**3GPP TSG-SA3 Meeting #104-e *S3-212490-r1***

**e-meeting, 16 - 27 August 2021**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.1* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.535** | **CR** | **0084** | **rev** | **-** | **Current version:** | **17.2.1** |  |
|  | | | | | | | | |
| *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:*** | IETF OSCORE as AKMA Ua\* protocol | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Ericsson, DT | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | DUMMY | | | | |  | ***Date:*** | | | 2021-08-09 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **B** |  | | | | | ***Release:*** | | | Rel-17 |
|  | *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:*** | | AKMA does not have any Ua\* protocol specification for constrained IoT devices. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Addition of a normative annex that specifies the IETF OSCORE as Ua\* protocol for constrained IoT devices. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | AKMA will not be used by IoT type of UEs. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 2, 3.3, Annex Y (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:*** | |  | | | | | | | | |

\*\*\* 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 TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[3] 3GPP TS 23.501: "System Architecture for the 5G System".

[4] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)".

[5] 3GPP TS 23.222: "Common API Framework for 3GPP Northbound APIs".

[6] IETF RFC 7542: "The Network Access Identifier".

[7] 3GPP TS 33.222: " Generic Authentication Architecture (GAA); Access to network application functions using HypertextTransfer Protocol over Transport Layer Security (HTTPS)".

[8] IETF RFC 2616 (1999): "Hypertext Transfer Protocol (HTTP) – HTTP/1.1".

[9] 3GPP TS 23.003: "Numbering, addressing and identification".

[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 \*\*\*

## 3.3 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

A-KID AKMA Key IDentifier

A-TID AKMA Temporary UE IDentifier

AAnF AKMA Anchor Function

AF Application Function

AKMA Authentication and Key Management for Applications

AMFAccess and Mobility Management Function

AUSFAUthentication Server Function

CBOR Concise Binary Object Representation

CoAP Constrained Application Protocol

KAF AKMA Application Key

KAKMA AKMA Anchor Key

KDF Key Derivation Function

NEFNetwork Exposure Function

OSCORE Object Security for Constrained RESTful Environments

RID Routing InDicator

UDM Unified Data Management

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

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

## Y.1 General

Object Security for Constrained RESTful Environments (OSCORE) [XX] 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 may 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 Ua\* protocol specified here, the UE is assumed to be CoAP Client and the AF is assumed to be CoAP Server. The UE and the AF can change CoAP roles after the Ua\* protocol has been completed. Figure Y.1-1 shows a network model of the OSCORE Ua\* protocol.



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

## Y.2 Requirements

The support of IETF OSCORE as a Ua\* protocol for the UE and AF is optional.

The requirements for OSCORE are described in [RFC8613]. 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 Profile for AKMA Ua\*

### Y.3.1 General

The IETF OSCORE profile for AKMA is specified in this clause by providing the details about the procedures, the OSCORE security context and how it is related to the AKMA KAF and the encoding of OSCORE messages using IETF 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 IETF OSCORE is used as a Ua\* protocol between a UE and an AF. The following gives the complementary description with respect to the procedure specified in clause 6.2. 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 AF. This is the Application Session Establishment Request in Step 1 in clause 6.2. The CoAP request shall consist of the following:

i) CoAP Method: POST

ii) URI of the AKMA resource on the AF. The URI shall have the format of <AF\_IP\_or\_FQDN>/akma, where AF\_IP\_or\_FQDN indicates the IP address or the FQDN of the Data Network (DN) host that hosts the AF.

NOTE: It is assumed that the AF IP address or FQDN is already provisioned to the UE for AKMA purposes.

iii) Payload: CoAP Security protocol identifer, A-KID, N1, AF-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".

The parameters N1, AF-SID and ?OSC-INP are specific to OSCORE. N1 is a nonce sent by the UE to the AF. The AF-SID is the OSCORE Sender Identifier for the AF 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 AF.

2) Steps 2-4 of clause 6.2 in this specification

3) The CoAP Server (AF) shall respond to the CoAP Client (UE) with a CoAP response. This is the Application Session Establishment Response in Step 5 in clause 6.2. The response shall have the following content:

i) Response Code: "Created"

ii) Payload: N2, UE-SID

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

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

5-6) The UE and AF 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

- AF-SID: The AF 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 profile of Ua\* shall have the following values:

- OMS = OSCORE Master Secret = HKDF(KAF, "AKMA-OSCORE")

- Master Salt = salt | N1 | N2

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

- AF Sender ID = AF-SID generated by CoAP Client and sent to the CoAP Server in the Application Session Establishment Response (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.3.3 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 CBOR payload encoding of the different information elements of the Application Session Request shall be as follows:

Request Payload = [ ; CBOR Array   
A-KID : bstr,  
 N1 : bstr,   
 AF-SID : bstr,   
 ? OSC-INP: bstr  
]

A-KID = [ ; CBOR Array  
 RID : tstr,  
 A-TID : bstr,  
 HPLMN-ID : tstr  
]

OSC-INP = { ; CBOR Map  
 ? 1 => int, ; version   
 ? 3 => int, ; hkdf   
 ? 4 => int, ; alg   
 ? 5 => bstr, ; salt   
 ? 6 => bstr ; contextId  
}

The CBOR payload encoding of the different information elements of the Application Session Response shall be as follows:

Reponse Payload = [ ; CBOR Array  
 N2 : bstr,   
 UE-SID : bstr  
]

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