs which support ADVANCED function.

# References

This test specification focus on following IKE related RFCs.

RFC2406 : IP Encapsulating Security Payload (ESP)

RFC2407 : The Internet IP Security Domain of Interpretation for ISAKMP

RFC2408 : Internet Sesurity Association and Key Management Protocol (ISAKMP)

RFC2409 : The Internet Key Exchange (IKE)

RFC3526 : More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)

RFC3566 : The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec

RFC3602 : The AES-CVC Cipher Algorithm and Its Use with IPsec

RFC4109 : Algorithms for Internet Key Exchange version 1 (IKEv1)

## ---TOC---

# 1. Test Details

This chapter contains detailed information, including terminology, which is described below.

Terminology:

TN  : Tester Node
NUT : Node Under Test (Target Implementation)
SGW : Security Gateway

Required Application:

All tests use ICMP Echo Request and Echo Reply messages by default. ICMP is independent from any implemented application and this adds clarity to the test. If the NUT can not apply IPsec for ICMPv6 packets, it is acceptable to use other protocols rather than ICMPv6. In this case, the device must support either ICMPv6, TCP or UDP. The application and port number are unspecified when TCP or UDP packets are used. The test coordinator should support any ports associated with an application used for the test. Applicants must mention the specific protocol and port that was used to execute the tests.

Topology:

In "2 Common Topology" the network topology for the test is shown.

# 2. Common Topology

- initiator Test

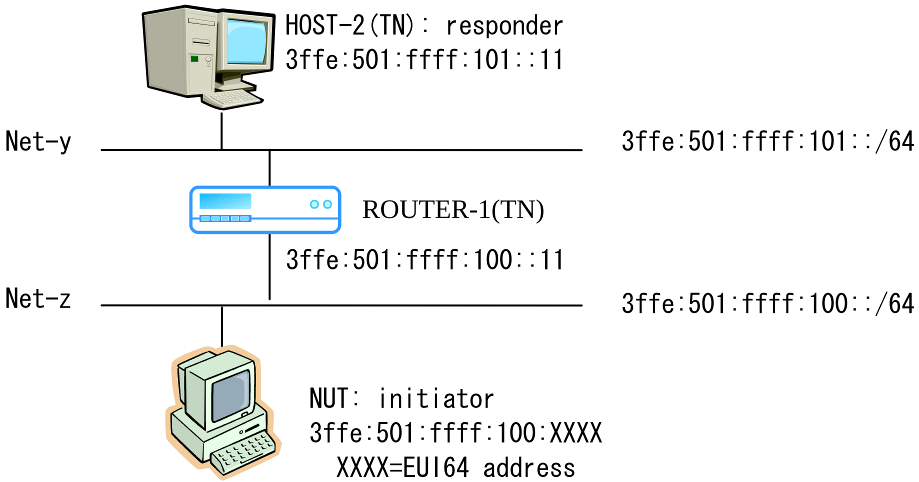


**Figure 1 Topology for End-Node vs. End-Node**

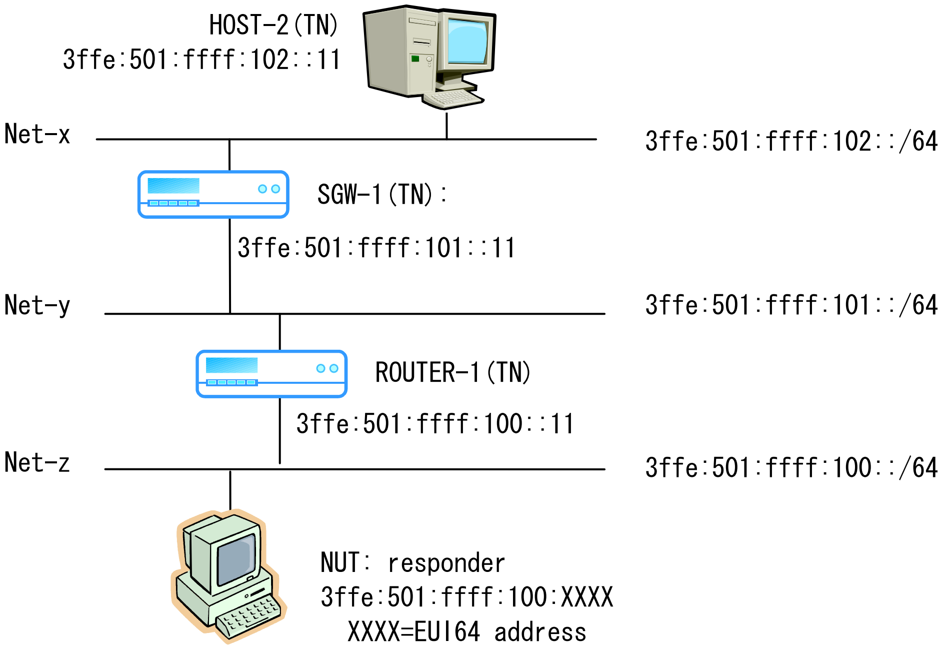


**Figure 2 Topology for End-Node vs. SGW**

- Responder Test

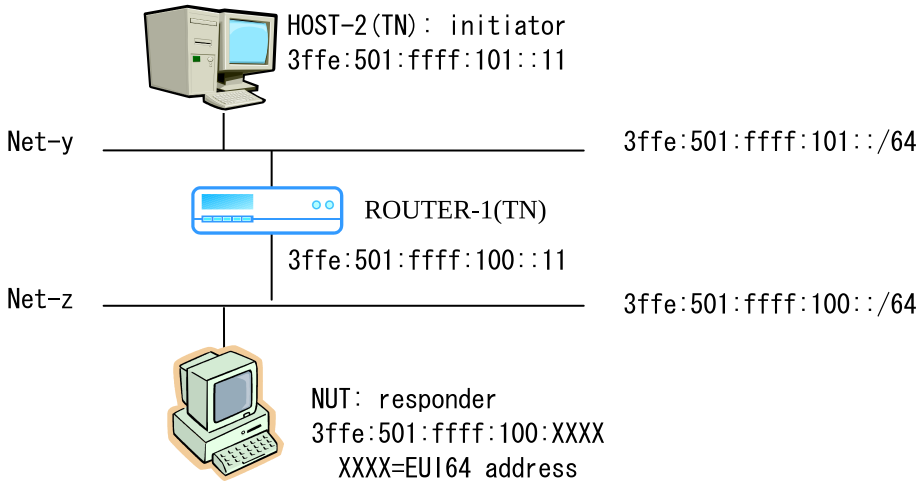


**Figure 3 Topology for End-Node vs. End-Node (Responder Test)**

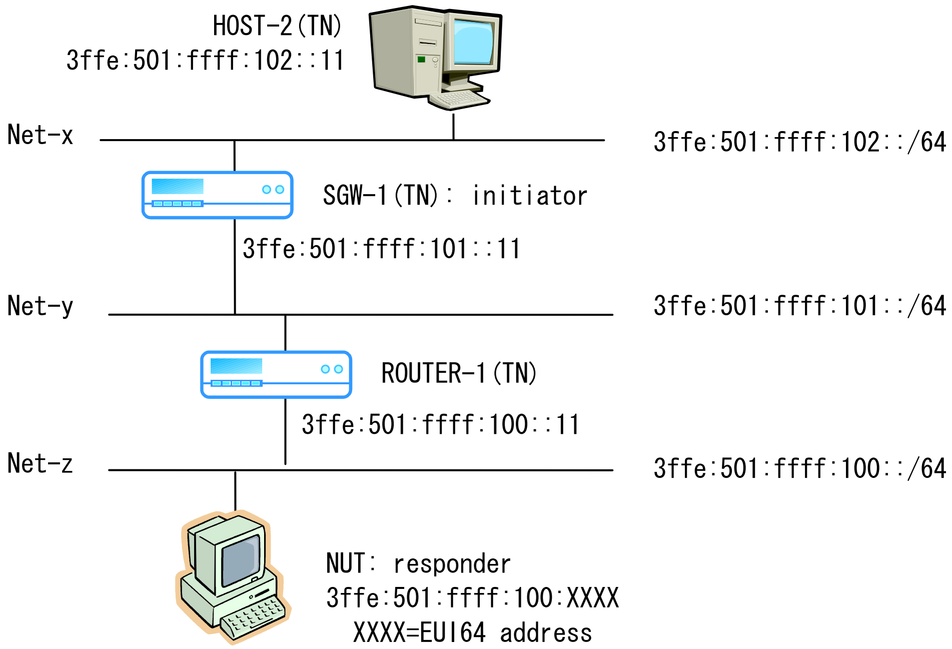


**Figure 4 Topology for End-Node vs. SGW (Responder Test)**

# 3. Common Configuration

Phase-1:

**Table 1. Phase-1 Common Configuration**

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Main | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Main | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

Phase-2:

**Table 2. Phase-2 Common Configuration**

| Machine | Src | Dest | Phase II | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | **Proto ID** | **Trans ID** | **Mode** | **Auth Alg** | **PH2 Lt** | **Upper** |
| NUT | NUT addr | HOST-2 addr | PROTO_IPSEC_ESP | ESP_3DES | Transport | HMAC-SHA | 8 Hour | any |
| HOST-2 | HOST-2 addr | NUT addr | PROTO_IPSEC_ESP | ESP_3DES | Transport | HMAC-SHA | 8 Hour | any |

# 4. Terminology

**Generic:**

| | |
|---|---|
| SGW: | Security Gateway |
| End-Node: | End Node |
| Initiator: | Initiator of IKE |
| Responder: | Responder of IKE |

**Configuration Table:**

| | |
|---|---|
| Ex Mode: | Exchange mode |
| IDx: | identity payload(FQDN or user FQDN can also be chosen as IDx) |
| Enc Alg: | IKE Encryption Algorithm |
| Hash Alg: | IKE Authentication Algorithm |
| Key Value: | pre-shared key value |
| PH1 Lt: | Phase-1 Lifetime |
| PH2 Lt: | Phase-2 Lifetime |
| Proto ID: | Protocol Identifier |
| Trans ID: | Transform Identifier |
| Mode: | Encapsulation Mode |
| Auth Alg: | Authentication Algorithm |
| Auth Method: | Authentication Method |
| DH Group: | Diffie-Hellman Group |
| Upper: | Upper Layer Protocol |
| NUT addr: | NUT address |
| HOST-2 addr: | HOST-2 address |

# 5. Description

Each test specification consists of following parts.

Purpose: The Purpose is the short statement describing what the test attempts to achieve. It is usually phrased as a simple assertion of the future or capability to be tested.

Category: The Category shows what classification of device must satisfy the test.

Initialization: The Initialization describes how to initialize and configure the NUT before starting each test. If a value is not provided, then the protocol’s default value is used.

Packets: The Packets describes the simple figure of packets which is used in the test. In this document, the packet name is represented in *Italic* style font.

Procedure: The Procedure describes step-by-step instructions for carrying out the test.

Judgment: The Judgment describes expected result. If we can observe as same result as the description of Judgment, the NUT passes the test.

References: The References section contains some parts of specification

# 6. End-Node Test

This Chapter describes the test specification for End-Node using Aggressive Mode (Phase1 exchange only). Please refer End-Node using Main Mode specification for Phase2.

## 6.1. Architecture

**Scope:**
Following tests focus on Internet Key Exchange Architecture.

**Overview:**
Tests in this section verify that a node properly process and transmit based on the Internet Key Exchange specification for End-Node using Aggressive Mode.

## 6.1.1. Position of payload

Purpose:

The SA payload MUST precede all other payloads in a phase 1 exchange.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
 * PHASE I
                         <AGGRESSIVE EXCHANGE>
 #    Initiator(NUT)          Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message which has correct position of payload must be received (The SA payload MUST precede all other payloads).
And must conform to above Configuration.

**References:**

RFC2409

### 6.1.2. ISAKMP Header format

Purpose:

ISAKMP Header Format

- Cookie field
  The cookies MUST NOT swap places when the direction of the ISAKMP SA changes.
  (The cookie must be set to Initiator cookie field.)
- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field is set as 1(Security Association Payload).)
- Version field
  Major Version 1
  Minor Version 0
- Exchange Type
  indicates the type of exchange being used.
  (In this test, this field is set as 4(aggressive mode).)
- Flags field
  Bits of the Flags field(except E,C,A bit) MUST be set to 0 prior to transmission.
  |0|0|0|0|0|A|C|E|
- Message ID field
  During Phase 1 negotiations, the value MUST be set to 0.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- **Configuration**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)           Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                        Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination

  Clean up SAD and SPD

Judgment:

The first message's ISAKMP Header Format must be base on description of RFC(see above Verification Points).(cookie is set to Initiator cookie filed,Major version=1 and Minor version=0 , Flags field is correct and Message ID=0).

References:

RFC2408 : 3.1 ISAKMP Header Format

### 6.1.3. Security Association Payload format

Purpose:

SA Payload Format

- Next Payload field
  This field MUST NOT contain the values for the Proposal(2) or Transform(3) payload. Place the value of the Next Payload in the Next Payload field. (In this test, this field is set as 0).
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0). Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Domain of Interpretation field
  This field MUST be present within the Sercurity Association payload.
  (In this test, this field is set as 1(IPsec DOI).)
- Situation field
  This field MUST be present within the Sercurity Association payload.
  Implementations MUST support SIT_IDENTITY_ONLY.
  (In this test, this field is set as 1(SIT_IDENTITY_ONLY).)

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                        Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination
  Clean up SAD and SPD

Judgment:

The first message's Security Association Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY
RFC2408 : 2.5.2 RESERVED Fields
3.4 Security Association Payload
2.5.2 RESERVED Fields
5.3 Generic Payload Header Processing
5.4 Security Association Payload Processing

### 6.1.4. Proposal Payload format

**Purpose:**

Proposal Payload Format

- Next Payload field
  This field MUST only contain the value "2" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In Phase I, this field only contain the value "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Proposal Number field
  Identifies the Proposal number for the current payload.
  (In Phase I, this field contain the value "1".)
- Protocol-ID field
  All implementations within the IPSEC DOI MUST support PROTO_ISAKMP.
- SPI size field
  Length in octets of the SPI as defined by the Protocol-Id.
- Number of Transforms field
  Specifies the number of transforms for the Proposal.
  (In this test, this field contain the value "1".)
- SPI field
  The sending entity's SPI.
  (In Phase I, this field is redundant and MAY be set to 0 or it MAY contain the transmitting entity's cookie.)

**Category:**

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

**Initialization:**

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder IKE parameter

    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #    Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                          Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination

  Clean up SAD and SPD

Judgment:

The first message's Proposal Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 2.4 Identifying Security Associations

### 6.1.5. Transform Payload format

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field only contain the value "0")
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In Phase I, this field only contain "1"(KEY_IKE))

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.
  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                     <AGGRESSIVE EXCHANGE>
 #    Initiator(NUT)        Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                     Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination
  Clean up SAD and SPD

Judgment:

The first message's Transform Payload Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.4.2.1 KEY_IKE

### 6.1.6. Transform Payload format (Multiple Transform Payload)

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field only contain the value "3" and "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (Example, in this test, this field is set as "1" and "2".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In Phase I, this field only contain "1"(KEY_IKE))
- If multiple offers are being made for phase 1 exchanges (Main Mode and Aggressive Mode)they MUST take the form of multiple Transform Payloads for a single Proposal Payload in a single SA payload.To put it another way, for phase 1 exchanges there MUST NOT be multiple Proposal Payloads for a single SA payload and there MUST NOT be multiple SA payloads.
- The multiple transforms MUST be presented with monotonically increasing numbers in the initiator's preference order.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Phase-1 sending multiple proposal)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  - ✧ Initiator and Responder IKE parameter

(It is shown that the mark of "*" expects monotonically increasing number.)
Any attribute is acceptable as proposal.

For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Trans # | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 1* | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| | | | | | 2* | DES | MD5 | pre-shared key | 2 | 8 Hour | |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #    Initiator(NUT)          Direction       Responder(TN)
(1)   HDR; SA, KE, Ni, IDii ========>
                             Judgement (Check *1)
```

1. Receive the first message from NUT

   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination

  Clean up SAD and SPD

Judgment:

The first message's Transform Payload Payload Format must be base on description of RFC(see above Verification Points).

References:

RFC2407 : 4.4.2.1 KEY_IKE<br>
RFC2408 : 2.5.2 RESERVED Fields

3.6 Transform Payload

4.2 Security Association Establishment

5.3 Generic Payload Header Processing

5.6 Transform Payload Processing

RFC2409 : 5. Exchanges

## 6.1.7. Transform payload SA Attributes (MD5)

Purpose:

IKE implementations MUST support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - DES in CBC mode<br>- MD5<br>- Authentication via pre-shared keys.<br>- MODP over default group number one. |

So, IKE implementations MUST support MD5.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support MD5)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES* | MD5 | pre-shared key* | 2* | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | MD5 | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                      Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(MD5:1) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4. Introduction

## 6.1.8. Transform payload SA Attributes (SHA)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

So, IKE implementations SHOULD support SHA.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES* | SHA | pre-shared key* | 2* | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(SHA:2) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction

### 6.1.9. Transform payload SA Attributes (DES)

Purpose:

IKE implementations MUST support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - DES in CBC mode<br>- MD5<br>- Authentication via pre-shared keys.<br>- MODP over default group number one. |

So, IKE implementations MUST support DES.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DES-CBC)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | DES | SHA* | pre-shared key* | 2* | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)         Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(DES:1) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction

## 6.1.10. Transform payload SA Attributes (3DES)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

So, IKE implementations SHOULD support 3DES.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology

  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder IKE parameter

    (It is shown that the mark of "*" permits anythings as attributes.)

    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA* | pre-shared key* | 2* | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA* | pre-shared key* | 2* | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                      Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(3DES:5) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction

## 6.1.11. Transform payload SA Attributes check (AES(128bit))

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - AES-128 in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

So, IKE implementations SHOULD support AES.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support AES-CBC)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | AES | SHA* | pre-shared key* | 2* | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | AES | SHA* | pre-shared key* | 2* | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(AES-CBC:7) must be included.
And must conform to above Configuration.

**References:**

RFC3602 : 5.  IKE Interactions

## 6.1.12. Transform payload SA Attributes check (PSK)

Purpose:

IKE implementations MUST support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - DES in CBC mode<br>- MD5<br>- Authentication via pre-shared keys.<br>- MODP over default group number one. |

So, IKE implementations MUST support pre-shared keys.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES* | SHA* | pre-shared key | 2* | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                      Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(PSK:1) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction

### 6.1.13. Transform payload SA Attributes (RSA sign)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- RSA signatures.<br>- MODP over group number two. |

So, IKE implementations SHOULD support RSA signatures.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES* | SHA* | RSA signatures | 2* | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                         Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(RSA sign:3) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction

## 6.1.14. Transform payload SA Attributes (DH1)

Purpose:

IKE implementations MUST support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - DES in CBC mode<br>- MD5<br>- Authentication via pre-shared keys.<br>- MODP over default group number one. |

So, IKE implementations MUST support DH1.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH1)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES* | SHA* | pre-shared key* | 1 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 1 | 8 Hour | HOST-2 addr |

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                  <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(DH1:1) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Intriduction

### 6.1.15. Transform payload SA Attributes check (DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

So, IKE implementations SHOULD support DH2.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES* | SHA* | pre-shared key* | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
#   Initiator(NUT)         Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(DH2:2) must be included.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction
          6.2 Second Oakley Group

## 6.1.16. Transform payload SA Attributes (DH5)

Purpose:

IKE implementations support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number five. |

So, IKE implementations support DH5.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH5)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    (It is shown that the mark of "*" permits anythings as attributes.)
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES* | SHA* | pre-shared key* | 5 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 5 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(DH5:5) must be included.
And must conform to above Configuration.

**References:**

RFC3526 : 2. 1536-bit MODP Group

## 6.1.17. Transform payload SA Attributes check (DH14)

Purpose:

IKE implementations support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number fourteen. |

So, IKE implementations support DH14.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH14)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  (It is shown that the mark of "*" permits anythings as attributes.)
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES* | SHA* | pre-shared key* | 14 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 14 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message Attributes(DH14:14) must be included.
And must conform to above Configuration.

**References:**

RFC3526 : 3.  2048-bit MODP Group

## 6.1.18. Key Exchange Payload Format (DH1)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 768 bit)

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH1)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 1 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 1 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)         Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination

  Clean up SAD and SPD

Judgment:

The first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

### 6.1.19. Key Exchange Payload Format (DH2)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1024 bit)

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction        Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                        Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

## 6.1.20. Key Exchange Payload Format (DH5)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1536 bit)

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH5)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 5 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 5 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                  <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)         Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination
  Clean up SAD and SPD

Judgment:

The first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

## 6.1.21. Key Exchange Payload Format check(DH14)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 2048 bit)

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH14)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 14 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 14 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                   <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)         Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination
  Clean up SAD and SPD

Judgment:

The first message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

## 6.1.22. Nonce Payload Format

Purpose:

Nonce Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Nonce Data field
  The length of nonce payload MUST be between 8 and 256 bytes inclusive.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                       Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message's Nonce Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
          5.13 Nonce Payload Processing
RFC2409 : 5. Exchanges

### 6.1.23. Identification Payload Format

Purpose:

ID Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.(In this test, this field is set as 5(ID_IPV6_ADDR).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port ID field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, this value is NUT IPv6 address.)
- During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
#    Initiator(NUT)           Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                         Judgement (Check *1)
```

1. Receive the first message from NUT

   In the first message (1), the initiator generates a proposal itconsiders adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

- Termination

  Clean up SAD and SPD

Judgment:

The first message's Identification Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

```
RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 3.8 Identification Payload
          5.3 Generic Payload Header Processing
          5.8 Identification Payload Process
```

## 6.1.24. HASH Payload Format

Purpose:

HASH Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Hash Data field
  Data that results from applying the hash routine to the ISAKMP message and/or state. (HASH_I=prf(SKEYID,g^xi|g^xr|CKY-I|CKY-R|SAi_b|IDii_b))

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)         Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                        <========       HDR; SA, KE, Nr, IDir, HASH_R
(3)  HDR[*]; HASH_I        ========>
                      Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

- **Termination**

  Clean up SAD and SPD

**Judgment:**

The first to the second message must be exchanged correctly.
The third message's HASH Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
5.11 Hash Payload Processing

### 6.1.25. Implementation of Aggressive Mode with pre-shared key

Purpose:

Implementation of Aggressive Mode with pre-shared key check.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
 * PHASE I
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                Judgement (Check *1)
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
(3)  HDR[*]; HASH_I         ========>
                Judgement (Check *2)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

```
 * PHASE II
                      <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
           SA, Ni       ========>
                Judgement (Check *3)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with

the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

In Phase I, the first to the third message must be exchanged correctly.
  Check *1
    Security Association, Key Exchange, Nonce, Identification Payload Format must be base on description of RFC.
  Check *2
    Hash Payload Format must be base on description of RFC.
In Phase II, the first message must be received.
  Check *3
    NUT must start Phase II negotiation.
And must conform to above Configuration.

**References:**

RFC2409 : 4. Introduction
          5. Exchanges

### 6.1.26. Certificate Request Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Type field
  Contains an encoding of the type of certificate requested
- Certificate Authority field
  Contains an encoding of an acceptable certificate authority for the type of certificate requested.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- **Configuration**
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #    Initiator(NUT)          Direction       Responder(TN)
(1)   HDR; SA, KE, Ni, IDii ========>
      CERT Req
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message's Certificate Request Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 3.10 Certificate Request Payload
          5.3 Generic Payload Header Processing
          5.10 Certificate Request Payload Processing

### 6.1.27. Signature Payload Format

Purpose:

Signature Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Signature Data field
  Data that results from applying the digital signature function to the ISAKMP message and/or state.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                       <========       HDR; SA, KE, Nr, IDir, SIG_R
(3)  HDR[*]; SIG_I        ========>
```

1. Receive the first message from NUT

   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN

   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

3. Receive the third message from NUT

   In the third (3) message, the initiator send the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

- Termination

  Clean up SAD and SPD

Judgment:

The first to the second message must be exchanged correctly.
The third message's Signature Payload Format must be base on description of

RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Processing
5.12 Signature Payload Processing

## 6.1.28. Certificate Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Encoding field
  This field indicates the type of certificate or certificate-related information contained in theCertificate Data field.
- Certificate Data field
  Actual encoding of certificate data

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".
- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator set the certificate of responder.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology". For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                     <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)        Direction       Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                        <========       HDR; SA, KE, Nr, IDir, SIG_R
                                           CERT Req
(3)  HDR[*]; SIG_I, CERT   ========>
```

1. Receive the first message from NUT

   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN

   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the responder send Certificate Request Payload

3. Receive the third message from NUT
   In the third (3) message, the initiator send the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the initiator send Certificate Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first to the second message must be exchanged correctly.
The third message's Certificate Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 3.9 Certificate Payload
          5.3 Generic Payload Header Processing
          5.9 Certificate Payload Processing

## 6.1.29. Implementation of Aggressive Mode with RSA signatures

Purpose:

Implementation of Aggressive Mode with RSA signatures check.

Category:

End-Node : End-Node : ADVANCED (This test is required for all End-Node NUTs which
support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
 * PHASE I
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)          Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
                Judgement (Check *1)
(2)                        <========      HDR; SA, KE, Nr, IDir, SIG_R
(3)  HDR[*]; SIG_I         ========>
                Judgement (Check *2)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted. Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

3. Receive the third message from NUT
   In the third (3) message, the initiator send the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

```
 * PHASE II
                      <QUICK MODE>
 #   Initiator(NUT)      Direction       Responder(TN)
(1)  HDR*, HASH(1),
           SA, Ni       ========>
                Judgement (Check *3)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).

And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

- Termination
  Clean up SAD and SPD

Judgment:

In Phase I, the first to the third message must be exchanged correctly.
  Check *1
      Security Association, Key Exchange, Nonce, Identification Payload Format must be base on description of RFC.
  Check *2
      Signature Payload Format must be base on description of RFC.
In Phase II, the first message must be received.
  Check *3
      NUT must start Phase II negotiation.
And must conform to above Configuration.

References:

RFC2409 : 4. Introduction
          5. Exchanges

## 6.1.30. Processing invalid ISAKMP Payload Length

Purpose:

If the ISAKMP message length and the value in the Payload Length field of the ISAKMP Header are not the same, then the ISAKMP message MUST be rejected. The receiving entity (initiator or responder) MUST do the following:

1. The event, UNEQUAL PAYLOAD LENGTHS, MAY be logged in the appropriate system audit file.
2. An Informational Exchange with a Notification payload containing the UNEQUAL-PAYLOAD-LENGTHS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Length field = 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)  Direction  Responder(TN)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                   <======== HDR; SA, KE,
                              Nr,IDir,HASH_R <-----Length field(ISAKMP header):
                                                                   0 (invalid)
(3-A)HDR[*];HASH_I     ========> X           <-----Must not transmit
         or
(3-B)HDR*; HASH(1);N/D========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or UNEQUAL-PAYLOAD-LENGTHS message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.1 General Message Processing

## 6.1.31. Processing invalid Responder Cookie field

Purpose:

Verify the Initiator and Responder "cookies". If the cookie validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID COOKIE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-COOKIE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    In TEST PROCEDURE, Responder Cookie field of the second message of AGGRESSIVE EXCHANGE is set to 0.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)  Direction    Responder(TN)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                 <========   HDR; SA, KE,
                              Nr, IDir, HASH_R  <-----Cookie field : 0(invalid)
(3-A)HDR[*]; HASH_I ========> X                <-----Must not transmit
        or
(3-B)HDR*;HASH(1);N/D========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-COOKIE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

## 6.1.32. Processing invalid Next Payload field

Purpose:

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Next Payload field = 127(invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)  Direction   Responder(TN)
(1)HDR;SA,KE,Ni,IDii========>
(2)               <========  HDR; SA, KE,
                           Nr, IDir, HASH_R <-----Next Payload field(ISAKMP
                                                       Header) : 127(invalid)
(3-A)HDR[*]; HASH_I  ========> X           <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

### 6.1.33. Processing invalid Major Version field (major 15,minor 0)

Purpose:

- Implementation SHOULD never accept packets with a major version number larger than its own.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:
  - (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.
  - (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
    This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:responder)
    **Major Version** : 15 (invalid value)
    **Minor Version** : 0
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)    Direction    Responder(TN)
(1)HDR;SA,KE,Ni,IDii========>
(2)                 <========  HDR; SA, KE,
                             Nr, IDir, HASH_R<-----Major Version : 15(invalid)
(3-A)HDR[*]; HASH_I ========> X             <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-MAJOR-VERSION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

## 6.1.34. Processing invalid Minor Version field (major 1,minor 15)

Purpose:

- Implementation SHOULD never accept packets with a minor version number larger than its own, given the major version numbers are identical.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    **Major Version** : 1
    **Minor Version** : 15 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

```
  This test check is following.
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)  Direction  Responder(TN)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                 <========HDR; SA, KE,
                             Nr, IDir, HASH_R<-----Minor Version : 15(invalid)
(3-A)HDR[*]; HASH_I  ========> X             <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation.  The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted. Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-MINOR-VERSION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

## 6.1.35. Processing invalid Exchange Type field

Purpose:

Check the Exchange Type field to confirm it is valid. If the Exchange Type field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID EXCHANGE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-EXCHANGE-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Exchange Type field = 31 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)  Direction Responder(TN)
(1)HDR;SA,KE,Ni,IDii========>
(2)                <========HDR;SA,KE,
                          Nr,IDir,HASH_R<----Exchange Type field:31(invalid)
(3-A)HDR[*]; HASH_I ========> X        <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-EXCHANGE-TYPE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

### 6.1.36. Processing invalid Flags field

Purpose:

Check the Flags field to ensure it contains correct values. If the Flags field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID FLAGS, MAY be logged in the appropriate systemaudit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-FLAGS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    Flags field = |1|1|1|1|1|0|0|0| (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #  Initiator(NUT)  Direction  Responder(TN)
(1)HDR;SA,KE,Ni,IDii========>
(2)                <======== HDR; SA, KE,
                             Nr,IDir,HASH_R <----Flags field :
                                            |1|1|1|1|1|0|0|0|(invalid value)
(3-A)HDR[*]; HASH_I  ========> X           <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
             Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-FLAGS message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

## 6.1.37. Processing invalid Message ID field

Purpose:

Check the Message ID field to ensure it contains correct values. If the Message ID validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID MESSAGE ID, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-MESSAGE-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Responder)
    **Message ID field = 1** (set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure**:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)     Direction  Responder(TN)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                  <======== HDR; SA, KE,
                               Nr,IDir,HASH_R <-----Message ID field :1
                                                                (invalid value)
(3-A)HDR[*]; HASH_I ========> X              <-----Must not transmit
         or
(3-B)HDR*; HASH(1); N/D     ========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment**:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-MESSAGE-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

### 6.1.38. Processing invalid Next Payload field

Purpose:

If the Next Payload field validation fails, the message is discarded.

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)
    **Next Payload field : 127** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)    Direction   Responder(TN)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                 <======== HDR; SA, KE,
                              Nr, IDir, HASH_R <-----Next Payload field : 127
                                                          (SA, invalid value)
(3-A)HDR[*]; HASH_I   ========> X              <-----Must not transmit
         or
(3-B)HDR*; HASH(1); N/D========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408：3.4 Security Association Payload
         5.3 Generic Payload Header Processing

### 6.1.39. Processing invalid RESERVED field

Purpose:

Verify the RESERVED field contains the value zero. If the value in the RESERVED field is not zero, the message is discarded and the following actions are taken:

(a) The event, INVALID RESERVED FIELD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

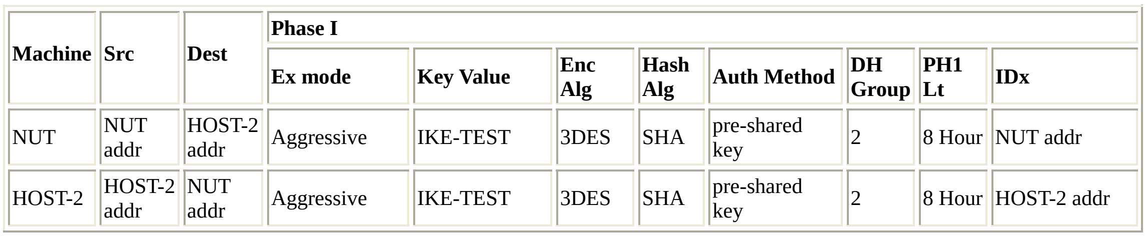
Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ SA Payload Format(HOST-2:Responder)
  RESERVED field : 1 (set to not zero, invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.



| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)   Direction  Responder(TN)
(1)HDR;SA,KE,Ni,Idii========>
(2)               <========HDR;SA,KE,
                          Dir,HASH_R<-----RESERVED field:1(SA,invalid value)
(3-A)HDR[*];HASH_I  ========> X      <-----Must not transmit
        or
(3-B)HDR*;HASH(1);N/D========>
     (HDR; N/D)
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned(* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(3-B) is returned).*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing

## 6.1.40. Processing invalid Next Payload field

Purpose:

- This field MUST NOT contain the values for the Proposal or Transform payloads as they are considered part of the security association negotiation.
- If the Next Payload field validation fails, the message is discarded.
- Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)
    **Next Payload field : 2**(Proposal Payload, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer ″Table 2. Phase-2 Common Configuration″ in Chapter ″Common Configuration″.

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)    Direction  Responder(TN)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                 <======== HDR; SA, KE,
                              Nr, IDir, HASH_R <-----Next Payload field(SA):
                                                              2(invalid value)
(3-A)HDR[*]; HASH_I  ========> X               <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

-

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 3.4 Security Association Payload
          5.3 Generic Payload Header Processing

## 6.1.41. Processing invalid DOI field

Purpose:

Determine if the Domain of Interpretation (DOI) is supported.
If the DOI determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID DOI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the DOI-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)
    Domain of Interpretation field : 0xffffffff (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #  Initiator(NUT)      Direction  Responder(TN)
(1)HDR;SA,KE,Ni,IDii    ========>
(2)                    <======== HDR;SA,KE,
                                Nr,IDir,HASH_R <-----DOI field :
                                                     0xffffffff(invalid value)
(3-A)HDR[*]; HASH_I    ========> X             <-----Must not transmit
        or
(3-B)HDR*; HASH(1);N/D ========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or DOI-NOT-SUPPORTED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

### 6.1.42. Processing invalid Situation field

Purpose:

Determine if the given situation can be protected. If the Situation determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SITUATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the SITUATION-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology

  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ SA Payload Format(HOST-2:Responder)

    Situation field : 0x80000000 (invalid value)
  - ✧ Initiator and Responder IKE parameter

    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                     <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)       Direction   Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
(2)                   <======== HDR; SA, KE,
                              Nr,IDir,HASH_R <-----Situation field :
                                                   0x80000000(invalid value)
(3-A)HDR[*];HASH_I    ========> X          <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-B) must not be returned (* or SITUATION-NOT-SUPPORTED message(3-A) is returned).
*option :if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

## 6.1.43. Processing invalid proposal(Encryption Algorithm)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 65000 | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology". For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)        Direction   Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                        <======== HDR;SA,KE,
                                     Nr,IDir,HASH_R <-----Invalid proposal
(3-A)HDR[*]; HASH_I        ========> X              <-----Must not transmit
        or
(3-B)HDR*; HASH(1); N/D    ========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

## 6.1.44. Processing invalid proposal(Hash Algorithm)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | 65000 | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)        Direction     Responder(TN)
(1) HDR;SA,KE,Ni,IDii     ========>
(2)                      <========     HDR; SA, KE,
                                       Nr, IDir, HASH_R <-----Invalid proposal
 (3-A)HDR[*]; HASH_I      ========> X                   <-----Must not transmit
         or
(3-B)HDR*; HASH(1); N/D ========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

## 6.1.45. Processing invalid proposal(Authentication method)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | 65000 | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)        Direction   Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                       <========  HDR; SA, KE,
                                      Nr, IDir, HASH_R <-----Invalid proposal
(3-A)HDR[*]; HASH_I        ========> X                <-----Must not transmit
        or
(3-B)HDR*; HASH(1); N/D    ========>
     (HDR; N/D)
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

### 6.1.46. Processing invalid proposal(Diffie-Hellman Group)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 32767 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)         Direction    Responder(TN)
(1)  HDR; SA, KE, Ni, IDii =========>
(2)                         <=========   HDR; SA, KE,
                                         Nr, IDir, HASH_R <-----Invalid proposal
(3-A)HDR[*]; HASH_I         =========> X                 <-----Must not transmit
         or
(3-B)HDR*; HASH(1); N/D     =========>
     (HDR; N/D)
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

## 6.1.47. Processing invalid proposal(Life Type)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ SA attribute(HOST-2:Responder, In Phase II)
  Life Type : 65000 (invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)        Direction   Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                        <========  HDR; SA, KE,
                                      Nr, IDir, HASH_R <-----Invalid proposal
(3-A)HDR[*]; HASH_I       ========> X                 <-----Must not transmit
        or
(3-B)HDR*; HASH(1); N/D    ========>
     (HDR; N/D)
              Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third(3-A) message must not be returned (* or NO-PROPOSAL-CHOSEN(3-B) message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

### 6.1.48. Processing invalid protocol-ID field

Purpose:

Determine if the Protocol is supported. If the Protocol-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID PROTOCOL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PROTOCOL-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Responder)
    **Protocol-ID field : 248** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)    Direction   Responder(TN)
(1) HDR;A,KE,Ni,IDii    ========>
(2)                     <======== HDR; SA, KE,
                                  Nr, IDir, HASH_R<-----Protocol-ID field : 248
                                                              (invalid value)
(3-A)HDR[*]; HASH_I     ========> X               <-----Must not transmit
          or
(3-B)HDR*; HASH(1); N/D ========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-PROTOCOL-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.5 Proposal Payload Processing

## 6.1.49. Processing invalid SPI field

Purpose:

Determine if the SPI is valid. If the SPI is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID SPI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SPI message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Responder)
    SPI field : SPI value is set as 1 (not same as cookie value, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                     <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)         Direction   Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <======== HDR; SA, KE,
                                    Nr, IDir, HASH_R <-----SPI field : 1
                                                           (invalid value)
(3-A)HDR[*]; HASH_I         ========> X              <-----Must not transmit
         or
(3-B)HDR*; HASH(1); N/D     ========>
     (HDR; N/D)
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-SPI message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.5 Proposal Payload Processing

## 6.1.50. Processing invalid proposal

Purpose:

Ensure the Proposals are presented according to the details given in section 3.5 and 4.2. If the proposals are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID PROPOSAL, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Proposal Payload Format(HOST-2:Responder)
  **Number of Transforms field** : **0**(invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
#   Initiator(NUT)    Direction  Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
(2)                  <========HDR; SA, KE,
                              Nr,IDir,HASH_R <-----Number of Transforms field:0
                                                          (invalid value)
(3-A)HDR[*]; HASH_I   ========> X          <-----Must not transmit
        or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
               Judgement (Check *1)
```

1. Receive the first message from NUT  
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN  
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT  
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**  
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned(*or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.5 Proposal Payload Processing

## 6.1.51. Processing invalid Transform-ID field

Purpose:

Determine if the Transform is supported. If the Transform-ID field contains an unknown or unsupported value, then that Transform payload MUST be ignored and MUST NOT cause the generation of an INVALID TRANSFORM event. If the Transform-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID TRANSFORM, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-TRANSFORM-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Responder)
    Transform-ID field : 248(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #  Initiator(NUT)   Direction   Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
(2)                  <========  HDR; SA, KE,
                                Nr, IDir, HASH_R <-----Transform-ID field : 248
                                                              (invalid value)
(3-A)HDR[*]; HASH_I   ========> X             <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**

  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-TRANSFORM-ID message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.6 Transform Payload Processing

## 6.1.52. Processing invalid Transform Payload

Purpose:

Ensure the Transforms are presented according to the details given in section 3.6 and 4.2. If the transforms are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID TRANSFORM, INVALID ATTRIBUTES, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Responder)
    SA Attributes field : not set (see below)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | | | | | | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)   Direction   Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
(2)                   <======== HDR; SA, KE,
                                Nr, IDir, HASH_R <-----SA Attributes field :
                                                          not set(invalid)
(3-A)HDR[*]; HASH_I   ========> X                <-----Must not transmit
         or
(3-B)HDR*; HASH(1); N/D ========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned(* or BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message(3-B) is returned).

*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.6 Transform Payload Processing

## 6.1.53. Multiple Transform Payloads check(modify proposal)

Purpose:

- If the initiator of an exchange notices that attribute values have changed or attributes have been added or deleted from an offer made, that response MUST be rejected.
- The initiator MUST verify that the Security Association payload received from the responder matches one of the proposals sent initially.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Initiator and Responder IKE parameter
  Any attribute is acceptable as proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Trans #** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 1 | DES | MD5 | pre-shared key | 2 | 8 Hour | NUT addr |
| | | | | | | 3DES | SHA | pre-shared key | 2 | 8 Hour | |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | | 65000 | 65000 | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)    Direction    Responder(TN)
(1)HDR;SA,KE,Ni,IDii========>
(2)                 <========   HDR; SA, KE,
                                Nr, IDir, HASH_R <-----modify proposal(invalid)
(3)HDR[*];HASH_I     ========> X                 <-----Must not transmit
                  Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function)

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned.

**References:**

RFC2408 : 4.2 Security Association Establishment
RFC2409 : 5. Exchanges

### 6.1.54. Processing invalid Key Exchange Data field

Purpose:

Determine if the Key Exchange is supported. If the Key Exchange determination fails,the message is discarded and the following actions are taken:

(a) The event, INVALID KEY INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-KEY-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

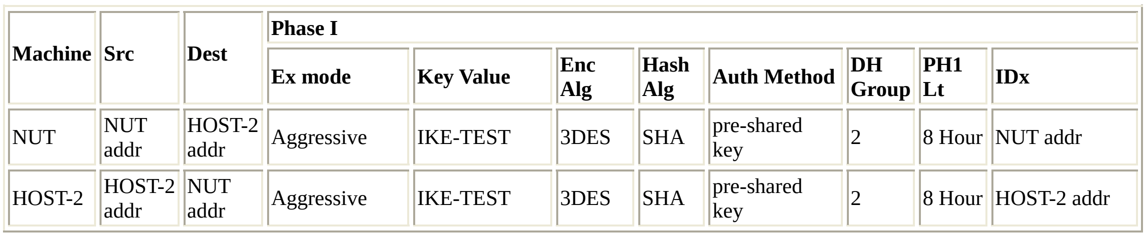
Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Key Exchange Payload Format(HOST-2:Responder)
  **Key Exchange Data field : 0(1byte)**(invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.



| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

### Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)   Direction  Responder(TN)
(1)HDR;SA,KE,Ni,IDii  ========>
(2)                   <======== HDR; SA, KE,
                                Nr,IDir,HASH_R<-----Key Exchange Data field: 0
                                                          (1byte)(invalid)
 (3-A)HDR[*]; HASH_I    ========> X           <-----Must not transmit
        or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

### Judgment:

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-KEY-INFORMATION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.7 Key Exchange Payload Processing

## 6.1.55. Processing invalid ID type field

Purpose:

Determine if the Identification Type is supported. This may be based on the DOI and Situation. If the Identification determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ID INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-ID-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Identification Payload Format(HOST-2:Responder)
    ID Type field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)       Direction      Responder(TN)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                     <========  HDR; SA, KE,
                                   Nr, IDir, HASH_R <-----ID Type field : 248
                                                           (invalid value)
(3-A)HDR[*]; HASH_I        ========> X               <-----Must not transmit
          or
(3-B)HDR*; HASH(1); N/D    ========>
     (HDR; N/D)
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-ID-INFORMATION message(3-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.8 Identification Payload Processing

## 6.1.56. Not include Identification Payload

Purpose:

All IPSEC DOI implementations MUST support SIT_IDENTITY_ONLY by including an Identification Payload in at least one of the Phase I Oakley exchanges and MUST abort any association setup that does not include an Identification Payload.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Responder(TN) does not send ID payload by the the second message.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

    For abbr., refer "Configuration Table" part in Chapter "Terminology".
    For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)    Direction   Responder(TN)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                  <======== HDR; SA, KE,
                               r,HASH_R <-----not include ID payload(invalid)
(3)HDR[*]; HASH_I     ========> X       <-----Must not transmit
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3) must not be returned.

**References:**

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY

### 6.1.57. Invalid Identification Payload receive

Purpose:

During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500. If an implementation receives any other values, this MUST be treated as an error and the security association setup MUST be aborted.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  ✧ Responder(TN)'s ID port fields of ID payload is set to 300. (invalid value)

  ✧ Responder(TN)'s protocol fields of ID payload is set to TCP. (invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

  For abbr., refer "Configuration Table" part in Chapter "Terminology".
  For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)     Direction    Responder(TN)
(1)HDR;SA,KE,Ni,IDii  ========>
(2)                   <========    HDR; SA, KE,
                                   Nr,IDir,HASH_R <----ID protocol/port:TCP/300
                                                               (invalid value)
 (3) HDR[*]; HASH_I    ========> X             <-----Must not transmit
                Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Receive the third message from NUT
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3) must not be returned.

**References:**

RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 5.8 Identification Payload Processing

## 6.1.58. Processing invalid Hash Payload

Purpose:

Determine if the Hash is supported. If the Hash determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-HASH-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Hash Payload Format(HOST-2:Responder)
    Hash Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #  Initiator(NUT)     Direction   Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
(2)                   <======== HDR; SA, KE,
                               Nr,IDir,HASH_R <----Hash Data field:not include
                                                          this field (invalid)
(3-A)HDR[*]; HASH_I   ========> X             <-----Must not transmit
        or
(3-B)HDR*; HASH(1);N/D ========>
     (HDR; N/D)
                 Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message(3-A) must not be returned (* or INVALID-HASH-INFORMATION message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.11 Hash Payload Processing

## 6.1.59. Processing invalid Hash Data field

Purpose:

Perform the Hash function as outlined in the DOI and/or Key Exchange protocol documents. If the Hash function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Hash Payload Format(HOST-2:Responder)
    Hash Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #  Initiator(NUT)    Direction  Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
(2)                  <======== HDR; SA, KE,
                              Nr,IDir,HASH_R <----Hash Data field : 0 (invalid)
(3-A)HDR[*]; HASH_I   ========> X           <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D  ========>
     (HDR; N/D)
               Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message must not be returned (* or AUTHENTICATION-FAILED message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.11 Hash Payload Processing

## 6.1.60. Processing invalid Signature Payload

Purpose:

Determine if the Signature is supported. If the Signature determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SIGNATURE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key.
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Responder)
    Signature Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
(1) HDR;SA,KE,Ni,IDii    ========>
(2)                      <========  HDR; SA, KE, Nr,
                                   IDir, SIG_R <-----Signature Data field : not
                                                    include this field(invalid)
(3-A)HDR[*]; SIG_I       ========> X           <-----Must not transmit
          or
(3-B)HDR*; HASH(1); N/D ========>
      (HDR; N/D)
                          Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message must not be returned (* or INVALID-SIGNATURE message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.12 Signature Payload Processing

## 6.1.61. Processing invalid Signature Data field

Purpose:

Perform the Signature function as outlined in the DOI and/or Key Exchange protocol documents. If the Signature function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Responder)
    Signature Data field : 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- **Pre-Sequence**
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
(1)HDR;SA,KE,Ni,IDii========>
(2)                   <========HDR;SA,KE,Nr,
                                IDir,SIG_R <-----Signature Data field:0(invalid)
(3-A)HDR[*]; SIG_I  ========> X         <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D========>
     (HDR; N/D)
                           Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message must not be accepted. And the third message must not be returned (* or AUTHENTICATION-FAILED message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.12 Signature Payload Processing

## 6.1.62. Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Responder)
    **Cert Encoding Type fild: 255** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 # Initiator(NUT)     Direction    Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
     CERT Req
(2)                    <======== HDR;SA,KE,Nr,IDir,SIG_R
                                  CERT, CERT Req <-----Cert Encoding Type fild
                                                 (CERT Req): 255(invalid)
(3-A)HDR[*];SIG_I,CERT========> X              <-----Must not transmit
        or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
                         Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the responder send Certificate and Certificate Request Payload

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message must not be returned (* or INVALID-CERT-ENCODING message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

## 6.1.63. Processing invalid Certificate Authority field

Purpose:

Determine if the Certificate Authority is supported for the specified Certificate Encoding. If the Certificate Authority is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE AUTHORITY, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-AUTHORITY message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Responder)
    **Certificate Authority field: 0** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 add |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #  Initiator(NUT)     Direction  Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
     CERT Req
(2)                   <======== HDR;SA,KE,Nr,IDir,SIG_R
                                CERT, CERT Req   <-----Cert Data field
                                                       (CERT Req): 0(invalid)
(3-A)HDR[*];SIG_I,CERT ========> X               <-----Must not transmit
        or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
                         Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information. And the initiator send Certificate Request Payload.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the responder send Certificate and Certificate Request Payload

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message must not be returned (* or INVALID-CERT-AUTHORITY message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.10 Certificate Request Payload Processing

## 6.1.64. Processing invalid Certificate Type with Certificate Authority

Purpose:

Process the Certificate Request. If a requested Certificate Type with the specified Certificate Authority is not available, then the payload is discarded and the following actions are taken:

(a) The event, CERTIFICATE-UNAVAILABLE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the CERTIFICATE-UNAVAILABLE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Responder)
    **Certificate Authority field: Distinguish Name**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #  Initiator(NUT)   Direction   Responder(TN)
(1)HDR;SA,KE,Ni,IDii========>
     CERT Req
(2)                    <========HDR;SA,KE,Nr,IDir,SIG_R
                                 CERT,CERT Req    <---Certificate Data field
                                                      (CERT Req):The value
                                                     which is not available
                                                     for Certificate Authority
 (3-A)HDR[*];SIG_I,CERT========>X             <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
                           Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the responder send Certificate and Certificate Request Payload

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment**:

The second message must not be accepted. And the third message(3-A) must not be returned(* or CERTIFICATE-UNAVAILABLE message(3-B) is returned).
*option : if you want to check the retruned Notify message.

**References**:

RFC2408 : 5.10 Certificate Request Payload Processing

## 6.1.65. Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is not supported, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Responder)
    **Cert Encoding field : 255**(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence

  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(NUT)   Direction  Responder(TN)
(1) HDR;SA,KE,Ni,IDii ========>
     CERT Req
(2)                  <======== HDR;SA,KE,Nr,IDir,SIG_R
                               CERT, CERT Req       <----Cert Encoding field
                                                        (CERT) : 255(invalid)
(3-A)HDR[*];SIG_I,CERT ========> X                  <-----Must not transmit
        or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
                        Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.

2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the responder send Certificate and Certificate Request Payload

3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message must not be returned (* or INVALID-CERT-ENCODING message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC 2408: 5.9 Certificate Payload Processing

## 6.1.66. Processing invalid Certificate Data field

Purpose:

Process the Certificate Data field. If the Certificate Data is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERTIFICATE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
 Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 1 Topology for End-Node vs. End-Node".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Responder)
    **Certificate Data field : 0** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
#   Initiator(NUT)  Direction   Responder(TN)
(1) HDR;SA,KE,Ni,IDii========>
     CERT Req
(2)                 <========HDR;SA,KE,Nr,IDir,SIG_R
                             CERT, CERT Req <----Certificate Encoding field
                                                         (CERT) : 0 (invalid)
(3-A)HDR[*];SIG_I,CERT========>X            <-----Must not transmit
         or
(3-B)HDR*;HASH(1);N/D ========>
     (HDR; N/D)
                        Judgement (Check *1)
```

1. Receive the first message from NUT
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.And the initiator send Certificate Request Payload.
2. Send the second message from TN
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the responder send Certificate and Certificate Request Payload
3. Receive the third message from NUT
   In the third message (3-B), the initiator indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination

  Clean up SAD and SPD

Judgment:

The second message must not be accepted. And the third message must not be returned (* or INVALID-CERTIFICATE message is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.9 Certificate Payload Processing

### 6.2.1 Position of payload

Purpose:

The SA payload MUST precede all other payloads in a phase 1 exchange.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

- Pre-Sequence
  In order to start the negotiation of IKE,
  NUT transmits Echo Request to TN(HOST-2).

Procedure:

This test check is following.

```
 * PHASE I
                    <AGGRESSIVE EXCHANGE>
#   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii =======>
```

```
(2)                        <========       HDR; SA, KE, Nr, IDir, HASH_R
                        Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

**Judgment:**

The second message which has correct position of payload must be received (The SA payload MUST precede all other payloads).
And must conform to above Configuration.

**References:**

RFC2409

## 6.2.2 ISAKMP Header format

Purpose:

ISAKMP Header Format

- Cookie field
  The cookies MUST NOT swap places when the direction of the ISAKMP SA changes.
  (The cookie must be set to Responder cookie field.)
- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
  (In this test, this field is set as 1(Security Association Payload).)
- Version field
  Major Version 1
  Minor Version 0
- Exchange Type
  indicates the type of exchange being used.
  (In this test, this field is set as 4(aggressive mode).)
- Flags field
  Bits of the Flags field(except E,C,A bit) MUST be set to 0 prior to transmission.
  |0|0|0|0|0|A|C|E|
- Message ID field
  During Phase 1 negotiations, the value MUST be set to 0.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology". For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                         Judgement (Check *1)
```

1. Send the first message from TN  
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT  
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- Termination  
  Clean up SAD and SPD

Judgment:

The first message must be accepted. And the second message's ISAKMP Header Format must be base on description of RFC(see above Verification Points).

(cookie is set to Responder cookie filed, Major version=1 and Minor version=0 , Flags field is correct and Message ID=0).

**References:**

RFC2408   3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing
RFC2409 : 4. Introduction

### 6.2.3 Security Association Payload format

Purpose:

SA Payload Format

- Next Payload field
  This field MUST NOT contain the values for the Proposal(2) or Transform(3) payload. Place the value of the Next Payload in the Next Payload field. (In this test, this field is set as 0).
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0). Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Domain of Interpretation field
  This field MUST be present within the Sercurity Association payload. (In this test, this field is set as 1(IPsec DOI).)
- Situation field
  This field MUST be present within the Sercurity Association payload. Implementations MUST support SIT_IDENTITY_ONLY. (In this test, this field is set as 1(SIT_IDENTITY_ONLY).)

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, HASH_R
                         Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Security Association Payload Format must be base on description of RFC(see above Verification Points).

**References:**

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY
RFC2408 : 2.5.2 RESERVED Fields
3.4 Security Association Payload
5.3 Generic Payload Header Processing
5.4 Security Association Payload Processing

### 6.2.4 Proposal Payload format

Purpose:

Proposal Payload Format

- Next Payload field
  This field MUST only contain the value "2" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In Phase I, this field only contain the value "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Proposal Number field
  Identifies the Proposal number for the current payload.
  (In Phase I, this field contain the value "1".)
- Protocol-ID field
  All implementations within the IPSEC DOI MUST support PROTO_ISAKMP.
- SPI size field
  Length in octets of the SPI as defined by the Protocol-Id.
- Number of Transforms field
  Specifies the number of transforms for the Proposal.
  (In this test, this field contain the value "1".)
- SPI field
  The sending entity's SPI.
  (In Phase I, this field is redundant and MAY be set to 0 or it MAY contain the transmitting entity's cookie.)

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                          <========       HDR; SA, KE, Nr, IDir, HASH_R
                          Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Proposal Payload Format must be base on description of RFC(see above Verification Points).

**References:**

RFC2407 : 4.4.1.1 PROTO_ISAKMP
RFC2408 : 2.5.2 RESERVED Fields
          3.5 Proposal Payload
          5.3 Generic Payload Header Processing
          5.5 Proposal Payload Processing

### 6.2.5 Transform Payload format

Purpose:

Transform Payload Format

- Next Payload field
  This field MUST only contain the value "3" or "0".
  Place the value of the Next Payload in the Next Payload field.
  (In responder, this field only contain the value "0").
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Transform Number field
  Identifies the Transform number for the current payload.
  (In this test, this field is set as "1".)
- Transform-ID field
  All implementations within the IPSEC DOI MUST support KEY_IKE.
  (In Phase I, this field only contain "1"(KEY_IKE))

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                          Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Transform Payload Format must be base on description of RFC(see above Verification Points).

**References:**

RFC2407 : 4.4.2.1 KEY_IKE
RFC2408 : 2.5.2 RESERVED Fields
          3.6 Transform Payload
          5.3 Generic Payload Header Processing
          5.6 Transform Payload Processing

## 6.2.6 Transform payload SA Attributes (DES,MD5,PSK,DH1)

Purpose:

IKE implementations MUST support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - DES in CBC mode<br>- MD5<br>- Authentication via pre-shared keys.<br>- MODP over default group number one. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DES-CBC,MD5,DH1)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | DES | MD5 | pre-shared key | 1 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | DES | MD5 | pre-shared key | 1 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                           Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(DES:1,MD5:1,PSK:1,DH1:1) must be correct.
And must conform to above Configuration.

**References:**

RFC2409 : 4. Introduction

## 6.2.7 Transform payload SA Attributes (DES,SHA,PSK,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DES-CBC)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | DES | SPROTO_IPSEC_AH | pre-shared key | 2 | 8 Hour | HOST-2 addr |

| Machine | Src | Dest | Phase II | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | Proto ID | Trans ID | Mode | Auth Alg | PH2 Lt | Upper |
| NUT | NUT addr | HOST-2 addr | PROTO_IPSEC_ESP | ESP_3DES | Transport | HMAC-SHA | 8 Hour | any |
| HOST-2 | HOST-2 addr | NUT addr | PROTO_IPSEC_ESP | SHA | Transport | HMAC-SHA | 8 Hour | any |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                        Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(DES:1,SHA:2,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

**References:**

RFC2409: 4.Introduction

### 6.2.8 Transform payload SA Attributes (AES-128,SHA,PSK,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - AES-128 in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support AES-CBC)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | AES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | AES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #    Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                          <========       HDR; SA, KE, Nr, IDir, HASH_R
                            Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect againstreplay attacks is also transmitted.Additionally, the responder ransmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(AES:7,SHA:2,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

**References:**

RFC 3602: 5.  IKE Interactions
          5.1.  Phase 1 Identifier

### 6.2.9 Transform payload SA Attributes (3DES,MD5,PSK,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- MD5<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support MD5)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | MD5 | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | MD5 | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                           Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,MD5:1,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction

### 6.2.10 Transform payload SA Attributes (3DES,SHA,PSK,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, HASH_R
                         Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH2:2) must be correct.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction
          6.2 Second Oakley Group

### 6.2.11 Transform payload SA Attributes (3DES,SHA,RSA sign,DH2)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- RSA signatures.<br>- MODP over group number two. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, SIG_R
                          Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned. The second message Attributes(3DES:1,SHA:2,RSA sign:3,DH2:2) must be correct. And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction

## 6.2.12 Transform payload SA Attributes (3DES, SHA, PSK, DH1)

Purpose:

IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over default group number one. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH1)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 1 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 1 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, HASH_R
                          Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH1:1) must be correct.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction
          6.1 First Oakley Default Group

## 6.2.13 Transform payload SA Attributes (3DES, SHA, PSK, DH5)

Purpose:

IKE implementations support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number five. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH5)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 5 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 5 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, HASH_R
                         Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH5:5) must be correct.
And must conform to above Configuration.

**References:**

RFC2409 : 4.Introduction
RFC3526 : 2.  1536-bit MODP Group

### 6.2.14 Transform payload SA Attributes (3DES, SHA, PSK, DH14)

Purpose:

IKE implementations support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number fourteen. |

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH14)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 14 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 14 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                        Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message must be returned.
The second message Attributes(3DES:5,SHA:2,PSK:1,DH14:14) must be correct.
And must conform to above Configuration.

**References:**

RFC 2409: 4.Introduction

## 6.2.15 Multiple Transform Payloads (Select proposal)

Purpose:

- An initiator MAY provide multiple proposals for negotiation; a responder MUST reply with only one
- The responder SHOULD retain the Proposal # field in the Proposal payload and the Transform # field in each Transform payload of the selected Proposal.
- IKE implementations SHOULD support the following attribute values

| Parameter | | Value |
|---|---|---|
| ISAKMP | SA Attributes | - 3DES in CBC mode<br>- SHA<br>- Authentication via pre-shared keys.<br>- MODP over group number two. |

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Trans # | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 1 | 65001 | 65001 | 65001 | 2 | 8 Hour | HOST-2 addr |
| | | | | | 2 | 3DES | SHA | pre-shared key | 2 | 8 Hour | |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
#   Initiator(TN)         Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                        Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted. And the second message that has only one proposal(3DES:5,SHA:2,PSK:1,DH2:2) and Transform # field = 2 must be returned. And must conform to above Configuration.

**References:**

RFC2408 : 4.1.1 Notation
          4.2 Security Association Establishment
RFC2409 : 3.2 Notation
          7.1 Phase 1 using Main Mode

## 6.2.16 Key Exchange Payload Format (DH1)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 768 bit)

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH1)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 1 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 1 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #    Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                          <========        HDR; SA, KE, Nr, IDir, HASH_R
                          Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protectionsuite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

## 6.2.17 Key Exchange Payload Format (DH2)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1024 bit)

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
#   Initiator(TN)           Direction        Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                          Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

### 6.2.18 Key Exchange Payload Format (DH5)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 1536 bit)

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH5)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 5 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 5 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #    Initiator(TN)         Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                         Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
          5.7 Key Exchange Payload Processing
RFC2409 : 5. Exchanges

## 6.2.19 Key Exchange Payload Format check(DH14)

Purpose:

KE Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Key Exchange Data field
  The Diffie-Hellman public value passed in a KE payload MUST be the length of the negotiated Diffie-Hellman group enforced.
  (In this test, this field length must be 2048 bit)

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support DH14)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 14 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 14 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                    <AGGRESSIVE EXCHANGE>
 #    Initiator(TN)          Direction       Responder(NUT)
(1)   HDR; SA, KE, Ni, IDii ========>
(2)                          <========       HDR; SA, KE, Nr, IDir, HASH_R
                      Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation.  The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Key Exchange Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

**References:**

RFC2408: 5.3 Generic Payload Header Processing
         5.7 Key Exchange Payload Processing
RFC2409: 5. Exchanges

### 6.2.20 Nonce Payload Format

Purpose:

Nonce Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Nonce Data field
  The length of nonce payload MUST be between 8 and 256 bytes inclusive.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                          Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's Nonce Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
          5.13 Nonce Payload Processing
RFC2409 : 5. Exchanges

## 6.2.21 Identification Payload FormatＰ

**Purpose:**

ID Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Identification Type field
  Value describing the identity information found in the Identification Data field.(In this test, this field is set as 5(ID_IPV6_ADDR).)
- Protocol ID field
  Value specifying an associated IP protocol ID (e.g. UDP/TCP)
- Port ID field
  Value specifying an associated port.
- Identification Data field
  Value, as indicated by the Identification Type.
  (In this test, this value is NUT IPv6 address.)
- During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500.

**Category:**

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

**Initialization:**

- **Network Topology**
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- **Configuration**
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, HASH_R
                           Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

Judgment:

The first message must be accepted.
And the second message's Identification Payload must be base on description of

RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2407 : 4.6.2 Identification Payload Content
RFC2408 : 3.8 Identification Payload
          5.3 Generic Payload Header Processing
          5.8 Identification Payload Processing

## 6.2.22 HASH Payload Format

Purpose:

HASH Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Hash Data field
  Data that results from applying the hash routine to the ISAKMP message and/or state.(HASH_R =prf(SKEYID,g^xr|g^xi|CKY-R|CKY-I|SAi_b|IDir_b))

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========       HDR; SA, KE, Nr, IDir, HASH_R
                         Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect againstreplay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must be accepted.
And the second message's HASH Payload must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing
          5.11 Hash Payload Processing

### 6.2.23 Implementation of Aggressive Mode with pre-shared key

Purpose:

Implementation of Aggressive Mode with pre-shared key check.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)           Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii  ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, HASH_R
                  Judgement (Check *1)
(3)  HDR[*]; HASH_I         ========>
```

1. Send the first message from TN

In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Send the third message from TN
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

＊ PHASE II

```
                         <QUICK MODE>
 #    Initiator(TN)       Direction       Responder(NUT)
(1)  HDR*, HASH(1),
           SA, Ni         ========>
(2)                       <========       HDR*, HASH(2), SA, Nr
                Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.
   HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

In Phase I, the first to the third message must be exchanged correctly.
 Check *1
 Security Association, Key Exchange, Nonce, Identification, Hash Payload
 Format must be base on description of RFC.
And ISAKMP SA must be established.
In Phase II,the first message must be accepted.
And the second message is returned.
 Check *2
 NUT must send second message with ISAKMP SA.
And must conform to above Configuration.

**References:**

RFC2409 : 4. Introduction
 5. Exchanges

## 6.2.24 cookie field

Purpose:

There is no relationship between the two SAs and the initiator and responder cookie pairs SHOULD be different.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 60 sec | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 60 sec | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

```
  This test check is following.
           <the first AGGRESSIVE EXCHANGE>
 # Initiator(TN)    Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>
(2)                    <========HDR;SA,KE,Nr,IDir,HASH_R<---- #1:responder cookie
(3)  HDR[*]; HASH_I ========>
                          Judgement (Check *1)
```

1. Send the first message from TN

In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted. Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Send the third message from TN
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

10sec after the first AGGRESSIVE EXCHANGE,
negotiation of IKE(the second AGGRESSIVE EXCHANGE) is started.

```
           <The second AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>
(2)                 <======== HDR;SA,KE,Nr,IDir,HASH_R <---- #2:responder cookie
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted. Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

Judgment:

In the first AGGRESSIVE EXCHANGE, the first to the third message must be exchanged correctly. In the second AGGRESSIVE EXCHANGE, The first message must be accepted. And the second message's responder cookie(#2) is not same as the first AGGRESSIVE EXCHANGE's responder cookie(#1).

References:

RFC2408 : 4.3 Security Association Modification

### 6.2.25 Signature Payload Format

Purpose:

Signature Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Signature Data field
  Data that results from applying the digital signature function
  to the ISAKMP message and/or state.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".
- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, SIG_R
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

- Termination
  Clean up SAD and SPD

Judgment:

The second message's Signature Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

References:

RFC2408 : 5.3 Generic Payload Header Processing
          5.12 Signature Payload Processing

## 6.2.26 Certificate Request Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Type field
  Contains an encoding of the type of certificate requested
- Certificate Authority field
  Contains an encoding of an acceptable certificate authority for the type of certificate requested.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.
    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
     CERT Req
(2)                         <========       HDR; SA, KE, Nr, IDir, SIG_R
                                            CERT, CERT Req
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.Additionally the responder send Certificate and Certificate Request Payload

- Termination
  Clean up SAD and SPD

Judgment:

The second message's Certificate Request Payload Format must be base on description of RFC(see above Verification Points).
And must conform to above Configuration.

References:

RFC2408 : 3.10 Certificate Request Payload
          5.3 Generic Payload Header Processing
       5.10 Certificate Request Payload Processing

## 6.2.27 Certificate Payload Format

Purpose:

Certificate Request Payload Format

- Next Payload field
  Place the value of the Next Payload in the Next Payload field.
- RESERVED Fields
  All RESERVED fields in the ISAKMP protocol MUST be set to zero (0).
  Place the value zero (0) in the RESERVED field.
- Payload Length field
  Place the length (in octets) of the payload in the Payload Length field.
- Certificate Encoding field
  This field indicates the type of certificate or certificate-related information contained in theCertificate Data field.
- Certificate Data field
  Actual encoding of certificate data

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)         Direction      Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
     CERT Req
 (2)                        <========       HDR; SA, KE, Nr, IDir, SIG_R
                                           CERT, CERT Req
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information. And the initiator send Certificate Request Payload.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.Additionally the responder send Certificate and Certificate Request Payload

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The second message's Certificate Payload Format must be base on description of RFC(see above Verification Points).And must conform to above Configuration.

**References:**

RFC2408 : 3.9 Certificate Payload
5.3 Generic Payload Header Processing
5.9 Certificate Payload Processing

## 6.2.28 Implementation of Aggressive Mode with RSA signatures

Purpose:

Implementation of Aggressive Mode with RSA signatures check.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)          Direction       Responder(NUT)
(1)  HDR; SA, KE, Ni, IDii ========>
(2)                         <========        HDR; SA, KE, Nr, IDir, SIG_R
                  Judgement (Check *1)
(3)  HDR[*]; SIG_I          ========>
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.
3. Send the third message from TN
   In the third (3) message, the initiator send the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
           SA, Ni       ========>
(2)                     <========       HDR*, HASH(2), SA, Nr
                  Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1)

is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.
   HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first to the third message must be exchanged correctly.
  Check *1
      Security Association, Key Exchange, Nonce, Identification, Signature Payload Format must be base on description of RFC.
And ISAKMP SA must be established.
In Phase II,the first message must be accepted.
And the second message is returned.
  Check *2
      NUT must send second message with ISAKMP SA.
And must conform to above Configuration.

**References:**

RFC2409 : 4. Introduction
          5. Exchanges

## 6.2.29 Processing invalid ISAKMP Payload Length field

Purpose:

If the ISAKMP message length and the value in the Payload Length field of the ISAKMP Header are not the same, then the ISAKMP message MUST be rejected. The receiving entity (initiator or responder) MUST do the following:

1. The event, UNEQUAL PAYLOAD LENGTHS, MAY be logged in the appropriate system audit file.
2. An Informational Exchange with a Notification payload containing the UNEQUAL-PAYLOAD-LENGTHS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Length field = 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction   Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                    <-----Length field
                                                      (ISAKMP header):0(invalid)
(2-A)               X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                    or
(2-B)                <======== HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or UNEQUAL-PAYLOAD-LENGTHS message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC 2408: 5.1 General Message Processing

## 6.2.30 Processing invalid Initiator Cookie field

Purpose:

Verify the Initiator and Responder "cookies". If the cookie validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID COOKIE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-COOKIE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    In TEST PROCEDURE, Initiator Cookie field of the third message of AGGRESSIVE EXCHANGE is set to 0(not same the first message's initiator cookie).
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction   Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                 <======== HDR;SA,KE,Nr,IDir,HASH_R
(3)HDR[*]; HASH_I    ========>                   <-----Cookie field : 0
                                                       (invalid(not same
(4)                 <========HDR*;HASH(1);N/D           as the first
                              (HDR; N/D)               message(1)'s cookie))
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Send the third message from TN
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

4. Receive the fourth message from NUT
   In the second message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

```
 * PHASE II
                        <QUICK MODE>
 #   Initiator(TN)    Direction     Responder(NUT)
(1)  HDR*, HASH(1),
           SA, Ni      ========>
(2)                 X <========  HDR*, HASH(2), SA, Nr  <-----Must not transmit
               Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

In AGGRESSIVE EXCHANGE, the first to the second message must be exchanged correctly.The third message must not be accepted. And must not establish ISAKMP SA(In QUICK MODE, the second message must not transmit) (* or INVALID-COOKIE message(4) may be returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

### 6.2.31 Processing invalid Next Payload field

Purpose:

Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Next Payload field = 127(invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)   Direction  Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>              <-----Next Payload field
                                              (ISAKMP Header) : 127(invalid)
(2-A)              X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                  or
(2-B)               <======== HDR; N/D
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-PAYLOAD-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

## 6.2.32 Processing invalid Major Version field (major 15,minor 0)

Purpose:

- Implementation SHOULD never accept packets with a major version number larger than its own.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Major Version 15 (invalid value)
    Minor Version 0
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology". For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)    Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                       <-----Major Version : 15
                                                                    (invalid)
(2-A)            X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                   or
(2-B)              <========  HDR; N/D
                        Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-MAJOR-VERSION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

### 6.2.33 Processing invalid Minor Version field (major 1,minor 15)

Purpose:

- Implementation SHOULD never accept packets with a minor version number larger than its own, given the major version numbers are identical.
- Check the Major and Minor Version fields to confirm they are correct (see section 3.1). If the Version field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ISAKMP VERSION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-MAJOR-VERSION or INVALID-MINOR-VERSION message type MAY be sent to the transmitting entity.
This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    **Major Version 1**
    **Minor Version 15** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)     Direction   Responder(NUT)
(1) HDR;SA,KE,Ni,IDii ========>                         <-----Minor Version :
                                                                  15(invalid)
(2-A)               X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                      or
(2-B)                <======== HDR; N/D
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-MINOR-VERSION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.1 ISAKMP Header Format
          5.2 ISAKMP Header Processing

## 6.2.34 Processing invalid Exchange Type field

Purpose:

Check the Exchange Type field to confirm it is valid. If the Exchange Type field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID EXCHANGE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-EXCHANGE-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- **Configuration**
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    **Exchange Type field = 31** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #  Initiator(TN)    Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                      <-----Exchange Type field :
                                                                 31 (invalid)
(2-A)              X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                 or
(2-B)               <======== HDR; N/D
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-EXCHANGE-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

## 6.2.35 Processing invalid Flags field

Purpose:

Check the Flags field to ensure it contains correct values. If the Flags field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID FLAGS, MAY be logged in the appropriate systemaudit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-FLAGS message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    Flags field = |1|1|1|1|1|0|0|0| (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure**:

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction   Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                        <-----Flags field :
                                                            |1|1|1|1|1|0|0|0|
                                                              (invalid value)
(2-A)               X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                or
(2-B)                 <======== HDR; N/D
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment**:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-FLAGS message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References**:

RFC 2408: 5.2 ISAKMP Header Processing

## 6.2.36 Processing invalid Message ID field

Purpose:

Check the Message ID field to ensure it contains correct values.
If the Message ID validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID MESSAGE ID, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-MESSAGE-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ ISAKMP Header Format(HOST-2:Initiator)
    **Message ID field = 1** (set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction      Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                        <-----Message ID field : 1
                                                              (invalid value)
(2-A)             X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                        or
(2-B)              <========  HDR; N/D
               Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-MESSAGE-ID message(2-B) is returned).

**References:**

RFC2408 : 5.2 ISAKMP Header Processing

## 6.2.37 Processing invalid Next Payload field

Purpose:

- If the Next Payload field validation fails, the message is discarded.
- Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

(a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    **Next Payload field : 127** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
# Initiator(TN)       Direction    Responder(NUT)
(1) HDR;SA,KE,Ni,IDii========>                        <-----Next Payload field:
                                                        127(SA,invalid value)
(2-A)               X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                      or
(2-B)                <======== HDR; N/D
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message must not be returned (* or INVALID-PAYLOAD-TYPE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 3.4 Security Association Payload
          5.3 Generic Payload Header Processing

## 6.2.38 Processing invalid RESERVED field

Purpose:

Verify the RESERVED field contains the value zero. If the value in the RESERVED field is not zero, the message is discarded and the following actions are taken:

(a) The event, INVALID RESERVED FIELD, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMEDmessage type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    **RESERVED field** : 1 (set to not zero, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology". For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                  <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction   Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                           <-----RESERVED field:
                                                           1(SA, invalid value)
(2-A)              X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                        or
(2-B)               <======== HDR; N/D
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(2-B) is returned).*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.3 Generic Payload Header Processing

## 6.2.39 Processing invalid Next Payload field

Purpose:

- This field MUST NOT contain the values for the Proposal or Transform payloads as they are considered part of the security association negotiation.
- If the Next Payload field validation fails, the message is discarded.
- Check the Next Payload field to confirm it is valid. If the Next Payload field validation fails, the message is discarded and the following actions are taken:

  (a) The event, INVALID NEXT PAYLOAD, MAY be logged in the appropriate system audit file.

  (b) An Informational Exchange with a Notification payload containing the INVALID-PAYLOAD-TYPE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    **Next Payload field : 2** (Proposal Payload, invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction     Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                    <-----Next Payload field(SA):
                                                                2(invalid value)
(2-A)              X<========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                       or
(2-B)               <======== HDR; N/D
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message must not be returned or INVALID-PAYLOAD-TYPE message(2-B) is returned.

**References:**

RFC2408 : 3.4 Security Association Payload
          5.3 Generic Payload Header Processing

## 6.2.40 Processing invalid DOI field

Purpose:

Determine if the Domain of Interpretation (DOI) is supported. If the DOI determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID DOI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the DOI-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ SA Payload Format(HOST-2:Initiator)
  Domain of Interpretation field : 0xffffffff (invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology". For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)   Direction      Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                        <-----DOI field :
                                                        0xffffffff(invalid value)
(2-A)              X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                         or
(2-B)               <========  HDR; N/D
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or DOI-NOT-SUPPORTED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

## 6.2.41 Processing invalid Situation field

Purpose:

Determine if the given situation can be protected. If the Situation determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SITUATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the SITUATION-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    Situation field : 0x80000000 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)    Direction   Responder(NUT)
(1) HDR;SA,KE,Ni,IDii ========>                    <-----Situation field :
                                                      0x80000000(invalid value)
(2-A)                X<======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                       or
(2-B)                 <========  HDR; N/D
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message (2-A) must not be returned (* or SITUATION-NOT-SUPPORTED message (2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

## 6.2.42 Processing invalid proposal (Encryption Algorithm)

**Purpose:**

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

**Category:**

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

**Initialization:**

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 65000 | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                     <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction      Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>                         <-----Invalid proposal

(2-A)              X<========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                 or
(2-B)               <========  HDR; N/D
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

## 6.2.43 Processing invalid proposal (Hash Algorithm)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted,then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | 65000 | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction       Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>                          <-----Invalid proposal
(2-A)             X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                        or
(2-B)              <========    HDR; N/D
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.4 Security Association Payload Processing

## 6.2.44 Processing invalid proposal (Authentication method)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | 65000 | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
# Initiator(TN)       Direction     Responder(NUT)
(1) HDR;SA,KE,Ni,IDii ========>                           <-----Invalid proposal

(2-A)               X<======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                     or
(2-B)                <========  HDR; N/D
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

### 6.2.45 Processing invalid proposal (Diffie-Hellman Group)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 32767 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                     <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction       Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                      <-----Invalid proposal
(2-A)              X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                   or
(2-B)               <========    HDR; N/D
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

## 6.2.46 Processing invalid proposal (Life Type)

Purpose:

Process the remaining payloads (i.e. Proposal, Transform) of the Security Association Payload. If the Security Association Proposal (as described in sections 5.5 and 5.6) is not accepted, then the following actions are taken:

(a) The event, INVALID PROPOSAL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the NO-PROPOSAL-CHOSEN message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ SA attribute(HOST-2:Initiator, In Phase II)
    Life Type : 65000 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(TN)       Direction     Responder(NUT)
(1) HDR;SA,KE,Ni,IDii ========>                          <-----Invalid proposal

(2-A)              X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                  or
(2-B)                <======== HDR; N/D
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or NO-PROPOSAL-CHOSEN message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.4 Security Association Payload Processing

## 6.2.47 IPSEC Situation Definition (SIT SECRECY)

Purpose:

If a responder does not support SIT_SECRECY, a SITUATION-NOT-SUPPORTED Notification Payload SHOULD be returned and the security association setup MUST be aborted.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    Situation : SIT_SECRECY
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction   Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>                   <-----Situation : SIT_SECRECY

(2-A)             X<========HDR;SA,KE,Nr,IDir,HASH_R<-----Must not transmit
                                or                     if NUT doesn't
(2-B)             <======== HDR; N/D                   supportsituation
                Judgement (Check *1)                   SIT_SECRECY.
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

**Judgment:**

If Responder(NUT) doesn't support situation SIT_SECRECY, then the first message must not be accepted. (* And the second message(SITUATION-NOT-SUPPORTED Notification Payload)(2-B) is returned).*option : if you want to check the retruned Notify message.

**References:**

RFC2407 : 4.2.2 SIT_SECRECY

### 6.2.48 IPSEC Situation Definition (SIT INTEGRITY)

Purpose:

If a responder does not support SIT_INTEGRITY, a SITUATION-NOT-SUPPORTED Notification Payload SHOULD be returned and the security association setup MUST be aborted.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ SA Payload Format(HOST-2:Initiator)
    Situation : SIT_INTEGRITY
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

### Procedure:

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)    Direction  Responder(NUT)
(1) HDR;SA,KE,Ni,IDii ========>                <-----Situation : SIT_INTEGRITY
(2-A)               X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                 or                           if NUT doesn't
(2-B)                <======== HDR; N/D                     supportsituation
                    Judgement (Check *1)                      SIT_INTEGRITY.
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

### Judgment:

If Responder(NUT) doesn't support situation SIT_INTEGRITY, then the first message must not be accepted. (* And the second message(SITUATION-NOT-SUPPORTED Notification Payload)(2-B) is returned).
*option : if you want to check the retruned Notify message.

### References:

RFC2407 : 4.2.3 SIT_INTEGRITY

### 6.2.49 Processing invalid Protocol-ID field

Purpose:

Determine if the Protocol is supported. If the Protocol-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID PROTOCOL, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-PROTOCOL-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Proposal Payload Format(HOST-2:Initiator)
    Protocol-ID field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

## Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)    Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                       <-----Protocol-ID field :
                                                           248 (invalid value)
(2-A)                X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                   or
(2-B)                  <========HDR; N/D
                     Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

## Judgment:

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-PROTOCOL-ID message(2-B) is returned).
*option : if you want to check the retruned Notify message.

## References:

RFC2408 : 5.5 Proposal Payload Processing

## 6.2.50 Processing invalid SPI field

Purpose:

Determine if the SPI is valid. If the SPI is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID SPI, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SPI message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

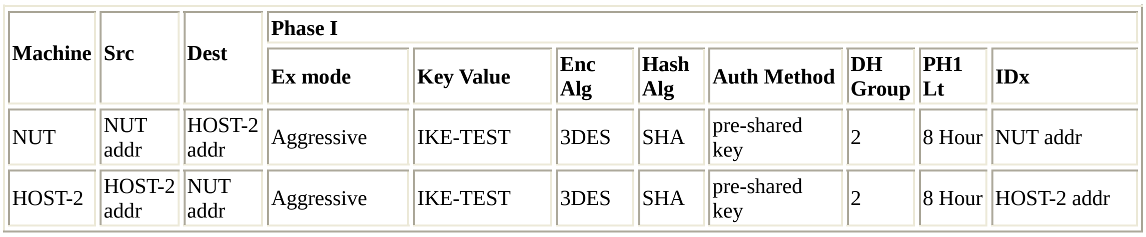
Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Proposal Payload Format(HOST-2:Initiator)
  SPI field : SPI value is set as 1 (not same cookie value, invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.



| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>                <-----SPI field : 1(invalid value)
(2-A)             X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                   or
(2-B)               <======== HDR; N/D
                  Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-SPI message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.5 Proposal Payload Processing

## 6.2.51 Processing invalid proposal

Purpose:

Ensure the Proposals are presented according to the details given in section 3.5 and 4.2. If the proposals are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID PROPOSAL, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- **Configuration**
  - ✧ Proposal Payload Format(HOST-2:Initiator)
    **Number of Transforms field : 0** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction     Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>              <-----Number of Transforms field : 0
                                                                (invalid value)
(2-A)              X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                   or
(2-B)                <========  HDR; N/D
                     Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or BAD-PROPOSAL-SYNTAX or PAYLOAD-MALFORMED message(2-B) is returned).*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.5 Proposal Payload Processing

## 6.2.52 Processing invalid Transform-ID field

Purpose:

Determine if the Transform is supported. If the Transform-ID field contains an unknown or unsupported value, then that Transform payload MUST be ignored and MUST NOT cause the generation of an INVALID TRANSFORM event. If the Transform-ID field is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID TRANSFORM, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-TRANSFORM-ID message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Transform Payload Format(HOST-2:Initiator)
    Transform-ID field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                        <-----Transform-ID field :
                                                              248(invalid value)
(2-A)              X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                       or
(2-B)                <======== HDR; N/D
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).
   Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-TRANSFORM-ID message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.6 Transform Payload Processing

## 6.2.53 Processing invalid Transform payload

Purpose:

Ensure the Transforms are presented according to the details given in section 3.6 and 4.2. If the transforms are not formed correctly, the following actions are taken:

(a) Possible events, BAD PROPOSAL SYNTAX, INVALID TRANSFORM, INVALID ATTRIBUTES, are logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Transform Payload Format(HOST-2:Initiator)
  SA Attributes field : not set (see below)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | | | | | | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction  Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>                       <-----SA Attributes field :
                                                                 not set(invalid)
(2-A)                X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                         or
(2-B)                 <========   HDR; N/D
                 Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or BAD-PROPOSAL-SYNTAX, PAYLOAD-MALFORMED or ATTRIBUTES-NOT-SUPPORTED message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.6 Transform Payload Processing

## 6.2.54 Multiple Transform Payloads check(reject proposal)

Purpose:

The receiving entity MUST select a single transform for each protocol in a proposal or reject the entire proposal.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Trans # | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 1 | 65001 | 65001 | 65001 | 32768 | 8 Hour | HOST-2 addr |
| | | | | | 2 | 65002 | 65002 | 65002 | 32768 | 8 Hour | |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(TN)     Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>                        <-----Multiple invalid
                                                           transform payloads
(2)               X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                         Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2) must not be returned.

**References:**

RFC2408 : 4.2 Security Association Establishment

## 6.2.55 Processing invalid Key Exchange Data field

Purpose:

Determine if the Key Exchange is supported. If the Key Exchange determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID KEY INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-KEY-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- **Network Topology**
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- **Configuration**
  - ✧ Key Exchange Payload Format(HOST-2:Initiator)
    **Key Exchange Data field : 0(1byte)** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                     <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction   Responder(NUT)
(1) HDR;SA,KE,Ni,IDii========>                  <-----Key Exchange Data field :
                                                       0(1byte)(invalid value)
(2-A)              X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                              or
(2-B)               <======== HDR; N/D
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-KEY-INFORMATION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.7 Key Exchange Payload Processing

## 6.2.56 Processing invalid ID type field

Purpose:

Determine if the Identification Type is supported. This may be based on the DOI and Situation. If the Identification determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID ID INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-ID-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Identification Payload Format(HOST-2:Initiator)
    ID Type field : 248 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #  Initiator(TN)          Direction       Responder(NUT)
(1) HDR;SA,KE,Ni,IDii ========>                         <-----ID Type field : 248
                                                                (invalid value)
(2-A)               X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                                         or
(2-B)                 <======== HDR*; HASH(1); N/D
                                   (HDR; N/D)
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or INVALID-ID-INFORMATION message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.8 Identification Payload Processing

## 6.2.57 Not include Identification Payload

Purpose:

All IPSEC DOI implementations MUST support SIT_IDENTITY_ONLY by including an Identification Payload in at least one of the Phase I Oakley exchanges and MUST abort any association setup that does not include an Identification Payload.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator(TN) does not send ID payload by the the fifth message.
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 #   Initiator(TN)    Direction  Responder(NUT)
 (1)HDR;SA,KE,Ni,IDii ========>                    <----not include ID payload
                                                                      (invalid)
(2)                X <========HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- Termination
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message must not be returned.

**References:**

RFC2407 : 4.2.1 SIT_IDENTITY_ONLY

## 6.2.58 Invalid Identification Payload receive

Purpose:

During Phase I negotiations, the ID port and protocol fields MUST be set to zero or to UDP port 500. If an implementation receives any other values, this MUST be treated as an error and the security association setup MUST be aborted.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator(TN)'s protocol fields of ID payload is set to TCP.(invalid value)
  - ✧ Initiator(TN)'s ID port fields of ID payload is set to 300.(invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
# Initiator(TN)      Direction  Responder(NUT)
(1) HDR;SA,KE,Ni,IDii ========>                         <-----ID protocol/port :
                                                          TCP/300(invalid value)
(2)                X <======== HDR;SA,KE,Nr,IDir,HASH_R <-----Must not transmit
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the results of the agreed upon authentication function(hash function).

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2) must not be returned.

**References:**

RFC2407 : 4.6.2 Identification Payload Content

## 6.2.59 Processing invalid Hash payload

Purpose:

Determine if the Hash is supported. If the Hash determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-HASH-INFORMATION message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Hash Payload Format(HOST-2:Initiator)
    **Hash Data field : not include this field** (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology". For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                      <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction  Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                 <======== HDR;SA,KE,Nr,IDir,HASH_R
(3)HDR[*];HASH_I    ========>              <----Hash Data field : not
                                                include this field (invalid)
(4)                <======== HDR*; HASH(1); N/D
                                (HDR; N/D)
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).

3. Send the third message from TN
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).

4. Receive the fourth message from NUT
   In the second message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

```
 * PHASE II
                      <QUICK MODE>
 #   Initiator(TN)    Direction    Responder(NUT)
(1)  HDR*, HASH(1),
         SA, Ni     ========>
(2)               X <========    HDR*,HASH(2),SA,Nr    <-----Must not transmit
                Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.
   HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

In AGGRESSIVE EXCHANGE, the first to the second message must be exchanged correctly.
The third message must not be accepted.
And must not establish ISAKMP SA(In QUICK MODE, the second message must not transmit(Check *2) (* or INVALID-HASH-INFORMATION message(4) may be returned (Check *1)).)
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.11 Hash Payload Processing

## 6.2.60 Processing invalid Hash Data field

Purpose:

Perform the Hash function as outlined in the DOI and/or Key Exchange protocol documents. If the Hash function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID HASH VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : BASIC (A requirement for all End-Node NUTs)
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  ✧ Hash Payload Format(HOST-2:Initiator)
  Hash Data field : 0 (invalid value)

  ✧ Initiator and Responder IKE parameter
  At least, following parameter must be included in proposal.

  For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | IKE-TEST | 3DES | SHA | pre-shared key | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                         <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii========>
(2)                 <======== HDR; SA, KE, Nr, IDir, HASH_R
(3)  HDR[*]; HASH_I ========>                         <-----Hash Data field :
(4)                <========  HDR*; HASH(1); N/D                  0 (invalid)
                                (HDR; N/D)
                           Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the results of the agreed upon authentication function(hash function).
3. Send the third message from TN
   In the third (3) message, the initiator send the results of the agreed upon authentication function(hash function).
4. Receive the fourth message from NUT
   In the second message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

* PHASE II

```
                        <QUICK MODE>
 # Initiator(TN)      Direction     Responder(NUT)
(1)HDR*,HASH(1),
          SA, Ni    ========>
(2)                X <========   HDR*,HASH(2),SA, Nr  <-----Must not transmit
                 Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

In AGGRESSIVE EXCHANGE, the first to the second message must be exchanged correctly.
The third message must not be accepted.
And must not establish ISAKMP SA(In QUICK MODE, the second message must not transmit(Check *2) (* or AUTHENTICATION-FAILED message(4) may be returned(Check *1)).)*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.11 Hash Payload Processing

### 6.2.61 Processing invalid Signature Payload

Purpose:

Determine if the Signature is supported. If the Signature determination fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE INFORMATION, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-SIGNATURE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key.
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Initiator)
    Signature Data field : not include this field (invalid)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>

(2)                 <======== HDR;SA,KE,Nr,IDir,SIG_R

(3)HDR[*];SIG_I      ========>                      <-----Signature Data field :
                                                           not include this field
 (4)                <======== HDR*; HASH(1); N/D                        (invalid)
                                (HDR; N/D)
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

3. Send the third message from TN
   In the third (3) message, the initiator send the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

4. Receive the fourth message from NUT
   In the second message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

＊ PHASE II

```
                    <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
           SA, Ni        ========>
(2)                    X <========  HDR*,HASH(2),SA, Nr <-----Must not transmit
                Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- Termination
  Clean up SAD and SPD

Judgment:

In AGGRESSIVE EXCHANGE, the first to the second message must be exchanged correctly.
The third message must not be accepted.
And must not establish ISAKMP SA(In QUICK MODE, the second message must not transmit(Check *2) (* or INVALID-SIGNATURE message(4) may be returned(Check *1)).)*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.12 Signature Payload Processing

## 6.2.62 Processing invalid Signature Data field

Purpose:

Perform the Signature function as outlined in the DOI and/or Key Exchange protocol documents. If the Signature function fails, the message is discarded and the following actions are taken:

(a) The event, INVALID SIGNATURE VALUE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the AUTHENTICATION-FAILED message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Initiator and Responder exchange the certificate of each other.
  - ✧ Signature Payload Format(HOST-2:Initiator)
    **Signature Data field : 0** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".

For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction     Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
(2)                  <========HDR;SA,KE,Nr,IDir,SIG_R
(3)HDR[*];SIG_I      ========>                    <---Signature Data field :
                                                                  0(invalid)
(4)                  <========   HDR; N/D
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.

3. Send the third message from TN
   In the third (3) message, the initiator send the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.

4. Receive the fourth message from NUT
   In the second message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

```
 * PHASE II
                      <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
           SA, Ni        ========>

(2)                    X <======== HDR*, HASH(2), SA, Nr <-----Must not transmit
                 Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

In AGGRESSIVE EXCHANGE, the first to the second message must be exchanged correctly.
The third message must not be accepted.
And must not establish ISAKMP SA(In QUICK MODE, the second message must not transmit(Check *2) (* or AUTHENTICATION-FAILED message(4) may be returned(Check *1)).) *option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.12 Signature Payload Processing

### 6.2.63 Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is invalid, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support
Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Initiator)
    Cert Encoding : 255 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                           <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction    Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
  CERT Req                                         <-----Cert Encoding Type
                                                          fild: 255(invalid)
(2)                 <========HDR;SA,KE,Nr,IDir,SIG_R <-----Must not transmit
                             CERT, CERT Req
                               or
(3)                 <========HDR*; HASH(1); N/D
                            (HDR; N/D)
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

**Judgment:**

The first message is not accepted. And the second message(2-A) is not returned (* or INVALID-CERT-ENCODING(2-B) message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.10 Certificate Request Payload Processing

## 6.2.64 Processing invalid Certificate Authority field

Purpose:

Determine if the Certificate Authority is supported for the specified Certificate Encoding. If the Certificate Authority is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE AUTHORITY, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-AUTHORITY message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Initiator)
    Certificate Authority field: 0 (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| **Machine** | **Src** | **Dest** | **Phase I** | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | **Ex mode** | **Key Value** | **Enc Alg** | **Hash Alg** | **Auth Method** | **DH Group** | **PH1 Lt** | **IDx** |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                          <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction      Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
    CERT Req                                          <-----Cert Data field:
                                                                 0(invalid)
(2)                  <======== HDR;SA,KE,Nr,IDir,SIG_R <-----Must not transmit
                               CERT, CERT Req
                         or
(3)                  <======== HDR*;HASH(1);N/D
                               (HDR; N/D)
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- Termination
  Clean up SAD and SPD

**Judgment:**

The first message is not accepted. And the second message(2-A) is not returned (* or INVALID-CERT-AUTHORITY(2-B) message is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.10 Certificate Request Payload Processing

## 6.2.65 Processing invalid Certificate Type with Certificate Authorityfield

Purpose:

Process the Certificate Request. If a requested Certificate Type with the specified Certificate Authority is not available, then the payload is discarded and the following actions are taken:

(a) The event, CERTIFICATE-UNAVAILABLE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the CERTIFICATE-UNAVAILABLE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

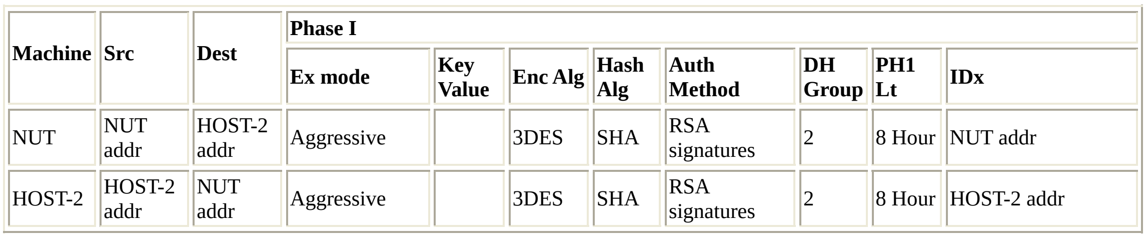
End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Request Payload Format(HOST-2:Initiator)
    **Certificate Authority field: Distinguish Name**
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.



| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
 # Initiator(TN)      Direction   Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
   CERT Req                                        <----Certificate Data
                                                       field: The value which
                                                        is not available for
                                                        Certificate Authority
(2)                 <========HDR;SA,KE,Nr,IDir,SIG_R<-----Must not transmit
                             CERT, CERT Req
                       or
(3)                 <========HDR*; HASH(1); N/D
                             (HDR; N/D)
                Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted.Additionally,the initiator transmits identification information.
   And the initiator send Certificate Request Payload.
2. Receive the second message from NUT
   In the second message (2-B), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

- **Termination**
  Clean up SAD and SPD

**Judgment:**

The first message must not be accepted. And the second message(2-A) must not be returned (* or CERTIFICATE-UNAVAILABLE message(2-B) is returned).
*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.10 Certificate Request Payload Processing

## 6.2.66 Processing invalid Certificate Encoding field

Purpose:

Determine if the Certificate Encoding is supported. If the Certificate Encoding is not supported, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE TYPE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERT-ENCODING message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Initiator)
    **Cert Encoding field : 255** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

Procedure:

This test check is following.

```
                        <AGGRESSIVE EXCHANGE>
 #  Initiator(TN)     Direction     Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
   CERT Req
(2)                  <========HDR;SA,KE,Nr,IDir,SIG_R
                              CERT, CERT Req
(3)HDR[*];SIG_I,CERT ========>                         <-----Cert Encoding Type
                                                             fild: 255(invalid)
(4)                  <======== HDR*; HASH(1); N/D
                               (HDR; N/D)
                   Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally,the responder transmits identification information and the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.Additionally the responder send Certificate and Certificate Request Payload
3. Send the third message from TN
   In the third (3) message, the initiator send the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the initiator send Certificate Request Payload.

4. Receive the fourth message from NUT
   In the second message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

```
 * PHASE II
                          <QUICK MODE>
 #   Initiator(TN)      Direction       Responder(NUT)
(1)  HDR*, HASH(1),
            SA, Ni        ========>
(2)                      X <======== HDR*, HASH(2), SA, Nr <-----Must not transmit
                  Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.
2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- Termination
  Clean up SAD and SPD

Judgment:

In AGGRESSIVE EXCHANGE, the first to the second message must be exchanged correctly.The third message must not be accepted.And must not establish ISAKMP SA(In QUICK MODE, the second message must not transmit(Check *2) (* or INVALID-SIGNATURE message(4) may be returned(Check *1)).)
*option : if you want to check the retruned Notify message.

References:

RFC2408 : 5.9 Certificate Payload Processing

### 6.2.67 Processing invalid Certificate Data field

Purpose:

Process the Certificate Data field. If the Certificate Data is invalid or improperly formatted, the payload is discarded and the following actions are taken:

(a) The event, INVALID CERTIFICATE, MAY be logged in the appropriate system audit file.

(b) An Informational Exchange with a Notification payload containing the INVALID-CERTIFICATE message type MAY be sent to the transmitting entity. This action is dictated by a system security policy.

Category:

End-Node : ADVANCED (This test is required for all End-Node NUTs which support Digital Signature (RSA))
SGW : N/A

Initialization:

- Network Topology
  Refer the topology "Figure 3 Topology for End-Node vs. End-Node (Responder Test)".

- Configuration
  - ✧ Initiator and Responder generate the public key and the secret key
  - ✧ Certificate Payload Format(HOST-2:Initiator)
    **Certificate Data field : 0** (invalid value)
  - ✧ Initiator and Responder IKE parameter
    At least, following parameter must be included in proposal.

    For Phase-1 configuration, use following parameter.

| Machine | Src | Dest | Phase I | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Ex mode | Key Value | Enc Alg | Hash Alg | Auth Method | DH Group | PH1 Lt | IDx |
| NUT | NUT addr | HOST-2 addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | NUT addr |
| HOST-2 | HOST-2 addr | NUT addr | Aggressive | | 3DES | SHA | RSA signatures | 2 | 8 Hour | HOST-2 addr |

For abbr., refer "Configuration Table" part in Chapter "Terminology".
For Phase-2 Configuration, refer "Table 2. Phase-2 Common Configuration" in Chapter "Common Configuration".

**Procedure:**

This test check is following.

```
                       <AGGRESSIVE EXCHANGE>
# Initiator(TN)     Direction   Responder(NUT)
(1)HDR;SA,KE,Ni,IDii ========>
   CERT Req
(2)                  <======== HDR;SA,KE,Nr,IDir,SIG_R
                               CERT, CERT Req
(3) HDR[*];SIG_I,CERT ========>                     <----Certificate Encoding
(4)                  <======== HDR*; HASH(1); N/D         field : 0 (invalid)
                               (HDR; N/D)
                    Judgement (Check *1)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes).Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks are also transmitted. Additionally, the initiator transmits identification information.
   And the initiator send Certificate Request Payload.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. Keying material used to arrive at a common shared secret and random information which is used to guarantee liveness and protect against replay attacks is also transmitted.Additionally, the responder transmits identification information and the signed data, SIG_R is the result of the negotiated digital signature algorithm applied to HASH_R.Additionally the responder send Certificate and Certificate Request Payload

3. Send the third message from TN
   In the third (3) message, the initiator send the signed data, SIG_I is the result of the negotiated digital signature algorithm applied to HASH_I.Additionally the initiator send Certificate Request Payload.

4. Receive the fourth message from NUT
   In the second message (4), the responder indicates either an ISAKMP Notify Payload or an ISAKMP delete Payload.

```
 * PHASE II
                        <QUICK MODE>
#   Initiator(TN)     Direction     Responder(NUT)
(1)  HDR*, HASH(1),
            SA, Ni      ========>
(2)                  X <======== HDR*, HASH(2), SA, Nr   <-----Must not transmit
                  Judgement (Check *2)
```

1. Send the first message from TN
   In the first message (1), the initiator generates a proposal it considers adequate to protect traffic for the given situation. The Security Association, Proposal, and Transform payloads are included in the Security Association payload (for notation purposes). And initiator send HASH(1) and Nonce. HASH(1) is the prf over the message id (M-ID) from the ISAKMP header concatenated with the entire message that follows the hash including all payload headers, but excluding any padding added for encryption. Nonce is random information which is used to guarantee liveness.

2. Receive the second message from NUT
   In the second message (2), the responder indicates the protection suite it has accepted with the Security Association, Proposal, and Transform payloads. And responder send HASH(2) and Nonce.
   HASH(2) is identical to HASH(1) except the initiator's nonce-- Ni, minus the payload header-- is added after M-ID but before the complete message. Nonce is random information which is used to guarantee liveness.

- Termination
  Clean up SAD and SPD

**Judgment:**

In AGGRESSIVE EXCHANGE, the first to the second message must be exchanged correctly.The third message must not be accepted.
And must not establish ISAKMP SA(In QUICK MODE, the second message must not transmit(Check *2) (* or INVALID-CERTIFICATE message(4) may be returned(Check *1)).)*option : if you want to check the retruned Notify message.

**References:**

RFC2408 : 5.9 Certificate Payload Processing