

Network Working Group
INTERNET-DRAFT
Updates: [5247](#) (if approved)
Intended status: Standards Track
Expires: January 29, 2021

DeKok, Alan
FreeRADIUS
29 July 2020

**EAP Session-Id Derivation for EAP-SIM, EAP-AKA, and PEAP
draft-ietf-emu-eap-session-id-06.txt**

Abstract

[RFC 5247](#) is updated to define and clarify EAP Session-Id derivation for multiple EAP methods. The derivation of Session-Id was not given for EAP-SIM or EAP-AKA when using the fast reconnect exchange instead of full authentication. The derivation of Session-Id for full authentication is clarified for both EAP-SIM and EAP-AKA. The derivation of Session-Id for PEAP is also given. The definition for PEAP follows the definition for other TLS-based EAP methods.

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on January 29, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	4
1.1.	Requirements Language	4
2.	Updates to RFC 5247 Appendix A	5
2.1.	EAP-AKA	5
2.2.	EAP-SIM	5
2.3.	Rationale for EAP-AKA and EAP-SIM updates	6
3.	Session-Id for PEAP	7
4.	Security Considerations	7
5.	IANA Considerations	8
6.	References	8
6.1.	Normative References	8
6.2.	Informative References	8

1. Introduction

EAP [[RFC3748](#)] Session-Id derivation has not been defined for EAP-SIM and EAP-AKA when using the fast reconnect exchange instead of full authentication. [[RFC5247](#)] defines the Session-Id for these EAP methods, but that derivation is only applicable for the full authentication case. The Session-Id derivation was not defined for EAP-AKA', but [[AKAP](#)] now defines it, along with other updates. As such, the definition for EAP-AKA' is not included here.

Further, the derivation of Session-Id for full authentication is clarified, as the text in [[RFC5247](#)] is ambiguous.

The IEEE has defined Fast Initial Link Setup (FILS) authentication [[FILS](#)], which needs the EAP Session-Id in order for the EAP Re-authentication Protocol (ERP) [[RFC6696](#)] to work. It is therefore important to address the existing deficiencies in the definition of EAP Session-Id.

Finally, [[RFC5247](#)] did not define Session-Id for PEAP [[MS-PEAP](#)], [[PEAP](#)]. We correct these deficiencies here by updating [[RFC5247](#)] with the Session-Id derivation during fast-reconnect exchange for EAP-SIM and EAP-AKA; clarifying the Session-Id derivation during full authentication for EAP-SIM and EAP-AKA; and defining the Session-Id derivation for PEAP which is the same for both full authentication and fast reconnect.

1.1. Requirements Language

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.

2. Updates to [RFC 5247 Appendix A](#)

This section updates [\[RFC5247\] Appendix A](#) to define Session-Id for fast reconnect exchange for EAP-AKA and EAP-SIM.

2.1. EAP-AKA

For EAP-AKA, [\[RFC5247\] Appendix A](#) says:

EAP-AKA

EAP-AKA is defined in [\[RFC4187\]](#). The EAP-AKA Session-Id is the concatenation of the EAP Type Code (0x17) with the contents of the RAND field from the AT_RAND attribute, followed by the contents of the AUTN field in the AT_AUTN attribute:

Session-Id = 0x17 || RAND || AUTN

It should say:

EAP-AKA

EAP-AKA is defined in [\[RFC4187\]](#). When using full authentication, the EAP-AKA Session-Id is the concatenation of the EAP Type Code (0x17) with the contents of the RAND field from the AT_RAND attribute, followed by the contents of the AUTN field in the AT_AUTN attribute:

Session-Id = 0x17 || RAND || AUTN

When using fast reconnect, the EAP-AKA Session-Id is the concatenation of the EAP Type Code (0x17) with the contents of the NONCE_S field from the AT_NONCE_S attribute, followed by the contents of the MAC field from the AT_MAC attribute from EAP-Request/AKA-Reauthentication:

Session-Id = 0x17 || NONCE_S || MAC

2.2. EAP-SIM

Similarly for EAP-SIM, [\[RFC5247\] Appendix A](#) says:

EAP-SIM

EAP-SIM is defined in [\[RFC4186\]](#). The EAP-SIM Session-Id is the concatenation of the EAP Type Code (0x12) with the contents of the RAND field from the AT_RAND attribute, followed by the contents of the NONCE_MT field in the AT_NONCE_MT attribute:

Session-Id = 0x12 || RAND || NONCE_MT

It should say:

EAP-SIM

EAP-SIM is defined in [\[RFC4186\]](#). When using full authentication, the EAP-SIM Session-Id is the concatenation of the EAP Type Code (0x12) with the contents of the RAND field from the AT_RAND attribute, followed by the contents of the NONCE_MT field in the AT_NONCE_MT attribute. [RFC 4186](#) says that EAP server should obtain "n" GSM triplets where "n=2" or "n=3".

For "n=2", the Session-Id is therefore defined as

Session-Id = 0x12 || RAND1 || RAND2 || NONCE_MT

which is 49 octets in length.

For "n=3", the Session-Id is therefore defined as

Session-Id = 0x12 || RAND1 || RAND2 || RAND3 || NONCE_MT

which is 65 octets in length.

Where RAND1, RAND2 and RAND3 correspond to the RAND value from the first, second and third GSM triplet respectively.

When using fast reconnect, the EAP-SIM Session-Id is the concatenation of the EAP Type Code (0x12) with the contents of the NONCE_S field from the AT_NONCE_S attribute, followed by the contents of the MAC field from the AT_MAC attribute from EAP-Request/SIM/Reauthentication:

Session-Id = 0x12 || NONCE_S || MAC

which is 33 octets in length.

2.3. Rationale for EAP-AKA and EAP-SIM updates

[RFC5247] was supposed to define exported parameters for existing EAP methods in [Appendix A](#). The way Session-Id was defined for EAP-AKA and EAP-SIM works only for the full authentication case, i.e., it cannot be used when the optional fast reconnect case is used since the used parameters (RAND, AUTN, NONCE_MT) are not used in the fast re-authentication case. Based on [\[RFC4187\] Section 5.2](#), and similar text in [\[RFC4186\] Section 5.2](#), NONCE_S corresponds to RAND and MAC in EAP-

Request/AKA-Reauthentication and EAP-Request/SIM/Reauthentication corresponds to AUTN. That would seem to imply that the Session-Id could be defined using NONCE_S and MAC instead of RAND and AUTN/NONCE_MT.

This derivation is done via a random value created by the server, along with a secret key and the peer's identity. We believe that this derivation is secure, though no formal analysis has been done.

3. Session-Id for PEAP

[RFC5247] did not define Session-Id for Microsoft's Protected EAP (PEAP). For consistency with the EAP-TLS definition given in [\[RFC5216\] Section 2.3](#), we define it as:

```
Session-Id = 0x19 || client.random || server.random
```

This definition is that same for both full authentication, and for fast reconnect.

This definition is already in wide-spread use in all known PEAP implementations.

Note that this definition for Session-Id only applies when TLS 1.2 or earlier is used. A different derivation is defined for TLS 1.3 in [\[TLS-EAP-TYPES\]](#).

4. Security Considerations

This specification defines EAP Session-Ids for ERP with EAP-SIM and EAP-AKA. It therefore enables ERP key hierarchy establishment using fast reconnect with EAP-SIM and EAP-AKA.

The Session-Id definitions given here are unique per session and unforgeable and unguessable by an outside party, as per the requirements of [\[RFC5247\] Section 10](#).

The definitions used here have been widely deployed for years, in all major EAP implementations. However, we acknowledge that very little security analysis has been done for these definitions. As a result, any security issues would result in serious issues for the Internet as a whole.

These updates do not modify the Security Considerations outlined in [RFC5247](#).

5. IANA Considerations

There are no actions for IANA. RFC EDITOR: This section may be removed before publication.

6. References

6.1. Normative References

[RFC2119]

Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [RFC 2119](#), March, 1997, <<http://www.rfc-editor.org/info/rfc2119>>.

[RFC3748]

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowitz, "Extensible Authentication Protocol (EAP)", [RFC 3748](#), June 2004.

[RFC5216]

Simon, D., Aboba, B., and R. Hurst, "The EAP-TLS Authentication Protocol", [RFC 5216](#), March 2008

[RFC5247]

Aboba, B., Simon, D., and P. Eronen, "Extensible Authentication Protocol (EAP) Key Management Framework", [RFC 5247](#), August 2008,

[RFC8174]

Leiba, B., "Ambiguity of Uppercase vs Lowercase in [RFC 2119](#) Key Words", [RFC 8174](#), May 2017, <<http://www.rfc-editor.org/info/rfc8174>>.

[FILS]

"IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 1: Fast Initial Link Setup", IEEE Std 802.11ai-2016, 2016.

6.2. Informative References

[RFC4186]

Haverinen, H. (Ed), Salowey, J., "Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)", [RFC 4186](#), January 2006.

[RFC4187]

Arkko, J., Haverinen, H., "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", [RFC 4187](#), January 2006.

[RFC6696]

Cao, Z. et al, "EAP Extensions for EAP Re-authentication Protocol (ERP)", [RFC 6696](#), July 2012.

[AKAP]

Arkko, J., et al, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')", [draft-ietf-emu-rfc5448bis-07.txt](#), March 2020.

[TLS-EAP-TYPES]

DeKok, A., "TLS-based EAP types and TLS 1.3" [draft-dekok-emu-tls-eap-types-02](#), April 2020.

[MS-PEAP]

Microsoft, "[[MS-PEAP](#)]: Protected Extensible Authentication Protocol (PEAP)", https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-peap/5308642b-90c9-4cc4-beec-fb367325c0f9

[PEAP]

Andersson, H., et al, "Protected EAP Protocol (PEAP)", [draft-josefsson-pppext-eap-tls-eap-05.txt](#), September 2002.

Acknowledgments

The issue corrected in this specification was first reported by Jouni Malinen in a technical errata at https://www.rfc-editor.org/errata_search.php/doc/html/rfc5247

The text in this document follows Jouni's suggestions.

Authors' Addresses

Alan DeKok
The FreeRADIUS Server Project

Email: aland@freeradius.org

