3GPP TSG-SA4 Meeting #111e *S4-201365*

11th -20th November 2020

|  |
| --- |
| *CR-Form-v11.4* |
|  **CHANGE REQUEST** |
|  |
|  | **26.512** | **CR** |  **0003** | **Rev** | **-** | **Current version:** | **16.0.0** |  |
|  |
| *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 |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  |

|  |
| --- |
| Removal of Editor’s notes in 5GMS3 |
|  |

 |
|  |  |
| ***Source to WG:*** | Huawei, HiSilicon |
| ***Source to TSG:*** | S4 |
|  |  |
| ***Work item code:*** | 5GMS3 |  | ***Date:*** | 2020-11-09 |
|  |  |  |  |  |
| ***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 several ENs need to be resolved.  |
|  |  |
| ***Summary of change:*** | Removal of editor’s notes about the dynamic policy invocation. |
|  |  |
| ***Consequences if not approved:*** | The spec is not complete with unsolved issues as ENs detailed. |
|  |  |
| ***Clauses affected:*** | 2, 4.7.3 |
|  |  |
|  | **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:*** |  |

\* \* \* \* 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 26.501: "5G Media Streaming (5GMS); General description and architecture".

[3] DASH Industry Forum, "Specification of Live Media Ingest"
<https://dashif-documents.azurewebsites.net/Ingest/master/DASH-IF-Ingest.pdf>

[4] 3GPP TS 26.247: "Progressive Download and Dynamic Adaptive Streaming over HTTP (3GP‑DASH)".

[5] Standard ECMA-262, 5.1 Edition, "ECMAScript Language Specification", June 2011.

[6] IETF RFC 6234: "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)".

[7] 3GPP TS 23.003: "Technical Specification Group Core Network and Terminals; Numbering, addressing and identification".

[8] ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005: "Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks".

[9] IETF RFC 7230: "Hypertext-Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[10] IETF RFC 4648: "The Base16, Base32, and Base64 Data Encodings".

[11] IEEE Standard 1003.1, Issue 7: "The Open Group Base Specifications", 2018.
https://pubs.opengroup.org/onlinepubs/9699919799/

[12] 3GPP TS 29.122, "T8 reference point for Northbound APIs"

[13] 3GPP TS 38.321, "NR; Medium Access Control (MAC) protocol specification".

[14] 3GPP TS 36.321, "Evolved Universal Terrestrial Radio Access (E-UTRA); Medium Access Control (MAC) protocol specification".

[15] 3GPP TS 27.007, "AT Command set for User Equipment (UE)".

[16] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3", August 2018.

[17] IETF RFC 7468: "Textual Encodings of PKIX, PKCS, and CMS Structures", April 2015.

[18] ISO 3166‑1: "Codes for the representation of names of countries and their subdivisions — Part 1: Country codes".

[19] ISO 3166‑2: "Codes for the representation of names of countries and their subdivisions — Part 2: Country subdivision code".

[20] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008.

[21] 3GPP TS 29.500, "5G System; Technical Realization of Service Based Architecture; Stage 3"

[22] 3GPP TS 29.501, "5G System; Principles and Guidelines for Services Definition; Stage 3"

[23] OpenAPI: "OpenAPI 3.0.0 Specification", <https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.0.md>.

[24] IETF RFC 7230: "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing".

[25] IETF RFC 7231: "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content".

[26] IETF RFC 7232: "Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests".

[27] IETF RFC 7233: "Hypertext Transfer Protocol (HTTP/1.1): Range Requests".

[28] IETF RFC 7234: "Hypertext Transfer Protocol (HTTP/1.1): Caching".

[29] IETF RFC 7235: "Hypertext Transfer Protocol (HTTP/1.1): Authentication".

[30] IETF RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2".

[31] IETF RFC 7540: "Hypertext Transfer Protocol Version 2 (HTTP/2)"

[32] ISO/IEC 23009-1: "Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats".

[33] 3GPP TS 23.503: "Policy and charging control framework for the 5G System (5GS); Stage 2".

[34] 3GPP TS 29.514: " 5G System; Policy Authorization Service; Stage 3".

[35] 3GPP TS 26.511: "5G Media Streaming (5GMS); Profiles, codecs and formats".

[XX] 3GPP TS 23.501: "System Architecture for the 5G System; Stage 2". \* \* \* \* Second change \* \* \* \*

### 4.7.3 Procedures for dynamic policy invocation

This procedure is used by a Media Session Handler to manage Dynamic Policy Instance resources via the M5d interface. A dynamic policy invocation consists of a Policy Template Id, flow description(s), a 5GMSd Application Service Configuration Id and potentially other parameters, according to TS 26.501 clause 5.7.

A Policy Template Id identifies the desired Policy Template to be applied to an application flow. A Policy Template includes properties such as specific QoS (e.g. background data) or different charging treatments. The 5GMSd AF combines the information from the Policy Template with dynamic information from the Media Session Handler to gather a complete set of parameters to invoke the N33 or N5 API call. The Policy Template may contain for example the AF identifier. Example values for a Policy Template Id are defined in Clause A.2.3.

The flow description allows the identification and classification of the media traffic, such as the packet filter sets specified in Clause 5.7.3 of TS 23.501 [XX].

In order to instantiate a new dynamic policy, the Media Session Handler shall first create a resource for the Dynamic Policy Instance on the 5GMSd AF. When the Media Session Handler needs several dynamic policies, it repeats the step as often as needed.

The Media Session Handler creates a new Dynamic Policy Instance by sending an HTTP POST message to the 5GMSd AF. The body of the HTTP POST message shall include 5GMSd Application Service Configuration Id, the Policy Template Id and the traffic descriptor. The traffic descriptor identifies the actual application flow(s) to be policed according to the Policy Template. If the operation is successful, the 5GMSd AF creates a new resource URL representing the Dynamic Policy Instance. In this case, the 5GMSd AF shall respond to the Media Session Handler with a 201 Created HTTP response message, including the URL for the newly created Dynamic Policy Instance resource as the value of the Location header field.

~~Editor’s Note: At minimum, the N5 and N33 API requires the UE IP Address at time of API invocation. The full Flow Description is an optional element, when more fine-grained traffic flow identification is required. It needs to be studied, how to enable usage of other traffic filtering parameters, such as an application id.~~

When invoking the N5/N33 APIs for dynamic policy invocation, the Application ID can also be used as an alternative traffic filtering parameter instead of the full Flow Description. The 5GMSd AF shall send the HTTP POST message to NEF for provisioning the PFDs to the PFDF for one or more external Application IDs as specified in TS 29.122 [12] Clause 4.4.10.

For N5 APIs invoked, the Application ID may be involved in the Npcf related services to indicate the particular service and PCF may use the Application ID to indicate to the SMF/UPF to perform the application detection as specified in TS 29.514 [34] Clause 4.2.2.2. For N33 APIs invoked, the 5GMSd AF Identifier shall be included in the Nnef related services and NEF shall map the AF Identifier to Application ID as specified in TS 29.122 [12] Clause 4.4.4 and Clause 4.4.13. Then NEF can invoke the N5 APIs with this Application ID associating to corresponding set of PFDs.

NOTE X: PFDF is functionality within NEF.

NOTE Y: It is up to operator configuration whether to use different external application identifiers that require a mapping to application identifiers known at the PFDF. The external application identifier can be the same as the application identifier known at the PFDF.

The Media Session Handler can modify the parameters of an existing Dynamic Policy Instance resource using either the HTTP PUT or PATCH methods, as appropriate to the desired update. When the policy template relates to QoS or a different charging scheme for a dynamic policy, the 5GMSd AF shall trigger the appropriate actions towards other Network Functions like PCF or NEF when all information is set.

The Media Session Handler can destroy a Dynamic Policy Instance resource using the HTTP DELETE method. As a result, the 5GMSd AF shall trigger the appropriate actions towards other Network Functions like PCF or NEF to remove the associated PCC rule.

Editor’s Note: Notification subscription will be added in the next version of the pCR.

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