**3GPP TSG-CT WG3 Meeting #110eC3-203530**

**E-Meeting, 02nd – 11th June 2020** (Revision of C3-203318)

**Source: Samsung**

**Title: Pseudo-CR on SEAL Security APIs**

**Spec: 3GPP TS 29.549 v1.2.0**

**Agenda item: 16.27**

**Document for: Decision**

**1. Introduction**

This contribution proposes the Identity and key management API aspects aligning to TS 33.434.

**2. Reason for Change**

SEAL Identity and Key management services are specified by SA3 in TS 33.434. As per TS 33.434,

1. There are no requirements for interactions between VAL server and the Identity management server. Hence, no Identity management APIs need to defined in TS 29.549.
2. Clause 6.3 specifies the Key management procedure and as per this procedure, the VAL server fetches key management information from the key management server. Hence, new Key management API need to be specified in TS 29.549.

**3. Conclusions**

1. Existing clauses related to Identity management APIs are deleted.

2. SS\_KeyInfoRetrieval API defined (Service and API definition, Open API file)

**4. Proposal**

It is proposed to agree the following changes to 3GPP TS 29.549 v1.2.0.

\* \* \* First Change \* \* \* \*

## 5.1 Introduction of SEAL services

The table 5.1-1 lists the SEAL server APIs below the service name. A service description clause for each API gives a general description of the related API.

Table 5.1-1: List of SEAL Service APIs

|  |  |  |  |
| --- | --- | --- | --- |
| Service Name | Service Operations | Operation Semantics | Consumer(s) |
| SS\_LocationReporting | Trigger\_Location\_Reporting | Request/ Response | VAL server |
| SS\_LocationInfoEvent | Subscribe\_Location\_Info | Subscribe/Notify | VAL server |
| Notify\_Location\_Info | VAL server |
| SS\_LocationInfoRetrieval | Obtain\_Location\_Info | Request/ Response | VAL server |
| SS\_GroupManagement | Query\_Group\_Info | Request/ Response | VAL server |
| Update\_Group\_Info | Request/ Response | VAL server |
| Create\_Group | Request/ Response | VAL server |
| Delete\_Group | Request/Response | VAL server |
| SS\_GroupManagementEvent | Subscribe\_Group\_Info\_Modification | Subscribe/Notify | VAL server |
| Notify\_Group\_Info\_Modification | VAL server |
| Notify\_Group\_Creation | VAL server |
| SS\_UserProfileRetrieval | Obtain\_User\_Profile | Request/ Response | VAL server |
| SS\_UserProfileEvent | Subscribe\_User\_Profile\_Update | Subscribe/Notify | VAL server |
| Notify\_User\_Profile\_Update | VAL server |
| SS\_NetworkResourceAdaptation | Reserve\_Network\_Resource | Request/Response | VAL server |
| Request\_Unicast\_Resource | Request/Response | VAL server |
| Update\_Unicast\_Resource | Request/Response | VAL server |
| Request\_Multicast\_Resource | Request/Response | VAL server |
| Notify\_UP\_Delivery\_Mode | Subscribe/Notify | VAL server |
| SS\_Events | Subscribe\_Event | Subscribe/Notify | VAL server |
| Notify\_Event | VAL server |
| Unsubscribe\_Event | VAL server |
| SS\_KeyInfoRetrieval | Obtain\_Key\_Info | Request/Response | VAL server |
| NOTE: The service operations of SS\_Events API are reused by the SS\_LocationInfoEvent, SS\_GroupManagementEvent and SS\_UserProfileEvent for events related services. |

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

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

## 5.7 Key management APIs

### 5.7.1 SS\_KeyInfoRetrieval API

#### 5.7.1.1 Service Description

##### 5.7.1.1.1 Overview

As specified in 3GPP TS 33.434 [AA], the SS\_KeyInfoRetrieval API, allows the VAL server via KM-S reference point to obtain the VAL service specific key management information from the key management server.

#### 5.7.1.2 Service Operations

##### 5.7.1.2.1 Introduction

The service operation defined for SS\_KeyInfoRetrieval API is shown in the table 5.7.1.2.1-1.

Table 5.7.1.2.1-1: Operations of the SS\_ KeyInfoRetrieval API

|  |  |  |
| --- | --- | --- |
| Service operation name | Description | Initiated by |
| Obtain\_Key\_Info | This service operation is used by VAL server to obtain key management information. | VAL server |

##### 5.7.1.2.2 Obtain\_Key\_Info

###### 5.7.1.2.2.1 General

This service operation is used by the VAL server to obtain VAL service specific key management information.

###### 5.7.1.2.2.2 VAL server obtaining VAL service specific key material using Obtain\_Key\_Info service operation

To obtain key management information specific to VAL service, the VAL server shall send HTTP GET request message to key management server, on Key records resource collection URI, with query parameters VAL service ID along with VAL user ID or VAL UE ID, URI of the target SEAL KMS, as specified in 7.6.1.2.2.3.1.

Upon receiving the HTTP GET message as described above, the key management server shall:

1. verify the identity of the VAL server and check if the VAL server is authorized to obtain key management information specific to VAL service, VAL user or VAL UE, the URI in the request is of target SEAL KMS and date/time of the request is in recent time window;

2. if the VAL server is authorized to obtain the requested key management information, the key management server shall;

a. return in the response message with key management information corresponding to the query parameters that were sent in the request message.

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

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

## 7.6 Key management APIs

### 7.6.1 SS\_KeyInfoRetrieval API

#### 7.6.1.1 API URI

The request URI used in each HTTP request from the VAL server towards the Key management server shall have the structure as defined in clause 6.5 with the following clarifications:

- The {apiName}shall be "ss-kir".

- The {apiVersion} shall be "v1".

- The {apiSpecificSuffixes} shall be set as described in clause 7.6.1.2.

#### 7.6.1.2 Resources

##### 7.6.1.2.1 Overview



Figure 7.6.1.2.1-1: Resource URI structure of the SS\_KeyInfoRetrieval API

Table 7.6.1.2.1-1 provides an overview of the resources and applicable HTTP methods.

Table 7.6.1.2.1-1: Resources and methods overview

|  |  |  |  |
| --- | --- | --- | --- |
| Resource name | Resource URI | HTTP method or custom operation | Description |
| Key records | {apiRoot}/ss-kir/<apiVersion>/key-records | GET | Retrieve key management information uniquely applicable to VAL service, VAL user or VAL UE. |

##### 7.6.1.2.2 Resource: Key Records

###### 7.6.1.2.2.1 Description

The Key Records resource represents the key management information of all VAL services that are created at a given key management server.

###### 7.6.1.2.2.2 Resource Definition

Resource URI: **{apiRoot}/ss-kir/<apiVersion>/key-records**

This resource shall support the resource URI variables defined in the table 7.6.1.2.x.2-1.

Table 7.6.1.2.x.2-1: Resource URI variables for this resource

|  |  |  |
| --- | --- | --- |
| Name | Data Type | Definition |
| apiRoot | string | See clause 6.5 |
| apiVersion | string | See clause 7.6.1.1 |

###### 7.6.1.2.2.3 Resource Standard Methods

7.6.1.2.2.3.1 GET

This operation retrieves VAL service key management information satisfying the filter criteria. This method shall support the URI query parameters specified in table 7.6.1.2.2.3.1-1.

Table 7.6.1.2.2.3.1-1: URI query parameters supported by the GET method on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Data type | P | Cardinality | Description |
| val-tgt | ValTargetUe | O | 0..1 | Identifying a VAL user or a VAL UE. |
| val-service-id | string | M | 1 | String identifying a VAL service. |
| skms-uri | Uri | M | 1 | The URI of the SEAL key management server to which the request is sent. |

This method shall support the request data structures specified in table 7.6.1.2.2.3.2-2 and the response data structures and response codes specified in table 7.6.1.2.2.3.2 -3.

Table 7.6.1.2.2.3.2-2: Data structures supported by the GET Request Body on this resource

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | P | Cardinality | Description |
| n/a |  |  |  |

Table 7.6.1.2.2.3.2-3: Data structures supported by the GET Response Body on this resource

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data type | P | Cardinality | Responsecodes | Description |
| ValKeyInfo | M | 1 | 200 OK | Key management information specific to VAL service, VAL user or VAL UE. This response shall include key management information matching the query parameters provided in the request.  |
| NOTE: The mandatory HTTP error status codes for the GET method listed in table 5.2.6-1 of 3GPP TS 29.122 [3] also apply. |

###### 7.6.1.2.2.4 Resource Custom Operations

None.

#### 7.6.1.3 Notifications

None.

#### 7.6.1.4 Data Model

##### 7.6.1.4.1 General

This clause specifies the application data model supported by the API. Data types listed in clause 6.2 apply to this API.

Table 7.6.1.4.1-1 specifies the data types defined specifically for the SS\_KeyInfoRetrieval API service.

Table 7.6.1.4.1-1: SS\_KeyInfoRetrieval API specific Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Section defined | Description | Applicability |
| ValKeyInfo | 7.6.1.4.2.3 | Key management information associated with VAL server, VAL user or VAL UE. |  |

Table 7.6.1.4.1-2 specifies data types re-used by the SS\_KeyInfoRetrieval API service.

Table 7.6.1.4.1-2: Re-used Data Types

|  |  |  |  |
| --- | --- | --- | --- |
| Data type | Reference | Comments | Applicability |
| ValTargetUe | Clause 7.3.1.4.2.x | Used to identify a VAL User ID or VAL UE ID applicable to key management information.  |  |

##### 7.6.1.4.2 Structured Data Types

###### 7.6.1.4.2.1 Introduction

###### 7.6.1.4.2.2 ValKeyInfo

Table 7.6.1.4.2.3-1: Definition of type ValKeyInfo

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Attribute name | Data type | P | Cardinality | Description | Applicability |
| userUri | Uri | M | 1 | URI of the user for which the response is intended. |  |
| skmsUri | Uri | M | 1 | The URI of the SEAL key management server sending the response. |  |
| skmsId | string | O | 0..1 | String identifying the SEAL key management server, sending the response. |  |
| valService | string | M | 1 | String identifying the VAL service. This attribute shall be same as in the HTTP GET request.  |  |
| valTgt | ValTargetUe | O | 0..1 | String identifying a VAL user or VAL UE. This value depends on the value that was in the HTTP GET request.  |  |
| dateTime | string | M | 1 | The Date and Time of the response. This represents the number of seconds from 1970-01-01T0:0:0Z as measured in UTC. |  |
| keyInfo | string | O | 0..1 | Key management information uniquely applicable to the requested VAL service, VAL user or VAL UE or VAL client.  |  |

##### 7.6.1.4.3 Simple data types and enumerations

None.

#### 7.6.1.5 Error Handling

General error responses are defined in clause 6.7.

#### 7.6.1.6 Feature Negotiation

General feature negotiation procedures are defined in clause 6.8.

Table 7.6.1.6-1: Supported Features

|  |  |  |
| --- | --- | --- |
| **Feature number** | **Feature Name** | **Description** |
|  |  |  |

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

## A.X SS\_KeyInfoRetrieval API

openapi: 3.0.0

info:

 title: SS\_KeyInfoRetrieval

 description: |

 API for SEAL Key Information Retrieval.

 © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

 All rights reserved.

 version: "1.0.0.alpha-1"

externalDocs:

 description: 3GPP TS 29.549 V1.2.0 Service Enabler Architecture Layer for Verticals (SEAL); Application Programming Interface (API) specification; Stage 3.

 url: http://www.3gpp.org/ftp/Specs/archive/29\_series/29.549/

security:

 - {}

 - oAuth2ClientCredentials: []

servers:

 - url: '{apiRoot}/ss-kir/v1'

 variables:

 apiRoot:

 default: https://example.com

 description: apiRoot as defined in clause 6.5 of 3GPP TS 29.549

paths:

 /key-records:

 get:

 description: Retrieve Key mamangement information specific to VAL service.

 parameters:

 - name: val-service-id

 in: query

 description: String identifying an individual VAL service

 required: true

 schema:

 type: string

 - name: skms-uri

 in: query

 description: Identifying the uri of the SKM-S.

 required: true

 schema:

 $ref: 'TS29122\_CommonData.yaml#/components/schemas/Uri'

 - name: val-tgt

 in: query

 description: Identifying a VAL target.

 required: false

 schema:

 $ref: 'TS29549\_SS\_UserProfileRetrieval.yaml#/components/schemas/ValTargetUe'

 responses:

 '200':

 description: The key management information of the VAL service, VAL User or VAL UE.

 content:

 application/json:

 schema:

 $ref: '#/components/schemas/ValKeyInfo'

 '400':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/400'

 '401':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/401'

 '403':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/403'

 '404':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/404'

 '406':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/404'

 '429':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/429'

 '500':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/500'

 '503':

 $ref: 'TS29122\_CommonData.yaml#/components/responses/503'

 default:

 $ref: 'TS29122\_CommonData.yaml#/components/responses/default'

components:

 securitySchemes:

 oAuth2ClientCredentials:

 type: oauth2

 flows:

 clientCredentials:

 tokenUrl: '{tokenUrl}'

 scopes: {}

 schemas:

 ValKeyInfo:

 type: object

 properties:

 userUri:

 $ref: 'TS29122\_CommonData.yaml#/components/schemas/Uri'

 skmsUri:

 $ref: 'TS29122\_CommonData.yaml#/components/schemas/Uri'

 skmsId:

 type: string

 description: String identifying the key management server.

 valService:

 type: string

 description: Unique identifier of a VAL Service.

 valTgt:

 $ref: 'TS29549\_SS\_UserProfileRetrieval.yaml#/components/schemas/ValTargetUe'

 dateTime:

 type: string

 description: Date and time when the response was sent.

 keyInfo:

 type: string

 description: Key management information specific to VAL service, VAL User or VAL UE.

 required:

 - userUri

 - skmsUri

 - valService

 - dateTime

\* \* \* End of Changes \* \* \* \*