EDHOC Authenticated with AKA

draft-chen-lake-edhoc-aka-02

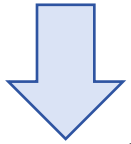
Presented by: Meiling Chen(China Mobile)

Session: IETF 125, LAKE WG

What has changed since IETF124

Comments:
From Göran Selander
- EDHOC-PSK provide forward secrecy
- An EAD item can be signalled as critical to mandate certain processing, see Section 3.8 of RFC 9528:
- Verification of EDHOC-PSK has already started, to reuse those results could be a large gain in effort and time, instead of doing something different.

From RAFAEL MARIN LOPEZ
- a full implementation of CoAP-EAP (RFC 9820) including OSCORE exchange，have tested as EAP method, EAP-EDHOC and, in particular, method 4 which is EDHOC-PSK.



draft-chen-lake-edhoc-aka-02 has undergone changes:EDHOC-AKA is redesigned based on EDHOC-PSK.

Use Case: Massive Satellite IoT (Non-Terrestrial Networks)

•**EDHOC** provides a lightweight, efficient, and forward-secure key exchange process.

•**AKA** as a credential, utilizes the largest and most mature identity and security infrastructure (SIM cards and mobile core networks), solving the problems of identity authentication and key management for a vast number of Internet of Things devices.

Scenario:
•A large-scale agricultural technology company deploys thousands of battery-powered soil moisture sensors across vast, remote farmlands. These areas lack terrestrial cellular coverage, so the sensors rely on satellite-based Non-Terrestrial Networks (NTN) for connectivity, which are often characterized by high latency and low bandwidth.

Actors:

- **Initiator:** A resource-constrained soil moisture sensor, equipped with a cellular modem and a SIM/eSIM.
- **Responder**: A cloud-based application server, operated by the agriculture company, which collects and analyzes sensor data.
- **Authentication Authority**: A Mobile Network Operator (MNO) that provides both the satellite connectivity and the SIM-based identity credentials.

How It Works: A Profile of EDHOC-PSK

We profile EDHOC-PSK and dynamically generate the PSK for each session.

Mechanism:

1. The 3GPP AKA challenge-response is carried inside External Authorization Data (EAD) fields.
2. A successful AKA exchange produces session keys CK and IK.
3. These keys are used to derive a session-specific PSK, called K_AKA.

K_AKA = EDHOC-KDF(CK, "K_AKA", IK, ...)

1. This K_AKA is then used as the PSK to complete the standard EDHOC-PSK message flow.

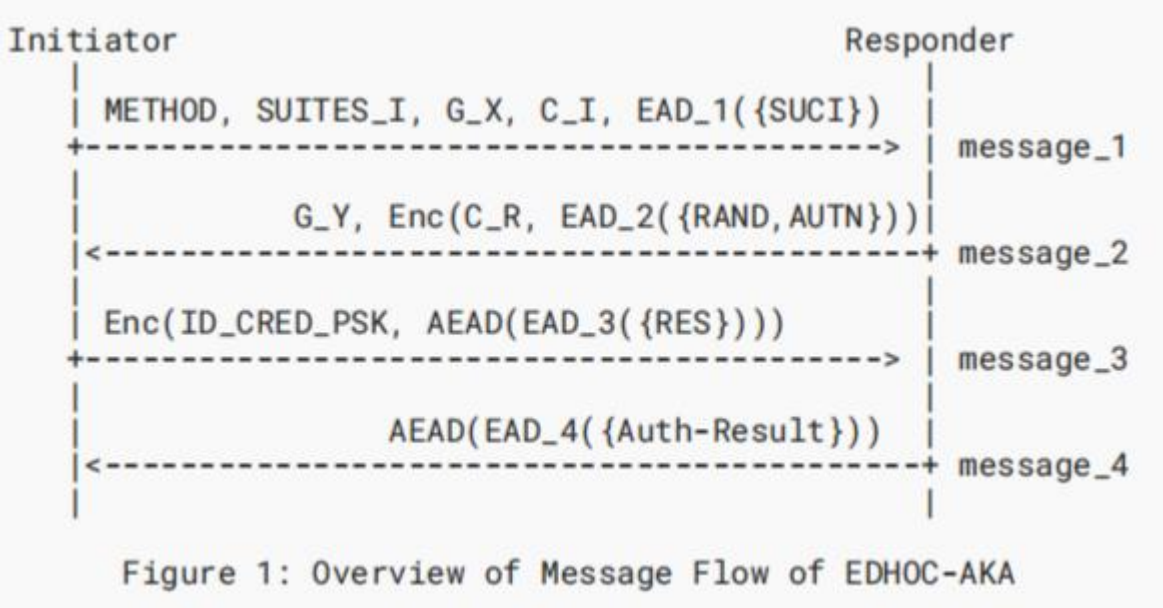


Figure 1: Overview of Message Flow of EDHOC-AKA

The AKA exchange is seamlessly embedded within the EDHOC handshake.

Summary & Next Steps

Summary:

- **A Necessary Profile:** EDHOC-AKA fills a critical need for authenticating massive-scale, SIM-based IoT devices.
- **Reuses & Integrates:** Leverages the globally deployed 3GPP AKA infrastructure instead of reinventing authentication.
- **Lightweight & Secure:** It's a profile of EDHOC-PSK, inheriting its security properties like identity protection and Perfect Forward Secrecy.
- **Simple Mechanism:** Uses the EAD mechanism as intended—for external authorization data—without altering the core EDHOC state machine.

Next Steps:

- This draft specifies the method type and the required EAD labels for IANA registration.
- We believe the approach is sound, simple, and solves a real-world problem.
- We welcome feedback from the working group.
- We request Working Group Adoption.

Thank You!
Questions?