**3GPP TSG-SA WG3 Meeting #100-e *S3-201650***

**e-Meeting, 17-21 Aug 2020** *revision of S3-20wxyz*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.434** | **CR** | **0001** | **Rev** | **-** | **Current version:** | **16.0.0** |  |
|  | | | | | | | | |
| *For* [***HELP***](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 |  | Radio Access Network |  | Core Network | **X** |

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | | | | | | | | | | |
| ***Title:*** | [33.434] KM Clarifications | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Motorola Solutions, Samsung | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | SEAL | | | | |  | ***Date:*** | | | 17-Aug-2020 |
|  |  | | | |  | |  | | |  |
| ***Category:*** | **F** |  | | | | | ***Release:*** | | | Rel-16 |
|  | *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-12 (Release 12)* *Rel-13 (Release 13) Rel-14 (Release 14) Rel-15 (Release 15) Rel-16 (Release 16)* | |
|  |  | | | | | | | | | |
| ***Reason for change:*** | | Based on the LS from CT3, clarifications should be made to the parameter descriptions in the SEAL KM Request and SEAL KM Response messages in 33.434. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | 1. Add clarification for the SEAL KM Request “Version”, “ClientID”, “SKMSUri” and “Date/Time” parameters. 2. Add clarification for the SEAL KM Response “Payload” parameter. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | The SEAL KM procedure may be implemented improperly. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | 5.3.2, 5.3.3 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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:*** | |  | | | | | | | | |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# 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 23.434: "Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows".

[3] IETF RFC 6749: "The OAuth 2.0 Authorization Framework".

[4] IETF RFC 6750: "The OAuth 2.0 Authorization Framework: Bearer Token Usage".

[5] OpenID Connect 1.0: "OpenID Connect Core 1.0 incorporating errata set 1", <http://openid.net/specs/openid-connect-core-1_0.html>.

[6] 3GPP TS 33.310: "Network Domain Security (NDS); Authentication Framework (AF)".

[7] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[8] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[9] IETF RFC 7521: "Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants".

[10] IETF RFC 7523: "JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants".

[11] IETF RFC 7797: " JSON Web Signature (JWS) Unencoded Payload Option ".

[12] IETF RFC 7515: "JSON Web Signature (JWS)".

[13] IETF RFC 7662: "OAuth 2.0 Token Introspection".

[14] 3GPP TS 33.210: " 3G security; Network Domain Security (NDS); IP network layer security".

[15] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[16] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[yy] 3GPP TS 29.122: "T8 reference point for Northbound Application Programming Interfaces (APIs) ".

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of change 1 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

### 5.3.2 SEAL KM Request message

A SKM-C may send a SEAL KM Request message to the SKM-S. This request shall be protected (via the HTTPS tunnel) and shall contain the access token acquired during the SEAL identity management authentication procedure (clause 5.2).

The content of the SEAL KM Request is shown in table 5.3.2-1.

Table 5.3.2-1: Contents of a SEAL KM Request

|  |  |
| --- | --- |
| Name | Description |
| Version | The version number of the SEAL key management request. |
| SKmsUri | The URI of the SKM-S to which the request is sent. |
| ServiceID | A string representing the VAL service/application related to the VAL client request. |
| ClientID | (Optional) A string representing the client. See note. |
| DeviceID | (Optional) A string representing the device. See note. |
| UserID | (Optional) A string representing the user. See note. |
| Date/Time | The Date and Time of the request. This number represents the number of seconds from 1970-01-01T0:0:0Z as measured in UTC. |
| NOTE: Only one of these fields may be present in any given SEAL KMS Request message. | |

The identities listed in table 5.3.2-1 map to SEAL identities defined in 3GPP TS 23.434 [2]. Namely, the ServiceID maps to the VAL service identity (VAL service ID), the ClientID maps to the VAL client or client on the VAL server, the DeviceID maps to the VAL UE identity (VAL UE ID), and the UserID maps to the VAL user identity (VAL user ID).

The ‘Version’ field identifies the version of the SEAL KM Request message. The current version is defined as “1.0.0”.

The ‘Date/Time’ field is used primarily as an anti-replay mechanism for SEAL key management requests and responses. If the ‘Date/Time’ field is significantly out of range (more than a few seconds), this could indicate a replay attack.

Upon receipt of a SEAL KM Request message, the SKM-S shall verify that:

- the access token is valid;

- the signature is valid;

- the SKmsUri is the SKM-S URI of the target SEAL KMS where the key information is stored; and

- the Date/Time is within a recent time window (e.g. 5 seconds).

If valid, the request is accepted and processed by the SKM-S. A standalone ServiceID, or a ServiceID in combination with a ClientID, DeviceID, or UserID may be present in the SEAL KM Request message. This combination may be used by the KMS to identify a specific key material record. Each key management record may be unique to a VAL application or VAL service. The format and content of a key management record is defined and securely provisioned into the SEAL KMS by the VAL application or VAL service owner/operator. The method used to provision the VAL service or VAL application key material into the KMS is out of scope for the present document. The method used to organize, manage, and maintain VAL service or VAL application key material within the KMS is out of scope of the present document.

### 5.3.3 SEAL KM Response message

The SEAL KM Response message is sent to the SKM-C in response to a SEAL KM Request message.

A successful SEAL key management procedure results in a SEAL KM Response message which typically includes a payload containing key management information uniquely applicable to the requested service, client or user. If an error occurs, an error code may be returned in the SEAL KM Response message.

The SEAL KM Response message shall be protected in transit via the HTTPS tunnel. The Payload within a SEAL KM Response message may be protected end-to-end between the SKM-C and SKM-S depending on the applicability of the underlying VAL service making the request. The method for securing a Payload end-to-end between the SKM-C and the SKM-S is outside the scope of the present document. The key material contents provided in a Payload are defined by the underlying VAL service and are outside the scope of the present document.

The content of a SEAL KM Response message is shown in table 5.3.3-1.

Table 5.3.3-1: Contents of a SEAL KM Response message

|  |  |
| --- | --- |
| Name | Description |
| UserUri | URI of the user for which the response is intended. |
| SKmsUri | The URI of the SKM-S sending the response. |
| ServiceID | A string representing the VAL service/application related to the VAL client request. This is the same field as received in the SEAL KM Request message. |
| SKmsID | (Optional) The ID of the SKM-S providing the response message. |
| ClientID | (Optional) A string representing the client (see note) |
| DeviceID | (Optional) A string representing the device (see note) |
| UserID | (Optional) A string representing the user. (see note) |
| Date/Time | The Date and Time of the response. This number represents the number of seconds from 1970-01-01T0:0:0Z as measured in UTC. |
| ErrorCode | (Optional) Reason code indicating the failure of the requested action. If not present, the key management request is assumed to be successful. |
| Payload | (Optional) Key management payload specific to the VAL user, client or application. This field is not present if an error occurs. |
| NOTE: If this field is present in the SEAL KM Request message then this field shall be present in the SEAL KM Response message and shall be the same value. | |

The identities listed in table 5.3.3-1 are described in clause 5.3.2.

If the SKM-S does not encounter an error during processing of the SEAL KM Request message, the SEAL KM Response message carries a set of security parameters contained in the “Payload” field.

If the SKM-S encounters an error while processing the SEAL KM Request message, an error value described in table 5.3.3-2 shall be returned in the ‘ErrorCode’ field of the SEAL KM Response message and the ‘Payload’ field shall not be present.

In the event of an error, the user and/or the operator of the VAL service, UE, or client may be notified.

Table 5.3.3-2: ‘ErrorCode’ values

|  |  |  |
| --- | --- | --- |
| ErrorCode | Description | Maps To |
| 01 | Unspecified error | “500 Internal Server Error” as described in Table 5.2.6-1 of TS 29.122 [yy] |
| 02 | Key Information not available for specified service, client, device or user. | “404 Not Found” as described in Table 5.2.6-1 of TS 29.122 [yy] |
| 03 | Request rejected | “401 Unauthorized” as described in Table 5.2.6-1 of TS 29.122 [yy] |
| 04 | Unable to validate request | “400 Bad Request” or “403 Forbidden” as described in Table 5.2.6-1 of TS 29.122 [yy] |
| 05-FF | Reserved | N/A |

The selection of the key material returned in the Payload of a SEAL KM Response message is determined by the ServiceID and (optionally) the ClientID, DeviceID or UserID. The combination of the ServiceID with the ClientID, DeviceID or UserID allows the VAL service to request a more specific set of key material.

For example, if a ClientID is included in the SEAL KM Request message, the KMS may return a Payload that contains a set of client specific key material applicable to the ClientID within the requesting VAL service (ServiceID). If the DeviceID is included, the KMS may return a Payload that contains device specific key material applicable to the DeviceID within the requesting VAL service (ServiceID). If the UserID is included, the KMS may return a Payload that contains user specific key material applicable to that UserID within the requesting VAL service (ServiceID).

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of change 2 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*