**3GPP TSG-SA3 Meeting #111 *draft\_S3-233423-r1***

**Berlin, Germany, 22 -26 May 2023**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  |  | **CR** |  | **rev** |  | **Current version:** |  |  |
|  | | | | | | | | |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* | | | | | | | | |
|  | | | | | | | | |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME | **X** | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** |  | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, THALES, Xiaomi | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** |  | | | | |  | ***Date:*** | | | 2023-06-01 |
|  |  | | | |  | |  | | |  |
| ***Category:*** |  |  | | | | | ***Release:*** | | | Rel-18s |
|  | *Use one of the following categories:* ***F*** *(correction)* ***A*** *(mirror corresponding to a change in an earlier release)* ***B*** *(addition of feature),* ***C*** *(functional modification of feature)* ***D*** *(editorial modification)*  Detailed explanations of the above categories can be found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | | | | | | | | *Use one of the following releases: Rel-8 (Release 8) Rel-9 (Release 9) Rel-10 (Release 10) Rel-11 (Release 11) … Rel-15 (Release 15) Rel-16 (Release 16) Rel-17 (Release 17) Rel-18 (Release 18)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | GBA does not have any Ua protocol specification for constrained IoT devices supporting Open Mobile Alliance (OMA) procedures. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of a normative annex that specifies the IETF OSCORE as a GBA Ua protocol for constrained IoT devices supporting Open Mobile Alliance (OMA) procedures. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | GBA will not be used by IoT UEs which support OMA procedures. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3.2, H.3, Annex Y (new), Y.1 (new), Y.2 (new), Y.2.1 (new), Y.2.2 (new), Y.2.3 (new), Y.2.4 (new), Y.3 (new), Y.3.1 (new), Y.3.2 (new), Y.3.3 (new), Y.3.4 (new), Y.3.5 (new) | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **Y** | **N** |  | | | |  | | |
| ***Other specs*** | |  | **X** | Other core specifications | | | | TS/TR ... CR ... | | |
| ***affected:*** | |  | **X** | Test specifications | | | | TS/TR ... CR ... | | |
| ***(show related CRs)*** | |  | **X** | O&M Specifications | | | | TS/TR ... CR ... | | |
|  | |  | | | | | | | | |
| ***Other comments:*** | |  | | | | | | | | |
|  | |  | | | | | | | | |
| ***This CR's revision history:*** | | History of this draft CR:  SA3#111 (2023-05): S3-233423 incorporates the following documents:  - S3-233375  SA3#110Adhoc-e (2023-04): S3-232213 incorporates the following documents:  - S3-231826  - S3-232212  SA3#110 (2023-02): S3-231474 which is the merger of  - S3-231282  - S3-231199  - S3-231373 | | | | | | | | |

\*\*\* 1st CHANGE \*\*\*

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TS 31.102: "Characteristics of the USIM application".

[2] 3GPP TS 33.102: "3G Security; Security architecture".

[3] Void

[4] IETF RFC 3310: "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)".

[5] 3GPP TS 33.221: "Generic Authentication Architecture (GAA); Support for Subscriber Certificates".

[6] Void

[7] Void

[8] Void

[9] Void.

[10] 3GPP TS 31.103: "Characteristics of the IP Multimedia Services Identity Module (ISIM) application".

[11] 3GPP TS 23.003: "Numbering, addressing and identification".

[12] Void

[13] 3GPP TS 33.210: "3G Security; Network domain security; IP network layer security".

[14] Void.

[15] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics".

[16] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services".

[17] Void.

[18] IETF RFC 2818: "HTTP over TLS".

[19] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[20] Void.

[21] Void.

[22] IETF RFC 2104: "HMAC: Keyed-Hashing for Message Authentication".

[23] ISO/IEC 10118-3:2004: "Information Technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions".

[24] IETF RFC 3629: "UTF-8, a transformation format of ISO 10646".

[25] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[26] 3GPP TS 33.246: "3G Security; Security of Multimedia Broadcast/Multicast Service (MBMS)".

[27] Void.

[28] Void

[29] 3GPP TS 24.109: "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details".

[30] (void)

[31] (void)

[32] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[33] Void

[34] 3GPP TS 23.002: “Network architecture “.

[35] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security Architecture".

[36] 3GPP TS 33.402: "3GPP System Architecture Evolution (SAE); Security aspects of non-3GPP accesses".

[37] "Unicode Standard Annex #15; Unicode Normalization Forms", Unicode 5.1.0, March 2008. <http://www.unicode.org>

[38] 3GPP TS 26.237: "IP Multimedia Subsystem (IMS) based Packet Switch Streaming (PSS) and Multimedia Broadcast/Multicast Service (MBMS) User Service; Protocols".

[39] 3GPP TS 33.224: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push Layer".

[40] 3GPP TS 33.328: "IMS Media plane security".

[41] Void

[42] (void)

[43] Void.

[44] IETF RFC 5705: "Keying Material Exporters for Transport Layer Security (TLS)".

[45] 3GPP TS 33.223: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) Push function".

[46] 3GPP TS 44.006 "Technical Specification Group GSM/EDGE Radio Access Network; Mobile Station - Base Station System (MS - BSS) interface; Data Link (DL) layer specification".

[47] 3GPP TS 43.020 "Technical Specification Group Services and system Aspects; Security related network functions".

[48] IETF RFC 5929 "Channel Bindings for TLS".

[49] 3GPP TS 33.303: "Proximity-based Services; Security Aspects".

[50] 3GPP TS 33.179: "Security of Mission Critical Push-To-Talk (MCPTT)".

[51] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[52] 3GPP TS 33.163: " Battery Efficient Security for very low Throughput Machine Type Communication (MTC) devices (BEST)".

[53] 3GPP TS 33.501: " Security architecture and procedures for 5G system".

[54] 3GPP TS 33.180: "Technical Specification Group Services and System Aspects; Security of the mission critical service".

[55] 3GPP TS 33.122: "Security Aspects of Common API Framework for 3GPP Northbound APIs".

[56] 3GPP TS 33.536: "Security Aspect of 3GPP Support for Advanced V2X Services".

[57] Void

[58] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[59] IETF RFC 8446 "The Transport Layer Security (TLS) Protocol Version 1.3".

[60] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[61] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[62] IETF RFC 7616: "HTTP Digest Access Authentication".

[63] IETF RFC 7230: " Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[64] 3GPP TS 23.502: "Procedures for the 5G System (5GS)".

[65] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[66] 3GPP TS 23.501: " System architecture for the 5G System (5GS)".

[67] 3GPP TS 33.503: "Security Aspects of Proximity based Services (ProSe) in the 5G System (5GS)".

[XX] IETF RFC 8613: "Object Security for Constrained RESTful Environments (OSCORE)"

[XY] IETF RFC 7252: "The Constrained Application Protocol (CoAP)"

[XZ] IETF RFC 8949: "Concise Binary Object Representation (CBOR)"

[XW] IETF RFC 8152: "CBOR Object Signing and Encryption (COSE)"

[ZZ] IETF RFC 5869: "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)"

\*\*\* 2nd CHANGE \*\*\*

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AK Anonymity Key

AKA Authentication and Key Agreement

B-TID Bootstrapping Transaction Identifier

BSF Bootstrapping Server Function

CA Certificate Authority

CBOR Concise Binary Object Representation

CoAP Constrained Application Protocol

FQDN Fully Qualified Domain Name

GAA Generic Authentication Architecture

GBA Generic Bootstrapping Architecture

GBA\_ME ME-based GBA

GBA\_U GBA with UICC-based enhancements

GUSS GBA User Security Settings

HLR Home Location Register

HSS Home Subscriber System

IK Integrity Key

KDF Key Derivation Function

Ks\_int\_NAF Derived key in GBA\_U which remains on UICC

Ks\_ext\_NAF Derived key in GBA\_U

MNO Mobile Network Operator

NAF Network Application Function

OSCORE Object Security for Constrained RESTful Environments

PKI Public Key Infrastructure

SLF Subscriber Locator Function

TMPI Temporary IP Multimedia Private Identity

USS User Security Setting

\*\*\* 3rd CHANGE \*\*\*

# H.3 Ua security protocol identifiers for 3GPP specified protocols

The following Ua security protocol identifiers are specified by 3GPP:

( 0x01,0x00,0x00,0x00,0x00 ) Ua security protocol according to TS 33.221 [5].

( 0x01,0x00,0x00,0x00,0x01 ) Ua security protocols according to TS 33.246 [26].

NOTE 1: TS 33.246 [26] provides key separation between the keys that are used within HTTP digest and MIKEY protocols.

( 0x01,0x00,0x00,0x00,0x02) Ua security protocol HTTP digest authentication according to TS 24.109 [29], unless HTTP digest authentication is used in the context of another Ua security protocol, which is already covered elsewhere in this Annex.

( 0x01,0x00,0x00,0x00,0x03 ) Ua security protocols used with HTTP-based security procedures for MBMS user services according to TS 26.237 [38].

( 0x01,0x00,0x00,0x00,0x04 ) Ua security protocols used with SIP-based security procedures for MBMS user services according to TS 26.237 [38].

( 0x01,0x00,0x00,0x00,0x05 ) Ua security protocols used with Generic Push Layer according to TS 33.224 [39], unless Generic Push Layer is used in the context of another Ua security protocol, which is already covered elsewhere in this Annex.

( 0x01,0x00,0x00,0x00,0x06 ) Ua security protocol for IMS UE to KMS http based message exchanges according to "IMS media plane security", TS 33.328 [40]

( 0x01,0x00,0x00,0x00,0x07 ) Ua security protocol for shared key TLS 1.3 given in clause 5.4.0.2 of TS 33.222 [25].

( 0x01,0x00,0x00,0x00,0x08 ) Ua security protocol for OSCORE according to Annex Y.

( 0x01,0x00,0x00, 0x01,0x00 ) Generation of TMPI according to Annex B.4.

NOTE 2: This protocol identifier is not strictly a Ua protocol identifier, but its use in key derivation function is exactly equal.to a Ua protocol identifier.

( 0x01,0x00,0x01,yy,zz ) Ua security protocol for "Shared key-based UE authentication with certificate-based NAF authentication", according to TS 33.222 [25] section 5.3, or "Shared key-based mutual authentication between UE and NAF" for TLS 1.2 (see above for Ua security protocol identifier for TLS 1.3 with shared keys), according to TS 33.222 [25] section 5.4.0.1. Here, "yy,zz" is the protection mechanism CipherSuite code according to the defined values for TLS CipherSuites in the IANA TLS Cipher Suite Registry which is referenced in RFC 8446 [59].

NOTE 3: The "Certificate based mutual authentication between UE and NAF” according to TS 33.222 [25] section 5.5 does not require a Ua protocol identifier.

NOTE 4: As an example: The TLS 1.2 CipherSuite TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256 has code = { 0xC0,0x2B }, thus the according protocol identifier shall be ( 0x01,0x00,0x01, 0xC0,0x2B  ).

( 0x01,0x00,0x02,yy,zz ) Ua security protocol for "Shared key-based UE authentication with certificate-based NAF authentication", according to TS 33.222 [25] Annex D. Here, "yy,zz" is the protection mechanism CipherSuite code according to the defined values for TLS CipherSuites in the IANA TLS Cipher Suite Registry which is referenced in RFC 8446 [59]. This Ua security protocol identifier is used for the case outlined in TS 33.222 [5] Annex D, where e.g. HTML FORM based authentication is used within a TLS tunnel.

NOTE 4: The third octet (0x02) distinguish this case from other protocols tunneled inside the TLS tunnel.

\*\*\* 4th CHANGE \*\*\*

# Annex Y (normative): Ua security protocol: Object Security for Constrained RESTful Environments (OSCORE)

## Y.1 General

This annex describes how to secure access to NAF using Object Security for Constrained RESTful Environments (OSCORE) [XX]. OSCORE is a lightweight security protocol protecting REST-based communication, designed for use with the Constrained Application Protocol (CoAP) [XY]. OSCORE protects the CoAP payload and REST parameters such as URI path, media type and method (GET, PUT, POST, DELETE, etc.) but is independent of transport, which makes it suitable for securing application data across gateways and with interchanging transport. OSCORE, like CoAP, is designed for proxy operations to support constrained devices e.g. sleeping for long times to save power. OSCORE could be used instead of or in addition to security protocols at other layers, e.g. transport layer security between the core network and AF.

In the context of the GBA Ua protocol specified in this clause, the UE is assumed to be CoAP Client and the NAF is assumed to be CoAP Server.Figure Y.1-1 shows a network model of the OSCORE GBA Ua protocol.



Figure Y.1-1: Network model of OSCORE in the context of GBA

## Y.2 Requirements

### Y.2.1 General

This Annex covers the aspects specific to the GBA Ua protocol based on OSCORE. This feature is optional to be supported for the UE and NAF. If the feature is supported, the following clauses apply.

### Y.2.2 Requirements on the UE

To utilise GBA as described in this document the UE shall be equipped with an CoAP capable client implementing the particular features of GBA as specified in this document.

The support of OSCORE as a GBA Ua protocol for the UE is optional.

The UE hosts the CoAP client which supports OSCORE. The CoAP client supporting OSCORE may reside in the ME or in the UICC or both might host a CoAP client supporting OSCORE independently of each other. When the CoAP capable client supporting OSCORE to be used is in the ME, Ks\_(ext)\_NAF shall be used as the shared key between the UE and the NAF. When the CoAP capable client supporting OSCORE to be used is located in the UICC, Ks\_int\_NAF shall be used as the shared key between the UE and the NAF.

### Y.2.3 Requirements on the NAF

To utilise GBA as described in this document the NAF shall support the features of GBA as specified in this document.

The support of OSCORE as a GBA Ua protocol for the NAF is optional.

It shall be possible that the NAF is configured to restrict the access to the service based on which key is used, (e.g., access is allowed only for those CoAP capable clients supporting OSCORE that reside in the UICC and use Ks\_int\_NAF). The key selection indication given in the USS shall overrule the local policy of the NAF.

### Y.2.4 Requirements on the OSCORE

The requirements for OSCORE are described in IETF RFC 6813 [XX]. OSCORE derives keys using an HMAC-based key derivation function (HKDF), and protects the communication using an authenticated encryption with additional data (AEAD) algorithm. The AEAD algorithm AES-CCM-16-64-128 defined in the IETF RFC 8152 [XW] with 128-bit key, 13-byte nonce, and 64-bit tag is mandatory to implement, as is HKDF with SHA-256. Other algorithms may be specified in the optional OSC-INP parameter.

## Y.3 OSCORE as a GBA Ua protocol

### Y.3.1 General

The OSCORE as a GBA Ua protocol is specified in this clause by providing the details about the procedures, the OSCORE security context and how it is related to the GBA Ks\_(ext/int)\_NAF and the encoding of OSCORE messages using CBOR specified in IETF RFC 8949 [XZ].

### Y.3.2 Procedures

This section explains how the procedures specified in this document have to be enhanced when OSCORE is used as a Ua protocol between a UE and an NAF. The following gives the complementary description with respect to the procedure specified in clause 4.5.3 or in clause 5.3.3. In the text below, the CoAP Client is assumed to be an application on the UE.

The procedure to establish OSCORE protected communication is shown in Figure Y.3.2-1 and includes the following steps:

1) The CoAP Client (UE) shall send a CoAP request to the NAF. This is the Application Request in Step 1 in clause 4.5.3 or in clause 5.3.3. The CoAP request shall consist of the following:

i) CoAP Method: POST

ii) URI of the GBA resource on the NAF. The URI shall have the format of <NAF\_IP\_or\_FQDN>/gba, where NAF\_IP\_or\_FQDN indicates the IP address or the FQDN of the host that hosts the NAF.

NOTE Y: It is assumed that the NAF IP address or FQDN is already provisioned to the UE for GBA purposes.

iii) Payload: CoAP Security protocol identifer, B-TID, key type indicator list, N1, NAF-SID, ?OSC-INP

The parameter CoAP Security protocol identifier is an octet that identifies the security protocol used for the CoAP transfer layer. In the case of OSCORE this parameter shall take the value of "01".

NOTE X: The parameter "CoAP Security protocol identifier" is used for distinguishing between different security protocols used in conjuction with CoAP. OSCORE is on one such protocol and others can potentially be introduced in the future.

The key type indicator list identifies the type of GBA keys used later for the establishement of the OSCORE security context. The UE includes all the different types of keys it supports. The UE shall use the following values:

a) 0x01 indicates that the UE accepts that AKA-based Ks\_(ext)\_NAF is used establish the OSCORE security context.

b) 0x02 indicates that the UE accepts that Ks\_int\_NAF is used to establish the OSCORE security context.

c) 0x04 indicates that the UE accepts that GBA\_Digest-based Ks\_NAF is used to establish the OSCORE security context.

The parameters N1, NAF-SID and ?OSC-INP are specific to OSCORE. N1 is a nonce sent by the UE to the NAF. The NAF-SID is the OSCORE Sender Identifier for the NAF and it is an identifier generated by the UE to enable short locally unique identifiers. The parameter "?OSC-INP" is an optional parameter denoting any additional OSCORE input provided by the UE to the NAF.

2) Steps 2-3 of clause 4.5.3 or of clause 5.3.3 in this specification. If the NAF receives an error message in these steps then the NAF may terminate the procedure.

3) The CoAP Server (NAF) shall respond to the CoAP Client (UE) with a CoAP response. This is the Application Answer in Step 4 in clause 4.5.3 or in clause 5.3.3. The response shall have the following content:

i) Response Code: "Created"

ii) Payload: Selected key type indicator, N2, UE-SID

- The parameter "Selected key type indicator" includes the specific key type indicator from the key type indicator list provided by the UE, which was selected by the NAF.

The parameters N2, UE-SID are specific to OSCORE. N2 is a nonce sent by the NAF to the UE. The UE-SID is the OSCORE Sender Identifier for the UE and it is an identifier generated by the NAF to enable short locally unique identifiers.

4a-4b) The UE and the NAF shall derive the OSCORE security context specified in clause Y.3.3.

5-6) The UE and NAF proceed using protected OSCORE requests/responses.



Figure Y.3.2-1: OSCORE Ua protocol

### Y.3.3 OSCORE Security context

The OSCORE security context consists of the following parts:

- OSCORE Master Secret (OMS): A shared key between the CoAP Client and CoAP Server.

- Master Salt: A shared salt shared between the CoAP Client and CoAP Server.

- UE-SID: The UE Sender Identifier

- NAF-SID: The NAF Sender Identifier

- OSCORE Version: The version of the OSCORE protocol

- HKDF: HMAC-based Key Derivation Function

- AEAD Algorithm: The algorithm used for encryption and integirty protection

- OSCORE ID Context: An identifier which identifies the OSCORE context

The OSCORE security context for the OSCORE Ua protocol shall have the following values:

- OMS = OSCORE Master Secret = HKDF(Ks\_(int/ext)\_NAF, "GBA-OSCORE"), where Ks\_(int/ext)\_NAF is the shared key between the UE and NAF and it follows the semantics of this document for GBA i.e. Ks\_(int/ext)\_NAF refers to Ks\_NAF from GBA\_ME, Ks\_int\_NAF or Ks\_ext\_NAF from GBA\_U.

- Master Salt = Request Payload | Response Payload

- UE Sender ID = UE-SID generated by CoAP Server and sent to the CoAP Client in the Application Response (Step 3 in clause Y.3.2)

- NAF Sender ID = NAF-SID generated by CoAP Client and sent to the CoAP Server in the Application Request (Step 1 in clause Y.3.2)

where HKDF shall be the HMAC-based Key Derivation Function specified in IETF RFC 5869 [ZZ]

The other OSCORE parameters in the OSCORE security context shall have default values unless superseded by the optional parameter OSC-INP provided by the CoAP Client in Step 1 in clause Y.3.2. The default values of the rest of the OSCORE parameters in the OSCORE security context are:

- OSCORE Version: default version 1

- HKDF: default HKDF with SHA-256

- AEAD Algorithm: default AES-CCM-16-64-128

- OSCORE ID Context: default nil

### Y.3.4 Refresh of OSCORE key material

OSCORE allows both the communication endpoints (UE or NAF) to renegotiate the OSCORE security context after the OSCORE security context is established, according to Appendix B.2 in IETF RFC 8613 [XX] , which is shown in the figure Y.3.4-1, alaternative A1.

Furthermore since the OSCORE master secret is derived from the Ks\_(int/ext)\_NAF and since GBA includes a separate bootstrapping protocol (Ub) the OSCORE key material can be refreshed by refreshing the Ks\_(int/ext)\_NAF key. As a result the NAF may respond to the UE that a new Ks\_(int/ext)\_NAF is needed by initiating an explict request or a respond to a UE request with an indicator "Ub bootstrapping required". Upon sending such explicit message or response to the UE, the NAF shall teminate any ongoing OSCORE session. Upon receiving such indicator the UE shall terminate any current ongoing OSCORE session and UE shall run the Ub bootstrapping and re-establish the OSCORE application session, figure Y.3.4-1, alternative steps A2.



Figure Y.3.4-1: OSCORE key refresh

### Y.3.5 OSCORE Ua protocol payload encoding

IETF CoAP and OSCORE shall use the IETF Concise Binary Object Representation (CBOR) specified in the IETF RFC 8949 [XZ] for payload encoding for efficient information transfer between constrained IoT devices.

The CoAP media type for CBOR encoding shall be:

- Media Type: application/cbor

- CoAP Content-Format: 60

The Request Payload in the Application Request message shall be formatted as a CBOR Array as follows:

Request Payload = [  
 B-TID : tstr,  
 key type indicator list: bstr,  
 N1 : bstr,   
 NAF-SID : bstr,   
 ? OSC-INP: bstr  
]OSC-INP = { //CBOR Map  
 ? 1 => int, ; version   
 ? 3 => int, ; hkdf   
 ? 4 => int, ; alg   
 ? 5 => bstr, ; salt   
 ? 6 => bstr ; contextId  
}

NOTE X: The key type indicator list is an octet with value equal to logical OR of the different key type indicators that the UE supports.

The Response Payload in the Application Answer shall be formatted as a CBOR Array as follows:

Request Payload = [  
 B-TID : tstr,  
 Selected key type indicator: bstr,  
 N1 : bstr,   
 NAF-SID : bstr,   
 ? OSC-INP: bstr  
]OSC-INP = {  
 ? 1 => int, ; version   
 ? 3 => int, ; hkdf   
 ? 4 => int, ; alg   
 ? 5 => bstr, ; salt   
 ? 6 => bstr ; contextId  
}

\*\*\* END OF CHANGES \*\*\*