**3GPP TSG-SA3 Meeting #98bis-e *S3-200650***

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

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

**Title: SEAL Key Management procedure**

**Document for: Approval**

**Agenda Item: 2.9**

# 1 Decision/action requested

***This document proposes a key management procedure for a SEAL service or VAL client to acquire key material from the SKM-S via the SEAL architecture.***

# 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 describes the procedure for a SEAL UE (VAL user) or VAL server requesting and receiving key management information from the SEAL KMS (SKM-S).

# 4 Detailed proposal

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

# Y.2 SEAL key management procedure

## Y.2.1 General

To enable security for SEAL services, a SEAL KM client (located in either a SEAL UE or VAL server) may request key material applicable to a particular SEAL service, VAL client or user.

Prior to making a key management request to the SEAL KMS (SKM-S), the VAL client or VAL user shall be authenticated by the SEAL identity management service (clause 6.2). In addition, secure connections shall be established between the SEAL client and the SKM-S (reference point KM-UU) and the VAL server and the SKM-S (reference point KM-S) prior to any associated key management requests.

As a result of the SEAL identity management authentication procedure, an access token scoped for key management services is provisioned to the SEAL UE. This access token is provided with each and every key management request to the SKM-S.

A VAL server is provisioned with an access token scoped for SEAL key management services and is provided with each and every key management request to the SKM-S. The method for provisioning this access token into the VAL server is out of scope of this document.

Figure Y.2.1-1 shows the SEAL key management procedure. A SKM client may send a SEAL KM Request message to the SKM-S. The SKM-S validates and processes the request and responds with a SEAL KM Response message. The response contains key management material specific to the SEAL service or the VAL server request, or alternatively, an error code if the SKM-S encounters a failure condition.



Figure Y.2.1-1: SEAL key management procedure

The procedure in Figure Y.2.1-1 is described here:

1. The SKM-C establishes a direct HTTPS connection to the SKM-S. Steps 2 and 3 are within this secure connection.

2. The SKM-C sends a SEAL KM Request message to the SKM-S. The request contains the authorization credentials obtained during authentication and message content specified in clause Y.2.2.

3. The SKM-S authorizes the request and if valid, sends a SEAL KM Response message containing the requested key material (or error code) as specified in clause Y.2.3.

As a successful result of this procedure, the VAL UE or VAL Server has securely obtained service specific key material for use within the VAL system.

 \*\*\*\*\*End of 1st Change\*\*\*\*\*