USGv6 Test Selection Tables*

IKEv2

I17-Interoperability: IKEv2_v2.0

Applicable Profile: NIST SP 500-267 A profile for IPv6 in the U.S. Government - Version 1.0, July 2008.

Configuration Option: IKEv2

Test Specification Id:

- [IKEv2-Interoperability] IPv6 Ready Logo Phase-2 Interoperability Test Scenario IKEv2, Version 1.1.0, June 8, 2010, [editor: IPv6 Ready Logo].

Reference:

- [RFC 4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 4306, December 2005.
- [RFC 4307] Schiller, J., "Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)", RFC 4307, December 2005.
- [RFC 4868] Kelly, S., S. Frankel., "Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec", RFC 4868, May 2007.

Device Type Definitions:

- **ROUTER:** A device capable of forwarding packets.
- **HOST:** A device which is not a ROUTER.
- **End-Node:** Both HOSTs and ROUTERs can be End-Nodes.
- **SGW:** A SGW is a specialized ROUTER.
  * NOTE: if the Device Under Test is a ROUTER and it supports Tunnel Mode, it should be tested as a SGW.

Interoperability Partner Requirements:

- Any host or router claiming compliance with the USGv6 profile MUST demonstrate evidence of interoperability with **three** or more existing independent implementations of IPv6. The three implementations must include at least one End-Node and at least one SGW.
- Can not change Target nodes once testing has begun.

IKEv2-Interoperability
If your Device Under Test (DUT) Type is **End-Node**:

- DUT = TAR-EN1 for all tests.
- TAR_EN2 = Independent Implementation Device B
- TAR_SGW1 = Independent Implementation Device C
- Third Interoperability Partner may be either an EN or SGW, and is satisfied by executing the test specification again using the following:
  - TAR_SWG1 = Independent Implementation SGW Device D
    or
  - TAR_EN2 = Independent Implementation End-Node Device D

If your Devide Under Test (DUT) Type is **SGW** :

- DUT = TAR_SGW1 for all tests.
- TAR_EN1 = Independent Implementation Device B
- TAR_SGW2 = Independent Implementation Device C
- Third Interoperability Partner may be either an EN or SGW, and is satisfied by executing the test specification again using the following:
  - TAR_EN1 = Independent Implemenation End-Node Device D
    or
  - TAR_SGW2 = Independent Implemenation SGW Device D

NOTE: If the SGW supports Transport Mode, Section 5.1 is tested where the DUT = TAR-EN1. TAR-EN2 = Device B

Notes:

- DH Group 24 should be used in place of DH Group 14 in tests that require it.

IKEv2 Test Check List

Reference	Test Specification Id	Test Number	Device Type	Passed
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.1 (A) (B): The Initial Exchanges	End-Node	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.1 (C) (D): The Initial Exchanges	SGW	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.1 (E) (F): The Initial Exchanges	End-Node/SGW	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.4 (A) (EE) (F) (FF): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.4 (K) (KK) (P) (LL): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.5 (A) (C) (G) (I): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.5 (M) (O) (S) (U): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.9 (E) (F) (G) (H): Multiple Transforms for IKE_SA	End-Node	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.9 (M) (N) (O) (P): Multiple Transforms for IKE_SA	SGW	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.13 (A) (B): RSA Digital Signature	End-Node	
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.13 (C) (D): RSA Digital Signature	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

AES-XCBC-MAC-96 SHOULD+ Tests				
Reference	**Test Specification Id**	**Test Number**	**Device Type**	**Passed**
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.4 (D) (I): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.4 (N) (S): Cryptographic Algorithm Negotiation for IKE_SA	SGW	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.5 (D) (J): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.5 (P) (V): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.8 (A) (B): Multiple Proposals for IKE_SA	End-Node	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.8 (C) (D): Multiple Proposals for IKE_SA	SGW	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.10 (A) (B): Multiple Proposals for CHILD_SA	End-Node	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.10 (C) (D): Multiple Proposals for CHILD_SA	SGW	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.11 (B) (E): Multiple Transforms for CHILD_SA	End-Node	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.11 (H) (K): Multiple Transforms for CHILD_SA	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

AES-XCBC-PRF-128 SHOULD+ Tests				
Reference	**Test Specification Id**	**Test Number**	**Device Type**	**Passed**
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.4 (C) (H): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4307	IKEv2-Interoperability	IKEv2Interop.1.4 (M) (R): Cryptographic Algorithm Negotiation for IKE_SA	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

HMAC-SHA-256-128 SHOULD+ Tests				
Reference	**Test Specification Id**	**Test Number**	**Device Type**	**Passed**
RFC 4868	IKEv2-Interoperability	IKEv2Interop.1.4 (CC) (DD): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4868	IKEv2-Interoperability	IKEv2Interop.1.4 (II) (JJ): Cryptographic Algorithm Negotiation for IKE_SA	SGW	

NOTE: The following tests are considered a **SHOULD+** for the IKEv2 Requirements as per the USGv6-v1 Profile.

HMAC-SHA-256 as a PRF SHOULD+ Tests				
Reference	**Test Specification Id**	**Test Number**	**Device Type**	**Passed**
RFC 4868	IKEv2-Interoperability	IKEv2Interop.1.4 (AA) (BB): Cryptographic Algorithm Negotiation for IKE_SA	End-Node	
RFC 4868	IKEv2-Interoperability	IKEv2Interop.1.4 (GG) (HH): Cryptographic Algorithm Negotiation for IKE_SA	SGW	

RFC 4868	IKEv2-Interoperability	IKEv2Interop.1.5 (AA) (BB): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node	
RFC 4868	IKEv2-Interoperability	IKEv2Interop.1.5 (CC) (DD): Cryptographic Algorithm Negotiation for CHILD_SA	SGW	

NOTE: The following tests are considered a **SHOULD** for the IKEv2 Requirements as per the USGv6-v1 Profile.

AES-CTR SHOULD Tests				
Reference	**Test Specification Id**	**Test Number**	**Device Type**	**Passed**

NOTE: The following tests have been omitted from the USGv6 Test Program for the IKEv2 Requirements. These tests are considered SHOULDs as defined by the IETF.

Not Required			
Reference	**Test Specification Id**	**Test Number**	**Device Type**
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.2: Rekeying CHILD_SA	End-Node/SGW
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.3: Rekeying IKE_SA	End-Node/SGW
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.4 (B) (E) (G) (J) (L) (O) (Q): Cryptographic Algorithm Negotiation for IKE_SA	End-Node/SGW
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.5 (B) (E) (F) (H) (K) (L) (N) (Q) (R) (T) (W) (X): Cryptographic Algorithm Negotiation for CHILD_SA	End-Node/SGW
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.6: Reuse of Diffie-Hellman Exponentials	End-Node/SGW
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.7: Identification Type	N/A
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.9 (A) (B) (C) (D) (I) (J) (K) (L): Multiple Transforms for IKE_SA	End-Node/SGW
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.11 (A) (C) (D) (F) (G) (I) (J) (L): Multiple Transforms for CHILD_SA	End-Node/SGW
RFC 4306	IKEv2-Interoperability	IKEv2Interop.1.12: Requesting an Internal Address on a Remote Network	End-Node/SGW

* The objective of this test selection sheet is to provide a reference for available test specifications that identifies tests applicable to the USGv6 IPv6 Profile.