**3GPP TSG- Meeting #126S4-231755**

**, USA, November 2023**

|  |
| --- |
| *CR-Form-v12.2* |
|  **CHANGE REQUEST** |
|  |
|  |  | **CR** | **0060** | **rev** | **-** | **Current version:** |  |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **x** |

|  |
| --- |
|  |
| ***Title:***  | [5GMS3] Correction of Server Certificate handling |
|  |  |
| ***Source to WG:*** | Ericsson LM |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | 5GMS3 |  | ***Date:*** | 3.11.2023 |
|  |  |  |  |  |
| ***Category:*** |  |  | ***Release:*** | Rel-17 |
|  | *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:*** | The relation between the Server Certificate and the Content Hosting Configuration is unclear. An Application Client verifies the Server Certification during TLS Session Establishment. One of the verification checks is the matching of the Domain Names, which are listed within the Certificate with the Domain Name of the actual request URL. The TLS session establishment fails, when the domain name matching fails. The Service Access Information is compiled based on the Content Hosting Configuration, usign either the domainNameAlias or the canonicalDomainName. However, it is not clear, whether these domain names are also present in the Server Certificate. |
|  |  |
| ***Summary of change:*** | The dependency to the Content Hosting Configuration is clarified within the Server Certificate Procedures for both cases, i.e. when the 5GMS System operator decides on the domain name in the certificate and when the 5GMS Application Provider decides on the domain names.An informative Annex is added, illustrating the conplete sequence of these two different server certificate creation alternatives. |
|  |  |
| ***Consequences if not approved:*** | Incorrect and ambiguous specifications lead to interoperability issues. |
|  |  |
| ***Clauses affected:*** | 4.3.3.2, 4.3.3.4, 4.3.6.1, 4.3.6.2, 4.3.6.3, 4.3.6.4, 4.3.6.5, 7.6.3.1, X (new) |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  |  |
| ***affected:*** |  | **x** |  Test specifications |  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications |  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

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

### 4.3.3 Content Hosting Provisioning procedures

#### 4.3.3.1 General

These procedures are used by the 5GMSd Application Provider and the 5GMSd AF on M1d to provision the content hosting feature for downlink streaming.

#### 4.3.3.2 Create Content Hosting Configuration

This procedure is used by the 5GMSd Application Provider to create a new Content Hosting Configuration. The 5GMSd Application Provider shall use the HTTP POST method for this purpose and the request message body shall include a ContentHostingConfiguration resource, as specified in clause 7.6.3.1.

- If the Content Hosting Configuration uses the Pull-based content ingest method, i.e. the pull attribute is set to True, then the IngestConfiguration.baseURL property shall be nominated by the 5GMSd Application Provider in the request message body. The 5GMSd AF shall return the IngestConfiguration.baseURL property value unchanged in its response message body.

- If the Content Hosting Configuration uses the Push-based content ingest method, i.e. the pull attribute is set to False, then the IngestConfiguration.baseURL property shall be nominated by the 5GMSd AF and returned in the response message body. It shall not be set by the 5GMSd Application Provider in the request message body.

In all cases, the DistributionConfiguration.baseURL property is read-only: it shall be omitted from the creation request and shall be assigned by the 5GMSd AF, allowing the value to be inspected by the 5GMSd Application Provider in the returned ContentHostingConfiguration resource representation, or by using the procedure specified in clause 4.3.3.3 below.

If the procedure is successful, the 5GMSd AF shall generate a resource identifier representing the new Content Hosting Configuration. In this case, the 5GMSd AF shall respond with a 201 (Created) HTTP response message and shall provide the URL to the newly created resource in the Location header field. The response message body may include a ContentHostingConfiguration resource (see clause 7.6.3.1) that represents the current state of the Content Hosting Configuration, including any fields set by the 5GMSd AF.

When both properties are set in a given distribution configuration by the 5GMSd Application Provider, it is a requirement that the value of domain‌Name‌Alias matches one of the Subject Alternative Names in the Server Certificate resource referenced by certificateId (allowing for wildcard matching). If this is not the case, the 5GMSd AF shall respond with a 400 (Bad Request) response message.

If the procedure is otherwise unsuccessful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

#### 4.3.3.3 Read Content Hosting Configuration properties

This procedure is used by the 5GMSd Application Provider to obtain the properties of an existing Content Hosting Configuration resource from the 5GMSd AF. The HTTP GET method shall be used for this purpose.

If the procedure is successful, the 5GMSd AF shall respond with a 200 (OK) response message that includes the ContentHostingConfiguration resource in the response message body.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

#### 4.3.3.4 Update Content Hosting Configuration properties

The update operation is invoked by the 5GMSd Application Provider to modify the properties of an existing ContentHostingConfiguration resource. All writeable properties except domainNameAlias may be updated. The HTTP PATCH or HTTP PUT methods shall be used for the update operation.

If the procedure is successful, the 5GMSd AF shall respond with a 200 (OK) and provide the content of the resource in the response, confirming the successful update operation.

When both properties are set in a given distribution configuration by the 5GMSd Application Provider, it is a requirement that the value of domain‌Name‌Alias matches one of the Subject Alternative Names in the Server Certificate resource referenced by certificateId (allowing for wildcard matching). If this is not the case, the 5GMSd AF shall respond with a 400 (Bad Request) response message.

the procedure is otherwise unsuccessful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

#### 4.3.3.5 Destroy Content Hosting Configuration

This operation is used by the 5GMSd Application Provider to destroy a Content Hosting Configuration resource and to terminate the related distribution. The HTTP DELETE method shall be used for this purpose. As a result, the 5GMSd AF will release any associated network resources, purge any cached content, and delete any corresponding configurations.

If the procedure is successful, the 5GMSd AF shall respond with a 200 (OK) response message.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

#### 4.3.3.6 Purge Content Hosting cache

This operation is used by the 5GMSd Application Provider to purge content from the 5GMSd AS Content Hosting cache. The HTTP POST method shall be used for this purpose with a regular expression describing the media resource URLs to be purged provided in the body of the request, as specified in clause 7.6.4.3. As a result, the 5GMSd AF purges any cached content whose URL matches the specified regular expression.

If the procedure is successful, the 5GMSd AF shall respond with a 200 (OK) response message.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clauses 6.3 and 7.6.4.3.

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

### 4.3.6 Server Certificate Provisioning procedures

#### 4.3.6.1 General

Each X.509 server certificate [8] presented by the 5GMSd AS at reference point M4d or at reference point xMB-U is represented by a Server Certificate resource at M1d. The Server Certificates Provisioning API as specified in clause 7.3 enables a Server Certificate resource to be created within the scope of a Provisioning Session, and subsequently referenced by a Content Hosting 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 5GMS System operator on behalf of the 5GMSd Application Provider; the other in which a certificate is generated by the 5GMSd Application Provider from a Certificate Signing Request solicited from the 5GMSd AF. Both methods shall be supported by implementations of the 5GMSd AF.

NOTE: As a consumer of media from the 5GMSd AS in a combined architecture using 5GMS and eMBMS, the BMSC needs to be able to trust the content it is receiving comes from a bona fide source. This issue is left to implementation.

#### 4.3.6.2 Create Server Certificate

This procedure is used by the 5GMSd Application Provider to request that the 5GMS System generates a new X.509 certificate [8] on its behalf within the scope of a Provisioning Session. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the 5GMSd System operator and the use of supplementary domain name aliases is not supported. The first Subject Alternative Name (subjectAltName) extension field of the certificate should be identical to its Common Name. Both fields may include a single wildcard ("\*") character at the start to indicate applicability to several different subdomains of the same domain.

NOTE 1: 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 5GMSd Application Provider shall use the HTTP POST method to create a new Server Certificate resource. Upon successful creation, the 5GMSd AF shall respond with a 201 (Created) response message and the URL of the resource, including its resource identifier, shall be returned in the HTTP Location header. The response message body may optionally include a copy of the X.509 certificate corresponding to the newly created Server Certificate resource, as specified in clause 7.3.3.2.

NOTE 2: The X.509 certificate corresponding to the newly created Server Certificate resource may not be available immediately for interrogation and use. See clause 4.3.6.4 below for more details.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

When the Server Certificate resource is subsequently referenced by a Content Hosting Configuration in the scope of the same Provisioning Session, the canonical domain name of all distribution configurations shall be a Fully-Qualified Domain Name (FQDN) that matches the Common Name and the first Subject Alternative Name in the referenced Server Certificate resource.

#### 4.3.6.3 Reserve Server Certificate

This procedure is used by the 5GMSd Application Provider to solicit a Certificate Signing Request (CSR) from the 5GMSd AF for the purpose of generating an X.509 certificate [8] independently of the 5GMSd System. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the 5GMSd System operator. 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 1: 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 5GMSd 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 [20]), to resolve to the address of a 5GMSd AS in the target 5GMS System.

The 5GMSd Application Provider may specify additional domains in its certificate reservation request to the 5GMSd 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 [20]). In this case, the 5GMSd Application Provider is responsible for ensuring that any FQDN aliases it provisions in Content Hosting Configurations matching these additional domains resolve to the canonical name of the 5GMSd AS in the target 5GMS System.

The 5GMSd Application Provider shall use the HTTP POST method to create a new Server Certificate. Upon successful creation of the resource, the 5GMSd AF shall respond with a 201 (Created) response message and the URL of the resource, including its resource identifier, shall be returned in the HTTP Location header. The Content‑Type response header and the body of the HTTP response message shall be as specified in clause 7.3.3.1.

If the procedure is not successful, the 5GMSd AF shall provide a response code as defined in clause 6.3.

#### 4.3.6.4 Retrieve Server Certificate

This procedure is used by the 5GMSd Application Provider to download a Server Certificate resource for inspection. The HTTP GET method shall be used for this purpose. If the requested resource exists and is populated with an X.509 certificate [8], the 5GMSd AF shall respond with 200 (OK) and shall return the requested Server Certificate in accordance with clause 7.3.3.2.

In the case where the X.509 certificate was provisioned by the 5GMSd System on behalf of the 5GMSd Application Provider according to clause 4.3.6.2 above, the HTTP response 503 (Service Unavailable) shall be returned until such time as the X.509 certificate is generated and available for download. The optional HTTP response header Retry-After should be included in such a response, indicating when the certificate is expected to become available for inspection and use.

In cases where the X.509 certificate is to be generated by the 5GMSd Application Provider from a Certificate Signing Request obtained according to clause 4.3.6.3 above, the HTTP response 204 (No Content) shall be returned until such time as the X.509 certificate has been uploaded using the procedure specified in clause 4.3.6.5 below.

#### 4.3.6.5 Upload Server Certificate

This procedure is used by a 5GMSd Application Provider to upload an X.509 certificate [8] that it has generated in response to a Certificate Signing Request solicited using the reservation procedure specified in clause 4.3.6.3 above. The HTTP PUT method shall be used for this purpose. The Content‑Type request header and the body of the HTTP request message shall be as specified in clause 7.3.3.2.

the 5GMSd AF shall verify that the party originating the upload is the same party that reserved the Server Certificate resource using the procedure specified in clause 4.3.6.3 above before accepting the supplied X.509 certificate. The 5GMSd AF shall also verify that the X.509 certificate uploaded corresponds to the Certificate Signing Request it issued for the Server Certificate resource in question. If there is a mismatch on either count, the HTTP response 403 (Forbidden) shall be returned.

Attempting to upload an X.509 certificate to a Server Certificate resource that has not been reserved shall elicit a 404 (Not Found) HTTP response.

When the Server Certificate resource is subsequently referenced by a Content Hosting Configuration in the scope of the same Provisioning Session, the 5GMS Application Provider shall set the domainNameAlias property of all distribution configurations to a Fully-Qualified Domain Name (FQDN) that matches one of the Subject Alternative Names in the referenced Server Certificate resource.

NOTE 2: Even if multiple distribution configurations in the same Content Hosting Configuration reference the same Server Certificate resource, they may each choose a different matching domain name alias.

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

#### 7.6.3.1 ContentHostingConfiguration resource

The data model for the ContentHostingConfiguration resource is specified in table 7.6.3.1-1 below:

Table 7.6.3.1-1: Definition of ContentHostingConfiguration resource

| Property name | Data Type | Cardinality | Description |
| --- | --- | --- | --- |
| name | String | 1..1 | A name for this Content Hosting Configuration. |
| ingestConfiguration | Object | 1..1 | Describes the 5GMSd Application Provider's origin server from which media resources will be ingested via interface M2d. |
|  pull | Boolean | 1..1 | Indicates whether to the 5GMSd AS shall use Pull or Push for ingesting the content. |
|  protocol | Uri | 1..1 | A fully-qualified term identifier allocated in the name space urn:3gpp:5gms:content-protocol that identifies the content ingest protocol.The set of supported protocols is defined in clause 8. |
|  baseURL | AbsoluteUrl | 0..1 | A base URL (i.e. one that includes a scheme, authority and, optionally, path segments) from which content is ingested at reference point M2d for this ingest configuration.In the case of Pull-based content ingest (pull flag is set to True), the base URL shall be provided to the 5GMSd AF to indicate the location from which content is to be pulled for this Content Hosting Configuration. A request received at reference point M4d is mapped by the 5GMSd AS to a URL at reference point M2d whose base is the value of this property.In the case of Push-based content ingest (pull flag is set to False), this property is populated by the 5GMSd AF and returned to the 5GMSd Application Provider to indicate the base URL to which content for this Content Hosting Configuration is to be published. |
| distributionConfigurations | Array(Object) | 1..1 | Specifies the distribution method and configuration for the ingested content.More than one distribution may be configured for the ingested content, e.g. to offer different distribution configurations such as DASH and HLS. |
|  entryPoint | M1‌Media‌Entry‌Point | 0..1 | The Media Entry Point when this distribution configuration is used to describe a single content item.Omitted when this distribution configuration describes multiple content items. |
|  relativePath | RelativeUrl | 1..1 | A relative path (i.e. without a scheme or any leading forward slash characters) to the resource for the Media Entry Point. The semantics are dependent on the value of ingestConfiguration.protocol, as specified in clause 8.The path shall be valid at reference point M2d when appended to the ingest base URL and at reference point M4d when appended to the distribution base URL. |
|  contentType | String | 1..1 | The MIME content type of the Media Entry Point.Used by the 5GMS Client to select a distribution configuration. |
|  profiles | Array(Uri) | 0..1 | An optional list of conformance profile identifiers associated with the Media Entry Point, each one expressed as a URI. A profile URI may indicate an interoperability point, for example.Used by the 5GMS Client to select a distribution configuration.If present, the array shall contain at least one item. |
|  contentPreparationTemplateId | ResourceId | 0..1 | Indicates that content preparation prior to distribution is requested by the 5GMSd Application Provider. It identifies the Content Preparation Template that shall be used as defined in clause 7.4. |
|  edgeResources‌ConfigurationId | ResourceId | 0..1 | When present, the 5GMSd AS supporting this content distribution shall be deployed as a set of one or more EAS instances. |
|  supplementary‌Distribution‌Networks | Array(<Distribution‌NetworkType, DistributionMode> | 0..1 | Specifies that the content for this distribution configuration is to be distributed via one of more supplementary networks. Each member of the array is a duple mapping a type of distribution network to a mode of distribution.The same DistributionNetworkType value shall appear at most once in the array. |
|  canonicalDomainName | String | 0..1 | All resources of the current distribution shall be accessible through this default Fully Qualified Domain Name assigned by the 5GMSd AF.If the certificateId property is also present, in this distribution configuration, the canonical domain name nominated by the 5GMSd AF shall match the CN field in the referenced Server Certificate resource and should also match its first subjectAltName extension field, allowing for wildcard matching in both cases. |
|  domainNameAlias | String | 0..1 | The 5GMSd Application Provider may assign another Fully-Qualified Domain Name (FQDN) through which media resources within the scope of this distribution configuration are additionally accessible from the 5GMSd AS at reference point M4d.This domain name is used by the 5GMSd AS to set appropriate CORS HTTP response headers at reference point M4d.If this property is present, the 5GMSd Application Provider is responsible for providing in the DNS a CNAME record that resolves domainNameAlias to canonicalDomainName.If the certificateId property is also present in this distribution configuration, the provided domain name alias shall match one of the subjectAltName extension fields in the referenced Server Certificate resource, allowing for wildcard matching. |
|  baseURL | AbsoluteUrl | 0..1 | A base URL (i.e. one that includes a scheme, authority and, optionally, path segments) from which content is made available to 5GMS Clients at reference point M4d for this distribution configuration.The value is chosen by the 5GMSd AF when the Content Hosting Configuration is provisioned. It is an error for the 5GMSd Application Provider to set this. |
|  pathRewriteRules | Array(Object) | 0..1 | An ordered list of rules for rewriting the request URL paths of media resource requests handled by the 5GMSd AS.If multiple rules match a particular resource’s path, only the first matching rule, in order of appearance in this array, shall be applied. |
|  requestPathPattern | String | 1..1 | A regular expression [5] against which the path part of each 5GMSd AS request URL, including the leading "/", and up to and including the final "/", shall be compared. (Any leaf path element following the final "/" shall be excluded from this comparison.)In the case of Pull-based ingest, the M4d download request path is used in the comparison.In the case of Push-based ingest, the M2d upload request path is used in the comparison.In either case, if the request path matches this pattern, the path mapping specified in the corresponding mappedPath shall be applied. |
|  mappedPath | String | 1..1 | A replacement for the portion of the 5GMSd AS request path that matches requestPathPattern.In the case of Pull-based ingest, ingestConfiguration.entryPoint is concatenated with the mapped path and any leaf path element from the original M4d download request to form the M2d origin request URL.In the case of Push-based ingest, canonicalDomainName (and, optionally, domainNameAlias) are concatenated with the mapped path and any leaf path element from the original M2d upload request to form the distribution URL(s) exposed over M4d. |
|  cachingConfigurations | Array(Object) | 0..1 | Defines a configuration of the 5GMSd AS cache for a matching subset of media resources ingested in relation to this Content Hosting Configuration. |
|  urlPatternFilter | String | 1..1 | A pattern that will be used to match media resource URLs to determine whether a given media resource is eligible for caching by the 5GMSd AS. The format of the pattern shall be a regular expression as specified in [5]. |
|  cachingDirectives | Object | 1..1 | If a urlPatternFilter applies to a resource, then the provided cachingDirectives shall be applied by the 5GMSd AS at M4d, potentially overwriting any origin caching directives ingested at M2d. |
|  statusCodeFilters | Array(Integer) | 0..1 | The set of HTTP origin response status codes to which these cachingDirectives apply. The filter shall be provided as a regular expression as specified in [5].If the list is empty, the CachingDirectives shall apply to all HTTP origin response status codes at M2d. |
|  noCache | Boolean | 1..1 | If set to True, this indicates that the media resources matching the filters shall not be cached by the 5GMSd AS and shall be marked as not to be cached when served by the 5GMSd AS at M4d. |
|  maxAge | Integer | 0..1 | The caching time-to-live period that shall be set on ingested media resources matching the filters. This determines the minimum period for which the 5GMSd AS shall cache matching media resources as well as the time-to-live period signalled by the 5GMSd AS at interface M4d when it serves such media resources.The time-to-live for a given media resource shall be calculated relative to the time it was ingested. |
|  geoFencing | Object | 0..N | Limit access to the content to the indicated geographic areas. |
|  locatorType | Uri | 1..1 | The type of the locators shall be indicated using a fully-qualified term identifier URI from the controlled vocabulary urn:3gpp:5gms:‌locator‑type, as specified in clause 7.6.4.6, or else from a vendor-specific vocabulary. |
|  locators | Array(String) | 1..1 | Array of locators from which access to the resources is to be allowed. The format of the locator strings shall be determined by the value of locatorType, as specified in clause 7.6.4.6. |
|  urlSignature | Object | 0..1 | Defines the URL signing scheme. Only correctly signed and valid URLs will be allowed to access the content resource at M4d. |
|  urlPattern | String | 1..1 | A pattern that shall be used by the 5GMSd AS to match M4d media resource URLs. The 5GMSd AS shall not serve a matching media resource at M4d unless it includes a valid authentication token calculated over the portion of the M4d request URL that matches this pattern. The format of the pattern shall be a regular expression as specified in [5]. |
|  tokenName | String | 1..1 | The name of the M4d request query parameter that the Media Player should use to present the authentication token when required to do so. |
|  passphraseName | String | 1..1 | The name of the query parameter that is used to refer to the passphrase when constructing the authentication token.Note that the token is not included in the cleartext part of the M4d URL query component. |
|  passphrase | String | 1..1 | The shared secret between the 5GMSd Application Provider and the 5GMSd AS for this distributionConfiguration.The passphrase is used in the computation and verification of the M4d authentication token but is never sent in-the-clear over that interface. |
|  tokenExpiryName | String | 1..1 | The name of the M4d request query parameter that the Media Player should use to present the token expiry field. |
|  useIPAddress | Boolean | 1..1 | If set to True, the IP address of the UE is included in the computation of the authentication token for resources that match urlPattern and access to matching media resources shall be allowed by the 5GMSd AF only when the M4d request is made from a UE with this IP address. |
|  ipAddressName | String | 0..1 | The name of the M4d request query parameter that is encoded as part of the authentication token if the useIPAddress flag is set to True.Note that the IP address is not passed in the cleartext part of the M4d URL query component. |
|  certificateId | ResourceId | 0..1 | When content is distributed using TLS [16], the X.509 [8] certificate for the origin domain is shared with the 5GMSd AF so that it can be presented by the 5GMSd AS in the TLS handshake at reference point M4d. This attribute indicates the identifier of the certificate to use. |

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

Annex X (Informative):
5GMS AS Certificate provisioning and discovery

# X.1 General

This annex describes 5GMS AS discovery by the 5GMS Client, including aspects of the discovery system provisioning. Clause X.2 describes the discovery procedure, leveraging the Domain Name System (DNS).

# X.2 5GMS AS discovery and media streaming access with a Server Certificate created by the 5GMS System

Figure X.2-1 illustrates the initial provisioning needed to allow discovery of a 5GMS AS by the 5GMS Client as well as the eventual 5GMS AS discovery sequence using the Domain Name System (DNS). Specific focus here is on the provisioning and usage of TLS Certificates. The desired outcome is that the 5GMS Client is satisfied that it has established a TLS connection with an authorized 5GMS AS instance.

Here, the *Server Certificate Create* procedure (see clause 4.3.6.2) is used to request that the 5GMS AF creates the server certificate resource. In this case, the certificate's Common Name (CN) is assigned in a domain under the control of the 5GMS System operator (i.e., the 5GMS System operator is the legitimate owner of the domain name). The 5GMS System operator may use a third-party DNS service to host the domain in question.

For example, the 5GMS System operator uses the full canonicalDomainName value <canonicalAsHostname>.‌<5GMS\_Operator>.‌net as the Common Name in the Server Certificate. The 5GMS AF embeds this host name in the distribution base URL it returns to the 5GMS Application Provider.

Table X.2‑1: Example Content Hosting Configuration corresponding to
Create Server Certificate procedure

|  |  |
| --- | --- |
| Content Hosting Configuration property | Example value |
| distributionConfigurations[n] |  |
|  canonicalDomainName | <canonicalAsHostname>.<5GMS\_Operator>.net |
|  domainNameAlias | Not present. |
|  baseURL | https://<canonicalAsHostname>.<5GMS\_Operator>.net/<af-nominated-base-path> |
|  certificateId | Pointing to Server Certificate resource with:- CN = <canonicalAsHostname>.<5GMS\_Operator>.net- subjectAltName[0] = <canonicalAsHostname>.<5GMS\_Operator>.net |

The 5GMS System operator may instead use the wildcarded domain name \*.<5GMS\_Operator>.net as the Common Name of the Server Certificate, in which case the 5GMS AF assigns a canonical host name for the 5GMS AS in this domain and embeds this in the distribution base URL it returns to the 5GMS Application Provider.

The Media Entry Point URL advertised via reference point M5 or M8 (used by the Media Player to access the content in the 5GMS AS at reference point M4) is then:

https://<uniqueHostname>.<5GMS\_Operator>.net/<af-nominated-base-path>/<relativePath>



Figure X.2-1: 5GMS AS discovery using DNS using 5GMS System created server certificates

At application service deployment time:

1. The 5GMS Application Provider creates a Provisioning Session using the procedure specified in clause 4.3.2.2. The 5GMS AF provides the Provisioning Session Id in its response to the 5GMS Application Provider.

2. The 5GMS Application Provider creates a Content Hosting Configuration using the procedure specified in clause 4.3.3.2. The 5GMS AF assigns a canonical domain name (distributionConfigurations.‌canonical‌Domain‌Name) which it includes in its respose to the 5GMS Application Provider.

3. The 5GMS Application Provider requests that the 5GMS AF creates a Server Certificate for this Provisioning Session using the procedure specified in clause 4.3.6.2 and the assigned cannonical domain name. The CertificateId is provided to the 5GMS Application Provider upon success.

4. The 5GMS Application Provider updates the Content Hosting Configuration using the procedure specified in clause 4.3.3.4, adding the Certificate Identifier of the newly created Server Certificate resource (i.e., modifying the value of distributionConfigurations.certificateId).

 Using configuration procedures at reference point M3 that are outside the scope of the present release, the 5GMS AF provisions the 5GMS AS with relevant information from the Provisioning Session, including the Server Certificate and Content Hosting Configuration.

5: If it has not already done so, the 5GMS AF provisions A and/or AAAA records in the DNS service mapping the canonical domain name of the 5GMS AS instance to its assigned IP address(es).

NOTE: The DNS service may be provided by a third-party service provider under the direction of the 5GMS System operator.

At application installation by a user at a UE:

6. A user triggers the download and installation of the 5GMS-Aware Application on a device. With the installation, a list of URLs (API endpoint addresses) for interacting with the 5GMS AF and AS is provided.

When content is selected :

7. When Service Access Information retrieval at reference point M5 is used (see clause 4.7.2.3), the 5GMS Client in the UE retrieves the Service Access Information. This may include media entry point URLs within the streamAccess.entryPoints array. Otherwise, the 5GMS-Aware Application obtains this information via reference point M8.

8. The 5GMS Client in the UE selects one of the offered Media Entry Point URLs corresponding to the its media stream handling capabilities.

9. The 5GMS Client extracts the Fully-Qualified Domain Name (FQDN) from the chosen media entry point URL and uses the DNS service to resolve its IP address.

10. When establishing the TLS connection to the 5GMS AS at reference point M4, the Media Stream Handler in the UE cites the FQDN of the media entry point URL in the Server Name Indication (SNI) field of the TLS Client Hello message. The 5GMS AS uses the value of the SNI field to look up the corresponding Server Certificate and returns it to the Media Stream Handler in its Server Hello response. If the Server Certificate was provisioned with a wildcard Common Name, appropriate matching rules are followed by the 5GMS AS to identify the correct Server Certificate to present to the Media Stream Handler.

11. The 5GMS Client validates the Server Certificate, including whether the value of the Common Name (or one of its Subject Alternative Names) matches the FQDN of the chosen Media Entry Point URL.

When all server certificate validation steps are successfully passed, the following steps are executed:

12. The 5GMS Client requests the resource identified by the media entry point URL using e.g. HTTP GET over the TLS connection established with the 5GMS AS at reference point M4.

# X.3 5GMS AS discovery and service access with a Server Certificate owned by the 5GMS Application Provider

Figure X.3-1 illustrates the initial provisioning needed to allow discovery of a 5GMS AS by the 5GMS Client as well as the eventual 5GMS AS discovery sequence using the Domain Name System (DNS). Specific focus here is on the provisioning and usage of TLS Certificates. The desired outcome is that the 5GMS Client is satisfied that it has established a TLS connection with an authorized 5GMS AS instance.

Here, the *Reserve Server Certificate* (see clause X) and *Upload Server Certificate* (see clause X) proceduresare used for creating the Server Certificate resource and for subsequently providing it to the 5GMS AF. In this case, the certificate’s Common Name (CN) is assigned in a domain under the control of the 5GMS Application Provider (i.e., Application Provider is the legitimate owner of the domain name). The 5GMS Application Provider may use the 5GMS System operator or any third party DNS service to host the domain in question.

For example, the 5GMS Application Provider wishes to use the alias <aliasHostname>.<AppProvider>.com to access content through the 5GMS AS and it includes its chosen host name as a parameter to the *Reserve Server Certificate* operation. In response, the 5GMS AF generates a Certificate Signing Request (CSR) which it returns to the 5GMS Application Provider. The 5GMS AF assigns a canonical host name for the 5GMS AS in a domain under its control. The 5GMS AF embeds the alias in the Fully-Qualified Domain Name in the distribution base URL of the Content Hosting Configuration it returns to the 5GMS Application Provider.

Table X.3‑1: Example Content Hosting Configuration corresponding to
Reserve/Upload Server Certificate procedure

|  |  |
| --- | --- |
| Content Hosting Configuration property | Example value |
| distributionConfigurations[n] |  |
|  canonicalDomainName | <canonicalAsHostname>.<5GMS\_Operator>.net |
|  domainNameAlias | <aliasHostname>.<AppProvider>.com |
|  baseURL | https://<aliasHostname>.<AppProvider>.com/<af-nominated-base-path> |
|  certificateId | Pointing to Server Certificate resource with:- CN = <canonicalAsHostname>.<5GMS\_Operator>.net- subjectAltName[0] = <canonicalAsHostname>.<5GMS\_Operator>.net- subjectAltName[1] = <aliasHostname>.<AppProvider>.com |

The 5GMS Application Provider additionally configures the 5GMS AF-nominated distributionConfigurations[n].‌canonical‌DomainName as a CNAME record for its chosen 5GMS AS domain name alias in its preferred DNS service.

Listing X.3-1: Example DNS CNAME record to support distribution configuration in table X.3‑1

|  |
| --- |
| <aliasHostname>.<AppProvider>.com. CNAME <canonicalAsHostname>.<5GMS\_Operator>.net |

The Media Entry Point URL advertised via reference point M5 or M8 (used by the Media Player to access the content <relativePath> at reference point M4) is then:

https://<aliasHostname>.<AppProvider>.com/<af-nominated-base-path>/<relativePath>



Figure X.3-1: 5GMS AS discovery using DNS using uploaded Server Certificates

At application service deployment time:

1. The 5GMS Application Provider creates a Provisioning Session using the procedure specified in clause 4.3.2.2. The 5GMS AF provides the Provisioning Session Id in its response to the 5GMS Application Provider.

2. The 5GMS Application Provider creates a CSR using the *Reserve Server Certificate* procedure of this Provisioning Session using the procedure specified in clause 4.3.6.3. The 5GMS Application Provider provides its Common Name and optionally Server Alternative Names (SAN) as input. The CSR and the CertificateId are provided upon success in the response.

3. The 5GMS Application Provider uses the CSR for obtaining the Server Certificate from its prefered Certificate Authority.

4. The Application Provider uses the Upload Server Certificate procedure (see clause 4.3.6.5) to upload the received Server Certificate.

5. The 5GMS Application Provider creates the Content Hosting Configuration using the procedure specified in clause 4.3.3.2, adding the Domain Name Alias distributionConfigurations.domainNameAlias and CertificateId of the uploaded Server Certificate (distributionConfigurations.certificateId). The 5GMS AF assigns a cannonical domain name (distributionConfigurations.canonicalDomainName) and provides its with the response.

 Using configuration procedures at reference point M3 that are outside the scope of the present release, the 5GMS AF provisions the 5GMS AS with relevant information from the Provisioning Session, including the Server Certificate and Content Hosting Configuration.

6: If it has not already done so, the 5GMS AF provisions A and/or AAAA records in the DNS service mapping the canonical name of the 5GMS AS instance to its assigned IP address(es).

NOTE 1: The DNS service may be provided by a third-party service provider under the direction of the 5GMS System operator.

7. The 5GMS Application Provider provisions DNS with the CNAME record mapping its chosen host name alias to the canonical name of the 5GMS AS instance.

NOTE 2: The 5GMS Application Provider may leverage the DNS of the 5GMS System.

At application installation by a user at a UE:

8. A user triggers the download and installation of the 5GMS aware Application on a device. With the installation, a list of URLs (API endpoint addresses) for interacting with the 5GMS AF and 5GMS AS is provided.

When content is selected:

9. When Service Access Information retrieval at reference point M5 is used (see clause 4.7.2.3), the 5GMS Client in the UE retrieves the Service Access Information. This may include media entry point URLs within the streamAccess.entryPoints array. Otherwise, the 5GMS-Aware Application obtains this information via reference point M8.

10. The 5GMS Client in the UE selects one of the offered Media Entry Point URLs corresponding to the its media stream handling capabilities.

11. The 5GMS Client extracts the Fully-Qualified Domain Name (FQDN) from the chosen Media Entry Point URL and uses the DNS service to resolve its IP address, first resolving the domain name alias to the canonical domain name using the 5GMS Application Provider’s nominated DNS service, and then resolving the canonical domain name to the IP address(es) using the 5GMS System operator’s nominated DNS service.

12. When establishing the TLS connection to the 5GMS AS at reference point M4, the Media Stream Handler in the UE cites the FQDN of the Media Entry Point URL in the Server Name Indication (SNI) field of the TLS Client Hello Message. The 5GMS AS uses the value of the SNI field to look up the corresponding Server Certificate and returns it to the Media Stream Handler in its Server Hello response.

NOTE 3: If the Server Certificate was provisioned with a wildcard Common Name, appropriate matching rules are followed by the 5GMS AS to identify the correct Server Certificate to present to the Media Stream Handler.

13. The 5GMS Client Validates the Server Certificate, including whether the value of the Common Name (or one of its Subject Alternative Names (SAN)) matches the FQDN of the chosen media entry point URL.

When all server certificate validation steps are successfully passed, the following steps are executed

14. The 5GMS Client requests the resource identified by the Media Entry Point URL using e.g. HTTP GET over the TLS connection established with the 5GMS AS at reference point M4.

\*\*\*\* Last Change \*\*\*\*