**3GPP TSG-S4 Meeting # 127-bis-e S4-240577**

**Online, April 8th - 12th, 2024**

|  |
| --- |
| *CR-Form-v12.2* |
| **PSEUDO CHANGE REQUEST** |
|  |
|  | **26.510** | **CR** |  | **rev** |  | **Current version:** | **1.1.4** |  |
|  |
| *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:***  | pCR on Usage of Server Certificates |
|  |  |
| ***Source to WG:*** | Qualcomm Inc. |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | 5GMS\_Pro\_Ph2 |  | ***Date:*** | 2nd April 2024 |
|  |  |  |  |  |
| ***Category:*** | B |  | ***Release:*** | Rel-18 |
|  | *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-16 (Release 16)Rel-17 (Release 17)Rel-18 (Release 18)Rel-19 (Release 19)* |
|  |  |
| ***Reason for change:*** | Adding support for server certificates for RTC and clarifying the creation of CSR requests. |
|  |  |
| ***Summary of change:*** |  |
|  |  |
| ***Consequences if not approved:*** |  |
|  |  |
| ***Clauses affected:*** | 5.2.1, 5.2.4.1, 5.2.4.3, 8.4.3.1 |
|  |  |
|  | **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:*** |  |

|  |
| --- |
| **First Change** |

### 5.2.1 Overview

A Media Application Provider may use the operations in this clause to provision the different features offered by the Media Delivery System in the Media AF. The Provisioning API exposed by the Media AF to the Media Application Provider at reference point M1 offers the following sets of operations:

1. Provisioning of *Provisioning Sessions* (see clause 5.2.2) to act as an umbrella for the following provisioning information. Each such Provisioning Session is uniquely identified by a system-dependent Provisioning Session identifier as well as by system-independent service identifier that is subsequently used by a Media-Aware Application to launch media session handling (see clause 10.2) via a 3GPP Service URL (see clause 6).

2. Discovery of the set of content ingest and/or egest protocols supported by the Media AS for a particular Provisioning Session (see clause 5.2.3):

- For downlink media streaming according to TS 26.512 [26512], discovery of the content ingest protocols available at reference point M2 and the content distribution protocols available at reference point M4.

- For uplink media streaming according to TS 26.512 [26512], discovery of the content contribution protocols available at reference point M4 and the content egest protocols available at reference point M2.

3. Provisioning of *Server Certificates* within the scope of a Provisioning Session (see clause 5.2.4) to be used by the Media AS to assert its identity to the Media Access Function in Media Clients during media delivery sessions at reference point M4.

4. Provisioning of *Content Preparation Templates* within the scope of a Provisioning Session (see clause 5.2.5) that can be used by the Media AS to manipulate media content ingested at reference point M2 or contributed at reference point M4.

5. Provisioning of *Edge Resources* within the scope of a Provisioning Session (see clause 5.2.6) to be used to instantiate the Media AS as a set of Edge Application Servers (EAS) in an Edge Data Network (EDN) using the APIs specified in TS 29.558 [29558].

5. Provisioning of *Policy Templates* within the scope of a Provisioning Session (see clause 5.2.7) that can be applied to M4 downlink/uplink media delivery sessions in order to realise different Service Operation Points as part of the Dynamic Policies feature (see clause 5.4.3).

7. Provisioning of media delivery by the Media AS within the scope of a Provisioning Session using the abovementioned building blocks:

- For downlink media streaming according to TS 26.512 [26512], provisioning of the *Content Hosting* feature of the Media AS (see clause 5.2.8), which offers functionality equivalent to that of a public Content Delivery Network (CDN): content ingest at reference point M2 for onward distribution by the Media AS to Media Clients via reference point M4 or via other distribution systems such as eMBMS or MBS.

 After discovering the set of ingest and distribution content protocols supported by the Media AS (see clause 5.2.2), the Media Application Provider may provision a Server Certificate (see clause 5.2.4), Content Preparation Template (see clause 5.2.5) and/or Edge Resources Configuration (see clause 5.2.6) for each Content Hosting distribution configuration to reference. The Media Application Provider may also provision one or more Policy Templates (see clause 5.2.7) to realise Service Operation Points pertaining to downlink media delivery.

- For uplink media streaming according to TS 26.512 [26512], provisioning of the *Content Publishing* feature of the Media AS (see clause 5.2.9), including content contribution by Media Clients at reference point M4 and subsequent content egest of content at reference point M2 after optional manipulation by a Content Preparation Template.

 After discovering the set of contribution and egest content protocols supported by the Media AS (see clause 5.2.2), the Media Application Provider may provision a Server Certificate (see clause 5.2.4), Content Preparation Template (see clause 5.2.5) and/or Edge Resources Configuration (see clause 5.2.6) for each Content Publishing contribution configuration to reference. The Media Application Provider may also provision one or more Policy Templates (see clause 5.2.7) to realise Service Operation Points relevant to the parent Provisioning Session.

* For Real-Time Communication (RTC) according to TS 26.113, provisioning of the RTC Configuration, which enables the Media Application Provider to provision a list of RTC application servers for use by the UE. The supported RTC AS functionalities are: WebRTC signalling server, STUN, and TURN servers. Each of these servers may also be associated with a Server Certificate to enable secure and authenticated access to it. The Media Application Provider may also provision one or more Policy Templates (see clause 5.2.7) to be applied to RTC session of that Media Application Provider.

8. Provisioning of *QoE metrics reporting* within the scope of a Provisioning Session (see clause 5.2.10) to configure how and how often the Media Client should report Quality of Experience metrics to the Media AF during the course of media delivery sessions at reference point M4.

9. Provisioning of *consumption reporting* within the scope of a Provisioning Session (see clause 5.2.11) to configure how often the Media Client should report downlink media consumption to the Media AF during the course of media delivery sessions at reference point M4.

10. Provisioning of rules for processing of UE data (as defined in TS 26.531 [26531]) related to media delivery sessions by the Data Collection AF instantiated in the Media AF (as defined in clause 4.7 of TS 26.501 [26501]), and for restricting its exposure over reference points R5 and R6 by means of Event Data Processing Configurations and Data Access Profiles for a particular Event ID.

NOTE: The *Network Assistance* feature is not provisioned by the Media Application Provider at reference point M1. Instead, it is provisioned at the discretion of the Media Delivery System operator using means beyond the scope of the present document.

|  |
| --- |
| **2nd Change** |

#### 5.2.4.1 General

Each X.509 server certificate [X.509] presented by the Media AS to the Media Client at reference point M4 is represented by a Server Certificate resource at reference point M1. The Server Certificates Provisioning API specified in clause 8.4 enables a Server Certificate resource to be created within the scope of a Provisioning Session, and subsequently referenced by a Content Hosting Configuration, Content Publishing Configuration, or an RTC Configuration created in the scope of the same Provisioning Session. That API supports two alternative provisioning methods for Server Certificate resources: one in which a certificate is generated by the Media Delivery System operator on behalf of the Media Application Provider; the other in which a certificate is generated by the Media Application Provider from a Certificate Signing Request solicited from the Media AF. Both methods shall be supported by implementations of the Media AF.

Under no circumstances shall the Media AF reveal the private key associated with a Certificate Signing Request to the Media Application Provider.

HTTP responses for successful and operation-specific failure cases are specified in the following clauses. For all other failure cases, an HTTP response indicating a response code in accordance with clause 7.1.6 shall be returned to the API client. In all failure cases a message body in accordance with clause 7.1.7 shall be included in the response message.

|  |
| --- |
| **2nd Change** |

#### 5.2.4.3 Reserve Server Certificate resource operation

This operation is used by the Media Application Provider to solicit a Certificate Signing Request (CSR) from the Media AF for the purpose of generating an X.509 certificate [X.509] independently of the Media Delivery System. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the Media Application Provider itself, or that of a third party acting on its behalf. The first Subject Alternative Name (subjectAltName) extension field of the certificate should be identical to its Common Name. The CN and subjectAltName fields may include a single wildcard ("\*") character at the start to indicate applicability to several different subdomains of the same domain.

NOTE: Modern TLS client implementations ignore the obsolete Common Name (CN) field of the X.509 certificate in favour of the first Subject Alternative Name (subjectAltName) extension field.

The Media Application Provider may specify additional domains in its certificate reservation request to the Media AF. If provided, these domain name aliases shall be included in the returned Certificate Signing Request using the Subject Alternative Name (subjectAltName) extension (see section 4.2.1.6 of RFC 5280 [RFC5280]). In this case, the Media Application Provider is responsible for ensuring that any FQDN aliases it subsequently provisions in Content Hosting Configurations or Content Publishing Configurations matching these additional domains resolve to the canonical domain name of the Media AS in the target Media Application System.

The Media Application Provider shall separately arrange for the FQDN carried in the Common Name of the certificate generated, or those of all Subject Alternative Name (subjectAltName) extensions in the same certificate (see section 4.2.1.6 of RFC 5280 [RFC5280]), to resolve to the address of a Media AS.

- For a media streaming according to TS 26.512 [26512], it should resolve to the domain name alias that is obtained after provisioning the Content Hosting feature per clause 5.2.8.2 or the Content Publishing feature per clause 5.2.9.2.

- For real-time media communication according to TS 26.113 [26113], it should resolve to the domain names of the RTC subfunctions that are provided as part of the RTC Configuration resource as specified in clause 5.2.13.

The Media Application Provider shall use the HTTP POST method to create a new Server Certificate. The request URL shall be a well-known sub-resource of the Provisioning Session resource representing its Server Certificates resource collection, as specified in clause 8.4.2, including the query parameter specified there. Domain name aliases (if any) shall be conveyed in the HTTP request message body, encoded as a JSON array of strings; otherwise, the request message body shall be omitted. Upon successful creation of the resource, the Media AF shall return a 201 (Created) response message and the URL of the resource, including the resource identifier of the reserved Server Certificate resource, shall be returned in the HTTP Location header. The HTTP response message shall provide a Certificate Signing Request as specified in clause 8.4.3.1.

If the list of additional domains in the HTTP request message is malformed, the Media AF shall return a 400 (Bad Request) response message.

If the request is acceptable but the Media AF is unable to generate a Certificate Signing Request, the creation operation shall fail with an HTTP response status code of 500 (Internal Server Error) and an error message body per clause 7.1.7. In this case, the Server Certificate resource shall remain in an uncreated state in the Media AF.

This operation may be performed multiple times by a Media Application Provider to provision different Server Certificate resources within the scope of a Provisioning Session. Each such resource is assigned a different Server Certificate resource identifier by the Media AF.

|  |
| --- |
| **2nd Change** |

#### 8.4.3.1 Certificate Signing Request

The Certificate Signing Request shall provide the FQDN of the Media AS that is to be included in the Subject and Subject Alternative Name extension of the certificate to be generated. If multiple FQDNs are provided in the Certificate Signing Request, they should be supplied as one value per line, with the first line indicating the primary FQDN of the Media AS.

The Certificate Signing Request shall comply with the Privacy-Enhanced Mail (PEM) textual format specified in RFC 7468 [RFC7468], i.e. a Base64-encoded DER certificate request or certificate, including leading and trailing encapsulation boundary lines.

The MIME content type of the Certificate Signing Request shall be application/x-pem-file.