Source: Samsung Electronics Co. Ltd

**Title: [FS\_MS\_NS\_Ph2] Key Issue on Bootstrapping Application Invocation on a Network Slice**

**Agenda Item: 8.9**

**Document for: Discussion and Agreement**

# **Introduction**

The 5GMS Application Provider performs service provisioning for a 5G Media Streaming session at the 5GMS AF as described in clause 5 of TS 26.501. When 5G Media Streaming session is setup in a Network Slice, and if the UE currently has access to more than one Network Slice, it is unclear how the 5GMS-aware Application and 5GMS Client on the UE discovers the appropriate Network Slice to use for the session.

This contribution provides clarity on the bootstrapping procedure for 5GMS application invocation on the appropriate Network Slice by looking into the 3GPP specification support for 5G network slicing, and the support for the same on Android and IOS UE devices.

# **Network slicing support in 3GPP specifications**

Clause 5.15 of TS 23501 describes the concept of network slicing in 5G. Clause 6.6 of TS 23503 describes the UE Policy information. As part of this policy information, specified is UE Route Selection Policy information which contains information about Traffic Descriptors and a list of Route Selection Descriptors associated with those traffic descriptors. The traffic descriptors specify components using which traffic can be identified/classified. The Route Selection Descriptor specifies details about route selection for the identified traffic. Table 6.6.2.1-2 of TS 23503 includes the following traffic descriptors:

**Table 1: Traffic descriptor details as part of URSP rules specified in TS 23503**

|  |  |
| --- | --- |
| **Traffic descriptor** | **Description (as specified in TS 23503)** |
| Application descriptors | It consists of OSId and OSAppId(s). (NOTE 2) |
| IP descriptors  (NOTE 5) | Destination IP 3 tuple(s) (IP address or IPv6 network prefix, port number, protocol ID of the protocol above IP). |
| Domain descriptors | FQDN(s) or a regular expression which are used as a domain name matching criteria (NOTE 6). |
| Non-IP descriptors  (NOTE 5) | Descriptor(s) for destination information of non-IP traffic |
| DNN | This is matched against the DNN information provided by the application. |
| Connection Capabilities | This is matched against the information provided by a UE application when it requests a network connection with certain capabilities. (NOTE 4) |
| NOTE 2: The information is used to identify the Application(s) that is(are) running on the UE's OS. The OSId does not include an OS version number. The OSAppId does not include a version number for the application.  NOTE 4: The format and some values of Connection Capabilities, e.g. "ims", "mms", "internet", etc., are defined in TS 24.526 [19]. More than one connection capabilities value can be provided.  NOTE 5: A URSP rule cannot contain the combination of the Traffic descriptor components IP descriptors and Non-IP descriptors.  NOTE 6: The match of this traffic descriptor does not require successful DNS resolution of the FQDN provided by the UE Application. | |

Table 6.6.2.1-3 describes route selection components such as the following:

**Table 2: Route selection components for a given traffic descriptor as part of URSP rules specified in TS 23503**

|  |  |
| --- | --- |
| **Route selection components** | **Description (as specified in TS 23503)** |
| SSC Mode Selection | One single value of SSC mode.  (NOTE 5) |
| Network Slice Selection | Either a single value or a list of values of S-NSSAI(s). |
| DNN Selection | Either a single value or a list of values of DNN(s). |
| PDU Session Type Selection | One single value of PDU Session Type |
| Non-Seamless Offload indication | Indicates if the traffic of the matching application is to be offloaded to non-3GPP access outside of a PDU Session. |
| ProSe Layer-3 UE-to-Network Relay Offload indication | Indicates if the traffic of the matching application is to be sent via a ProSe Layer-3 UE-to-Network Relay outside of a PDU session. |
| Access Type preference | Indicates the preferred Access Type (3GPP or non-3GPP or Multi-Access) when the UE establishes a PDU Session for the matching application. |
| PDU Session Pair ID | An indication shared by redundant PDU Sessions as described in clause 5.33.2.1 of TS 23.501 [2]. |
| RSN | The RSN as described in clause 5.33.2.1 of TS 23.501 [2]. |
| NOTE 2: At least one of the route selection components shall be present.  NOTE 3: When the Subscription Information contains only one S-NSSAI in UDR, the PCF needs not provision the UE with S-NSSAI in the Network Slice Selection information. The "match all" URSP rule has one S-NSSAI at most.  NOTE 4: If this indication is present in a Route Selection Descriptor, no other components shall be included in the Route Selection Descriptor.  NOTE 5: The SSC Mode 3 shall only be used when the PDU Session Type is IP. | |

When the UE receives information in Table 1 and Table 2 of this contribution in URSP rules, the UE uses traffic detection rules in Table 1 to identify traffic, and depending on the precedence information of different route selection descriptors specified for a given traffic descriptor, applies the route selection component with highest precedence for the identified traffic.

For network slice selection, the ‘Network Slice Selection’ route selection component is useful. Theoretically, a Network Slice can be selected for routing traffic that is identified using any of the traffic descriptor components specified in Table 1. This means, for a 5G Media Streaming application on the UE, a Network Slice can be selected for routing traffic of this application if any of the traffic descriptor components can be specified that matches the application.

Among the different traffic descriptors, of interest in this contribution are the following traffic descriptor component types specified in Table 5.2.1 of TS 24526.

**Table 3: Traffic descriptors as specified in Table 5.2.1 of TS 24526**

|  |
| --- |
| ..  ..  Traffic descriptor (octets v+5 to w)  The traffic descriptor field is of variable size and contains a variable number (at least one) of traffic descriptor components. Each traffic descriptor component shall be encoded as a sequence of one octet traffic descriptor component type identifier and a traffic descriptor component value field. The traffic descriptor component type identifier shall be transmitted first.  Traffic descriptor component type identifier  Bits 8 7 6 5 4 3 2 1  0 0 0 0 0 0 0 1 Match-all type 0 0 0 0 1 0 0 0 OS Id + OS App Id type (NOTE 1)(NOTE 3) 0 0 0 1 0 0 0 0 IPv4 remote address type 0 0 1 0 0 0 0 1 IPv6 remote address/prefix length type ..  0 1 1 1 0 0 0 0 Type of service/traffic class type ..  1 0 1 0 0 0 0 0 OS App Id type (NOTE 3)  ..  ..  For "OS Id + OS App Id type", the traffic descriptor component value field shall be encoded as a sequence of a sixteen octet OS Id field, a one octet OS App Id length field, and an OS App Id field. The OS Id field shall be transmitted first. The OS Id field contains a Universally Unique Identifier (UUID) as specified in IETF RFC 4122 [16].  ..  For "type of service/traffic class type", the traffic descriptor component value field shall be encoded as a sequence of a one octet type-of-service/traffic class field and a one octet type-of-service/traffic class mask field. The type-of-service/traffic class field shall be transmitted first.  ..  For "OS App Id type", the traffic descriptor component value field shall be encoded as a one octet OS App Id length field and an OS App Id field.  .. |

# **Network slicing support in Android**

As stated in [1], starting Android 12, “Android provides support for 5G network slicing, the use of network virtualization to divide single network connections into multiple distinct virtual connections that provide different amounts of resources to different types of traffic”.

“Android 12 introduces the following enterprise network slicing capabilities; which network operators can provide to their enterprise clients:

* *Enterprise device slicing for fully-managed devices*: For enterprises who provide [fully managed](https://developers.google.com/android/work/requirements/fully-managed-device) company devices to their employees, network providers can provide them with one or more active enterprise network slices where traffic on the company devices are routed to. From Android 12, Android allows carriers to provide enterprise slices through URSP rules, instead of setting up slices through APNs.
* *Enterprise business app slicing for devices with work profiles*: For enterprises using the [work profile](https://developers.google.com/android/work/requirements/work-profile) solution, Android 12 allows devices to route the traffic from all apps in the work profile to an enterprise network slice. Enterprises can enable this capability through a [Device Policy Controller (DPC)](https://developer.android.com/work/dpc/build-dpc#create_profile).

The work profile solution provides an automatic level of authentication and access control that enterprises require to ensure that only traffic from enterprise apps in the work profile are routed to the enterprise network slice. *Apps in the work profile don't need to be modified to explicitly request the enterprise network slice*.”

To support network slicing in Android, Android telephony and connectivity platform

* provides telephony APIs to support slicing based on 5G slicing capabilities in the modem
* converts requests for slice categories into “traffic descriptors” which are then passed to the modem for URSP traffic matching and route selection
* route traffic from all apps to the corresponding connection

From [1], a network operator, based on negotiation with the enterprise clients, sets up one or more Network Slices. Enterprise devices that are fully managed can access the Network Slices set up for the enterprise. Alternatively, for devices setup with a work profile, Android enables use of above Network Slices for apps in the work profile. The apps in the personal profile continue to use the default network slice (e.g., eMBB).

To enable 5G slicing on devices setup with a work profile, enterprise admins enable work profile app traffic routing to the enterprise network slice on a per-employee basis using the Android DevicePolicyManager (DPM) API.

Following are the slice categories supported by different Android versions:

* Slice categories supported by Android 12 and higher: “ENTERPRISE”
* Slice categories supported by Android 13 and higher: “ENTERPRISE”, “ENTERPRISE 2”, “ENTERPRISE 3”, “ENTERPRISE 4”, “ENTERPRISE 5”, “CBS”, “PRIORITIZE\_LATENCY”, “PRIORITIZE\_BANDWIDTH”

According to [1], for URSP rule construction, carriers use the following Android-specific values for OSId:

|  |  |  |
| --- | --- | --- |
| ID | Value | Description |
| OSId | 97a498e3-fc92-5c94-8986-0333d06e4e47 | The OSId for Android is a version 5 UUID generated with the namespace ISO OID and the name "Android". |

In addition, carriers must configure URSP rules for each slice traffic with the traffic descriptor component as “OS Id + OS App Id” type. For example, the "ENTERPRISE" slice must have a value of 0x97A498E3FC925C9489860333D06E4E470A454E5445525052495345. This value is a concatenation of the OSId, the length of the OSAppId (0x0A), and the OSAppId. The OS App Id for different slice categories according to [1]:



[1] describes example URSP rules for all slice categories. Following is an example URSP rule for ENTERPRISE1 traffic:



[1] describes example URSP rules for all supported slice categories (8).

Management of different profiles in Android is performed separately. For a device with two profiles – personal and work - When applications are installed in Android, they can be either installed in the personal profile, or in the work profile, or in both. When applications have to be installed in both the profiles, the app is installed separately in each of the profiles i.e. they are two different app instances on the device – one in each of the profile. Installation is supported by two different app stores – one in each of the profiles. Therefore, an application invocation is bound to a single profile i.e. a single network context. If, as specified in [1] that *Apps in the work profile don't need to be modified to explicitly request the enterprise network slice*, this means that all apps share the OS App Id because the combination of OS Id + OS App Id has to result to the same network slice selection information in the URSP rules. For this to be possible, Android 12 and higher facilitates apps to request certain Network Slices by allowing them to register with one or more of the given OS App Ids. So, when an app (example MyApp) does a registration with a given App Id (e.g., 0x454E5445525052495345 assigned for “ENTERPRISE” Network Slice), the app MyApp, given appropriate rights, will be able to access the ENTERPRISE Network Slice that the UE has access to. By doing this, all the traffic belonging to MyApp is routed through the ENTERPRISE Network Slice.

[2] and [3] describe enhanced network slicing support with Android 14 where dynamic network slicing is provided to UE applications. With Android 14, end users are able to purchase and activate Network Slices on demand. Users may be able to request enhanced performance for specific times for any application that can use a 5G network slice provisioned by the communication service provider (CSP). Not many details are available for Android 14 support for such a capability.

### Workflow for bootstrapping application invocation to a Network slice

Following is a workflow for bootstrapping an application invocation to a Network Slice:

1. When the application is installed on the UE, it registers with one of the supported OS App Ids of Android[1]. Android device management makes sure that the apps provide the correct OS App Id while installation and/or invocation
2. The UE receives URSP rules as described in TS 23502. The URSP rules have the necessary traffic descriptors with a combination of OS Id + OS App Id
3. When application is started by the end user, application requests access to certain Network Slice connection
4. The request for slice categories is converted to traffic descriptors which is then passed to the modem where URSP matching and route selection takes place.
5. Android telephony and connectivity platform uses the route selection information to route application traffic over the selected Network Slice. All traffic related to the application are routed through the selected network Slice.
6. Once the Network Slice is selected, application can use PDU Sessions in the Network Slice for necessary operations.

# **Network slicing support in IOS**

[4] describes support for 5G network slicing in Apple IOS devices. According to [4]:

“*iOS 17 and iPadOS 17 offer organizations the ability to assign specific network slices to managed apps on their carrier's 5G Standalone (SA) network. This causes all traffic for a designated managed app to be routed to the slice identified by a specified Data Network Name (DNN). The ability to assign network slices is available through the corresponding MDM app installation and settings commands or declarative app configuration. (Declarative app configuration will be available in a future update to iOS 17 and iPadOS 17.) If both Network Slicing and VPN are configured for an app or device, the VPN connection takes precedence over the Network Slice, rendering the Network Slice unused.”*

No further details for support of 5G network slicing in Apple IOS devices is available as of this date.

# **References**

[1] “5G Network Slicing”, Android documentation, <https://source.android.com/docs/core/connect/5g-slicing>

[2] “Ericsson brings on-demand network slicing capability to Android 14 devices”, <https://www.ericsson.com/en/news/2023/7/ericsson-brings-on-demand-network-slicing-capability-to-android-14-devices>

[3] “Nokia introduces on-demand network slicing to boost customer experience”, <https://www.nokia.com/about-us/news/releases/2023/06/15/nokia-introduces-on-demand-network-slicing-to-boost-customer-experience/>

[4] “Apple device support for private 5G and LTE networks”, https://support.apple.com/guide/deployment/support-for-private-5g-and-lte-networks-depac6747317/web

# **Proposal**

We propose following change be adopted into TR 26.941.

**===== 1. CHANGE =====**

## 6.X Key Issue #x: Bootstrapping application invocation on Network Slice

### 6.X.1 Description

#### 6.X.1.1 Discover appropriate Network Slice for 5GMS procedures

Clauses 5 and 6 of TS 26.501 [20] describe the high-level procedures for downlink and uplink media streaming respectively. As part of these procedures, the 5GMS Application Provider performs service provisioning at the 5GMS AF. The 5GMS-Aware Application subsequently receives Service Access Information from the 5GMS Application Provider over reference point M8 or else acquires it directly from the 5GMS AF over reference point M5. If the UE currently has access to more than one Network Slice, it is unclear how the 5GMS-Aware Application and the 5GMS Client on the UE discover the appropriate Network Slice to use to establish a new media streaming session.

Open issues:

- How the bootstrapping of the application invocation on a Network Slice happens before the 5GMS Client performs 5G Media Streaming operations.

#### 6.X.2.1 Candidate solution #1: Bootstrapping based on Traffic Descriptor information

Assumptions:- The 5GMS-Aware Application developer is aware of different OS App Ids supported by the UE operating system.

Figure 6.X.2.1‑1 below illustrates the procedure for bootstrapping application invocation on a Network Slice



Figure 6.X.2.1‑1: Call flow for bootstrapping application invocation on a Network Slice

The steps are as follows:

1. The 5GMS-Aware Application is installed on the UE, and and is programmed to invoke network connection API using pre-defined OS App Id supported by the UE operating system.

2. The 5GMS Application Provider provisions the media streaming session in the 5GMS AF at reference point M1 and the 5GMS Client retrieves Service Access Information from the 5GMS AF at reference point M5.

a. The 5GMS Application Provider provisions 5G Media Streaming at the 5GMS AF with one or more network slices.

b. The 5GMS Client retrieves Service Access Information from the 5GMS AF.

NOTE: Step 2b is performed if the 5GMS-Aware Application did not receive the complete Service Access Information from the 5GMS Application Provider over M8.

3. If the 5GMS AF is in the trusted Data Network, it interacts directly with the PCF, using the Npcf\_PolicyAuthorization service as defined in clause 5.2.5.3 of TS 23.502 [15], to configure the QoS for the media streaming session.

4. Alternatively, if the 5GMS AF is in the external Data Network, it may use the Nnef\_AFsessionWithQoS service as defined in clause 5.2.6.9 of TS 23.502 [15] to configure the QoS for the media streaming session. The NEF may invoke the Npcf\_PolicyAuthorization service on behalf of the 5GMS Application Provider to configure the QoS for the media streaming session.

5. The PCF constructs URSP rules and provisions them in the UE as described in clause 6.6.2.2 of TS 23.503 [16]. The URSP rules consists of traffic descriptors with OS Id and OS App Id components, and corresponding route selection descriptor information with Network Slices to use.

6. Based on OS App Id configured for the 5GMS-Aware Application, the UE operating system enables selection of the appropriate Network Slice using the received traffic descriptor information inside the URSP rules.

NOTE: If multiple network slices are provided for the same traffic descriptor, the precedence information in the route selection descriptor is used to find the appropriate Network Slice.

7. The 5GMS-Aware Application initiaites a media streaming session with the 5GMS Client at reference point M6.

8. The 5GMS Client checks to see if a PDU Session already exists in the selected Network Slice using an OS-specific API. If a PDU Session already exists, 5GMS Client picks the PDU Session for further interaction with media streaming endpoints.

9. Alternatively, if no PDU Session exists in the Network Slice, the 5GMS Client uses an OS-specific API to create a PDU Session using the UE-requested PDU Session establishment procedure specified in clause 4.3.2.2 of TS 23.502 [15]. The UE interacts with the AMF to establish a new PDU Session, passing X as parameters.

10. Once the PDU Session is available, the 5GMS Client interacts with DNS system to resolve the IP address of the 5GMS AF and 5GMS AS instances.

11. The 5GMS Client interacts with the 5GMS AF for media session handling procedures as specified in clause 11 of TS 26.512 [21].

12. The 5GMS Client interacts witht the 5GMS AS for media streaming as specified in clause 10 of TS 26.512 [21].