

# USGv6 Test Selection Tables

## IPv6 IPsec SHA-512-VPN Requirements (IPsec, IKEv2)

**F11-Conformance:** Security Requirements R1v1.0

**Applicable Profile:** NIST SP 500-267B Revision 1 USGv6 Profile – November 2020.

**Test Specification Id:**

- [[IPsec Conformance](#)] IPv6 Ready Test Specification IPsec and IKEv2, [editor: [IPv6 Ready Logo](#)].

IPsec-SHA-512-VPN Capability			
Reference	Test Specification Id	Test Number	Device Type
[RFC 8247]	IPsec-Conformance	IPsec.Conf.1.1.1.3: IKE_SA_INIT Cryptographic Algorithm Negotiation (F) SHA512	SGW
[RFC 8221]	IPsec-Conformance	IPsec.Conf.1.1.2.5: IKE_AUTH Cryptographic Algorithm Negotiation (G) SHA512	SGW
[RFC 8247]	IPsec-Conformance	IPsec.Conf.1.2.1.3: IKE_SA_INIT Cryptographic Algorithm Negotiation (F) SHA512	SGW
[RFC 8221]	IPsec-Conformance	IPsec.Conf.1.2.2.5: IKE_AUTH Cryptographic Algorithm Negotiation (G) SHA512	SGW
[RFC 8221]	IPsec-Conformance	IPsec.Conf.4.1.3. SGW ESP Algorithms (C) AES256 / SHA512	SGW

### References:

- [RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017, <https://www.rfc-editor.org/info/rfc8221> .
- [RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017. Online at: <https://tools.ietf.org/html/rfc8247>

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