EMU
Internet-Draft
Updates: 9048 (if approved)
Intended status: Standards Track
Expires: 30 November 2026

T. Wan
CableLabs

29 May 2026

EAP-AKA' Identity Fragmentation
draft-wan-emu-aka-prime-identity-fragmentation-00

Abstract

This document updates EAP-AKA' (RFC 9048) by defining the use of the AT_FRAGMENT mechanism, as defined in I-D.ietf-emu-pqc-eapaka, for fragmentation of the AT_IDENTITY attribute. This update allows a peer to convey a large network access identifier, such as a Subscription Concealed Identifier (SUCI), during the EAP-AKA' identity exchange when the encoded identity is too large to fit reliably in a single EAP packet. This is intended to support large SUCI values produced by post-quantum cryptographic concealment schemes, while preserving the existing EAP-AKA' challenge and key derivation procedures.

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 30 November 2026.

Copyright Notice

Table of Contents

1. Introduction 2
2. Requirements Language 3
3. Terminology 3
4. Identity Fragmentation 4
4.1. Overview 4
4.2. AT_FRAGMENT_SUPPORTED 6
4.3. Fragmentation Procedure 7
4.4. Reassembly Procedure 7
4.5. Error Handling 7
4.6. Backward Compatibility 8
5. Security Considerations 8
6. Privacy Considerations 8
7. IANA Considerations 9
8. References 9
8.1. Normative References 9
8.2. Informative References 10
Acknowledgments 10
Author's Address 10

1. Introduction

EAP-AKA' [RFC9048] is an improved Extensible Authentication Protocol (EAP) [RFC3748] method based on the Authentication and Key Agreement protocol. EAP-AKA' supports the use of 5G identifiers, including the Subscription Concealed Identifier (SUCI), during identity exchange. In EAP-AKA', the peer's identity can be conveyed either in the initial EAP-Response/Identity packet or in the AT_IDENTITY attribute in an EAP-Response/AKA-Identity packet.

Some SUCI concealment schemes may produce encoded identities that are larger than can be carried reliably in a single EAP packet. This can become more likely when post-quantum cryptographic (PQC) schemes are used for Subscription Permanent Identifier (SUPI) concealment. For example, a PQC-protected SUCI may require a few thousand octets [TS33501] when the scheme input and scheme output are encoded as part of the identity.

EAP [RFC3748] does not provide a generic fragmentation mechanism, and expects EAP methods that may carry large payloads to provide method-specific fragmentation. This document specifies how the generic AT_FRAGMENT mechanism defined in I-D.ietf-emu-pqc-eapaka can be used to fragment AT_IDENTITY during the EAP-AKA' identity exchange.

The mechanism defined here is intentionally scoped. It does not provide a general EAP-AKA' fragmentation layer for all attributes or all EAP-AKA' packets. It only fragments the identity value that would otherwise be carried in AT_IDENTITY. This avoids changes to the EAP-AKA' challenge, response, AT_MAC validation, and key derivation procedures.

This document does not alter the processing of AT_IDENTITY when identity fragmentation is not used.

This document makes the following updates to RFC 9048:

* It defines the AT_FRAGMENT_SUPPORTED attribute, which allows an EAP-AKA' server to indicate support for fragmented identity transport and to advertise the maximum supported fragment size and maximum reassembled attribute size.

* It permits an EAP-AKA' peer to use the AT_FRAGMENT mechanism defined in I-D.ietf-emu-pqc-eapaka to transport an identity value that cannot be carried in a single AT_IDENTITY attribute.

Except for the procedures described above, this document does not modify any other aspect of the EAP-AKA' protocol specified in RFC 9048.

2. 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.

3. Terminology

This document uses the terminology of [RFC3748], [RFC4187], [RFC5448], and [RFC9048].

The following additional terms are used:

Large identity: An identity value that is too large to fit reliably

in a single EAP-Response/AKA-Identity packet as an AT_IDENTITY attribute.

Reassembled identity: The identity value obtained after successful reassembly of all fragments belonging to the same AT_IDENTITY value.

4. Identity Fragmentation

4.1. Overview

Since EAP [RFC3748] does not provide a generic fragmentation mechanism, a large identity value cannot be fragmented within the initial EAP-Response/Identity exchange. Therefore, a peer that needs to convey a large identity first responds with an anonymous identity in EAP-Response/Identity and then provides the large identity during the EAP-AKA' identity exchange using the procedures defined in this document.

After receiving an anonymous identity from a peer, the server requests the peer identity using EAP-Request/AKA-Identity packet containing AT_FRAGMENT_SUPPORTED. The attribute advertises support for fragmented identity transport and indicates the maximum supported fragment size and reassembled identity size.

If the peer supports this extension and needs to send a large identity, the peer sends the identity as a sequence of EAP-Response/AKA-Identity packets. Each such response contains one or more AT_FRAGMENT attributes carrying fragmented portions of the AT_IDENTITY value. Fragment acknowledgement, retransmission, and sequencing follow the procedures defined for AT_FRAGMENT in I-D.ietf-emu-pqc-eapaka. This preserves the lock-step EAP request and response model.

After receiving all AT_FRAGMENT payloads, the server reassembles the identity value and processes the reassembled value as if it had been received in a single AT_IDENTITY attribute. The server then continues with the normal EAP-AKA' exchange.

Figure 1 shows the message flow of fragmented identity transport for a large SUCI.

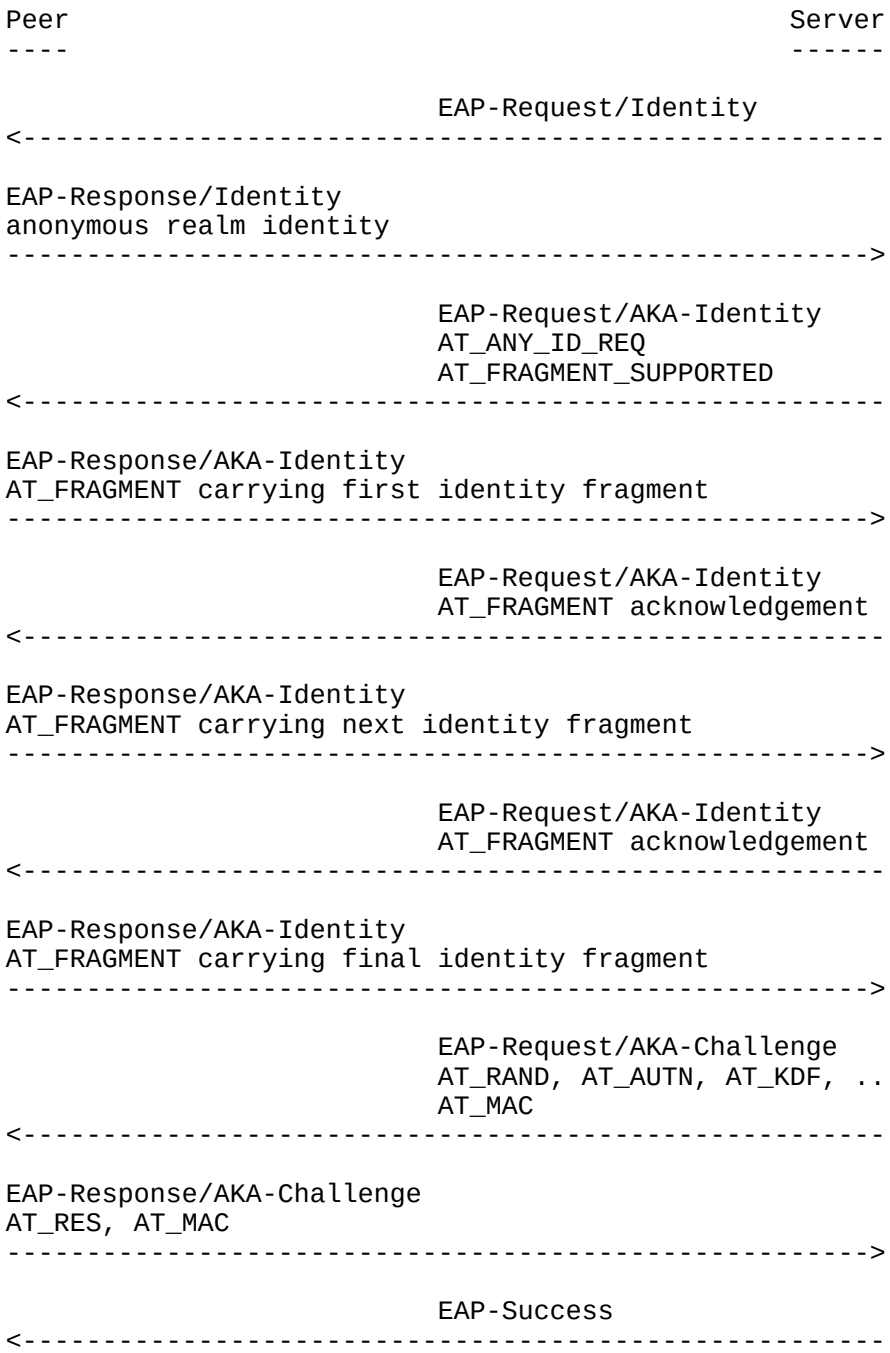


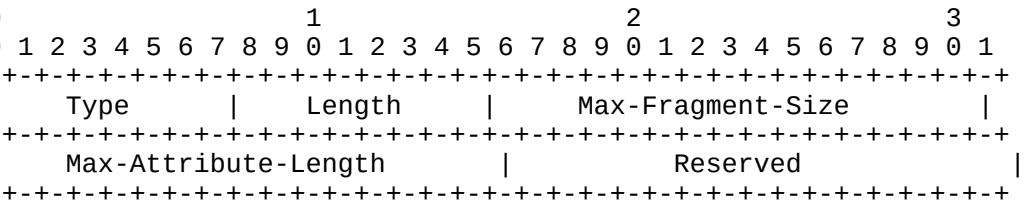
Figure 1: Identity Fragmentation during EAP-AKA' Identity Exchange

4.2. AT_FRAGMENT_SUPPORTED

AT_FRAGMENT_SUPPORTED is sent by the server in an EAP-Request/AKA-Identity packet to indicate support for use of AT_FRAGMENT during identity exchange.

The peer MUST NOT send AT_FRAGMENT carrying identity fragments unless the server has advertised AT_FRAGMENT_SUPPORTED in the same EAP-AKA' identity exchange.

The format of AT_FRAGMENT_SUPPORTED is:



Type: TBD1.

Length:

1. The length of this attribute in units of four octets. The total attribute length is 8 octets.

Max-Fragment-Size: The maximum number of payload octets that the server is willing to receive in a single AT_FRAGMENT attribute. A server SHOULD advertise a value that is smaller than the minimal EAP MTU of 1020 bytes.

Max-Attribute-Length: The maximum number of octets in a complete reassembled EAP-AKA' attribute value that the server is willing to accept when AT_FRAGMENT is used. For this specification, the applicable reassembled attribute value is the AT_IDENTITY value. The server MAY configure this value based on the maximum identity size it is willing to accept. A server supporting large SUCI transport SHOULD support at least 3000 octets, as required by [TS33501].

Reserved: Reserved for future use. The sender MUST set this field to zero. The receiver MUST ignore this field.

4.3. Fragmentation Procedure

If the peer determines that the identity value cannot be carried in a single AT_IDENTITY attribute and the server has advertised AT_FRAGMENT_SUPPORTED, the peer fragments the identity using AT_FRAGMENT.

The peer MUST NOT transmit AT_FRAGMENT carrying identity data unless AT_FRAGMENT_SUPPORTED has been received during the current EAP-AKA' identity exchange.

The peer MUST follow the AT_FRAGMENT procedures specified in I-D.ietf-emu-pqc-eapaka.

The fragment payload size MUST NOT exceed the Max-Fragment-Size advertised by the server.

4.4. Reassembly Procedure

Upon receipt of AT_FRAGMENT carrying portions of an AT_IDENTITY value, the server performs validation and reassembly according to I-D.ietf-emu-pqc-eapaka.

The server MUST verify that the reassembled attribute length does not exceed the advertised Max-Attribute-Length. If the reassembled attribute length exceeds Max-Attribute-Length, the server MUST fail the EAP-AKA' exchange.

After successful reassembly, the resulting octet sequence is processed as the value of AT_IDENTITY, and the server continues processing according to RFC 9048.

4.5. Error Handling

If a peer or server detects an error in the fragmentation exchange, it MUST fail the EAP-AKA' exchange according to the error handling procedures of [RFC9048].

A server SHOULD treat the following as fragmentation errors:

* receipt of AT_FRAGMENT without prior advertisement of AT_FRAGMENT_SUPPORTED;

* malformed AT_FRAGMENT attribute;

* reassembled identity length exceeds Max-Attribute-Length;

* reassembly timeout;

* identity syntax failure after reassembly.

The server MAY send EAP-Failure after detecting a fragmentation error.

4.6. Backward Compatibility

This extension is backward compatible with existing EAP-AKA' peers and servers.

A peer that does not implement this specification will ignore the AT_FRAGMENT_SUPPORTED attribute advertised by the server.

A compliant peer MUST NOT use AT_FRAGMENT carrying identity fragments unless the server advertises AT_FRAGMENT_SUPPORTED. Therefore, a server that does not implement this specification will not receive AT_FRAGMENT from a compliant peer.

5. Security Considerations

As in RFC 9048, AT_FRAGMENT payloads carrying identity information are exchanged before AT_MAC protection becomes available. This specification does not change that property.

This specification does not change any other security properties of EAP-AKA' [RFC9048].

Fragmentation can increase denial-of-service risk because a server may need to allocate state before authentication completes. Servers MUST enforce limits on reassembled attribute length, fragment size, and reassembly lifetime.

6. Privacy Considerations

This extension is intended to preserve the ability to use concealed identities when those identities become large. A peer that cannot send a large SUCI because fragmentation is unavailable may otherwise be forced to fail authentication or use a less private identity. This extension therefore improves privacy in deployments where concealed identities exceed practical single-packet limits.

Fragment counts and packet sizes may reveal approximate identity length. This document does not attempt to hide the length of the concealed identity. An implementation MAY pad the identity before fragmentation if local policy requires length hiding, but such padding is outside the scope of this document.

7. IANA Considerations

IANA is requested to allocate one new Attribute Type value from the “EAP-AKA and EAP-SIM Parameters” registry:

Value	Attribute Name	Reference
TBD1	AT_FRAGMENT_SUPPORTED	RFC-TBD

Table 1

8. References

8.1. Normative References

[I-D.ietf-emu-pqc-eapaka] "Post-Quantum Cryptography (PQC) Enhancements for EAP-AKA’", <https://datatracker.ietf.org/doc/draft-ietf-emu-pqc-eapaka/>.

[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>.

[RFC3748] Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., and H. Levkowetz, Ed., "Extensible Authentication Protocol (EAP)", RFC 3748, DOI 10.17487/RFC3748, June 2004, <https://www.rfc-editor.org/info/rfc3748>.

[RFC4187] Arkko, J. and H. Haverinen, "Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA)", RFC 4187, DOI 10.17487/RFC4187, January 2006, <https://www.rfc-editor.org/info/rfc4187>.

[RFC5448] Arkko, J., Lehtovirta, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA’)", RFC 5448, DOI 10.17487/RFC5448, May 2009, <https://www.rfc-editor.org/info/rfc5448>.

[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>.

[RFC9048] Arkko, J., Lehtovirta, V., Torvinen, V., and P. Eronen, "Improved Extensible Authentication Protocol Method for 3GPP Mobile Network Authentication and Key Agreement (EAP-AKA’)", RFC 9048, DOI 10.17487/RFC9048, October 2021, <https://www.rfc-editor.org/info/rfc9048>.

8.2. Informative References

[TS23501] 3GPP, "3GPP TS 23.501: System architecture for the 5G System (5GS)", <https://www.3gpp.org/ftp/Specs/archive/23_series/23.501/>.

[TS33501] 3GPP, "3GPP TS 33.501: Security architecture and procedures for 5G System", <https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/>.

Acknowledgments

The author thanks the participants of 3GPP SA3 and IETF EMU working groups for discussions on supporting large SUCI values. The author also thanks the authors of I-D.ietf-emu-pqc-eapaka for defining the AT_FRAMENT mechanism that is reused in this document.

Author’s Address

T. Wan
CableLabs
Email: t.wan@cablelabs.com