**SA WG2 Meeting #140e S2-2004848r06**

**Aug 19th – Sept 1st, 2020 ; Elbonia (revision of S2-2004848)**

**Source: Nokia, Nokia Shanghai Bell**

**Title: KI 1: Update to Solution #13**

**Document for: Agreement (P-CR)**

**Agenda Item: 8.3**

**Work Item / Release: FS\_enh\_EC / Rel-17**

*Abstract of the contribution: KI 1: Update to Solution #13*

# 1 Discussion

Update of the solution:

* Explaining the need of the solution: why a 3rd part AF may need to configure 5GC with the sets of FQDN(s) to associate with a (DNN, S-NSSAI)
* Some configuration of URSP upon AF request is already (in R16) possible for 5G VN group data but here the data configuration is not meant for 5G VN group members but to corporate users or users of a specific application that are not meant to only communicate with each other
* Splitting up into 2 alternatives one to configure the URSP and another one for the UE configuration of DNS servers
* Removing EN

# 2 Proposal

**It is proposed to update TR 23.748 as follows**

*FIRST CHANGE*

## 6.13 Solution #13: 5GC support for UE selection of the DNS to use

### 6.13.1 Description

#### 6.13.1.1 Overview

The operator may negotiate with a Third party (typically a Corporate represented by an AF) dedicated DNN(s) and/or S-NSSAI(s) for the traffic of UE(s) of this third party. UE(s) of the third party may be identified by a group identifier.

This solution addresses policies that the third party would want to get enforced for the traffic of UE(s) of this third party including for cases where traffic of UE(s) of this third party is subject to traffic offload.

The applications (FQDN(s)) reached by UE(s) of this third party may correspond to:

1. corporate applications only reachable via a specific (DNN, S-NSSAI) negotiated with the operator ; corresponding URSP rules or usage of DNS server shall only point to this (DNN, S-NSSAI)
2. corporate applications reachable via a general purpose (DNN, S-NSSAI) but only in some DNAI ; e.g. the corporate applications are only accessible when the UE is in some location corresponding to the corporate premises,
3. internet applications not reachable via a specific (DNN, S-NSSAI) negotiated with the operator but only reachable via a general purpose (DNN, S-NSSAI) ; e.g. traffic of UE(s) of this third party targeting Internet applications is not to be sent to a specific (DNN, S-NSSAI) negotiated with the operator as this traffic is not expected to cross the Intranet of the corporate,
4. internet applications reachable via both a specific (DNN, S-NSSAI) negotiated with the operator and via a general purpose (DNN, S-NSSAI) for which the third party may want to set preferences between these 2 kinds of connectivity,
5. etc…

The cases a), b), … above may correspond to different corporate that have different policies.

Some configuration of URSP upon AF request is already (in R16) possible for 5G VN group data but here the data configuration is not meant for 5G VN group members but to corporate users or users of a specific application that are not meant to only communicate with each other

The solution relates to KI 1 and addresses how an AF can provide the 5GC with information about the relative precedence of data (PDU) Sessions (e.g. relative precedence of (DNN, S-NSSAI)) to use to reach different domains (sets of FQDN) possibly depending on the DNAI where traffic of this PDU Session may be offloaded

.

.

The solution relies on:

- 5GC can get from AF information on the domains (set of FQDN(s)) supported on a DN / local access to a DN (DNAI); these domains may be associated with a set of DN priority information. This information may be translated by NEF and is stored in UDR for further possible PCF consumption. This is further described in clause 6.13.2.1; The DN priority information indicates the relative priority (DN priority value) of one or any (DNN, S-NSSAI) for the domains (set of FQDN(s)) indicated by the AF.

The AF can associate the same set of FQDN(s) with different DN priority values for different (DNN, S-NSSAI)

NOTE: this is to cover case d) above where the AF of a corporate would try to configure the following for the UE(s) of this corporate: internet applications are reachable with lower priority via a specific corporate (DNN, S-NSSAI) negotiated with the operator and are reachable with Higher priority via a general purpose (DNN, S-NSSAI) (generic Internet access of the operator),

.

- .

Information on the domains (set of FQDN(s)) supported on a DN / local access to a DN (DNAI) is later on called "DN priorities for appDomains". It consists of a list of rules that each associates a FQDN filter with DN priority information:

- A FQDN filter corresponds to a (possibly set of) FQDN (with possible wildcarding such as such as "\*.example.com") and is associated with a filtering /rule priority.

- one or more set of DN priority information that each may correspond to:

- a (DNN, S-NSSAI). This may be provided by the AF or determined by the NEF based on the AF identity when it is not provided by the AF and the AF provides only one instance of DN priority information.

- a default DN priority value to be used for the FQDN(s) identified by the FQDN filter when DN priority for DNAI is not provided or does not apply.

- a list of DN priority for DNAI that each associate a DN priority value and a DNAI for the FQDN(s) identified by the FQDN filter / rule when the DNAI applies to the PDU Session.

- An optional spatial Validity condition that indicate where the rule is to apply. This may correspond to a geographical area, a list of TAI or a (set of) DNAI

NOTE 3: For example, for a DN related with corporate access, the FQDN(s) corresponding to corporate services can be associated with a higher DN priority value than FQDN(s) for internet-based services (when the corporate also has an access to the Internet thus allowing also access to internet based services). The AF(s) corresponding to different corporate or different services can’t co-ordinate the DN priority values between themselves. The co-ordination between DN priority values set by different AF is done by the PCF as explained in clause 6.13.2.1

This "DN priorities for appDomains" information may be used by 5GC at 2 levels:

1. URSP alternative: to set the Rule Precedence of URSP rules whose Traffic descriptor / Domain descriptor corresponds to such domains (sets of FQDN). The solution uses the existing Rel-16 URSP rules without change for UE perspective. Only change is how the PCF derive the URSP rules based on "DN priorities for AppDomains". UE use URSP for matching a PDU Session, as defined in R16
2. DNS alternative: DNS configuration on the UE i.e. which DNS server a multi Homed UE will consider for a DNS look-up. This alternative is meant for Applications or Browser DNS clients for which USRP would not be applicable;

The solution addresses following Connectivity Models:

- Multiple PDU sessions including some more local PDU Sessions and PDU Sessions to corporate DN: the information on the domains (set of FQDN(s)) supported on a DN may then be received from a third party DN and has to be mapped with operator policies.

- Session Breakout.

#### 6.13.1.2 URSP Alternative

On the UE interface this alternative reuses R16 interface (URSP configured by the PCF) without change for UE perspective. The difference with R16 lies on the fact that the AF API can provide guidance on URSP building

- is not related with 5G VN group,

- allows the AF to provide different rules for the same domains (sets of FQDN(s)) with different DN priority values for different (DNN, S-NSSAI): typically a DN priority value for the (DNN, S-NSSAI) dedicated to the corporate that the AF represents and another DN priority value for any other (DNN, S-NSSAI)

An example of How the DN priority per Appdomain can influence the URSP rule generation in PCF is the following

A corporate wishes for the UE its employees (members of a group for corporate users) that

* They use a specific DNN “My-corporate” when the UE try reach \*.corporate.com.
* They preferably use another DNN for other Internet applications: they can use the specific DNN “My-corporate” but with lower priority
* With the exception that when traffic offload to DNAI xx takes place, the members of a group for corporate users should now use specific DNN “My-corporate” for all applications (this is because in this case a direct and cheaper connectivity to the Internet via the corporate Intranet is used)

The corporate via a NEF API associates following DN priorities for appDomains rules with the Group of corporate users

- domain \*.corporate.com is associated with DNN “My-corporate” with high default priority, and low priority for DNAI xx

- other domains is associated with DNN “My-corporate” with low priority

#### 6.13.1.3 DNS Alternative

A UE that has multiple PDU Sessions will receive multiple DNS server address and needs to know which of these DNS servers it needs to use to translate a target FQDN.

NOTE 1: RFC 6731 [26] specifies how a DHCP server can express preferences and domains for DNS server information it provides to DHCP clients. However, RFC 6731 [26] does not specify how the DHCP server acquires specific knowledge of domains and networks. An administrator may choose to utilize the different preference values, for instance by manual configuration (RFC 6731 [26] clause 3). And 3GPP has not defined whether and how to use RFC 6731 [26] (for example considering Session Breakout and Multiple PDU sessions defined in clause 4.2 of this TR).

NOTE 2: In the case of multiple PDU Sessions for a UE, information on (different) DNS servers that the UE can use are advertised on each of these different PDU Sessions. This currently may use NAS (PCO), RA (Router Advertisement messages), or DHCP to transfer this information to the UE but 3GPP currently does not define how to guide the UE to select the right DNS server (considering e.g. relative priorities).

At PDU Session establishment, the PCF transforms this DN priorities for appDomains information into PDU Session related Policy used by SMF to send DNS configuration information to the UE

The DNS configuration received from the SMF does not provide the trigger to establish PDU sessions but it provides the DNS priorities after/during the PDU session establishment.

The UE uses the DNS information received from the SMF (NAS, DHCP, etc…) to configure its IP stack.

NOTE: whether the EAS information associated with the old DNS configuration needs be cleaned is to be solved as part of KI 2?

The DNS Alternative is specifically meant for a UE that has access to one DNN (one single PDU Session) but is multi-homed (per IPV6 multihoming) or because an UL CL has been inserted to the PDU Session.

### 6.13.2 Procedures

#### 6.13.2.1 Configuring appDomain information on PCF



Figure 6.13.2.1-1: Configuring DN priorities for appDomains information on PCF

1. An Application Function (AF) invokes NEF API (e.g. Nnef\_ServiceParameter API) to communicate DN priorities for appDomains (as defined in clause 6.13.1) to Network Exposure Function (NEF). This information may be associated ("target") with an individual UE or with a group of UE (for example all UE(s) of a corporate) or with any UE.

2. The NEF may translate the AF identity into a target (DNN, S-NSSAI). The NEF stores the information (after possible translation by NEF) including in the UDR (corresponding data set and subset are indicated in step 5).

3. The UDR responds to NEF.

4. The NEF responds to the AF.

5. The PCF may acquire (GET or SUBSCRIBE to notifications on change of) policy data from UDR including the DN priorities for appDomains information.

The PCF(s) that have subscribed to notification on modifications of AF requests (Data Set = Application Data; Data Subset = DN priorities for appDomains, Data Key = S-NSSAI and DNN) receive(s) a Nudr\_DM\_Notify notification of data change from the UDR. Potentially also Internal Group Identifier or SUPI may be used as Data Key if the AF requests "targets" the external identity of an individual UE or a group of UE.

6. the applies this information to determine policies to build URSP or policies related with DNS priority selection in the UE.

The PCF may receive different policies from different AF (e.g. receive policies from a third party AF corresponding a corporate group of users and also apply policies applying to any UE received from different AF(s) managing Edge computing application deployments). The PCF needs to build an unique map of relative priorities between (DNN, S-NSSAI) for a given domain (range of FQDN) (to be sent to the UE as URSP, see § 6.13.2.2 or as DNS priorities see § 6.13.2.3). For this purpose the PCF considers local policies to resolve the potential conflicts, policies that take into account the identity of the AF that has provided a DN priorities for appDomains policy.

#### 6.13.2.2 Usage of DN priorities for appDomains information to configure URSP

1 The UE Registers

2. The AMF selects a PCF and establishes an AM Policy Association with the PCF by invoking Npcf\_AMPolicyControl\_Create operation (providing the IMSI Group of the UE.

 All steps above are as for TS 23.502 [3] clause 4.2.2.2.2 (with no intended changes)

3. If the PCF does not have relevant policy data (e;g; policy data related with for the Group the UE is belonging to), it sends a corresponding request to the UDR by invoking Nudr\_DataRepository\_Query operation. The PCF may also request notifications from the UDR about changes on the corresponding policy information (including DN priorities for appDomains for an IMSI group by invoking Nudr\_DataRepository\_Subscribe.

4. The UDR responds to the PCF with Nudr\_DataRepository\_Query response including DN priorities for appDomains that includes the list specific domains (and networks).

The DN priorities for appDomains information configured on PCF by mechanisms described in the § 6.13.2.2 and recalled above may be used to generate USRP sent to the UE;

#### 6.13.2.3 SMF influence on UE preferences between multiple Recursive DNS Servers

This clause applies to the DNS Alternative.

Figure 6.13.2.3-1 illustrates the SMF influence on UE preferences between multiple Recursive DNS Servers and the delivery of DNS Configuration information to UE as part of PDU Session Establishment procedure (defined in TS 23.502 [3] clause 4.3.2).



Figure 6.13.2.3-1: SMF influence on preferences and domains and networks for multiple Recursive DNS Servers.

1. The UE initiates a UE Requested PDU Session Establishment procedure to a (DNN, S-NSSAI).

2. The AMF selects an SMF and sends Nsmf\_PDUSession\_CreateSMContext Request to SMF.

3. SMF selects a PCF.

4. SMF establishes a SM Policy Association with the PCF by invoking Npcf\_SMPolicyControl\_Create operation providing the (DNN, S-NSSAI) of the PDU Session.

 All steps above are as for TS 23.502 [3] clause 4.3.2.2.1 (with no intended changes)

5. If the PCF does not have policy data for the (DNN, S-NSSAI) of the PDU Session, it sends a corresponding request to the UDR by invoking Nudr\_DataRepository\_Query operation. The PCF may request notifications from the UDR about changes on the corresponding policy information (including DN priorities for appDomains mapping to DNN and S-NSSAI) by invoking Nudr\_DataRepository\_Subscribe.

6. The UDR responds to the PCF with Nudr\_DataRepository\_Query response including DN priorities for appDomains that includes the list specific domains (and networks).

 Steps 5 and 6 may be omitted if the PCF had subscribed to notification of this data change as defined in step 4 of TS 23.502 [3] Figure 4.3.6.2-1or in step 5 of Figure 6.13.2.1-1.

PCF decides on DNS preferences for (DNN, S-NSSAI) using the DN priorities for appDomains information received from UDR but also local policies (see also step 7 and § 6.13.2.1). The output of this decision is called DNS Configuration information. The PCF can then use the DNS Configuration information to provide it to SMF

7. The PCF responds to the SMF with Npcf\_SMPolicyControl\_Create response including DNS Configuration information.

 The PCF is responsible to transform "DN priorities for appDomains" information into "DNS configuration information" to be provided to SMF. “DNS configuration information” has the same format than DN priorities for appDomains" but with DN priority values that have been normalized based on PCF policies as explained below.

For the determination of "DNS configuration information" to be provided to SMF, the PCF may take into account locally configured policies related with (DNN, S-NSSAI)

Editor's note: It is FFS if and how roaming can be supported, e.g. how to support URSP in LBO roaming, or how to support AF influence for traffic routing in HR roaming.

8. SMF communicates the DNS Configuration information in PDU Session Establishment Response by:

- including DNS Configuration information in Extended PCO IE (8.a); or

- when acting as DHCP server by including in DHCP RDNSS option when communicating with UE using DHCP (8.b); or

- in RA (per RFC 8106).

 If PCC does not apply to a PDU Session, the SMF determines locally the DNS Configuration information

If the PCF determines that DNS Configuration information has changed (because e.g. DN priorities for appDomains information has changed) it can provide a new DNS Configuration information as part of a Npcf\_SMPolicyControl\_Update. The SMF may provide the corresponding information to the UE:

- Via NAS PCO sent in a network initiated PDU Session modification procedure; or

- Via Router Advertisement ('RA' per IETF RFC 8106) (in IPv6 case);

- Via DHCP FORCERENEW and DHCP INFORM defined in DHCP reconfigure extension (RFC 3203) that are subject to authentication of DHCP message as defined in RFC 3118 forcing the UE to get again the DNS configuration via DHCP. This alternative may not be supported by the UE in which case the SMF may be unable to transfer an update of DNS Configuration information unless it executes a SSC mode 3 procedure.

### 6.13.3 Impacts on services, entities and interfaces

- NEF: new API information to support and to convert into policy data stored in UDR. This API has commonalities with the API used for 5G VN groups

- UDR: new (policy) data format (DN priorities for appDomains) to manage.

- PCF: retrieve new UDR (policy) data and determine DNS Configuration information to be provided to SMF via PDU Session level policy data.

- SMF: send DNS Configuration information via PCO / DHCP / Router Advertisement to the UE.

- UE: new DNS Configuration information for the PDU Session.

The content of the DNS configuration that is provided to the UE has the same format as the DHCP RDNSS option (when sent in PCO or via the DHCP RDNSS option or as defined in RFC 8106 in IPv6 case) ..

.

*NEXT CHANGE (3)*