**3GPP TSG-SA WG3 Meeting #98Bis-e *S3-200648***

**e-Meeting, 14-17 April 2020** *revision of S3-19abcd*

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| *CR-Form-v12.0* | | | | | | | | |
| **DRAFT CHANGE REQUEST** | | | | | | | | |
|  | | | | | | | | |
|  | **33.180** | **CR** | **Draft CR** | **Rev** | **-** | **Current version:** | **16.3.0** |  |
|  | | | | | | | | |
| *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:*** | [33.180] R16 TrK-ID and InK-ID indication | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Source to WG:*** | Motorola Solutions | | | | | | | | | |
| ***Source to TSG:*** | S3 | | | | | | | | | |
|  |  | | | | | | | | | |
| ***Work item code:*** | MCXSec | | | | |  | ***Date:*** | | | 14-Mar-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:*** | | The TrK-ID and signing key ID are missing from the KMS request and response messages. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Summary of change:*** | | Add TrK-ID and signing key ID to KMS request and response messages | | | | | | | | |
|  | |  | | | | | | | | |
| ***Consequences if not approved:*** | | Transport of key material from KMS to MC clients may not be protected. | | | | | | | | |
|  | |  | | | | | | | | |
| ***Clauses affected:*** | | D.2.2, D.3, D.3.1 | | | | | | | | |
|  | |  | | | | | | | | |
|  | | **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 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

## D.2.2 KMS request security

The content of the KMS request type XML payload is:

Table D.2.2-1: Contents of a KMS request type XML

|  |  |
| --- | --- |
| Name | Description |
| Version | (Attribute) The version number of the key provision XML (1.1.0). |
| UserUri | URI of the user for which is making the request. |
| KmsUri | The URI of the KMS to which the request is sent. |
| ClientId | (Optional) A string representing the client |
| DeviceId | (Optional) A string representing the device |
| Time | Date/time that the request is made by the client. |
| ClientReqUrl | The resource URI to which the HTTP POST request is sent. |
| KrrList | (Optional) Zero or more KMS Redirect Responses (KRRs). Only used when posting to the ‘redirect' subdirectory. |
| ClientError | (Optional) If a previous failure had occurred, this complex type can provide error information to the KMS |
| TrK-ID | (Optional) The ID of the TrK used for confidentiality protection of key management payloads. |
| Signature-ID | (Optional) The ID of the key used to sign KMS messages. |

When application confidentiality is required by the MC operator, the TrK-ID of the TrK currently residing in the MC UE shall be included in the KMS request message as shown in Table D.2.2-1.

When a signature is applied to the KMS request, the Signature-ID field in Table D.2.2-1 shall be present and indicate either the InK-ID if the InK is used or the TrK-ID if the TrK is used. When a signature is applied and the InK is present, the InK shall be used. When a signature is applied and an InK is not present but a TrK is present, then the TrK shall be used.

The XML schema for the SignedKmsRequestType is provided in Clause D.3.5.2.

If the KMS supports authenticated requests, upon receipt of a SignedKmsRequestType attached to a KMS Request, the KMS shall verify that:

- the signature is valid, based on the UserUri and the InK or TrK used to sign the message.

- the XML is valid.

- the KmsUri is the KMS's KMS URI.

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

- the ClientReqUrl is the same as the resource URI to which the HTTP POST request is sent.

If so, the request is accepted and processed.

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

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

# D.3 KMS responses

## D.3.1 General

This clause defines the HTTP responses made by the KMS to KMS requests. The KMS attaches XML content to the HTTP responses. The XML serves to provision the client based upon its request.

Though a "KmsResponse" message containing a "KmsMessage" Type is the general response to any request, the content of the "KmsMessage" varies depending on the exact response type (i.e. KmsInit, KmsKeyProv, KmsCertCache, KmsLookup).

The content provided within a KmsInit, KmsKeyProv, KmsCertCache or KmsLookup may include a TrK, InK, KMS URIs, (public) KMS Certificates, (private) user Key Set provisioning, or combinations thereof.

The “KmsResponse” message is shown in Table D.3.1-1.

Table D.3.1-1: Contents of a KmsResponse message

|  |  |
| --- | --- |
| Name | Description |
| UserUri | URI of the user for which the response is intended. |
| KmsUri | The URI of the KMS sending the response. |
| KmsId | (Optional) The ID of the KMS providing the response message. |
| Time | Date/time that the response is sent by the KMS. |
| ClientReqUrl | The resource client URI from where the request originated. |
| KmsMessage | One of the following response types: KmsInit, KmsKeyProv, KmsCertCache, or KmsLookup. |
| TrK-ID | (Optional) The ID of the TrK used to confidentiality protect the KmsMessage. |
| Signature-ID | (Optional) The ID of the key used to sign the KmsMessage. |

In response to a "KMS Initialize" request, the KMS shall respond with the KMS's own certificate (the Root KMS certificate), and may respond with a new TrK and/or a new InK. The data is returned within a "KMSInit" tag.

In response to a "KMS KeyProvision" request, the KMS shall provision appropriate user Key Sets within a "KMSKeyProv" tag, and may also respond with a new TrK and/or a new InK.

In response to a "KMS CertCache" request, the KMS shall provision a cache of KMS certificates allowing inter-domain communications within a "KMSCertCache" tag.

In response to a "KMS Cert" request, the KMS shall provision a single KMS certificate within a "KMSCertCache" tag. If the requested KMS Certificate is not available, then an error message is returned.

In response to a "KMS Lookup" request, the KMS shall provide information on the KMS URI associated with the requested SIP URI, within a "KMSLookup" tag.

The KMS does not respond to a "KMS Redirect Upload" message, unless an error occurs.

When confidentiality is applied to the KmsResponse payload (KmsMessage), the KMS shall use the TrK currently residing in the MC UE to encrypt the KmsMessage. The associated TrK-ID shall then be included in the KmsResponse message as shown in Table D.3.1-1.

When a signature is applied to the KmsResponse message, the Signature-ID field in Table D.3.1-1 shall be present and indicate either the InK-ID if the InK is used or the TrK-ID if the TrK is used. When a signature is applied and the InK is present, the InK shall be used. When a signature is applied and an InK is not present but a TrK is present, then the TrK shall be used.

The XML schema for the SignedKmsRequestType is provided in Clause D.3.5.2.

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

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* START of change 3 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* END of change 3 \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*