Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

M. Chen
L. Su
China Mobile

20 October 2025

EDHOC Authenticated with AKA
draft-chen-lake-edhoc-aka-01

Abstract

This document defines the EDHOC-AKA authentication method based on the Authentication and Key Agreement(AKA) protocol and the Ephemeral Diffie-Hellman Over COSE(EDHOC) key exchange protocol. This method is designed to provide efficient mobile communication network access authentication for scenarios with limited computing and network resources (such as Non-Terrestrial Network, NTN). EDHOC-AKA utilizes the pre-shared long-term key and employs symmetric cryptography techniques to achieve mutual authentication and key derivation. It ensures security while significantly enhancing the authentication efficiency.

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 23 April 2026.

Copyright Notice

Table of Contents

1. Introduction

This document defines a AKA authentication method for the Ephemeral Diffie-Hellman Over COSE (EDHOC) key exchange protocol [RFC9528]. AKA is a symmetric ciper, it achieves key agreement through mutual authentication between the mobile users and networks, and subsequently generates data encryption keys and integrity protection keys. In this document, Initiator stands for the mobile user and Responder stands for the network. AKA relies on long-term keys which is provided out-of-band and realize dynamic symmetric key derivation. Symmetric key authentication offers greater computational efficiency compared to the methods outlined in [RFC9528].

The Authentication and Key Agreement (AKA) is an authentication mechanism for devices wishing to access mobile networks. [RFC4187] (EAP-AKA) made the use of this mechanism possible within the Extensible Authentication Protocol (EAP) framework. [RFC5448] (EAP-AKA') was an improved version of EAP-AKA. [RFC9048]is the most recent specification of EAP-AKA'related to 5G networks.

The parameters in the authentication vectors of EDHOC-AKA and EAP-AKA’ are remain consistent and defined in the new field CRED_AKA_X. This document only considers two parties and the interaction between networks is out of scope.

2. Terminology

The following terms are used:

* AKA: Authentication and Key Agreement.

3. Protocol

This document specifies a new EDHOC authentication method (see Section 3.2 of [RFC9528]) referred to as the Authentication and Key Agreement method for the Ephemeral Diffie-Hellman Over COSE key exchange protocol (EDHOC-AKA). Authentication is based on a long-term key shared between the Initiator and the Responder. As in the methods defined in [RFC9528], CRED_I and CRED_R are authentication credentials containing identifying information for the Initiator and Responder, respectively. We defined CRED_AKA_I and CRED_AKA_R to hold the authentication vector of AKA for the Initiator and Responder, respectively. We have added a new method to indicate that the Initiator and Responder support AKA authentication.

3.1. Credentials

According to RFC 9528 and the existing specifications of AKA, designing a new authentication method (Method = 5)and defining new credential parameter CRED_AKA_X, it is necessary to ensure that the Initiator (I) and the Responder (R) meet the following core requirements:

* The Initiator and Responder are assumed to share a long-term key, or it is possible to obtain the derived parameters indirectly.

* The explicit indication of the authentication method is AKA, and it also carries the necessary identity credential information.

The requirements for Initiator

* The long-term key K and user identifier must be pre-set and stored in a secure environment.

* Support the capability of generating the 5-tuple of AKA (RAND/AUTN/XRES/CK/IK).

The requirements for Responder

* Based on the SUPI/SUCI in EAD_1, route to the network, the division between the visiting network and the home network is out of scope.

* Obtain the AKA five-tuple (or generate dynamic vector) from network

3.1.1. CRED_AKA_X

CRED_AKA is a COSE header map containing header parameters that indicate the AKA authentication parameters. CRED_AKA_X is uesed to refer to CRED_AKA_I or CRED_AKA_R, CRED_AKA_I and CRED_AKA_R are authentication credentials associated with the AKA.

CRED_AKA_R: Contains the AKA parameters sent by the responder, typically including: * AT_RAND: Random Number Challenge * AT_AUTN: Authentication Token

CRED_AKA_I: Contains parameters for the responder’s response to the challenge, typically including: * AT_RES: Authentication Response

An example of CRED_AKA_I and CRED_AKA_R is shown below: TBD

3.1.2. Encoding and processing

The AKA parameters should be encoded in the CWT format and the encryption and signature methods for them should be standardized in COSE.

NOTE: Encode AKA in CWT format. Need to standardize the encryption and signature of CWT-AKA in COSE. RFC Editor: Remove this note.

3.2. Message Flow of EDHOC-AKA

The message flow of EDHOC-AKA follows the structure defined in [RFC9528], with authentication based on symmetric keys rather than public keys.

The Responder authenticates the Initiator first. Figure 1 illustrates the message flow of the EDHOC-AKA authentication method.

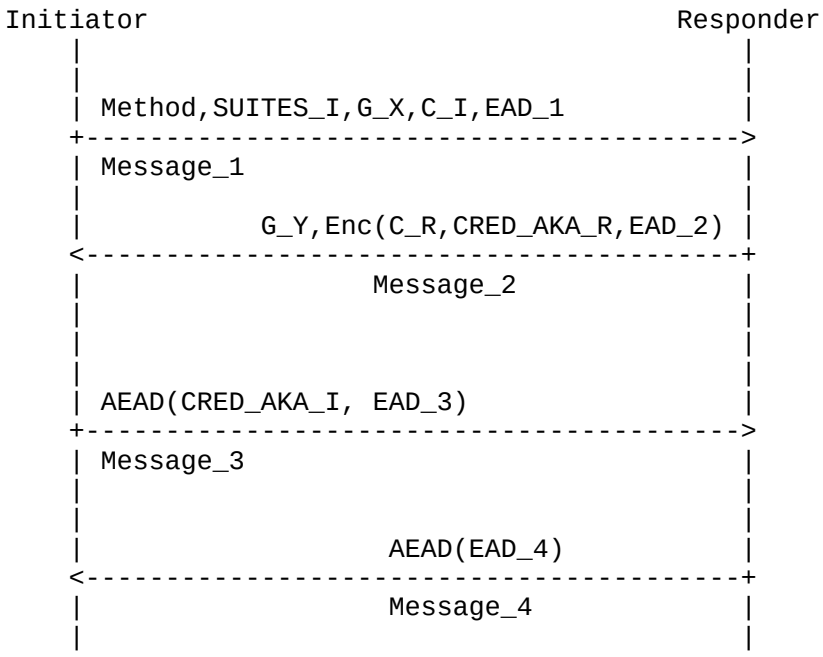

Figure 1: Overview of Message Flow of EDHOC-AKA

EDHOC message_4 is required to indicate EDHOC-AKA authentication success.

EAD_1 = Initiator identity, it usually represents a pseudo identity rather than the user's genuine and long-term identity. Based on this pseudo identity, the real identity can be retrieved on the Responder side.

Both endpoints are authenticated with AKA (TBD1：METHOD = 5)

NOTE: Assuming TBD1 = 5, to be confirmed by IANA. RFC Editor: Remove this note.

4. Key Derivation

The key derivation of EDHOC-AKA is similar to that of EDHOC-PSK, but the source of the key PRK_4e3m is different. The derivation methods of PRK_2e and PRK_3e2m are exactly the same as those of the standard EDHOC (based on G_XY). The key difference lies in PRK_4e3m: In EDHOC-PSK: PRK_4e3m = EDHOC_Extract(SALT_4e3m, PSK) In EDHOC-AKA: PRK_4e3m = EDHOC_Extract(SALT_4e3m, K_AKA) Here, K_AKA is the key material generated from the AKA process. In 3GPP AKA, this is usually derived by the key derivation function using CK (encryption

key) and IK (integrity key) as inputs to generate a new key for the specific service (EDHOC). The subsequent derived keys PRK_out and so on are securely derived from PRK_4e3m, ensuring the independence and forward security of the final session key.

5. Message Formating and Processing

5.1. Message1

Message 1 (Initiator -> Responder) METHOD = 5: Clearly declare that this conversation uses AKA authentication. EAD_1: include the permanent identity (such as SUPI) or temporary identity (such as GUTI) of the initiating party, to assist the responder (service network) in requesting an authentication vector from its network.

5.2. Message2

Message 2 (Responder -> Initiator) The responder obtains the AKA authentication vectors (RAND, AUTN, XRES, CK, IK) from the network. The responder sends the challenge RAND and AUTN to the initiator through CRED_AKA_R. The remaining part of Message 2 (G_Y, C_R) is consistent with the standard EDHOC. The encryption structure Enc(C_R, CRED_AKA_R, EAD_2) is encrypted using the key stream derived from PRK_2e, similar to EDHOC-PSK.

5.3. Message3

Message 3 (Initiator -> Responder) The initiating party (UE) uses its built-in USIM card and long-term key K to verify the AUTN. If the verification is successful, the response RES and session keys CK, IK are calculated. The initiating party sends RES through CRED_AKA_I to the responding party. The responding party verifies whether the received RES matches the expected XRES, thereby completing the authentication of the initiating party.

5.4. Message4

Message 4 (Responder -> Initiator) This message should be sent as it provides clear key confirmation to the initiator and authenticates the responder. It is also an AEAD encryption structure, proving that the responder has successfully derived the session key.

6. IANA Considerations

IANA is requested to register the following entry in the "EDHOC Method Type" registry under the group name "Ephemeral Diffie-Hellman Over COSE (EDHOC)".

Value	Initiator Authentication Key	Responder Authentication Key
TBD2	EDHOC-AKA	EDHOC-AKA

Table 1: Addition to the EDHOC Method Type Registry.

NOTE: Suggested value: TBD1 = 5. RFC Editor: Remove this note.

7. Security Considerations

Mutual authentication: Strong mutual authentication is achieved through the AKA challenge-response mechanism. Identity protection: The permanent identity of the initiator (such as SUPI) is only transmitted in the possible EAD_1 and can be replaced by a temporary identity. The identity of the responder is protected in the message flow. Forward security: Based on the temporary Diffie-Hellman exchange, even if the long-term subscription key K or the CK/IK derived from AKA is leaked, the past session will not be decrypted. Key binding: The final session key PRK_out is simultaneously bound to the temporary DH shared secret G_XY and the key K_AKA derived from AKA, providing stronger security.

8. Informative References

[RFC9528] Selander, G., Preu Mattsson, J., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", RFC 9528, DOI 10.17487/RFC9528, March 2024, <https://www.rfc-editor.org/rfc/rfc9528>.

[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/rfc/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/rfc/rfc5448>.

[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/rfc/rfc9048>.

Authors' Addresses

Meiling Chen
China Mobile
BeiJing
China
Email: chenmeiling@chinamobile.com

Li Su
China Mobile
BeiJing
China
Email: suli@chinamobile.com