Workgroup: CoRE Working Group
Internet-Draft:
draft-hoeglund-core-oscore-key-limits-02
Updates: 8613 (if approved)
Published: 25 October 2021
Intended Status: Standards Track
Expires: 28 April 2022
Authors: R. Höglund   M. Tiloca
         RISE AB   RISE AB

Key Update for OSCORE (KUDOS)

Abstract

Object Security for Constrained RESTful Environments (OSCORE) uses AEAD algorithms to ensure confidentiality and integrity of exchanged messages. Due to known issues allowing forgery attacks against AEAD algorithms, limits should be followed on the number of times a specific key is used for encryption or decryption. This document defines how two OSCORE peers must follow these limits and what steps they must take to preserve the security of their communications. Therefore, this document updates RFC8613. Furthermore, this document specifies Key Update for OSCORE (KUDOS), a lightweight procedure that two peers can use to update their keying material and establish a new OSCORE Security Context.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Object Security for Constrained RESTful Environments (OSCORE) [RFC8613] provides end-to-end protection of CoAP [RFC7252] messages at the application-layer, ensuring message confidentiality and integrity, replay protection, as well as binding of response to request between a sender and a recipient.

In particular, OSCORE uses AEAD algorithms to provide confidentiality and integrity of messages exchanged between two peers. Due to known issues allowing forgery attacks against AEAD algorithms, limits should be followed on the number of times a specific key is used to perform encryption or decryption [I-D.irtf-cfrg-aead-limits].

Should these limits be exceeded, an adversary may break the security properties of the AEAD algorithm, such as message confidentiality and integrity, e.g. by performing a message forgery attack. The original OSCORE specification [RFC8613] does not consider such limits.

This document updates [RFC8613] as follows.

- It defines when a peer must stop using an OSCORE Security Context shared with another peer, due to the reached key usage limits. When this happens, the two peers have to establish a new Security Context with new keying material, in order to continue their secure communication with OSCORE.

- It specifies KUDOS, a lightweight key update procedure that the two peers can use in order to update their current keying material and establish a new OSCORE Security Context. This deprecates and replaces the procedure specified in Appendix B.2 of [RFC8613].

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 the CoAP [RFC7252] and OSCORE [RFC8613] protocols.

2. AEAD Key Usage Limits in OSCORE

The following sections details how key usage limits for AEAD algorithms must be considered when using OSCORE. It covers specific limits for common AEAD algorithms used with OSCORE; necessary additions to the OSCORE Security Context, updates to the OSCORE message processing, and existing methods for rekeying OSCORE.

2.1. Problem Overview

The OSCORE security protocol [RFC8613] uses AEAD algorithms to provide integrity and confidentiality of messages, as exchanged between two peers sharing an OSCORE Security Context.

When processing messages with OSCORE, each peer should follow specific limits as to the number of times it uses a specific key. This applies separately to the Sender Key used to encrypt outgoing messages, and to the Recipient Key used to decrypt and verify incoming protected messages.

Exceeding these limits may allow an adversary to break the security properties of the AEAD algorithm, such as message confidentiality and integrity, e.g. by performing a message forgery attack.

The following refers to the two parameters 'q' and 'v' introduced in [I-D.irtf-cfrg-aead-limits], to use when deploying an AEAD algorithm.

- 'q': this parameter has as value the number of messages protected with a specific key, i.e. the number of times the AEAD algorithm has been invoked to encrypt data with that key.

- 'v': this parameter has as value the number of alleged forgery attempts that have been made against a specific key, i.e. the amount of failed decryptions that has been done with the AEAD algorithm for that key.

When a peer uses OSCORE:

- The key used to protect outgoing messages is its Sender Key, in its Sender Context.

- The key used to decrypt and verify incoming messages is its Recipient Key, in its Recipient Context.

Both keys are derived as part of the establishment of the OSCORE Security Context, as defined in Section 3.2 of [RFC8613].

As mentioned above, exceeding specific limits for the 'q' or 'v' value can weaken the security properties of the AEAD algorithm used, thus compromising secure communication requirements.

Therefore, in order to preserve the security of the used AEAD algorithm, OSCORE has to observe limits for the 'q' and 'v' values, throughout the lifetime of the used AEAD keys.

2.1.1. Limits for 'q' and 'v'

Formulas for calculating the security levels as Integrity Advantage (IA) and Confidentiality Advantage (CA) probabilities, are presented in [I-D.irtf-cfrg-aead-limits]. These formulas take as input specific values for 'q' and 'v' (see section Section 2.1) and for 'l', i.e., the maximum length of each message (in cipher blocks).

For the algorithms that can be used as AEAD Algorithm for OSCORE shows in Figure 1, the key property to achieve is having IA and CA values which are no larger than p = 2^-64, which will ensure a safe security level for the AEAD Algorithm. This can be entailed by using the values q = 2^20, v = 2^20, and l = 2^10, that this document recommends to use for these algorithms.

Figure 1 shows the resulting IA and CA probabilities enjoyed by the considered algorithms, when taking the value of 'q', 'v' and 'l' above as input to the formulas defined in [I-D.irtf-cfrg-aead-limits].

Algorithm name	IA probability	CA probability
AEAD_AES_128_CCM	2^-64	2^-66
AEAD_AES_128_GCM	2^-97	2^-89
AEAD_AES_256_GCM	2^-97	2^-89
AEAD_CHACHA20_POLY1305	2^-73	-

Figure 1: Probabilities for algorithms based on chosen q, v and l values.

For the AEAD_AES_128_CCM_8 algorithm when used as AEAD Algorithm for OSCORE, larger IA and CA values are achieved, depending on the value of 'q', 'v' and 'l'. Figure 2 shows the resulting IA and CA probabilities enjoyed by AEAD_AES_128_CCM_8, when taking different values of 'q', 'v' and 'l' as input to the formulas defined in [I-D.irtf-cfrg-aead-limits].

As shown in Figure 2, it is especially possible to achieve the lowest IA = 2^-54 and a good CA = 2^-70 by considering the largest possible value of the (q, v, l) triplet equal to (2^20, 2^10, 2^8), while still keeping a good security level. Note that the value of 'l' does not impact on IA, while CA displays good values for every considered value of 'l'.

When AEAD_AES_128_CCM_8 is used as AEAD Algorithm for OSCORE, this document recommends to use the triplet (q, v, l) = (2^20, 2^10, 2^8) and to never use a triplet (q, v, l) such that the resulting IA and CA probabilities are higher than 2^-54.

'q', 'v' and 'l'	IA probability	CA probability
q=2^20, v=2^20, l=2^8	2^-44	2^-70
q=2^15, v=2^20, l=2^8	2^-44	2^-80
q=2^10, v=2^20, l=2^8	2^-44	2^-90
q=2^20, v=2^15, l=2^8	2^-49	2^-70
q=2^15, v=2^15, l=2^8	2^-49	2^-80
q=2^10, v=2^15, l=2^8	2^-49	2^-90
q=2^20, v=2^14, l=2^8	2^-50	2^-70
q=2^15, v=2^14, l=2^8	2^-50	2^-80
q=2^10, v=2^14, l=2^8	2^-50	2^-90
q=2^20, v=2^10, l=2^8	2^-54	2^-70
q=2^15, v=2^10, l=2^8	2^-54	2^-80
q=2^10, v=2^10, l=2^8	2^-54	2^-90
q=2^20, v=2^20, l=2^6	2^-44	2^-74
q=2^15, v=2^20, l=2^6	2^-44	2^-84
q=2^10, v=2^20, l=2^6	2^-44	2^-94
q=2^20, v=2^15, l=2^6	2^-49	2^-74
q=2^15, v=2^15, l=2^6	2^-49	2^-84
q=2^10, v=2^15, l=2^6	2^-49	2^-94
q=2^20, v=2^14, l=2^6	2^-50	2^-74
q=2^15, v=2^14, l=2^6	2^-50	2^-84
q=2^10, v=2^14, l=2^6	2^-50	2^-94
q=2^20, v=2^10, l=2^6	2^-54	2^-74
q=2^15, v=2^10, l=2^6	2^-54	2^-84
q=2^10, v=2^10, l=2^6	2^-54	2^-94

Figure 2: Probabilities for AEAD_AES_128_CCM_8 based on chosen q, v and l values.

The algorithms using AES presented in this draft all use a block size of 16 bytes (128 bits), while AEAD_CHACHA20_POLY1305 uses a block size of 64 bytes (512 bits). As 'l' is defined as the maximum size of each message in blocks, different block sizes will result in different maximum messages sizes for the same value of 'l'. Figure 3 presents the resulting maximum message size in bytes for the different algorithms and values of 'l' presented in this document.

Algorithm name	l=2^6 in bytes	l=2^8 in bytes	l=2^10 in bytes
AEAD_AES_128_CCM	1024	4096	16384
AEAD_AES_128_GCM	1024	4096	16384
AEAD_AES_256_GCM	1024	4096	16384
AEAD_AES_128_CCM_8	1024	4096	16384
AEAD_CHACHA20_POLY1305	4096	16384	65536

Figure 3: Maximum length of each message (in bytes)

2.2. Additional Information in the Security Context

In addition to what defined in Section 3.1 of [RFC8613], the OSCORE Security Context MUST also include the following information.

2.2.1. Common Context

The Common Context is extended to include the following parameter.

* 'exp': with value the expiration time of the OSCORE Security Context, as a non-negative integer. The parameter contains a numeric value representing the number of seconds from 1970-01-01T00:00:00Z UTC until the specified UTC date/time, ignoring leap seconds, analogous to what specified for NumericDate in Section 2 of [RFC7519].

  At the time indicated in this field, a peer MUST stop using this Security Context to process any incoming or outgoing message, and is required to establish a new Security Context to continue OSCORE-protected communications with the other peer.

2.2.2. Sender Context

The Sender Context is extended to include the following parameters.

* 'count_q': a non-negative integer counter, keeping track of the current 'q' value for the Sender Key. At any time, 'count_q' has as value the number of messages that have been encrypted using the Sender Key. The value of 'count_q' is set to 0 when establishing the Sender Context.

* 'limit_q': a non-negative integer, which specifies the highest value that 'count_q' is allowed to reach, before stopping using the Sender Key to process outgoing messages.

The value of 'limit_q' depends on the AEAD algorithm specified in the Common Context, considering the properties of that algorithm. The value of 'limit_q' is determined according to Section 2.1.1.

2.2.3. Recipient Context

The Recipient Context is extended to include the following parameters.

- 'count_v': a non-negative integer counter, keeping track of the current 'v' value for the Recipient Key. At any time, 'count_v' has as value the number of failed decryptions occurred on incoming messages using the Recipient Key. The value of 'count_v' is set to 0 when establishing the Recipient Context.

- 'limit_v': a non-negative integer, which specifies the highest value that 'count_v' is allowed to reach, before stopping using the Recipient Key to process incoming messages.

  The value of 'limit_v' depends on the AEAD algorithm specified in the Common Context, considering the properties of that algorithm. The value of 'limit_v' is determined according to Section 2.1.1.

2.3. OSCORE Messages Processing

In order to keep track of the 'q' and 'v' values and ensure that AEAD keys are not used beyond reaching their limits, the processing of OSCORE messages is extended as defined in this section. A limitation that is introduced is that, in order to not exceed the selected value for 'l', the total size of the COSE plaintext, authentication Tag, and possible cipher padding for a message may not exceed the block size for the selected algorithm multiplied with 'l'.

In particular, the processing of OSCORE messages follows the steps outlined in Section 8 of [RFC8613], with the additions defined below.

2.3.1. Protecting a Request or a Response

Before encrypting the COSE object using the Sender Key, the 'count_q' counter MUST be incremented.

If 'count_q' exceeds the 'limit_q' limit, the message processing MUST be aborted. From then on, the Sender Key MUST NOT be used to encrypt further messages.

2.3.2. Verifying a Request or a Response

If an incoming message is detected to be a replay (see Section 7.4 of [RFC8613]), the 'count_v' counter MUST NOT be incremented.

If the decryption and verification of the COSE object using the Recipient Key fails, the 'count_v' counter MUST be incremented.

After 'count_v' has exceeded the 'limit_v' limit, incoming messages MUST NOT be decrypted and verified using the Recipient Key, and their processing MUST be aborted.

3. Current methods for Rekeying OSCORE

Before the limit of 'q' or 'v' defined in Section 2.1.1 has been reached for an OSCORE Security Context, the two peers have to establish a new OSCORE Security Context, in order to continue using OSCORE for secure communication.

In practice, the two peers have to establish new Sender and Recipient Keys, as the keys actually used by the AEAD algorithm. When this happens, both peers reset their 'count_q' and 'count_v' values to 0 (see Section 2.2).

Other specifications define a number of ways to accomplish this, as summarized below.

- The two peers can run the procedure defined in Appendix B.2 of [RFC8613]. That is, the two peers exchange three or four messages, protected with temporary Security Contexts adding randomness to the ID Context.

  As a result, the two peers establish a new OSCORE Security Context with new ID Context, Sender Key and Recipient Key, while keeping the same OSCORE Master Secret and OSCORE Master Salt from the old OSCORE Security Context.

  This procedure does not require any additional components to what OSCORE already provides, and it does not provide perfect forward secrecy.

  The procedure defined in Appendix B.2 of [RFC8613] is used in 6TiSCH networks [RFC7554][RFC8180] when handling failure events. That is, a node acting as Join Registrar/Coordinator (JRC) assists new devices, namely "pledges", to securely join the network as per the Constrained Join Protocol [RFC9031]. In particular, a pledge exchanges OSCORE-protected messages with the JRC, from which it obtains a short identifier, link-layer keying material and other configuration parameters. As per Section 8.3.3 of [RFC9031], a JRC that experiences a failure event may likely lose information about joined nodes, including their assigned identifiers. Then, the reinitialized JRC can establish a new OSCORE Security Context with each pledge, through the procedure defined in Appendix B.2 of [RFC8613].

- The two peers can run the OSCORE profile [I-D.ietf-ace-oscore-profile] of the Authentication and Authorization for Constrained Environments (ACE) Framework [I-D.ietf-ace-oauth-authz].

  When a CoAP client uploads an Access Token to a CoAP server as an access credential, the two peers also exchange two nonces. Then, the two peers use the two nonces together with information provided by the ACE Authorization Server that issued the Access Token, in order to derive an OSCORE Security Context.

  This procedure does not provide perfect forward secrecy.

- The two peers can run the EDHOC key exchange protocol based on Diffie-Hellman and defined in [I-D.ietf-lake-edhoc], in order to establish a pseudo-random key in a mutually authenticated way.

  Then, the two peers can use the established pseudo-random key to derive external application keys. This allows the two peers to securely derive especially an OSCORE Master Secret and an OSCORE Master Salt, from which an OSCORE Security Context can be established.

  This procedure additionally provides perfect forward secrecy.

- If one peer is acting as LwM2M Client and the other peer as LwM2M Server, according to the OMA Lightweight Machine to Machine Core specification [LwM2M], then the LwM2M Client peer may take the initiative to bootstrap again with the LwM2M Bootstrap Server, and receive again an OSCORE Security Context. Alternatively, the LwM2M Server can instruct the LwM2M Client to initiate this procedure.

  If the OSCORE Security Context information on the LwM2M Bootstrap Server has been updated, the LwM2M Client will thus receive a fresh OSCORE Security Context to use with the LwM2M Server.

  In addition to that, the LwM2M Client, the LwM2M Server as well as the LwM2M Bootstrap server are required to use the procedure defined in Appendix B.2 of [RFC8613] and overviewed above, when they use a certain OSCORE Security Context for the first time [LwM2M-Transport].

Manually updating the OSCORE Security Context at the two peers should be a last resort option, and it might often be not practical or feasible.

Even when any of the alternatives mentioned above is available, it is RECOMMENDED that two OSCORE peers update their Security Context by using the KUDOS procedure as defined in Section 4 of this document.

It is RECOMMENDED that the peer initiating the key update procedure starts it before reaching the 'q' or 'v' limits. Otherwise, the AEAD keys possibly to be used during the key update procedure itself may already be or become invalid before the rekeying is completed, which may prevent a successful establishment of the new OSCORE Security Context altogether.

4. Key Update for OSCORE (KUDOS)

This section defines KUDOS, a lightweight procedure that two OSCORE peers can use to update their keying material and establish a new OSCORE Security Context.

KUDOS relies on the support function updateCtx() defined in Section 4.2 and the message exchange defined in Section 4.3. The following properties are fulfilled.

*KUDOS can be initiated by either peer. In particular, the client or the server may start KUDOS by sending the first rekeying message.

*The new OSCORE Security Context enjoys Perfect Forward Secrecy.

*The same ID Context value used in the old OSCORE Security Context is preserved in the new Security Context. Furthermore, the ID Context value never changes throughout the KUDOS execution.

*KUDOS is robust against a peer rebooting, and it especially avoids the reuse of AEAD (nonce, key) pairs.

*KUDOS completes in one round trip. The two peers achieve mutual proof-of-possession in the following exchange, which is protected with the newly established OSCORE Security Context.

4.1. Extensions to the OSCORE Option

In order to support the message exchange for establishing a new OSCORE Security Context as defined in Section 4.3, this document extends the use of the OSCORE option originally defined in [RFC8613] as follows.

*This document defines the usage of the seventh least significant bit, called "Extension-1 Flag", in the first byte of the OSCORE option containing the OSCORE flag bits. This flag bit is specified in Section 6.1.

  When the Extension-1 Flag is set to 1, the second byte of the OSCORE option MUST include the set of OSCORE flag bits 8-15.

- This document defines the usage of the first least significant bit "ID Detail Flag", 'd', in the second byte of the OSCORE option containing the OSCORE flag bits. This flag bit is specified in Section 6.1.

  When it is set to 1, the compressed COSE object contains an 'id detail', to be used for the steps defined in Section 4.3. In particular, the 1 byte following 'kid context' (if any) encodes the length x of 'id detail', and the following x bytes encode 'id detail'.

- The second-to-eighth least significant bits in the second byte of the OSCORE option containing the OSCORE flag bits are reserved for future use. These bits SHALL be set to zero when not in use. According to this specification, if any of these bits are set to 1, the message is considered to be malformed and decompression fails as specified in item 2 of Section 8.2 of [RFC8613].

Figure 4 shows the OSCORE option value including also 'id detail'.

```
 0 1 2 3 4 5 6 7   8   9   10  11  12  13  14  15 <----- n bytes ----->
+-+-+-+-+-+-+-+-+---+---+---+---+---+---+---+---+---------------------+
|0|1|0|h|k|  n  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | d | Partial IV (if any) |
+-+-+-+-+-+-+-+-+---+---+---+---+---+---+---+---+---------------------+

 <- 1 byte -> <----- s bytes ------> <- 1 byte -> <----- x bytes ---->
+------------+----------------------+---------------------------------+
| s (if any) | kid context (if any) | x (if any) | id detail (if any) |
+------------+----------------------+------------+--------------------+

+------------------+
| kid (if any) ... |
+------------------+
```

Figure 4: The OSCORE option value, including 'id detail'

4.2. Function for Security Context Update

The updateCtx() function shown in Figure 5 takes as input a nonce N as well as an OSCORE Security Context CTX_IN, and returns as output a new OSCORE Security Context CTX_OUT.

As a first step, the updateCtx() function derives the new values of the Master Secret and Master Salt for CTX_OUT, according to one of the two following methods. The used method depends on how the two peers established their original Security Context, i.e., the

Security Context that they shared before performing KUDOS with one another for the first time.

- If the original Security Context was established by running the EDHOC protocol [I-D.ietf-lake-edhoc], the following applies.

  First, the EDHOC key PRK_4x3m shared by the two peers is updated using the EDHOC-KeyUpdate() function defined in Section 4.4 of [I-D.ietf-lake-edhoc], which takes the nonce N as input.

  After that, the EDHOC-Exporter() function defined in Section 4.3 of [I-D.ietf-lake-edhoc] is used to derive the new values for the Master Secret and Master Salt, consistently with what is defined in Appendix A.2 of [I-D.ietf-lake-edhoc]. In particular, the context parameter provided as second argument to the EDHOC-Exporter() function is the empty CBOR byte string (0x40) [RFC8949], which is denoted as h''.

  Note that, compared to the compliance requirements in Section 7 of [I-D.ietf-lake-edhoc], a peer MUST support the EDHOC-KeyUpdate() function, in case it establishes an original Security Context through the EDHOC protocol and intends to perform KUDOS.

- If the original Security Context was established through other means than the EDHOC protocol, the new Master Secret is derived through an HKDF-Expand() step, which takes as input N as well as the Master Secret value from the Security Context CTX_IN. Instead, the new Master Salt takes N as value.

In either case, the derivation of new values follows the same approach used in TLS 1.3, which is also based on HKDF-Expand (see Section 7.1 of [RFC8446]) and used for computing new keying material in case of key update (see Section 4.6.3 of [RFC8446]).

After that, the new Master Secret and Master Salt parameters are used to derive a new Security Context CTX_OUT as per Section 3.2 of [RFC8613]. Any other parameter required for the derivation takes the same value as in the Security Context CTX_IN. Finally, the function returns the newly derived Security Context CTX_OUT.

```
updateCtx(N, CTX_IN) {

  CTX_OUT       // The new Security Context
  MSECRET_NEW   // The new Master Secret
  MSALT_NEW     // The new Master Salt

  if <the original Security Context was established through EDHOC> {

    EDHOC-KeyUpdate(N)
    // This results in updating the key PRK_4x3m of the
    // EDHOC session, i.e., PRK_4x3m = Extract(N, PRK_4x3m)

    MSECRET_NEW = EDHOC-Exporter("OSCORE_Master_Secret",
                                 h'', key_length)
      = EDHOC-KDF(PRK_4x3m, TH_4,
                  "OSCORE_Master_Secret", h'', key_length)

    MSALT_NEW = EDHOC-Exporter("OSCORE_Master_Salt",
                               h'', salt_length)
      = EDHOC-KDF(PRK_4x3m, TH_4,
                  "OSCORE_Master_Salt", h'', salt_length)

  }
  else {
    Master Secret Length = < Size of CTX_IN.MasterSecret in bytes >

    MSECRET_NEW = HKDF-Expand-Label(CTX_IN.MasterSecret, Label,
                                    N, Master Secret Length)
                = HKDF-Expand(CTX_IN.MasterSecret, HkdfLabel,
                              Master Secret Length)

    MSALT_NEW = N;
  }

  < Derive CTX_OUT using MSECRET_NEW and MSALT_NEW,
    together with other parameters from CTX_IN >

  Return CTX_OUT;

}

Where HkdfLabel is defined as

struct {
    uint16 length = Length;
    opaque label<7..255> = "oscore " + Label;
    opaque context<0..255> = Context;
} HkdfLabel;
```

Figure 5: Function for deriving a new OSCORE Security Context

4.3. Establishment of the New OSCORE Security Context

This section defines the actual KUDOS procedure performed by two peers to update their OSCORE keying material. Before starting KUDOS, the two peers share the OSCORE Security Context CTX_OLD. Once completed the KUDOS execution, the two peers agree on a newly established OSCORE Security Context CTX_NEW.

In particular, each peer contributes by generating a fresh value R1 or R2, and providing it to the other peer. The byte string concatenation of the two values, hereafter denoted as R1 | R2, is used as input N by the updateCtx() function, in order to derive the new OSCORE Security Context CTX_NEW. As for any new OSCORE Security Context, the Sender Sequence Number and the replay window are re-initialized accordingly (see Section 3.2.2 of [RFC8613]).

Once a peer has successfully derived the new OSCORE Security Context CTX_NEW, that peer MUST terminate all the ongoing observations it has with the other peer as protected with the old Security Context CTX_OLD.

Once a peer has successfully decrypted and verified an incoming message protected with CTX_NEW, that peer MUST discard the old Security Context CTX_OLD.

KUDOS can be started by the client or the server, as defined in Section 4.3.1 and Section 4.3.2, respectively. The following properties hold for both the client- and server-initiated version of KUDOS.

- The initiator always offers the fresh value R1.

- The responder always offers the fresh value R2.

- The responder is always the first one deriving the new OSCORE Security Context CTX_NEW.

- The initiator is always the first one achieving key confirmation, hence able to safely discard the old OSCORE Security Context CTX_OLD.

- Both the initiator and the responder use the same respective OSCORE Sender ID and Recipient ID. Also, they both preserve and use the same OSCORE ID Context from CTX_OLD.

The length of the nonces R1, and R2 is application specific. The application needs to set the length of each nonce such that the probability of its value being repeated is negligible; typically, at least 8 bytes long.

4.3.1. Client-Initiated Key Update

Figure 6 shows the KUDOS workflow with the client acting as initiator.

```
                   Client               Server
                (initiator)          (responder)
                     |                    |
Generate R1          |                    |
                     |                    |
CTX_1 =              |                    |
  updateCtx(R1,      |                    |
            CTX_OLD) |                    |
                     |                    |
                     |     Request #1     |
Protect with CTX_1   |------------------->|
                     | OSCORE Option:     | CTX_1 =
                     |   ...              |   update(R1,
                     |   d flag: 1        |          CTX_OLD)
                     |   ...              |
                     |   ID Detail: R1    | Verify with CTX_1
                     |   ...              |
                     |                    | Generate R2
                     |                    |
                     |                    | CTX_NEW =
                     |                    |   update(R1|R2,
                     |                    |          CTX_OLD)
                     |                    |
                     |     Response #1    |
                     |<-------------------| Protect with CTX_NEW
CTX_NEW =            | OSCORE Option:     |
  updateCtx(R1|R2,   |   ...              |
            CTX_OLD) |   d flag: 1        |
                     |   ...              |
Verify with CTX_NEW  |   ID Detail: R2    |
                     |   ...              |
Discard CTX_OLD      |                    |
                     |                    |

// The actual key update process ends here.
// The two peers can use the new Security Context CTX_NEW.

                     |                    |
                     |     Request #2     |
Protect with CTX_NEW |------------------->|
                     |                    | Verify with CTX_NEW
                     |                    |
                     |                    | Discard CTX_OLD
                     |                    |
                     |     Response #2    |
                     |<-------------------| Protect with CTX_NEW
Verify with CTX_NEW  |                    |
                     |                    |
```

Figure 6: Client-Initiated KUDOS Workflow

First, the client generates a random value R1, and uses the nonce N = R1 together with the old Security Context CTX_OLD, in order to derive a temporary Security Context CTX_1. Then, the client sends an OSCORE request to the server, protected with the Security Context CTX_1. In particular, the request has the 'd' flag bit set to 1 and specifies R1 as 'id detail' (see Section 4.1).

Upon receiving the OSCORE request, the server retrieves the value R1 from the 'id detail' of the request, and uses the nonce N = R1 together with the old Security Context CTX_OLD, in order to derive the temporary Security Context CTX_1. Then, the server verifies the request by using the Security Context CTX_1.

After that, the server generates a random value R2, and uses the nonce N = R1 | R2 together with the old Security Context CTX_OLD, in order to derive the new Security Context CTX_NEW. Then, the server sends an OSCORE response to the client, protected with the new Security Context CTX_NEW. In particular, the response has the 'd' flag bit set to 1 and specifies R2 as 'id detail'.

Upon receiving the OSCORE response, the client retrieves the value R2 from the 'id detail' of the response. Since the client has received a response to an OSCORE request it made with the 'd' flag bit set to 1, the client uses the nonce N = R1 | R2 together with the old Security Context CTX_OLD, in order to derive the new Security Context CTX_NEW. Finally, the client verifies the response by using the Security Context CTX_NEW and deletes the old Security Context CTX_OLD.

After that, the client can send a new OSCORE request protected with the new Security Context CTX_NEW. When successfully verifying the request using the Security Context CTX_NEW, the server deletes the old Security Context CTX_OLD and can reply with an OSCORE response protected with the new Security Context CTX_NEW.

From then on, the two peers can protect their message exchanges by using the new Security Context CTX_NEW.

4.3.2. Server-Initiated Key Update

Figure 7 shows the KUDOS workflow with the server acting as initiator.

```
                   Client               Server
                (responder)          (initiator)
                     |                    |
                     |     Request #1     |
Protect with CTX_OLD |-------------------->|
                     |                    | Verify with CTX_OLD
                     |                    |
                     |                    | Generate R1
                     |                    |
                     |                    | CTX_1 =
                     |                    |   updateCtx(R1,
                     |                    |             CTX_OLD)
                     |                    |
                     |     Response #1    |
                     |<-------------------| Protect with CTX_1
CTX_1 =              | OSCORE Option:     |
  updateCtx(R1,      |   ...              |
            CTX_OLD) |   d flag: 1        |
                     |   ...              |
Verify with CTX_1    |   ID Detail: R1    |
                     |   ...              |
Generate R2          |                    |
                     |                    |
CTX_NEW =            |                    |
  updateCtx(R1|R2,   |                    |
            CTX_OLD) |                    |
                     |                    |
                     |     Request #2     |
Protect with CTX_NEW |-------------------->|
                     | OSCORE Option:     | CTX_NEW =
                     |   ...              |   updateCtx(R1|R2,
                     |   d flag: 1        |             CTX_OLD)
                     |   ...              |
                     |   ID Detail: R1|R2 | Verify with CTX_NEW
                     |   ...              |
                     |                    | Discard CTX_OLD
                     |                    |

// The actual key update process ends here.
// The two peers can use the new Security Context CTX_NEW.

                     |     Response #2    |
                     |<-------------------| Protect with CTX_NEW
Verify with CTX_NEW  |                    |
                     |                    |
Discard CTX_OLD      |                    |
                     |                    |
```

Figure 7: Server-Initiated KUDOS Workflow

First, the client sends a normal OSCORE request to the server, protected with the old Security Context CTX_OLD and with the 'd' flag bit set to 0.

Upon receiving the OSCORE request and after having verified it with the old Security Context CTX_OLD as usual, the server generates a random value R1 and uses the nonce N = R1 together with the old Security Context CTX_OLD, in order to derive a temporary Security Context CTX_1. Then, the server sends an OSCORE response to the client, protected with the Security Context CTX_1. In particular, the response has the 'd' flag bit set to 1 and specifies R1 as 'id detail' (see Section 4.1).

Upon receiving the OSCORE response, the client retrieves the value R1 from the 'id detail' of the response, and uses the nonce N = R1 together with the old Security Context CTX_OLD, in order to derive the temporary Security Context CTX_1. Then, the client verifies the response by using the Security Context CTX_1.

After that, the client generates a random value R2, and uses the nonce N = R1 | R2 together with the old Security Context CTX_OLD, in order to derive the new Security Context CTX_NEW. Then, the client sends an OSCORE request to the server, protected with the new Security Context CTX_NEW. In particular, the request has the 'd' flag bit set to 1 and specifies R1 | R2 as 'id detail'.

Upon receiving the OSCORE request, the server retrieves the value R1 | R2 from the request. Then, the server verifies that: i) the value R1 is identical to the value R1 specified in a previous OSCORE response with the 'd' flag bit set to 1; and ii) the value R1 | R2 has not been received before in an OSCORE request with the 'd' flag bit set to 1. If the verification succeeds, the server uses the nonce N = R1 | R2 together with the old Security Context CTX_OLD, in order to derive the new Security Context CTX_NEW. Finally, the server verifies the request by using the Security Context CTX_NEW and deletes the old Security Context CTX_OLD.

After that, the server can send an OSCORE response protected with the new Security Context CTX_NEW. When successfully verifying the response using the Security Context CTX_NEW, the client deletes the old Security Context CTX_OLD.

From then on, the two peers can protect their message exchanges by using the new Security Context CTX_NEW.

4.4. Retention Policies

Applications MAY define policies that allows a peer to also temporarily keep the old Security Context CTX_OLD, rather than simply overwriting it to become CTX_NEW. This allows the peer to decrypt late, still on-the-fly incoming messages protected with CTX_OLD.

When enforcing such policies, the following applies.

- Outgoing messages MUST be protected by using only CTX_NEW.

- Incoming messages MUST first be attempted to decrypt by using CTX_NEW. If decryption fails, a second attempt can use CTX_OLD.

- When an amount of time defined by the policy has elapsed since the establishment of CTX_NEW, the peer deletes CTX_OLD.

4.5. Discussion

KUDOS is intended to deprecate and replace the procedure defined in Appendix B.2 of [RFC8613], as fundamentally achieving the same goal, while displaying a number of improvements and advantages.

In particular, it is especially convenient for the handling of failure events concerning the JRC node in 6TiSCH networks (see Section 3). That is, among its intrinsic advantages compared to the procedure defined in Appendix B.2 of [RFC8613], KUDOS preserves the same ID Context value, when establishing a new OSCORE Security Context.

Since the JRC uses ID Context values as identifiers of network nodes, namely "pledge identifiers", the above implies that the JRC does not have anymore to perform a mapping between a new, different ID Context value and a certain pledge identifier (see Section 8.3.3 of [RFC9031]). It follows that pledge identifiers can remain constant once assigned, and thus ID Context values used as pledge identifiers can be employed in the long-term as originally intended.

5. Security Considerations

This document mainly covers security considerations about using AEAD keys in OSCORE and their usage limits, in addition to the security considerations of [RFC8613].

Depending on the specific key update procedure used to establish a new OSCORE Security Context, the related security considerations also apply.

TODO: Add more considerations.

6. IANA Considerations

This document has the following actions for IANA.

6.1. OSCORE Flag Bits Registry

IANA is asked to add the following entries to the "OSCORE Flag Bits" registry within the "Constrained RESTful Environments (CoRE) Parameters" registry group.

Bit Position	Name	Description	Reference
1	Extension-1 Flag	Set to 1 if the OSCORE Option specifies a second byte of OSCORE flag bits	[This Document]
15	ID Detail Flag	Set to 1 if the compressed COSE object contains 'id detail'	[This Document]

7. References

7.1. Normative References

[I-D.ietf-lake-edhoc] Selander, G., Mattsson, J. P., and F. Palombini, "Ephemeral Diffie-Hellman Over COSE (EDHOC)", Work in Progress, Internet-Draft, draft-ietf-lake-edhoc-12, 20 October 2021, <https://www.ietf.org/archive/id/draft-ietf-lake-edhoc-12.txt>.

[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>.

[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/info/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/info/rfc8174>.

[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/info/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/info/rfc8949>.

7.2. Informative References

[I-D.ietf-ace-oauth-authz] Seitz, L., Selander, G., Wahlstroem, E., Erdtman, S., and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE) using the OAuth 2.0 Framework (ACE-OAuth)", Work in Progress, Internet-Draft, draft-ietf-ace-oauth-authz-45, 29 August 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-oauth-authz-45.txt>.

[I-D.ietf-ace-oscore-profile] Palombini, F., Seitz, L., Selander, G., and M. Gunnarsson, "OSCORE Profile of the Authentication and Authorization for Constrained Environments Framework", Work in Progress, Internet-Draft, draft-ietf-ace-oscore-profile-19, 6 May 2021, <https://www.ietf.org/archive/id/draft-ietf-ace-oscore-profile-19.txt>.

[I-D.irtf-cfrg-aead-limits] Günther, F., Thomson, M., and C. A. Wood, "Usage Limits on AEAD Algorithms", Work in Progress, Internet-Draft, draft-irtf-cfrg-aead-limits-03, 12 July 2021, <https://www.ietf.org/archive/id/draft-irtf-cfrg-aead-limits-03.txt>.

[LwM2M] Open Mobile Alliance, "Lightweight Machine to Machine Technical Specification - Core, Approved Version 1.2, OMA-TS-LightweightM2M_Core-V1_2-20201110-A", November 2020, <http://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-TS-LightweightM2M_Core-V1_2-20201110-A.pdf>.

[LwM2M-Transport] Open Mobile Alliance, "Lightweight Machine to Machine Technical Specification - Transport Bindings, Approved Version 1.2, OMA-TS-LightweightM2M_Transport-V1_2-20201110-A", November 2020, <http://www.openmobilealliance.org/release/LightweightM2M/V1_2-20201110-A/OMA-TS-LightweightM2M_Transport-V1_2-20201110-A.pdf>.

[RFC7519] Jones, M., Bradley, J., and N. Sakimura, "JSON Web Token (JWT)", RFC 7519, DOI 10.17487/RFC7519, May 2015, <https://www.rfc-editor.org/info/rfc7519>.

[RFC7554]
Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC 7554, DOI 10.17487/RFC7554, May 2015, <https://www.rfc-editor.org/info/rfc7554>.

[RFC8180] Vilajosana, X., Ed., Pister, K., and T. Watteyne, "Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e (6TiSCH) Configuration", BCP 210, RFC 8180, DOI 10.17487/RFC8180, May 2017, <https://www.rfc-editor.org/info/rfc8180>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC9031] Vučinić, M., Ed., Simon, J., Pister, K., and M. Richardson, "Constrained Join Protocol (CoJP) for 6TiSCH", RFC 9031, DOI 10.17487/RFC9031, May 2021, <https://www.rfc-editor.org/info/rfc9031>.

Acknowledgments

The authors sincerely thank Christian Amsuess, John Mattsson and Goeran Selander for their feedback and comments.

The work on this document has been partly supported by VINNOVA and the Celtic-Next project CRITISEC; and by the H2020 project SIFIS-Home (Grant agreement 952652).

Authors' Addresses

Rikard Höglund
RISE AB
Isafjordsgatan 22
SE-16440 Stockholm Kista
Sweden

Email: rikard.hoglund@ri.se

Marco Tiloca
RISE AB
Isafjordsgatan 22
SE-16440 Stockholm Kista
Sweden

Email: marco.tiloca@ri.se