LAKE
Internet-Draft
Intended status: Informational
Expires: 3 September 2026

C. Amsüss

2 March 2026

Applying Generate Random Extensions And Sustain Extensibility (GREASE) to EDHOC Extensibility
draft-ietf-lake-edhoc-grease-01

Abstract

This document applies the extensibility mechanism GREASE (Generate Random Extensions And Sustain Extensibility), which was pioneered for TLS, to the EDHOC ecosystem. It reserves a set of non-critical EAD labels and unusable cipher suites that may be included in messages to ensure peers correctly handle unknown values.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the Lightweight Authenticated Key Exchange Working Group mailing list (lake@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/lake/.

Source for this draft and an issue tracker can be found at https://github.com/lake-wg/grease.

Status of This Memo

Table of Contents

1. Introduction

This document applies the extensibility mechanism GREASE (Generate Random Extensions And Sustain Extensibility), which was pioneered for TLS in [RFC8701], to the EDHOC [RFC9528] ecosystem.

The introduction of [RFC8701] and Section 3.3 of [RFC9170] provide comprehensive motivation for adding such extensions; [I-D.edm-protocol-greasing-02] provides additional background that influenced this document.

The extension points of the EDHOC protocol ([RFC9528]) are cipher suites, methods, EADs (External Authorization Data items) and COSE headers. This document utilizes the cipher suite and EAD extension points.

Unlike in TLS GREASE [RFC8701], EDHOC is operating on tight bandwidth and message size budget, with some messages just barely fitting within relevant networks' fragmentation limits. Thus, more than with TLS GREASE, it is up to implementations to decide whether in their particular use case they can afford to send addtional data.

1.1. Variability in other extension points

If the selected method is unsupported by the peer, EDHOC does not conclude successfully. While values could be reserved for these for use as GREASE, these failed attempts would not be verified between the EDHOC participants without maintaining state between attempted EDHOC sessions. Such an addition is considered impractical for constrained devices, and thus out of scope for this document.

Recommendations for GREASE Section 4 of [I-D.edm-protocol-greasing-02] also include varying other aspects of the protocol, such as varying sequences of elements. EDHOC has little known variability, and intentionally limits choice at times (for example, Section 3.3.2 of [RFC9528] allows only the numeric identifier form where that is possible). Where variation is allowed, e.g. in padding or in the ordering of EAD options, applications are encouraged to exercise it.

The extension point of COSE headers (identifying other ID_CRED_x types) is beyond the scope of this document, and might be addressed orthogonally in the COSE header registry.

2. The GREASE EAD labels

This document registers the following EAD labels as GREASE EADs:

160, 41120, 43690, 44975

These EADs are available in all EDHOC messages. The EADs are used in their positive (non-critical) form.

It is expected that future documents register additional values with the same semantics.

2.1. Use of GREASE EADs by message senders

A sender of an EDHOC message MAY send a GREASE EAD using the non-critical (positive) form at any time, with any or no EAD value (that is, with or without a byte string of any usable length), in any message.

Senders SHOULD consider the properties of the network their messages are sent over, and refrain from adding GREASE when its use would be detrimental to the network (for example, they might use it less frequently when the added size causes fragmentation of the message).

On networks where the data added by the grease EADs does not significantly impact the network, senders SHOULD irregularly send arbitrary (possibly random) GREASE EADs with their messages to ensure that errors resulting from the use of GREASE are detected.

The GREASE EADs MAY be used as an alternative form of padding.

2.1.1. Pattern for limited fingerprinting

A method of applying GREASE is suggested as follows:

* For every message, use GREASE with a random probability of 1 in 64.

* Pick a random GREASE label out of the uniform distribution of available options.

* Pick a random length from the uniformly distributed interval 9 to 40 (inclusive).

* Add the selected GREASE label with a value of the selected length, filled with random bytes.

2.2. Use of GREASE EADs by message recipients

A party receiving a GREASE EAD MUST NOT alter its behavior in any way that would allow random GREASE EADs to alter the security context that gets established.

It MAY alter its behavior in other ways; in particular, it SHOULD randomly insert GREASE EADs in later messages of an exchange in which unprocessed EADs (including GREASE EADs) were present.

Implementations SHOULD NOT attempt to recognize GREASE EADs, and apply the default processing rules.

3. GREASE cipher suites

This document registers the following cipher suites:

160, 41120, -41121, 43690

It is expected that future documents register additional values with the same semantics.

An initiator may insert a GREASE cipher suite at any position in its sequence of preferred cipher suites.

A responder MUST NOT support any of these cipher suites, and MUST treat them like any other cipher suite it does not support.

Thus, these cipher suites never occur as the selected cipher suite. An initiator whose choice of a GREASE cipher suite is accepted needs to discontinue the protocol.

4. Processing of GREASE related failures

It is RECOMMENDED that any counters or statistics about successful and failed connections distinguish between connections in which GREASE was applied and those in which it was not applied. Any operator feedback channel, be it immediately to the user or through network monitoring, SHOULD warn the operator if there are errors that were determined to originate from the use of GREASE or that are significantly likely to originate from there. This provides a feedback path as described in Section 4.4 of [RFC9170].

Whether logging of GREASE related failed connection details is appropriate depends on the privacy policies of the application.

5. Privacy considerations

The way in which GREASE is applied can contribute to identifying which implementation of EDHOC is being used. Implementers of EDHOC are encouraged to use the algorithm described in Section 2.1.1, both to reduce the likelihood of their implementation to be identified through the use of GREASE and to increase the anonymity set of other users of the same algorithm.

6. Security Considerations

The use of the GREASE option has no impact on security in a correct EDHOC implementation.

7. IANA considerations

7.1. EDHOC EADs

IANA is requested to register four new entries into the EDHOC External Authorization Data Registry established in [RFC9528]:

160, 41120, 43690, 44975

All share the name "GREASE", the description "Arbitrary data to ensure extensibility", and this document as a reference.

7.2. EDHOC cipher suites

IANA is requested to register four new values into the EDHOC Cipher Suites Registry established in [RFC9528]:

160, 41120, -41121, 43690

All share the name "GREASE", the array N/A, the description "Unimplementable cipher suite to ensure extensibility", and this document as a reference.

8. References

8.1. Normative 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>.

8.2. Informative References

[RFC8701] Benjamin, D., "Applying Generate Random Extensions And Sustain Extensibility (GREASE) to TLS Extensibility", RFC 8701, DOI 10.17487/RFC8701, January 2020, <https://www.rfc-editor.org/rfc/rfc8701>.

[RFC9170] Thomson, M. and T. Pauly, "Long-Term Viability of Protocol Extension Mechanisms", RFC 9170, DOI 10.17487/RFC9170, December 2021, <https://www.rfc-editor.org/rfc/rfc9170>.

[I-D.edm-protocol-greasing-02]
Pardue, L., "Maintaining Protocols Using Grease and Variability", Work in Progress, Internet-Draft, draft-edm-protocol-greasing-02, 10 July 2023, <https://datatracker.ietf.org/doc/html/draft-edm-protocol-greasing-02>.

Appendix A. Using extension points beyond successful EDHOC runs

Some ways of using the extension points, in particular the critical (negative) use of the GREASE EAD labels and placing a GREASE cipher suite in the selected position do not result in the successful continuation of the EDHOC session.

They can be useful during testing (e.g. to verify that a peer does indeed implement the correct behavior of not silently tolerating critical EAD items it can not process), particulary when they allow a testing system to provoke an error response from the implementation under test. However, this document is concerned with test performed during successful operation, therefore that application is out of scope.

Appendix B. Change log

Since draft-ietf-lake-edhoc-grease-00: Resolve all open issues.

* Question on "is this better than padding" removed. (There are currently implementations of EDHOC that can’t use all EAD values but can do padding).

* Question of COSE header extension deferred to COSE maintenance.

* Use of GREASE values in critical form is out of scope, but appendix illustrates that it can make sense to do, and emphasizes that indeed those options do cause errors when used with negative sign.

Since draft-amsuess-lake-edhoc-grease-01:

* Document was adopted in LAKE.

* Instead of discouraging GREASE around fragmentation limits wholesale, suggest reduced frequency.

* Editorial fix to fingerprinting section.

Since draft-amsuess-lake-edhoc-grease-00:

* Expanded introduction section to just point to the abstract any more.

Since draft-amsuess-core-edhoc-grease-01:

* Update references to RFC9528

* Change target WG to LAKE, renaming to draft-amsuess-lake-edhoc-grease

* Process RFC9170

  - Add a section on failure processing

  - Reference where appropriate

* Process draft-edm-protocol-greasing-02

  - Variability outside of extension points

  - Be firmer against recognizing GREASE values

  - Point out that future options may be registered (instead of the suggested algorithmic registrations)

Since -00:

* Fixed a mix-up between positivity and criticality of options.

* Adjusted numbers accordingly to once more fit in the 0xa. pattern (actually they’re using 0x.a, but that doesn’t work the same way with CBOR).

* Text improvements around recipient side processing.

Acknowledgements

Marco Tiloca pointed out a critical error in the numeric constructions. Gran Selander provided input to reduce mistakable text.

Author’s Address

Christian Amsss
Austria
Email: christian@amsuess.com