**3GPP TSG-SA3 Meeting #98bis-e *S3-200651***

**e-meeting, 14-17 April 2020** Revision of S3-20xxxx

**Source: Motorola Solutions, Samsung, Huawei, Hisilicon**

**Title: SEAL Key Management Request and Response messages**

**Document for: Approval**

**Agenda Item: 2.9**

# 1 Decision/action requested

***This document proposes key management messages for a SEAL key management service.***

# 2 References

[1] 3GPP TS 23.434 Service Enabler Architecture Layer for Verticals (SEAL); Functional architecture and information flows.

[2] SP-190901 New WID on Security aspects of SEAL.

# 3 Rationale

This pCR defines the request and response messages used by a SEAL UE or VAL server to request and receive key management information from the SEAL KMS (SKM-S).

# 4 Detailed proposal

\*\*\*\*\*Start of 1st Change\*\*\*\*\*

### Y.2.2 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 6.2).

The content of the SEAL KM Request is shown in Table Y.2.2-1.

Table Y.2.2-1: Contents of a SEAL KM Request

|  |  |
| --- | --- |
| Name | Description |
| Version | The version number of the SEAL key management request (0.0.0). |
| 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 1. |
| DeviceID | (Optional) A string representing the device. See NOTE 1. |
| UserID | (Optional) A string representing the user. See NOTE 1. |
| 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 1: Only one of these fields may be present in any given SEAL KMS Request message. |

The identities listed in Table Y.2.2-1 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, the DeviceID maps to the VAL UE identity (VAL UE ID), and the UserID maps to the VAL user identity (VAL user ID).

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, 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. Any combination of ClientID, DeviceID, ServiceID and 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 this document. The method used to organize, manage, and maintain VAL service or VAL application key material within the KMS is out of scope of this document.

### Y.2.3 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 this document. The key material contents provided in a Payload are defined by the underlying VAL service and are outside the scope of this document.

The content of a SEAL KM Response message is shown in Table Y.2.3-1.

Table Y.2.3-1: 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 1) |
| DeviceID | (Optional) A string representing the device (see NOTE 1) |
| UserID | (Optional) A string representing the user. (see NOTE 1) |
| 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 may not be present if 1) an error occurs or 2) if the request does not require a payload. |
| NOTE 1: 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 Y.2.3-1 are described in clause Y.2.2.

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 1st Change\*\*\*\*\*