Network Working Group
Internet-Draft
Updates: 5723, 6617, 6631, 7296, 8784, 9370 (if approved)
Intended status: Standards Track
Expires: 10 October 2025

V. Smyslov
ELVIS-PLUS

8 April 2025

Use of Variable-Length Output Preudo-Random Functions (PRFs) in the Internet Key Exchange Protocol Version 2 (IKEv2)

draft-smyslov-ipsecme-ikev2-prf-plus-01

Abstract

This document specifies the use of variable-length output Preudo-Random Functions (PRFs) in the Internet Key Exchange Protocol Version 2 (IKEv2). Current IKEv2 specification relies on traditional PRFs with fixed output length for key derivation and uses iterative application of a PRF (called "prf+") in cases when longer output is required. Appearance of PRFs that can output as much bits as requested allows to streamline the key derivation functions of IKEv2.

This document updates RFCs 5723, 6617, 6631, 7296, 8784, 9370 for the cases when variable-length output Preudo-Random Functions are used in IKEv2 and its extensions.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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

This Internet-Draft will expire on 10 October 2025.

Copyright Notice

Table of Contents

1. Introduction

The Internet Key Exchange protocol version 2 (IKEv2) [RFC7296] is used in the IP Security (IPsec) architecture for the Security Association (SA) parameters negotiation and for establishing an authenticated shared secret. As part of the SA parameters negotiation a Pseudo-Random Function (PRF) is agreed upon. Keying materials for established SAs are then derived from the shared secret using the negotiated PRF.

For the purpose of deriving variable-size keying material to accomodate the use of cryptographic algorithms with different properties, a construction called prf+ is used in IKEv2. This construction servers the role of a Key Deriation Function (KDF) in IKEv2 and is defined in Section 2.13 of [RFC7296] and is provided here for convenience:

```
prf+ (K,S) = T1 | T2 | T3 | T4 | ...

where:
T1 = prf (K, S | 0x01)
T2 = prf (K, T1 | S | 0x02)
T3 = prf (K, T2 | S | 0x03)
T4 = prf (K, T3 | S | 0x04)
```

This construction allows to get more output bits than the output length of the negotiated PRF by applying it iteratively.

Modern achievements in cryptography bore new class of cryptographic primitives - PRFs with variable-length output. These functions are able to produce as many pseudorandom bits as requested in one call. One example of such PRFs is KMAC [SP-800-185].

When variable-length output PRFs are considered for the use in IKEv2 for the key derivation purposes, it is possible either to keep the prf+ construction always performung exactly one iteration with the PRF producing the needed number of output bits at once, or to remove the prf+ construction completely and replace it with a single call to the PRF, that would also produce the needed number of output bits. This is discussed in Section 8.3.2 of [I-D.salter-ipsecme-sha3] for the case of KMAC.

Since it is envisioned that more variable-length output PRFs could appear in future, this specification aims establish a uniform approach for using them in IKEv2. This document updates a number of RFCs specified IKEv2 and its extensions for the cases when variable-length output Preudo-Random Functions are used: [RFC7296], [RFC5723], [RFC6617], [RFC6631], [RFC8784], and [RFC9370].

2. Terminology and Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. Use of Variable-Length Output PRFs in IKEv2

When a new preudo-random function is introduced for use in IKEv2, the corresponding document must define whether the preudo-random function has fixed or variable output length. This doesn’t affect the process of code point allocation for this prf, but affects the way it is used in IKEv2 for the purposes of key derivation.

In particular, when a variable-length output pseudo-random function is negotiated in IKEv2 in the Pseudo-random Function (PRF) transform type, then the following rules have affect.

1. When such a PRF is defined for the use in IKEv2, a preferred key size for this function MUST be specified.

2. When such a PRF is used in the context of "prf", then its output length MUST be set to the preferred key size of this PRF.

3. When such a PRF is used in the context of "prf+", then the prf+ construction MUST NOT be used. Instead, the PRF output length MUST be set to the required number of pseudorandom bits in the current context and the use of prf+ is replaced with a single call to this PRF.

4. If an API to such a PRF includes additional inputs, like "customization string" in KMAC, then these inputs MUST be null (e.g. zero-length string).

4. Security Considerations

It is assumed that variable-output length PRFs are cryptographically strong and doesn’t decrease the entropy of the input key if the output length is at least the size of the key.

5. IANA Considerations

This specification makes no request to IANA.

6. Acknowledgements

This document was inspired by draft-salter-ipsecme-sha3 (Use of SHA-3 in the Internet Key Exchange Protocol Version 2 (IKEv2) and IPsec).

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

7.2. Informative References

[RFC5723] Sheffer, Y. and H. Tschofenig, "Internet Key Exchange Protocol Version 2 (IKEv2) Session Resumption", RFC 5723, DOI 10.17487/RFC5723, January 2010, <https://www.rfc-editor.org/info/rfc5723>.

[RFC6617] Harkins, D., "Secure Pre-Shared Key (PSK) Authentication for the Internet Key Exchange Protocol (IKE)", RFC 6617, DOI 10.17487/RFC6617, June 2012, <https://www.rfc-editor.org/info/rfc6617>.

[RFC6631] Kuegler, D. and Y. Sheffer, "Password Authenticated Connection Establishment with the Internet Key Exchange Protocol version 2 (IKEv2)", RFC 6631, DOI 10.17487/RFC6631, June 2012, <https://www.rfc-editor.org/info/rfc6631>.

[RFC8784] Fluhrer, S., Kampanakis, P., McGrew, D., and V. Smyslov, "Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Post-quantum Security", RFC 8784, DOI 10.17487/RFC8784, June 2020, <https://www.rfc-editor.org/info/rfc8784>.

[RFC9370] Tjhai, CJ., Tomlinson, M., Bartlett, G., Fluhrer, S., Van Geest, D., Garcia-Morchon, O., and V. Smyslov, "Multiple Key Exchanges in the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 9370, DOI 10.17487/RFC9370, May 2023, <https://www.rfc-editor.org/info/rfc9370>.

[SP-800-185] Kelsey, J., Change, S., and R. Perlner, "SHA-3 derived functions: cSHAKE, KMAC, TupleHash and ParallelHash", National Institute of Standards and Technology, DOI 10.6028/nist.sp.800-185, December 2016, <https://doi.org/10.6028/nist.sp.800-185>.

[I-D.salter-ipsecme-sha3] S, B., R, A., and J. C, "Use of SHA-3 in the Internet Key Exchange Protocol Version 2 (IKEv2) and IPsec", Work in Progress, Internet-Draft, draft-salter-ipsecme-sha3-00, 4 October 2024, <https://datatracker.ietf.org/doc/html/draft-salter-ipsecme-sha3-00>.

Author’s Address

Valery Smyslov
ELVIS-PLUS
PO Box 81
Moscow (Zelenograd)
124460
Russian Federation
Phone: +7 495 276 0211
Email: svan@elvis.ru