**3GPP TSG-SA WG6 Meeting #39-bis-e S6-201936**

**e-meeting, 12th – 20th October 2020 (revision of S6-201872)**

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **23.434** | **CR** | **0030** | **rev** | **1** | **Current version:** | **16.5.0** |  |
|  |
| *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:***  | Resolution of ENs on security aspects |
|  |  |
| ***Source to WG:*** | Samsung |
| ***Source to TSG:*** | S6 |
|  |  |
| ***Work item code:*** | SEAL |  | ***Date:*** | 2020-10-07 |
|  |  |  |  |  |
| ***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 canbe 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:*** | There are multiple unresolved Editor’s notes related to SEAL security aspects which have dependency on SA3 specification. The stage 2 security aspects are specified in 3GPP TS 33.434 and the stage 3 security aspects are specified in 3GPP TS 29.549. These ENs need to be resolved with references to appropriate clause numbers from 3GPP TS 33.434 and the API aspects in TS 29.549. For the ENs where is no mapping to SA3 specification, the EN is just removed.  |
|  |  |
| ***Summary of change:*** | Resolve security related ENs with appropriate subclauses from TS 33.434 and TS 29.549.  |
|  |  |
| ***Consequences if not approved:*** | Without ENs resolution, the security aspects of SEAL are not clear and will lead to misinterpretations. |
|  |  |
| ***Clauses affected:*** | 2, 6.5.2.9.2, 7.1, 12.3.2, 12.3.3.2, 12.3.3.3, 12.4.1, 12.4.2, 12.4.2.1, 12.4.2.2, 13.2.4.2, 13.2.4.3, 13.2.5.2, 13.2.5.5, 13.3, 13.4.1, 13.4.2, 13.4.2.1, 13.4.2.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  |  |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  |  |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  |  |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\* \* \* First 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 22.104: "Service requirements for cyber-physical control applications in vertical domains".

[3] 3GPP TS 23.379: "Functional architecture and information flows to support Mission Critical Push To Talk (MCPTT); Stage 2".

[4] 3GPP TS 23.280: "Common functional architecture to support mission critical services; Stage 2".

[5] 3GPP TS 23.281: "Functional architecture and information flows to support Mission Critical Video (MCVideo); Stage 2".

[6] 3GPP TS 23.282: "Functional architecture and information flows to support Mission Critical Data (MCData); Stage 2".

[7] 3GPP TS 23.286: "Application layer support for V2X services; Functional architecture and information flows".

[8] 3GPP TS 23.222: "Functional architecture and information flows to support Common API Framework for 3GPP Northbound APIs; Stage 2".

[9] 3GPP TS 23.401: "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access".

[10] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2".

[11] 3GPP TS 23.502: "Procedures for the 5G System; Stage 2".

[12] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[13] 3GPP TS 23.682: "Architecture enhancements to facilitate communications with packet data networks and applications".

[14] 3GPP TS 23.002: "Network Architecture".

[15] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[16] 3GPP TS 23.468: "Group Communication System Enablers for LTE (GCSE\_LTE); Stage 2".

[17] 3GPP TS 23.246: "Multimedia Broadcast/Multicast Service (MBMS); Architecture and functional description".

[18] 3GPP TS 23.203: "Policy and charging control architecture".

[19] 3GPP TS 23.503: "Policy and Charging Control Framework for the 5G System; Stage 2".

[20] 3GPP TS 26.348: "Northbound Application Programming Interface (API) for Multimedia Broadcast/Multicast Service (MBMS) at the xMB reference point".

[21] 3GPP TS 29.214: "Policy and charging control over Rx reference point".

[22] 3GPP TS 29.468: "Group Communication System Enablers for LTE (GCSE\_LTE); MB2 Reference Point; Stage 3".

[23] 3GPP TS 36.300: "Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2".

[24] IETF RFC 6733 (October 2012): "Diameter Base Protocol".

[25] ETSI TS 102 894-2 (V1.2.1): "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionaryMultimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[26] ETSI TS 102 965 (V1.4.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

[27] ISO TS 17419: "Intelligent Transport Systems - Cooperative systems - Classification and management of ITS applications in a global context".

[28] 3GPP TS 26.346: "Multimedia Broadcast/Multicast Service (MBMS); Protocols and codecs".

[29] 3GPP TS 33.434: "Service Enabler Architecture Layer (SEAL); Security aspects for Verticals".

[xx] 3GPP TS 29.549: "Service Enabler Architecture Layer for Verticals (SEAL); Application Programming Interface (API) specification; Stage3".

\* \* \* Next Change \* \* \* \*

##### 6.5.2.9.2 Reference point SEAL-X1 (between the key management server and the group management server)

The SEAL-X1 reference point, which exists between the key management server and the group management server, provides a means for the key management server to provide security related information (e.g. encryption keys) to the group management server.

The SEAL-X1 reference point shall use the HTTP-1 and HTTP-2 reference points and may use the HTTP-3 reference point for transport and routing of security related information to the group management server.

NOTE: SEAL-X1 is specified in subclause 5.1.1.1 of 3GPP TS 33.434 [29].

\* \* \*Next Change \* \* \* \*

## 7.1 User identity (User ID)

The VAL user presents the user identity to the identity management server during a user authentication transaction, to provide the identity management client a means for VAL service authentication. In general, since identity management is a common SEAL service, it uses a set of credentials (e.g. biometrics, secureID, username/password) that may not necessarily be tied to a single VAL service. The user credentials uniquely identifies the VAL user to the identity management server.

NOTE: The specific security and authentication mechanisms required in order to use the user ID is specified in 3GPP TS 33.434 [29].

Editor's note: The naming and definition of the identities in subclause  7 may require further study (e.g. renaming user identity to VAL user identity, and renaming VAL user identity to VAL service user identity).

\* \* \*Next Change \* \* \* \*

### 12.3.2 Information flows

NOTE: The procedure for identity management is specified in subclause 5.2.3 and 5.2.4 of 3GPP TS 33.434 [29].

\* \* \*Next Change \* \* \* \*

#### 12.3.3.2 Primary VAL system

Figure 12.3.3.2-1 is a high level user authentication and authorization flow.

NOTE: The specific user authentication and authorization architecture required by the VAL services in order to realize the VAL user authentication and authorization is specified in subclauses 5.2.3, 5.2.4 and 5.2.5 of 3GPP TS 33.434 [29].

The user authentication process shown in figure 12.3.3.2-1 may take place in some scenarios as a separate step independently from a SIP registration phase, for example if the SIP core is outside the domain of the VAL server.

Editor's note: The procedure described in this subclause as shown in Figure 12.3.3.2-1 may require further study.

A procedure for user authentication is illustrated in figure 12.3.3.2-1. Other alternatives may be possible, such as authenticating the user within the SIP registration phase.



Figure 12.3.3.2-1: VAL user authentication and registration with Primary VAL system, single domain

1. In this step the identity management client begins the user authorization procedure. The VAL user supplies the user credentials (e.g. biometrics, secureID, username/password) for verification with the identity management server. This step may occur before or after step 3. In a VAL system with multiple VAL services, a single user authentication as in step 1 can be used for multiple VAL service authorizations for the user.

2. The signalling user agent establishes a secure connection to the SIP core for the purpose of SIP level authentication and registration.

3. The signalling user agent completes the SIP level registration with the SIP core (and an optional third-party registration with the VAL service server(s)).

NOTE 1: The VAL client(s) perform the corresponding VAL service authorization for the user by utilizing the result of this procedure.

NOTE 2: Steps 2 and 3 are not required to be performed if the VAL service does not use SIP.

\* \* \*Next Change \* \* \* \*

#### 12.3.3.3 Interconnection partner VAL system

Where communications with a partner VAL system using interconnection are required, user authorization takes place in the serving VAL system of the VAL service user, using the VAL user service authorization procedure specified in subclauses 5.2.5 and 5.2.6 of 3GPP TS 33.434 [29].

\* \* \*Next Change \* \* \* \*

### 12.4.1 General

There are no APIs defined for SEAL Identity Management.

### 12.4.2 Void

#### 12.4.2.1 Void

#### 12.4.2.2 Void

\* \* \*Next Change \* \* \* \*

#### 13.2.4.2 Key management client

The key management functional entity acts as the application client for key management functions. It interacts with the key management server. The key management client also supports interactions with the corresponding key management client between the two UEs.

NOTE: The functionality of the key management client is specified in subclause 5.3 of 3GPP TS 33. 434 [29].

\* \* \*Next Change \* \* \* \*

#### 13.2.4.3 Key management server

The key management server is a functional entity that stores and provides security related information (e.g. encryption keys) to the key management client, group management server and vertical application server to achieve the security goals of confidentiality and integrity of media and signalling. The key management server acts as CAPIF's API exposing function as specified in 3GPP TS 23.222 [8]. The key management server also supports interactions with the corresponding key management server in distributed SEAL deployments.

NOTE: The functionality of the key management server is specified in subclause 5.3 of 3GPP TS 33.434 [29].

\* \* \*Next Change \* \* \* \*

#### 13.2.5.2 KM-UU

The interactions related to key management functions between the key management client and the key management server are supported by KM-UU reference point. This reference point utilizes Uu reference point as described in 3GPP TS 23.401 [9] and 3GPP TS 23.501 [10].

KM-UU reference point provides a means for the key management server to provide security related information (e.g. encryption keys) to the key management client. The KM-UU reference point shall use the HTTP-1 and HTTP-2 signalling control plane reference points for transport and routing of security related information to the key management client.

NOTE: KM-UU reference point is specified in subclause 5.1.1.4 of 3GPP TS 33.434 [29].

\* \* \*Next Change \* \* \* \*

#### 13.2.5.5 KM-S

The interactions related to key management functions between the VAL server(s) and the key management server are supported by KM-S reference point. This reference point is an instance of CAPIF-2 reference point as specified in 3GPP TS 23.222 [8].

KM-S reference point provides a means for the key management server to provide security related information (e.g. encryption keys) to the VAL server. The KM-S reference point shall use the HTTP-1 and HTTP-2 signalling control plane reference points for transport and routing of security related information to the VAL server.

NOTE: KM-S is specified in subclause 5.1.1.4 of 3GPP TS 33.434 [29].

\* \* \*Next Change \* \* \* \*

## 13.3 Procedures and information flows for key management

NOTE: The procedure for key management is specified in subclause  5.3 of 3GPP TS 33.434 [29].

\* \* \*Next Change \* \* \* \*

### 13.4.1 General

The SEAL APIs for Key Management are specified in subclauses 5.7.1 and 7.6.1 of 3GPP TS 29.549 [xx].

### 13.4.2 Void

#### 13.4.2.1 Void

#### 13.4.2.2 Void

\* \* \* End of Change \* \* \* \*