CoRE Working Group
Internet-Draft
Updates: 8613 (if approved)
Intended status: Standards Track
Expires: 8 January 2026

M. Tiloca
RISE AB
J. Preu Mattsson
Ericsson AB

7 July 2025

# Encrypted Partial IV in the Constrained Application Protocol (CoAP) OSCORE Option

draft-tiloca-core-oscore-piv-enc-00

## Abstract

The security protocol Object Security for Constrained RESTful Environments (OSCORE) provides end-to-end protection of messages exchanged with the Constrained Application Protocol (CoAP). Messages protected with OSCORE include a CoAP OSCORE option, where the field Partial IV specifies the sequence number value used by the message sender. In the interest of encrypting as much information as reasonably possible, this document defines a lightweight add-on method for encrypting the Partial IV within the OSCORE option. Therefore, it updates RFC 8613. Combined with the update of OSCORE identifiers, the encryption of Partial IV values helps counteracting on-path adversaries that attempt to correlate the sequence numbers observed in different network paths, in order to track OSCORE endpoints that perform a network path migration. The defined encryption method is applicable also to the security protocol Group Object Security for Constrained RESTful Environments (Group OSCORE).

## Discussion Venues

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

Discussion of this document takes place on the Constrained RESTful Environments Working Group mailing list (core@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/core/.

Source for this draft and an issue tracker can be found at https://gitlab.com/crimson84/draft-tiloca-core-oscore-piv-enc.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 8 January 2026.

## Copyright Notice



## Table of Contents

## 1. Introduction

The security protocol Object Security for Constrained RESTful Environments (OSCORE) [RFC8613] provides end-to-end protection of messages exchanged with the Constrained Application Protocol (CoAP) [RFC7252]. OSCORE operates at the application layer by using CBOR Object Signing and Encryption (COSE) [RFC9052] and is independent of the specific transport used to exchange CoAP messages.

Messages protected with OSCORE include the CoAP OSCORE option, which specifies information for the message recipient to correctly perform decryption and verification upon message reception. In particular, the OSCORE option can include a Partial IV, which specifies the sequence number value used by a sender endpoint when protecting an outgoing message. A Partial IV is always present in request messages, while it is typically absent in response messages, with a few exceptions mandating its presence.

Following a message protection with OSCORE, the OSCORE option added to the message is not encrypted, since its content provides a recipient endpoint with information for processing the OSCORE-protected incoming message. However, sending the Partial IV in plaintext enables on-path adversaries to perform trivial tracking of OSCORE endpoints across different network paths, by correlating the sequence numbers observed in those network paths (e.g., following a network path migration, possibly across different network segments).

In the interest of encrypting as much information as reasonably possible, this document updates [RFC8613] and defines a lightweight add-on method for encrypting the Partial IV within the OSCORE option.

This method does not require an in-band signaling and its use does not arbitrarily change on a per-message basis. Instead, upon establishing an OSCORE Security Context, the communicating OSCORE endpoints already have an agreement on either encrypting or not encrypting the Partial IV when they use that Security Context, for every OSCORE-protected message where a Partial IV is included.

Like for the overall protection of messages with OSCORE, the encryption of the Partial IV is agnostic of how exactly the OSCORE Security Context was established and of how the agreement on encrypting the Partial IV was reached. Nevertheless, this document also defines means that endpoints can use to reach that agreement. Absent an explicit agreement, the Partial IV specified in the OSCORE option remains unencrypted, in order to preserve interoperability.

Although it is a self-standing functionality, the encryption of the Partial IV is intended to be combined with the update of OSCORE identifiers defined in [I-D.ietf-core-oscore-id-update]. When OSCORE endpoints perform a network path migration with consequent change of their addressing information, such a combination helps against on-path adversaries that attempt to track OSCORE endpoints across different network paths.

The encryption method defined in this document is applicable also to the security protocol Group Object Security for Constrained RESTful Environments (Group OSCORE) [I-D.ietf-core-oscore-groupcomm] that protects group communication for CoAP [I-D.ietf-core-groupcomm-bis]. In the interest of such a case, this document also defines means to synchronize the members of an OSCORE group with respect to the encryption of the Partial IV within the group.

### 1.1. Terminology

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.

Readers are expected to be familiar with the terms and concepts related to CoAP [RFC7252], Concise Data Definition Language (CDDL) [RFC8610], Concise Binary Object Representation (CBOR) [RFC8949], COSE [RFC9052], OSCORE [RFC8613], and Group OSCORE [I-D.ietf-core-oscore-groupcomm].

## 2. PIV Encryption Key

When the encryption of the Partial IV is enabled, the (Group) OSCORE Security Context is extended with one additional parameter in the Common Context.

The new parameter PIV Encryption Key specifies the encryption key for deriving a keystream to encrypt/decrypt a Partial IV, when this is included in a message protected with (Group) OSCORE.

The PIV Encryption Key is derived as defined for the Sender/Recipient Keys in Section 3.2.1 of [RFC8613], with the following differences.

* The ’id’ element of the ’info’ array is the empty byte string.

* The ’type’ element of the ’info’ array is "PIVEKey". The label is an ASCII string and does not include a trailing NUL byte.

* If the Security Context is used for Group OSCORE and the Group Encryption Algorithm in the Common Context is set (see Section 2.1.7 of [I-D.ietf-core-oscore-groupcomm]), then:

  - The 'alg_aead' element of the 'info' array specifies the Group Encryption Algorithm from the Common Context encoded as a CBOR integer or text string, consistently with the "Value" field in the entry of the "COSE Algorithms" Registry for this algorithm [COSE.Algorithms].

  - The L parameter of the HKDF and the 'L' element of the 'info' array are the length in bytes of the key for the Group Encryption Algorithm specified in the Common Context. While the obtained PIV Encryption Key is never used with the Group Encryption Algorithm, its length was chosen to obtain a matching level of security.

* If the Security Context is used for Group OSCORE and the Group Encryption Algorithm in the Common Context is not set (see Section 2.1.7 of [I-D.ietf-core-oscore-groupcomm]), then:

  - The 'alg_aead' element of the 'info' array specifies the AEAD Algorithm from the Common Context (see Section 2.1.1 of [I-D.ietf-core-oscore-groupcomm]) encoded as a CBOR integer or text string, consistently with the "Value" field in the entry of the "COSE Algorithms" Registry for this algorithm [COSE.Algorithms].

  - The L parameter of the HKDF and the 'L' element of the 'info' array are the length in bytes of the key for the AEAD Algorithm specified in the Common Context. While the obtained PIV Encryption Key is never used with the AEAD Algorithm, its length was chosen to obtain a matching level of security.

## 3. Encryption of the Partial IV

Once composed an OSCORE-protected outgoing message MSG that includes the Partial IV in the OSCORE option (see Section 6.1 of [RFC8613]), the sender endpoint performs the following steps.

1. Compose SAMPLE as the first N bytes of the CoAP payload of MSG, where N = min(LENGTH, 16) and LENGTH denotes the length in bytes of the CoAP payload of MSG.

   Note that:

   * LENGTH is guaranteed to have a minimum value of 9.

* If MSG was protected with OSCORE [RFC8613] or instead with Group OSCORE using the pairwise mode (see Section 8 of [I-D.ietf-core-oscore-groupcomm]), then the CoAP payload is the ciphertext of the COSE object.

* If MSG was protected with Group OSCORE using the group mode (see Section 7 of [I-D.ietf-core-oscore-groupcomm]), then the CoAP payload is the ciphertext of the COSE object concatenated with the encrypted countersignature.

2. Compose INPUT as follows:

   * If the length of SAMPLE is less than 16 bytes, INPUT is obtained by left-padding SAMPLE with zeroes to exactly 16 bytes.

   * If the length of SAMPLE is 16 bytes, then INPUT takes SAMPLE.

3. Compute the 16-byte IV_KEYSTREAM as below:

   IV_KEYSTREAM = AES-ECB(PIV Encryption Key, INPUT)

   where:

   * AES-ECB is the AES algorithm in ECB mode [AES].

   * PIV Encryption Key is taken from the Common Context of the Security Context used to produce MSG (see Section 2). It is used as encryption key for the AES-ECB encryption.

   * INPUT is the result of Step 2. It is used as plaintext for the AES-ECB encryption.

4. Compute the encrypted Partial IV, by XORing the plain Partial IV from the OSCORE option of MSG with the Q bytes from the IV_KEYSTREAM's start, where Q is the length in bytes of the plain Partial IV.

   For example, if the plain Partial IV from the OSCORE option of MSG is 0x001122 (Q = 3 bytes) and IV_KEYSTREAM is 0xffeeddccbbaa99887766554433221100 (16 bytes), then the bytes of IV_KEYSTREAM to XOR with the plain Partial IV are 0xffeedd.

5. Replace the plain Partial IV in the OSCORE option of MSG with the encrypted Partial IV computed at Step 4.

Once completed the steps above, the sender endpoint transmits MSG as expected.

## 4. Decryption of the Partial IV

Upon receiving an incoming message MSG that includes an encrypted Partial IV and after having retrieved the (Group) OSCORE Security Context to process the message, the recipient endpoint performs the following steps.

1. Compute IV_KEYSTREAM by means of the same method defined at Steps 1-3 of Section 3.

2. Compute the plain Partial IV, by XORing the encrypted Partial IV from the OSCORE option of MSG with the Q bytes from the IV_KEYSTREAM's start, where Q is the length in bytes of the encrypted Partial IV.

3. Replace the encrypted Partial IV in the OSCORE option of MSG with the plain Partial IV computed at Step 2.

Once completed the steps above, the recipient endpoint continues processing MSG as expected.

## 5. Considerations on Effectiveness

If an endpoint that encrypts the Partial IV expects to send more than 256 messages including a Partial IV and protected with the same Sender Context, then that Sender Context SHOULD use 65536 as lowest value for the Sender Sequence Number of that endpoint.

This ensures that the Partial IV is encoded in at least 3 bytes in the OSCORE option, hence defeating attempts to track an endpoint by leveraging the transition between the encoding of Partial IVs from 1 to 2 bytes in size, or from 2 to 3 bytes in size.

## 6. Agreement on Encrypting the Partial IV

Absent explicit information associated with the (Group) OSCORE Security Context used and an agreement with its peer(s), an endpoint does not encrypt/decrypt the Partial IV when using that Security Context, thereby preserving interoperability.

The rest of this section defines means that endpoints can use to reach an agreement about encrypting the Partial IV as specified in this document.

### 6.1. Agreement for OSCORE

TBD

Editor’s note: expected means to cover include:

* Pre-provisioning
* In EDHOC
* In the OSCORE profile of the ACE framework
* In OMA Lightweight Machine-to-Machine (LwM2M)

### 6.2. Agreement for Group OSCORE

TBD

Editor’s note: expected means to cover include:

* The OSCORE Group Manager based on the ACE framework
  - Messages to (candidate) group members
  - Messages to external signature verifiers
  - Message to/from an Administrator
* A CoAP server supporting observe multicast notifications and self-managing the OSCORE group for its group observations.

## 7. Security Considerations

The same security considerations from [RFC8613] and [I-D.ietf-core-oscore-groupcomm] hold for this document when messages are protected with OSCORE or Group OSCORE, respectively. Furthermore, the following considerations also apply.

### 7.1. Limitations

The method defined in this document provides confidentiality protection of the Partial IV against passive adversaries.

An active adversary could guess the plain Partial IV and have a recipient OSCORE endpoint confirm the guesses, e.g., taking advantage of timing side channels. For instance, this can be the case when the recipient endpoint discards an incoming message that is detected as a replay, i.e., without attempting to decrypt and verify the message and hence revealing information through timing side channels.

Similarly, depending on whether the processing of an incoming request message fails due to a replay detection or instead to a failed decryption and verification, the recipient endpoint would follow-up by sending different, unprotected error response messages, which the adversary can leverage to confirm the guesses.

## 7.2. Encryption Robustness

When performing the steps at Section 3 and Section 4, using the same PIV Encryption Key and SAMPLE more than once risks compromising the encryption of the Partial IV. That is, encrypting two different Partial IVs by leveraging the same PIV Encryption Key and SAMPLE reveals the exclusive OR of the encrypted Partial IVs.

Assuming that SAMPLE is consistent with the outcome of a pseudorandom function (PRF), if L bits are sampled, then the odds that two SAMPLE byte strings of length L are identical approach P = 2^(-L/2), that is, the birthday bound. For messages protected with (Group) OSCORE, SAMPLE has a minimum length L_MIN of 72 bits and a maximum length L_MAX of 128 bits. Therefore, P is at least 2^36 (when the CoAP payload has a length of L_MIN bits) and at most 2^64 (when the CoAP payload has a length of L_MAX bits or more).

## 7.3. Impact on Endpoint Trackability

The method defined in [I-D.ietf-core-oscore-id-update] allows OSCORE endpoints to update their OSCORE identifiers. Switching to a new OSCORE identifier is particularly useful when an endpoint migrates to a new network path, as it counteracts attempts to track the endpoint across different network paths by leveraging its OSCORE identifier.

Clearly, an on-path adversary might still be able to track an endpoint, e.g., by leveraging addressing information that does not change upon network migration or by attempting to correlate the Partial IV values observed on different network paths. The method for encrypting the OSCORE Partial IV defined in this document helps against the latter. That is, in case the OSCORE Partial IV is not encrypted, endpoints could be successfully tracked even when different OSCORE identifiers are used on each network path.

The tracking of an OSCORE endpoint that migrates to a new network path can be largely counteracted by using the method defined in this document, if combined with the use of new source addressing information (e.g., IP address and link-layer address) and of a new OSCORE identifier that the endpoint has not used before in other network paths. This does not prevent other properties of network packets, e.g., their timing or length, from being used to correlate activities of the same endpoint across different network paths.

## 8. IANA Considerations

TBD

Editor’s note: expected actions are registrations of new parameters that effectively enable the means defined in Section 6.

## 9. References

### 9.1. Normative References

[AES] NIST, "Advanced encryption standard (AES)", May 2023, <https://doi.org/10.6028/NIST.FIPS.197-upd1>.

[COSE.Algorithms] IANA, "COSE Algorithms", <https://www.iana.org/assignments/cose/cose.xhtml#algorithms>.

[I-D.ietf-core-oscore-groupcomm] Tiloca, M., Selander, G., Palombini, F., Mattsson, J. P., and R. Hglund, "Group Object Security for Constrained RESTful Environments (Group OSCORE)", Work in Progress, Internet-Draft, draft-ietf-core-oscore-groupcomm-26, 5 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-oscore-groupcomm-26>.

[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/rfc/rfc2119>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, DOI 10.17487/RFC7252, June 2014, <https://www.rfc-editor.org/rfc/rfc7252>.

[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/rfc/rfc8174>.

[RFC8610] Birkholz, H., Vigano, C., and C. Bormann, "Concise Data Definition Language (CDDL): A Notational Convention to Express Concise Binary Object Representation (CBOR) and JSON Data Structures", RFC 8610, DOI 10.17487/RFC8610, June 2019, <https://www.rfc-editor.org/rfc/rfc8610>.

[RFC8613] Selander, G., Mattsson, J., Palombini, F., and L. Seitz, "Object Security for Constrained RESTful Environments (OSCORE)", RFC 8613, DOI 10.17487/RFC8613, July 2019, <https://www.rfc-editor.org/rfc/rfc8613>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9052] Schaad, J., "CBOR Object Signing and Encryption (COSE): Structures and Process", STD 96, RFC 9052, DOI 10.17487/RFC9052, August 2022, <https://www.rfc-editor.org/rfc/rfc9052>.

### 9.2. Informative References

[I-D.ietf-core-groupcomm-bis] Dijk, E. and M. Tiloca, "Group Communication for the Constrained Application Protocol (CoAP)", Work in Progress, Internet-Draft, draft-ietf-core-groupcomm-bis-14, 2 July 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-groupcomm-bis-14>.

[I-D.ietf-core-oscore-id-update] Hglund, R. and M. Tiloca, "Identifier Update for OSCORE", Work in Progress, Internet-Draft, draft-ietf-core-oscore-id-update-02, 8 January 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-core-oscore-id-update-02>.

## Acknowledgments

The authors sincerely thank Rikard Hglund and Gran Selander for their comments and feedback.

This work was supported by the Sweden’s Innovation Agency VINNOVA within the EUREKA CELTIC-NEXT project CYPRESS.

## Authors’ Addresses

Marco Tiloca
RISE AB
Isafjordsgatan 22
SE-164 40 Kista
Sweden
Email: marco.tiloca@ri.se

John Preu Mattsson
Ericsson AB
SE-164 80 Stockholm
Sweden
Email: john.mattsson@ericsson.com