(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 April 2021 (15.04.2021)

WIPO | PCT

(10) International Publication Number
WO 2021/069056 A1

(51) International Patent Classification:
H04W 48/18 (2009.01) *H04W 8/18* (2009.01)
H04W 60/00 (2009.01)

(21) International Application Number:
PCT/EP2019/077107

(22) International Filing Date:
07 October 2019 (07.10.2019)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **HUAWEI TECHNOLOGIES CO., LTD.** [CN/CN]; Huawei Administration Building Bantian Longgang District, Shenzhen, Guangdong 518129 (CN).

(72) Inventor; and

(71) Applicant *(for US only)*: **MARY, Sheeba, Backia** [IN/SE]; Huawei Technologies Sweden AB Skalholtsgatan 9, 16440 Kista (SE).

(72) Inventors: **ZHU, Fenqin**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE). **CONSOLI, Antonio**; Huawei Technologies Sweden AB Skalholtsgatan 9, 16440 Kista (SE). **HAMIDIAN, Ali**; Huawei Technologies Sweden AB Skalholtsgatan 9, 16440 Kista (SE).

(74) Agent: **KREUZ, Georg**; Huawei Technologies Duesseldorf GmbH Riesstr. 25, 80992 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

WO 2021/069056 A1

(54) Title: A FIRST NETWORK ENTITY AND A SECOND NETWORK ENTITY FOR ENFORCING NETWORK SLICE POLICY

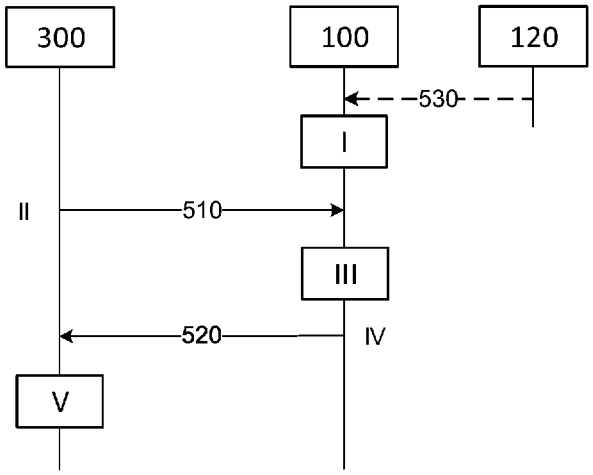

Fig. 7

(57) Abstract: The disclosure relates to provisioning and enforcement of network slice information in a communication network. A first network entity (100) receive a network slice information request, NSIR, (510) from a second network entity (300), wherein the NSIR (510) indicates at least one of a network slice information and/or a client device identity, ID. In response to the reception of the NSIR (510), the first network entity (100) obtains and transmits a network slice information notification, NSIN, (520) to the second network entity (300). The NSIN (520) indicates a network slice control information comprising at least part of the network slice information and a network slice policy information. Furthermore, the disclosure also relates to a client device 600, corresponding methods and a computer program.

[Continued on next page]

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

A FIRST NETWORK ENTITY AND A SECOND NETWORK ENTITY FOR ENFORCING NETWORK SLICE POLICY

Technical Field

The application relates to a first network entity and a second network entity for enforcing network slice policy. Furthermore, the application also relates to a client device, corresponding methods, and a computer program.

Background

Network slicing is one of the key features of 5th generation mobile communication system (5G) networks. 3GPP define a network slice as a logical network that provides specific network capabilities and network characteristics. The network slice can be tailored based on the specific requirements associated with a service level agreement (SLA) agreed between network slice customer (NSC) and network slice provider (NSP). A network slice may span across multiple parts of the network, e.g. terminal, access network, core network and transport network.

The network slice may comprise dedicated and/or shared resources, e.g. in terms of processing power, storage, and bandwidth and may be isolated from the other network slices. The NG.116 GSMA, "Generic Network Slice Template Version 1.0" describes the concept of generic slice template (GST) from which several network slice types descriptions can be derived. Some of the parameters in the GST point explicitly to the definition of parameters and bounds on the service delivered to the end customer.

However, the enforcement of some of these bounds or of some of these parameters is not supported by the 5th generation mobile communication system (5GS) yet.

Summary

An objective of embodiments of the disclosure is to provide a solution which mitigates or solves the drawbacks and problems of conventional solutions.

The above and further objectives are solved by the subject matter of the independent claims. Further advantageous embodiments of the disclosure can be found in the dependent claims.

According to a first aspect of the disclosure, the above mentioned and other objectives are achieved with a first network entity for a communication system, the first network entity being configured to

receive a network slice information request, NSIR, from a second network entity, wherein the NSIR indicates at least one of a network slice information and/or a client device identity, ID;

obtain a network slice information notification, NSIN, in response to the reception of the NSIR, wherein the NSIN indicates a network slice control information; and

transmit the obtained NSIN to the second network entity.

An advantage of the first network entity according to the first aspect is that any network function can request the network slice related policy information containing network slice attributes and related real-time network slice capability from the first network entity to enforce slice limitations as agreed between the network operator and the slice service provider as part of the SLA.

In an implementation form of a first network entity according to the first aspect, the network slice information is at least one of: a network function ID, a network slice instance ID, a network slice type, a network slice subscription type, and a single network slice selection assistance information.

An advantage with this implementation form is that the network slice identification information received by the network service consumers will support in identification of received network slice policy information related to the network slices.

In an implementation form of a first network entity according to the first aspect, the network slice control information comprises at least part of the network slice information, and the network slice control information further comprises a network slice policy information, wherein the network slice policy information indicates at least one of: a network slice status information, slice identification information, a maximum allowed PDU sessions per network slice, a maximum number of allowed client devices per network slice, a maximum uplink data rate supported for a client device, and a maximum downlink data rate supported for a client device.

That the network slice control information comprises at least part of the network slice information can be understood to mean that the network slice control information may comprise a subset of the network slice information indicated in the NSIR.

An advantage with this implementation form is that the network slice identification and corresponding network slice status information provided to the network service consumers will contain the slice availability and unavailability information to support the network service

consumers in efficient slice selection and determination of client device slice configuration information.

In an implementation form of a first network entity according to the first aspect, the network slice status information has any of the attributes: available during a validity period, availability level, permanently not available, or temporarily not available.

An advantage with this implementation form is that the slice availability and unavailability information along with the availability levels indicate to the network service consumers whether a slice can be selected or not for any upcoming service requests to ensure the required service level. The information on unavailability cases such as “permanently not available”, or “temporarily not available”, will prevent the network slice consumers from selecting an unavailable slice and hence a service disruption can be prevented.

In an implementation form of a first network entity according to the first aspect, obtain the NSIN comprises

fetch network slice related policy information from a policy control function, PCF, or a unified data repository, UDR, upon receiving the NSIR from the second network entity.

An advantage with this implementation form is that the network slice related policy information containing all slice attributes and limitation/required bounds, slice capability and status information generated based on analytics can either be stored at the PCF or can be stored in the UDR and fetched by the first network entity, when required to provide network slice related policy information for the network slice consumers for their efficient slice operation and corresponding service provision.

In an implementation form of a first network entity according to the first aspect, the first network entity is further configured to

receive a configuration message from an Operation Administration and Management, OAM, previous to receiving the NSIR from the second network entity, wherein the configuration message indicates a network slice policy.

An advantage with this implementation form is that this helps either the OAM to provide the slice SLA information containing network slice descriptor with slice attributes and their required bounds (maximum/minimum) to the first network entity or these information can be configured by the operator at the first network entity to enforce the slice SLA/policy over the slice operations in the 5G System.

In an implementation form of a first network entity according to the first aspect, the first network entity comprises: a policy control function, PCF, and/or a network data analysis function, NWDAF.

An advantage with this implementation form is that the slice SLA/policy related information can be managed and enforced by the PCF or by the NWDAF in all the service consumers.

According to a second aspect of the disclosure, the above mentioned and other objectives are achieved with a second network entity for a communication system, the second network entity being configured to

send a NSIR to a first network entity, wherein the NSIR indicates least one of a network slice information and/or a client device ID;

receive a NSIN from the first network entity in response to the transmission of the NSIR, wherein the NSIN indicates a network slice control information.

An advantage of the second network entity according to the second aspect is that the first network entity can provide the network slice related policy information containing network slice attributes and related real-time network slice capability from PCF or NWDAF to enforce slice limitations as agreed between the network operator and the slice service provider as part of the SLA.

In an implementation form of a second network entity according to the second aspect, the network slice information is at least one of: a network function ID, a network slice instance ID, a network slice type, a network slice subscription type, and a single network slice selection assistance information.

An advantage with this implementation form is that the network slice identification information provided to the network service consumers will support in identification of received network slice policy information related to the network slices.

In an implementation form of a second network entity according to the second aspect, the received network slice control information comprises at least part of the network slice information, and the network slice control information further comprises a network slice policy information, wherein the network slice policy information indicates at least one of: a network slice status information, slice identification information, a maximum allowed PDU sessions per network slice, a maximum number of allowed client devices per network slice, a maximum

uplink data rate supported for a client device, and a maximum downlink data rate supported for a client device.

That the network slice control information comprises at least part of the network slice information can be understood to mean that the network slice control information may comprise a subset of the network slice information indicated in the NSIR.

An advantage with this implementation form is that the network slice identification and the corresponding network slice status information for the slice attributes (such as maximum allowed PDU sessions per network slice, a maximum number of allowed client devices per network slice, a maximum uplink data rate supported for a client device, and a maximum downlink data rate supported for a client device) received by the network service consumers will contain the slice availability and unavailability information to support the network service consumers in efficient slice selection and determination of client device slice configuration information.

In an implementation form of a second network entity according to the second aspect, the network slice status information has any of the attributes: available during a validity period, availability level, permanently not available, or temporarily not available.

An advantage with this implementation form is that the slice availability and unavailability information along with the availability levels indicate to the network service consumers whether a slice can be selected or not for any upcoming service requests to ensure the required service level. The information on unavailability cases such as “permanently not available”, or “temporarily not available”, will prevent the network slice consumers from selecting an unavailable slice and hence a service disruption can be prevented.

In an implementation form of a second network entity according to the second aspect, the second network entity is an access and mobility management function, AMF, or a network slice selection function, NSSF, and further configured to

determine allowed network slice selection assistance information, NSSAI, based on the received NSIN.

The second network entity may further be configured to select a network slice instance, NSI, based on the received NSIN.

An advantage with this implementation form is that the network service consumers such as AMF and NSSF can use the received network slice status information containing slice attributes and corresponding usage/availability levels to perform various slice operations such as, selection of available slice for service request, determination of allowed NSSAI for client devices and selection of network slice instance to request service provision. The received slice information prevents the network service consumers from selecting and using the unavailable slices, thereby preventing service failure.

In an implementation form of a second network entity according to the second aspect, the second network entity is an AMF or a NSSF, and further configured to

determine a configured NSSAI based on based on the received NSIN.

The second network entity may further be configured to select a NSI based on the received NSIN.

An advantage with this implementation form is that the network service consumers such as AMF and NSSF can use the received network slice status information containing slice attributes and corresponding usage/availability levels to perform various slice operations such as, selection of available slice for service request, determination of configured NSSAI for client devices and selection of network slice instance to request service provision. The received slice information prevents the network service consumers from selecting and using the unavailable slices, thereby preventing service failure.

In an implementation form of a second network entity according to the second aspect, the second network entity is a session management function, SMF, and further configured to

select a user plane function, UPF, for a protocol data unit, PDU, session based on the received NSIN.

An advantage with this implementation form is that the SMF being a network service consumer can use the received network slice status information containing slice attributes and corresponding usage/availability levels to perform UPF selection to establish or modify a client device PDU Session. The received slice information prevents the SMF from selecting and using an unavailable or overloaded UPF slice to prevent PDU Session failure.

According to a third aspect of the disclosure, the above mentioned and other objectives are achieved with a client device for a communication system, the client device being configured to

obtain a first control message indicating a first network slice information;

receive a second control message from a first network entity, wherein the second control message indicates a second network slice information; and

select a network slice for a subsequent service based on the first network slice information and the second network slice information.

An advantage of the client device according to the third aspect is that the first network entity can configure the client device with network slice selection policy (NSSP) containing s-NSSAI(s) determined based on the available slice SLA or slice policy related information (along with slice availability and attribute usage status derived from the analytics provided by the NWDAF). The first network entity can also configure the client device as a part of NSSP with additional/alternate s-NSSAI(s) determined based on slice SLA or slice policy related information to support the client device to use the alternate slice in case the first slice becomes unavailable. The network slice selection information configuration in the client device by the first network entity based on slice SLA/policy and slice availability status will prevent service failure due to slice unavailability.

In an implementation form of a client device according to the third aspect, the second network slice information is a network slice unavailability notification.

An advantage with this implementation form is that the network notifies the client device with a slice unavailability indication in case a requested slice is unavailable at the network side. This helps the client device to perform alternative steps configured in the client device side to re-initiate service request to available slices if a first slice is unavailable.

In an implementation form of a client device according to the third aspect, receive the second control message comprises

receive the second control message during initial registration procedure or a location update procedure.

An advantage with this implementation form is that during the initial registration or a location update procedure, the first network entity can configure the client device with network slice selection policy (NSSP) containing s-NSSAI(s) determined based on the available slice SLA or slice policy related information (along with slice availability and attribute usage status derived from the analytics provided by the NWDAF). The first network entity can also configure the client device as a part of NSSP with additional/alternate s-NSSAI(s) determined based on slice SLA or slice policy related information to support the client device to use the alternate

slice in case the first slice becomes unavailable. The network slice selection information configuration in the client device by the first network entity based on slice SLA/policy and slice availability status will prevent service failure due to slice unavailability.

In an implementation form of a client device according to the third aspect, the second network slice information comprises at least one of: a rule ID with an alternate S-NSSAI, an allowed NSSAI, and a configured NSSAI.

An advantage with this implementation form is that the network can provide slice information to the client device based on the available network slice SLA/policy information and slice status. The slice information that can be provided to the client device includes, rule ID and the alternate s-NSSAI to be added as part of NSSP, the allowed NSSAI and/or configured NSSAI determined based on the slice SLA/policy and slice status information available at the network (PCF/NWDAF).

In an implementation form of a client device according to the third aspect, the client device is configured to any of: an active state, an inactive state or an idle state.

An advantage with this implementation form is that the client device can receive the alternate S-NSSAI(s), configured NSSAI and/or the allowed NSSAI when the client device is in an active state, an inactive state or an idle state to update the client device with available slice information.

In an implementation form of a client device according to the third aspect, the second control message is received in a NAS message, a client device policy container, or a radio resource control message when the client device is in an active state.

An advantage with this implementation form is that the client device can receive the alternate S-NSSAI(s), configured NSSAI and/or the allowed NSSAI in any NAS message, a client device policy container, or a radio resource control message when the client device is in an active state, an inactive state or an idle state to update the client device with available slice information.

According to a fourth aspect of the disclosure, the above mentioned and other objectives are achieved with a method for a first network entity, the method comprises

receiving a NSIR from a second network entity, wherein the NSIR indicates at least one of a network slice information and/or a client device identity, ID;

obtaining a NSIN in response to the reception of the NSIR, wherein the NSIN indicates a network slice control information; and

transmitting the obtained NSIN to the second network entity.

The method according to the fourth aspect can be extended into implementation forms corresponding to the implementation forms of the first network entity according to the first aspect. Hence, an implementation form of the method comprises the feature(s) of the corresponding implementation form of the first network entity.

The advantages of the methods according to the fourth aspect are the same as those for the corresponding implementation forms of the first network entity according to the first aspect.

According to a fifth aspect of the disclosure, the above mentioned and other objectives are achieved with a method for a second network entity, the method comprises

sending a NSIR to a first network entity, wherein the NSIR indicates least one of a network slice information and/or a client device ID;

receiving a NSIN from the first network entity in response to the transmission of the NSIR, wherein the NSIN indicates a network slice control information.

The method according to the fifth aspect can be extended into implementation forms corresponding to the implementation forms of the second network entity according to the second aspect. Hence, an implementation form of the method comprises the feature(s) of the corresponding implementation form of the second network entity.

The advantages of the methods according to the fifth aspect are the same as those for the corresponding implementation forms of the second network entity according to the second aspect.

According to a sixth aspect of the disclosure, the above mentioned and other objectives are achieved with a method for a client device, the method comprises

obtaining a first control message indicating a first network slice information;

receiving a second control message from a first network entity, wherein the second control message indicates a second network slice information; and

selecting a network slice for a subsequent service based on the first network slice information and the second network slice information.

The method according to the sixth aspect can be extended into implementation forms corresponding to the implementation forms of the second network entity according to the third aspect. Hence, an implementation form of the method comprises the feature(s) of the corresponding implementation form of the client device.

The advantages of the methods according to the sixth aspect are the same as those for the corresponding implementation forms of the client device according to the third aspect.

According to a seventh aspect of the disclosure, the above mentioned and other objectives are achieved with a device, the device comprises

a processor, and

a memory coupled to the processor and having processor-executable instructions stored thereon, which when executed by the processor, cause the processor to perform the method according to any one of the fourth, fifth, or sixth aspect.

The disclosure also relates to a computer program, characterized in program code, which when run by at least one processor causes said at least one processor to execute any method according to embodiments of the disclosure. Further, the disclosure also relates to a computer program product comprising a computer readable medium and said mentioned computer program, wherein said computer program is included in the computer readable medium, and comprises of one or more from the group: ROM (Read-Only Memory), PROM (Programmable ROM), EPROM (Erasable PROM), Flash memory, EEPROM (Electrically EPROM) and hard disk drive.

Further applications and advantages of the embodiments of the disclosure will be apparent from the following detailed description.

Brief Description of the Drawings

The appended drawings are intended to clarify and explain different embodiments of the disclosure, in which:

- Fig. 1 shows a first network entity according to an embodiment of the disclosure;
- Fig. 2 shows a method for a first network entity according to an embodiment of the disclosure;
- Fig. 3 shows a second network entity according to an embodiment of the disclosure;
- Fig. 4 shows a method for a second network entity according to an embodiment of the disclosure;

- Fig. 5 shows a client device according to an embodiment of the disclosure;
- Fig. 6 shows a method for a client device according to an embodiment of the disclosure;
- Fig. 7 shows signalling between a first network entity and a second network entity according to an embodiment of the disclosure;
- Fig. 8 shows signaling between a client device and a first network entity according to an embodiment of the disclosure;
- Fig. 9 shows network slice provision by a first network entity according to an embodiment of the disclosure;
- Fig. 10 shows an access management network slice information procedure according to an embodiment of the disclosure.

Detailed Description

The NG.116 GSMA, "Generic Network Slice Template Version 1.0" describes the concept of generic slice template (GST) from which several network slice types descriptions can be derived. Some of the parameters in the GST point explicitly to the definition of parameters and bounds on the service delivered to the end customer. However, the enforcement of some of these bounds or of some of these parameters is not supported by the 5G system yet.

For instance, the GST aims at the limitation of the number of PDU sessions per slice, or the number of devices supported per network slice, or the maximum uplink (UL) or downlink (DL) data rate per network slice, which is not the same as the aggregate maximum bit rate (AMBR) for a user equipment (UE), rather a rate limitation per UE and/or single network slice selection assistance information (S-NSSAI). These parameters cannot be enforced today as the 5G system lacks the ability to do so.

This disclosure provides 5G system enhancements to support the GST related parameters and bounds enforcement in the network slice operations. The current 5G system does not have any network slice based policy specified for 5G network slice selection, control and usage. Further without a network slice related policy information in the 5G system, no network slice related enforcement per UE or slice is possible. Therefore, to implement the control and/or limitations of network slice operations and/or capabilities based on various attribute values put forth by the GSMA GST as specified in NG.116 is not feasible without a corresponding network slice policy to enforce in the 5G system.

Fig. 1 shows a first network entity 100 according to an embodiment of the disclosure. In the embodiment shown in Fig. 1, the first network entity 100 comprises a processor 102, a transceiver 104 and a memory 106. The processor 102 is coupled to the transceiver 104 and

the memory 106 by communication means 108 known in the art. The first network entity 100 may be configured for both wireless and wired communications in wireless and wired communication systems, respectively. The wireless communication capability may be provided with an antenna or antenna array 110 coupled to the transceiver 104, while the wired communication capability may be provided with a wired communication interface 112 coupled to the transceiver 104.

The processor 102 may be referred to as one or more general-purpose CPU, one or more digital signal processor (DSP), one or more application-specific integrated circuit (ASIC), one or more field programmable gate array (FPGA), one or more programmable logic device, one or more discrete gate, one or more transistor logic device, one or more discrete hardware component, one or more chipset.

The memory 106 may be a read-only memory, a random access memory, or a non-volatile random access memory (NVRAM).

The transceiver 104 may be a transceiver circuit, a power controller, an antenna, or an interface which communicates with other modules or devices.

In embodiments, the transceiver 104 may be a separate chipset, or it is integrated with processor in one chipset. While in some implementations, the transceiver 104 the memory 106 and the processor 102 are integrated in one chipset.

That the first network entity 100 is configured to perform certain actions can in this disclosure be understood to mean that the first network entity 100 comprises suitable means, such as e.g. the processor 102 and the transceiver 104, configured to perform said actions.

According to embodiments of the disclosure the first network entity 100 is configured to receive a network slice information request (NSIR) 510 from a second network entity 300, wherein the NSIR 510 indicates at least one of a network slice information and/or a client device identity (ID).

The first network entity 100 is further configured to obtain a network slice information notification (NSIN) 520 in response to the reception of the NSIR 510, wherein the NSIN 520 indicates a network slice control information.

Furthermore, the first network entity 100 is configured to transmit the obtained NSIN 520 to the second network entity 300.

Fig. 2 shows a flow chart of a corresponding method 200 which may be executed in a first network entity 100, such as the one shown in Fig. 1. The method 200 comprises receiving 202 a NSIR 510 from a second network entity 300, wherein the NSIR 510 indicates at least one of a network slice information and/or a client device ID. The method 200 further comprises obtaining 204 a NSIN 520 in response to the reception of the NSIR 510, wherein the NSIN 520 indicates a network slice control information. Furthermore, the method 200 comprises transmitting 206 the obtained NSIN 520 to the second network entity 300.

Fig. 3 shows a second network entity 300 according to an embodiment of the disclosure. In the embodiment shown in Fig. 3, the second network entity 300 comprises a processor 302, a transceiver 304 and a memory 306. The processor 302 is coupled to the transceiver 304 and the memory 306 by communication means 308 known in the art. The second network entity 300 may be configured for both wireless and wired communications in wireless and wired communication systems, respectively. The wireless communication capability may be provided with an antenna or antenna array 310 coupled to the transceiver 304, while the wired communication capability may be provided with a wired communication interface 312 coupled to the transceiver 304.

The processor 302 may be referred to as one or more general-purpose CPU, one or more digital signal processor (DSP), one or more application-specific integrated circuit (ASIC), one or more field programmable gate array (FPGA), one or more programmable logic device, one or more discrete gate, one or more transistor logic device, one or more discrete hardware component, one or more chipset.

The memory 306 may be a read-only memory, a random access memory, or a non-volatile random access memory (NVRAM).

The transceiver 304 may be a transceiver circuit, a power controller, an antenna, or an interface which communicates with other modules or devices.

In embodiments, the transceiver 304 may be a separate chipset, or it is integrated with processor in one chipset. While in some implementations, the transceiver 304, the memory 306 and the processor 302 are integrated in one chipset.

That the second network entity 300 is configured to perform certain actions can in this disclosure be understood to mean that the second network entity 300 comprises suitable means, such as e.g. the processor 302 and the transceiver 304, configured to perform said actions.

According to embodiments of the disclosure the second network entity 300 is configured to send a NSIR 510 to a first network entity 100, wherein the NSIR 510 indicates least one of a network slice information and/or a client device ID. The second network entity 300 is further configured to receive a NSIN 520 from the first network entity 100 in response to the transmission of the NSIR 510, wherein the NSIN 520 indicates a network slice control information.

Fig. 4 shows a flow chart of a corresponding method 400 which may be executed in a second network entity 300, such as the one shown in Fig. 3. The method 400 comprises sending 402 a NSIR 510 to a first network entity 100, wherein the NSIR 510 indicates least one of a network slice information and/or a client device ID. The method 400 further comprises receiving 404 a NSIN 520 from the first network entity 100 in response to the transmission of the NSIR 510, wherein the NSIN 520 indicates a network slice control information.

Fig. 5 shows a client device 600 according to an embodiment of the disclosure. In the embodiment shown in Fig. 5, the client device 600 comprises a processor 602, a transceiver 604 and a memory 606. The processor 602 is coupled to the transceiver 604 and the memory 606 by communication means 608 known in the art. The client device 600 may be configured for both wireless and wired communications in wireless and wired communication systems, respectively. The wireless communication capability may be provided with an antenna or antenna array 610 coupled to the transceiver 604, while the wired communication capability may be provided with a wired communication interface 612 coupled to the transceiver 604.

The processor 602 may be referred to as one or more general-purpose CPU, one or more digital signal processor (DSP), one or more application-specific integrated circuit (ASIC), one or more field programmable gate array (FPGA), one or more programmable logic device, one or more discrete gate, one or more transistor logic device, one or more discrete hardware component, one or more chipset.

The memory 606 may be a read-only memory, a random access memory, or a non-volatile random access memory (NVRAM).

The transceiver 604 may be a transceiver circuit, a power controller, an antenna, or an interface which communicates with other modules or devices.

In embodiments, the transceiver 604 may be a separate chipset, or it is integrated with processor in one chipset. While in some implementations, the transceiver 604, the memory 606 and the processor 602 are integrated in one chipset.

That the client device 600 is configured to perform certain actions can in this disclosure be understood to mean that the client device 600 comprises suitable means, such as e.g. the processor 602 and the transceiver 604, configured to perform said actions.

According to embodiments of the disclosure the client device 600 is configured to obtain a first control message 540 indicating a first network slice information. The client device 600 is further configured to receive a second control message 550 from a first network entity 100, wherein the second control message 550 indicates a second network slice information, and select a network slice for a subsequent service based on the first network slice information and the second network slice information.

Fig. 6 shows a flow chart of a corresponding method 700 which may be executed in a client device 600, such as the one shown in Fig. 5. The method 700 comprises obtaining 702 a first control message 540 indicating a first network slice information.

The method 700 further comprises receiving 704 a second control message 550 from a first network entity 100, wherein the second control message 550 indicates a second network slice information, and selecting 706 a network slice for a subsequent service based on the first network slice information and the second network slice information.

Fig. 7 shows signaling between the first network entity 100 and the second network entity 300 for provisioning and enforcement of network slice information according to an embodiment of the disclosure. The first network entity 100 may comprise a policy control function (PCF) and/or a network data analysis function (NWDAF). The second network entity 300 may be an access and mobility management function (AMF), a network slice selection function (NSSF), a session management function (SMF), and/or another network function (NF).

In step I in Fig. 7, the first network entity 100 may be configured with network slice related policy (NSRP) information. The NSRP information may be configured in the first network entity 100 e.g. from an operation administration and management (OAM) or by the operator

based on the slice SLA agreed between the operator and the network slice customer for any vertical service. The NSRP information may further be generated and/or configured by the first network entity 100 locally based on the slice SLA received from the OAM.

In embodiments, the first network entity 100 may receive a configuration message 530 from an OAM 120, where the configuration message 530 indicates a network slice policy. The configuration message 530 may further indicate a network slice SLA including e.g. slice attributes and required bounds and/or capability).

The configuration message 530 from the OAM 120 may be received previous to receiving the NSIR 510 from the second network entity 300, as indicated in Fig. 7.

In such embodiments, the first network entity 100 may generate the NSRP information based on the network slice policy and/or the network slice SLA received in the configuration message 530. The first network entity 100 may further generate NSRP information such as e.g. slice availability from the slice analytics information provided from a network data analytics function (NWDAF) for different second network entities 300. The NSRP information may be information used by the control plane functions to enforce the slice related policy decisions in both control plane and user plane functions.

In step II in Fig. 7, the second network entity 300 sends a NSIR 510 to the first network entity 100. In embodiments, the NSIR 510 may be termed but non-limiting example a Npcf_NetworkSliceStatusRequest or a Npcf_NSRPSliceStatusRequest service operation. The NSIR 510 indicates at least one of a network slice information and/or a client device ID.

The network slice information may be at least one of: a network function ID, a network slice instance ID, a network slice type, a network slice subscription type, and a single network slice selection assistance information (S-NSSAI).

The second network entity 300 may e.g. send the NSIR 510 to request the slice availability status from the first network entity 100 whenever the second network entity 300 requires the slice availability status. Furthermore, the second network entity 300 may have a subscription with the first network entity 100 for network slice information service operations. If the second network entity 300 has a subscription with the first network entity 100, the second network entity 300 may be notified about the availability of the network slice information if the network slice status changed.

The first network entity 100 receives the NSIR 510 from the second network entity 300, where the NSIR 510 indicates at least one of the network slice information and/or the client device ID. In response to the reception of the NSIR 510, the first network entity 100 obtains a NSIN 520 in step III in Fig. 7.

The NSIN 520 may indicate a network slice control information. The network slice control information may comprise at least part of the network slice information. Thus, the network slice control information may comprise at least one of: a network function ID, a network slice instance ID, a network slice type, a network slice subscription type, and a single network slice selection assistance information (S-NSSAI). In embodiments, the at least part of the network slice information comprised a subset of the network slice information comprised in the NSIR 510.

The network slice control information may further comprise a network slice policy information. The network slice policy information may indicate at least one of: a network slice status information, slice identification information, a maximum allowed PDU sessions per network slice, a maximum number of allowed client devices per network slice, a maximum uplink data rate supported for a client device, and a maximum downlink data rate supported for a client device.

In embodiments, the network slice status information may have any of the attributes: available during a validity period, availability level, permanently not available, or temporarily not available.

In embodiments, obtaining the NSIN 520 may comprise fetching NSRP information from a PCF or a unified data repository (UDR) upon receiving the NSIR 510 from the second network entity 300. Thus, the first network entity 100 may fetch the NSRP information and further determine and/or derive the NSIN 520 based on the fetched NSRP information.

The NSIN 520 may in embodiments indicate a subset of the NSRP information. The first network entity 100 may e.g. check a locally stored network slice policy set ID(s) corresponding to the client device ID and further fetches the NSRP information from the PCF or the UDR to determine the requested slice availability information for any network slice and/or slice service type. The NSRP information may be stored in the PCF or in the UDR in a similar way as for other policy information, as will be further described below.

In step IV in Fig. 7, the first network entity 100 transmits the NSIN 520 to the second network entity 300. In embodiments, the NSIN 520 may be termed but non-limiting as Npcf_NetworkSliceStatusNotify or Npcf_NSRPolicyAuthorization_Notify service operation. Thus, the second network entity 300 may receive the NSIN 520 from the first network entity 100 in response to the transmission of the NSIR 510.

From the NSIN 520, the second network entity 300 may obtain the network slice control information indicated in the NSIN 520, e.g. the at least part of the network slice information and further the network slice policy information.

As described above, the network slice information may be at least one of: a network function ID, a network slice instance ID, a network slice type, a network slice subscription type, and an S-NSSAI.

The network slice policy information may be at least one of: a network slice status information, slice identification information, a maximum allowed PDU sessions per network slice, a maximum number of allowed client devices per network slice, a maximum uplink data rate supported for a client device, and a maximum downlink data rate supported for a client device.

Furthermore, the network slice status information may have any of the attributes: available during a validity period, availability level, permanently not available, or temporarily not available. In other worlds, the second network entity 300 may obtain information related to network slice policy and network slice availability from the first network entity 100.

Based on the received NSIN 520, the second network entity 300 may perform at least one network slice related operation in step V in Fig. 7. The network slice related operation may e.g. comprise determine allowed NSSAI or configured NSSAI, or select a user plane function (UPF) for a protocol data unit (PDU) session. The network slice related operation performed in step V in Fig. 7 may depend on the use case and/or the role of the second network entity 300.

When the second network entity 300 is an AMF or a NSSF, the second network entity 300 may determine an allowed NSSAI and/or a configured NSSAI based on the received NSIN 520. The second network entity 300 may further select a network slice instance (NSI) based on the NSIN 520.

For example, the second network entity 300 as AMF may determine the allowed NSSAI for a client device, such as e.g. the client device 600, during the client device registration procedure.

The determined allowed NSSAI may in this case be provided to the client device 600 in the registration accept message.

Furthermore, the second network entity 300 as NSSF may determine the allowed NSSAI and the configure NSSAI for the client device 600 during the client device configuration update procedure. The slice related configuration of the client device 600 may then be updated based on the determined allowed NSSAI and the determined configured NSSAI and the client device 600 may use the updated slice related configuration for its service requests towards the network.

When the second network entity 300 is a SMF, the second network entity 300 may select a UPF for a PDU session based on the received NSIN 520. For example, the second network entity 300 as SMF may select a UPF for a PDU session for the client device 600 during a PDU session establishment or modification procedure. The selected UPF may in this case be used to established or modified the PDU session.

In this way, the established or modified PDU session is based on the network slice control information received from the first network entity 100, thereby helping the operator to control the agreed slice SLA in the 5G System.

Furthermore, the second network entity 300 may in embodiments be a network repository function (NRF). In such embodiments, the second network entity 300 may update the slice availability and selection information stored locally in the NRF based on the received NSIN 520.

The NSRP information in the first network entity 100 may further be used to configure the client device 600 with alternative and/or additional slice information. For example, if the first network entity 100 considers a slice unavailable based on the NSRP information, the first network entity 100 may provide the client device 600 with a “slice unavailability” notification and/or cause value in any service reject message and further provide a “select alternative slice” indicator.

Fig. 8 shows signaling between the client device 600 and the first network entity 100 according to such embodiments. The client device 600 may be configured to any of: an active state, an inactive state or an idle state.

In step I in Fig. 8, the client device 600 may obtain a first control message 540 indicating a first network slice information. The first network slice information may comprise at least one of: a network slice selection policy with S-NSSAI(s), allowed NSSAI, and a configured NSSAI.

In the embodiment shown in Fig. 8, the client device 600 obtains the first control message 540 from the first network entity 100. However, the client device 600 may in embodiments instead obtain the first control message 540 from another network entity or internally within the client device 600. In the latter case, the first network slice information may e.g. have been configured in the client device 600 or previously received.

In step II in Fig. 8, the client device 600 may receive a second control message 550 from the first network entity 100. The client device 600 may e.g. receive the second control message 550 during initial registration procedure, service establishing procedure, or a location update procedure.

When the client device 600 is in the active state, the second control message 550 may be received in a non-access stratum (NAS) message, a client device policy container, or a radio resource control message from first network entity 100 during e.g. initial registration, registration with 5GS when the client device moves from another system to 5GS, change of location of the client device 600, and change of subscribed S-NSSAIs, or the client device 600 initials service request from idle or inactive state.

The received second control message 550 indicates a second network slice information. The second network slice information may be a network slice unavailability notification. The second network slice information may further comprise at least one of: a rule ID with an alternate S-NSSAI, an allowed NSSAI, and a configured NSSAI.

The two types of second network slice information may be comprised in one second control message 550 or may be comprised in a respective second control message 550. Thus, the client device 600 may in embodiments receive one second control message 550 indicating a network slice unavailability notification, and another second control message 550 indicating at least one of: a rule ID with an alternate S-NSSAI, an allowed NSSAI, and a configured NSSAI.

Based on the first network slice information and the second network slice information, the client device 600 may, in step III in Fig. 8, select a network slice for a subsequent service. The client device 600 may e.g. selected to use a received alternate S-NSSAI for a subsequent service request to the network.

In the following embodiments, the first network entity 100 comprises a PCF, the second entity 300 corresponds to an AMF, SMF, NSSF or any NF, and the client device 600 corresponds to a UE. As previously described, the NSRP information may be configured in the PCF either by the OAM or by the operator based on the slice SLA agreed between the operator and the network slice customer for any vertical service.

Furthermore, the NSRP can be generated and/or configured by the PCF locally based on the slice SLA received from the OAM. The NSRP is used by the control plane functions to enforce the slice related policy decisions in both control plane and user plane functions. The agreed network slice type (NEST) between the operator and the network slice customer may contain the generic slice template (GST) with filled-in slice attribute values. The NEST may be used as the slice SLA to generate the NSRP and related information in the PCF. The NSRP information structure may be generated at the PCF to enforce the SLA based slice control and limitation across different NFs, e.g. different network slices, in the 5G System.

Table 1 below shows the NSRP information structure according to an embodiment. The NSRP information shown here may cover mainly certain slice attributes like, “maximum number of PDU sessions” supported by a slice, “maximum number of UEs” supported by a slice, “maximum UL data rate” and “maximum downlink data rate” supported for a UE and/or by a slice.

The NSRP information may be extended to include any other required slice attributes for the network slice policy enforcement. For example, “maximum network slice resource (A/B/C) supported for a UE”. The NSRP information may further be generated for any network slice during any of the following scenarios:

(a) when a new NF instance is instantiated and registered,
(b) when a new NF slice is created,
(c) when a NF requests the PCF to create subscription for slice status notification, and
(d) when a PCF decides to enforce a slice policy control in any NF or slice

The NSRP information generated at the PCF for any network slice, the slice granularity may be any level, e.g. network slice, network slice instance, and network slice subset/subnet, may contain at least information on network slice (e.g. identification, slice service type, or slice subscription type), slice attribute name or identification information, slice category, PCF controls over the slice attribute value modification based on the dynamic need, slice attribute

consumption status monitor to check the real-time/predict slice availability and scope of the slice attribute.

Table 1

Slice Attribute/ Information Name	**Description**	**Category**	**Required/ Expected Slice Attribute Limit Levels**	**PCF permitted to modify for dynamically provided information**	**Attribute Status Monitor to check slice availability & to trigger notifications <u>Based on Analytics Received from NWDAF</u> Slice actual status monitored and managed with the following availability levels**	**Scope**
Slice Information	- NF ID - Defines the scope of the policy such as NSSAI/s-NSSAI/ Network Slice Instance ID/ Network slice type Information/Slice service Type/Slice Subscription Type	Mandatory		Yes	• Available/Not available (Timer/Permanent /Temporary)	Slice
Maximum number of PDU Sessions	The maximum number of PDU session allowed	Conditional (If the slice type is URLLC/V2X)	- Maximum Limit / Threshold - Average Limit	Yes	• Available/Not available (Timer) • Currently allowed • Availability Status	Slice
Maximum number of UEs	The maximum number of UEs allowed	Conditional (If the slice type is URLLC/V2X /MIoT/eMBB)	- Maximum Limit / Threshold - Average Limit	Yes	• Available/Not available (Timer) • Currently allowed • Availability Status	Slice

Maximum UL Data Rate	The maximum UL data rate supported for a UE	Conditional (If the slice type is eMBB or based on the subscription type)	Upper bound and lower bound for Maximum UL Data Rate	Yes	• Available/Not available (Timer) • Current Status	Slice and/or UE
Maximum DL Data Rate	The maximum DL data rate supported for a UE	Conditional (If the slice type is eMBB or based on the subscription type)	Upper bound and lower bound for Downlink UL Data Rate	Yes	• Available/Not available (Timer) • Current Status	Slice and/or UE
Any Slice attribute (e.g. Maximum network slice resource (A/B/C) supported for a UE)	Description of the slice attribute (Character/Scalability attribute)	Following conditions will apply	- Maximum Limit / Threshold - Average Limit	Yes	• Available/Not available (Timer) • Currently allowed • Availability Status	Slice and/or UE

Either all or specific slice attributes for any slice can be considered to be included in the NSRP information based on any of the conditional factors listed below, where conditional may be understood to mean that the attribute's value is mandatory if a certain condition exists.

1. Condition 1: If the scope of the NSRP is per service instance or slice subset
2. Condition 2: Based on the slice type, e.g. non-public network (NPN) or public land mobile network (PLMN), and/or slice service type, e.g. ultra-reliable low latency communication (URLLC), vehicle to anything (V2X), mobile internet of things (MIoT), or enhanced mobile broadband (eMBB), the limitations can be imposed on the slice
3. Condition 3: Based on the slice tracking area(s)
4. Condition 4: Based on the network function
5. Condition 5: Based on at least one of: UE subscription type, UE type (e.g. gateway UE, 5G residential gateway (5G-RG), 5G cable residential gateway (5G-CRG), fixed network RG (FN-RG)), UE group ID, and closed access group ID

The PCF can compute the current/future NF's slice status and/or availability based the slice SLA based reference information such as maximum slice's limitation (slice attribute value) in the NSRP and networks slice data analytics information, e.g. the slice load, received from the NWDAF. The slice related analytics information can also be stored as a part of the NSRP information to support PCF in the appropriate decision making and enforcement activities.

The PCF can receive notifications on changes in the configured NSRP. Upon reception of a notification, the PCF can make the slice policy control decisions necessary to accommodate the change in the slice limit/control and need to update the unified data management/unified data repository (UDM/UDR), SMF, AMF and NSSF accordingly.

The NSRP configured in the PCF can be specific to any level of network slice granularity such as network slice, network slice instance (NSI), network slice service instance, per NSSAI, per S-NSSAI, per network slice type etc. The attributes in the NSRP can be included on various conditional aspects mentioned above as opposed to the mandatory attribute information on slice identification, i.e. NSRP granularity based information.

The network slice attribute, "number of UEs per network slice" can be tracked considering the number of UEs in registration management (RM) registered state in a network by any NF such as PCF, NWDAF, AMF, SMF, or any NF service consumer/producer based on roaming and non-roaming scenarios in the home PLMN (HPLMN) and/or visited PLMN (VPLMN) accordingly.

The network slice attribute, "number of PDU Sessions per network slice" can be tracked considering the "PDU session status" IEs of any PDU session with only "active" values as accountable for counting by any NF such as PCF, NWDAF, AMF, SMF, or any NF service consumer/producer based on roaming and non-roaming scenarios in the HPLMN and/or VPLMN accordingly.

The NSRP information may, as previously described, be stored either in the PCF or in the UDR similar to other policy information. When the NSRP information is stored in the PCF, the NSRP information may be stored locally in the PCF and a corresponding network slice capability information "required network capability IE" per UE slice subscription may be stored along with the "UE subscription information" in the UDR. Further, during the UE registration procedure the proposed "required network slice capability IE" based on NSRP information may be stored in UDR along with the UE subscription information.

In case of roaming scenarios, the “required network capability IE” containing required network slice information may be shared by the UDM along with the subscription information between the PLMNs and the slice control and limitations may hence be enforced effectively. The (H-) PCF may store the latest list of network slice policy set ID(s) and its contents, i.e. the NSRP information, in the (H-)PCF.

When the NSRP information is stored in the UDR, the (H-)PCF may store the latest list of network slice policy set ID(s) and its contents in the (H-) UDR using for example Nudr_DM(DataManagement)_Create/Nudr_DM Update including data set “policy data (network slice policy data NF, slice and service identification info)” and data subset “policy set entry (NEST values/the NSRP)”. The (H-)PCF may retrieve the network slice policy data from (H-)UDR using Nudr_DM_Query.

In the 5G system, the NSRP based on the agreed SLA may be enforced using the proposed PCF service operation messages, e.g. the Npcf_NSRPolicyAuthorization service operations such as Create/Update/Delete/Notify/Subscribe/Unsubscribe, in various NFs, e.g. AMF, SMF, NSSF, NRF. The NSRP based on the agreed SLA may be enforced during the corresponding slice related operations, e.g. network slice selection, network slice configuration determination for UE etc.

The proposed PCF based Npcf_NSRPAuthorization or Npcf_NSRPControl service operations for example authorises an NF service consumer request and creates policies, e.g. NSRP information, as requested by the authorised NF service consumer for the corresponding slices. This service allows the NF service consumer to subscribe/unsubscribe to the notification of slice status, availability, slice capability, resource usage report etc.

The information for notification will be generated by the PCF as part of the NSRP information using e.g. the received network slice analytics information from the NWDAF, as mentioned above.

The following table, table 2, illustrates non-limiting examples of PCF NSRP services operations.

Table 2

Service Name	Service Operations	Operation Semantics	Example Consumer (s)
Npcf_NSR PolicyAuthorization / Control	Create	Request/Response	SMF, AMF, NSSF, NRF and any NF
	Update	Request/Response	SMF, AMF, NSSF, NRF and any NF
	Delete	Request/Response	SMF, AMF, NSSF, NRF and any NF
	Notify	Subscribe/Notify	SMF, AMF, NSSF, NRF and any NF
	Subscribe		SMF, AMF, NSSF, NRF and any NF
	Unsubscribe		SMF, AMF, NSSF, NRF and any NF

Further details of the respective PCF NSRP service operation are listed below:

Npcf_NSRPolicyAuthorization_Create service operation

- **Description:** Authorize the request, and optionally determines and installs network slice related policy control data according to the information provided by the NF Consumer.
- **Inputs, Required:** Network function information and slice information (NF ID, NSI, S-NSSAI, allowed NSSAI, configured NSSAI, data network name (DNN)), service request information
- **Inputs, Optional:** UE ID (subscriber permanent identifier (SUPI) or any UE ID), UE type
- **Outputs, Required:** Success or failure (reason for failure)
- **Outputs, Optional:** The service information that can be accepted by the PCF.

Npcf_NSRPolicyAuthorization_Update service operation

- **Description:** Provides updated slice information to the PCF.
- **Description:** Authorize the request, and optionally determines and installs network slice related policy control data according to the information provided by the NF Consumer.

- **Inputs, Required:** Network function information and slice information (NF ID, NSI, S-NSSAI, allowed NSSAI, configured NSSAI, DNN), service request Information
- **Inputs, Optional:** UE ID (SUPI or any UE ID), UE type
- **Outputs, Required:** Success or failure (reason for failure)
- **Outputs, Optional:** The service information that can be accepted by the PCF.

Npcf_NSRPolicyAuthorization_Delete service operation

- **Description:** Provides means for the NF service consumers to delete the context of network slice level information related to the NSRP information.
- **Inputs, Required:** Identification of the network slice and service type
- **Inputs, Optional:** UE ID
- **Outputs, Required:** Success or failure (reason for failure)
- **Outputs Optional:** The service information that can be accepted by the PCF.

Npcf_NSRPolicyAuthorization_Notify service operation

- **Description:** PCF notifies to the NF service consumers about the subscribed events such as when a slice is unavailable anymore, fully loaded or is about to be overloaded or any other important slice service/resource or UE service/resource status. Notify service operation can also be used to notify the slice availability status on a specific request from the NF service consumers.
- **Inputs, Required:** Event ID, network function and network slice identification information, notification correlation information
- **Inputs, Optional:** Event information
- **Outputs, Required:** Operation execution result indication
- **Outputs Optional:** None

Npcf_NSRPolicyAuthorization_Subscribe service operation

- **Description:** Provided by the PCF for NF consumers to explicitly subscribe the notification of events (slice availability, slice unavailability, slice fully loaded, slice overloaded, other slice status and/or capability etc.).
- **Inputs, Required:** Network function and network slice identification information, target of PCF event reporting, event reporting information, notification target address (notification correlation ID)
- **Inputs, Optional:** UE ID, event filter, subscription correlation ID (in case of modification of the event subscription).
- **Outputs, Required:** When the subscription is accepted
- **Outputs Optional:** None

Npcf_NSRPolicyAuthorization_Unsubscribe service operation

- **Description:** Enable NF service consumers to explicitly unsubscribe the notification of PCF events related to Npcf_NSRPolicyAuthorization_Subscribe operation.
- **Inputs, Required:** Subscription correlation.
- **Inputs, Optional:** None
- **Outputs, Required:** Success or failure
- **Outputs Optional:** None

In the roaming case, the slice SLA may further be guaranteed across different PLMNs. For example, the network slice customer may have a slice agreement with an Operator 1, e.g. PLMN 1, for a specific slice type, e.g. slice X.

If the UEs who has subscribed to that slice type moves from PLMN 1 to another network, e.g. PLMN 2, the service for the roaming UEs should be ensured in the target network slices, e.g. slice Y, in the target network, e.g. PLMN 2, similar to the source slice type, e.g. slice X, with all the required slice attributes both character and scalability and capability to offer the UE with the required quality of service (QoS) and quality of experience (QoE).

The following are various NSRP information sharing methods across different PLMNs to ensure slice SLA/NSRP during roaming scenarios.

Provision by UDM to V-PCF Variant 1:

The PCF may perform storage and retrieval of agreed/required NRSP (slice SLA)/slice capability for a UE's slice subscription/subscribed NSSAI similar to other policy data in the UDR.

In roaming case, the UDM may provide to the VPLMN the agreed and/or required NRSP (SLA)/slice capability and "required network slice capability IE" for the UE subscription along with the S-NSSAIs from the subscribed S-NSSAIs the HPLMN allows for the UE in the VPLMN. In local breakout, the V-PCF can make use of the received agreed/required NRSP (SLA)/slice capability and "required network slice capability IE" to enforce the policy, i.e. slice attributes, in V-PLMN.

In home routed roaming, the H-PCF will have the NSRP and "required network slice capability IE" to enforce the slice attributes in the HPLMN.

Sharing between (H-)PCF and (V-)PCF variant 2:

In roaming case, the V-PCF receives the required NSRP and "required network slice capability IE" from the H-PCF and store it locally to enforce the slice attribute requirements, e.g. similar to the UE policy specified in TS 23.503.

Slice SLA between PLMNs variant 3:

The roaming agreements shared between HPLMN and VPLMN can include the agreed slice attribute values per subscription type and the NRSP agreed for a network slice service type.

In embodiments, UE route selection policy (URSP) may be extended based on NSRP to address slice unavailability. The extended URSP (E-URSP) may be a rule which contains a network slice selection policy (NSSP) with additional and/or alternate s-NSSAI(s) for the UE to use during the slice unavailability scenario.

The alternate s-NSSAIs of NSSP configured in the UE is determined by the PCF based on the NSRP configured and slice availability information computed in the PCF. The NSSP is used by the UE to associate the matching application with S-NSSAI. NSSP is proposed to contain one additional s-NSSAI for the UE to handle slice unavailability or slice overloaded situation. The URSP includes a prioritized list of URSP rules.

The UE is provisioned with E-URSP rules by the PCF based on the configured network slice related policy (slice SLA) and NSRP information available (network slice availability information) in the HPLMN. When the UE is roaming, the PCF in the HPLMN may update the E-URSP rule in the UE based on the locally available NSRP information.

In addition, the UE may also be pre-configured with E-URSP rules, e.g. by the operator, considering the slice SLA. Only the E-URSP rules provisioned by the PCF is used by the UE, if both E-URSP rules provisioned by the PCF and pre-configured E-URSP rules are present.

During UE configuration update (UCU) that happens for registration/re-registration of UE, this NSSP with alternate s-NSSAI can be configured. No separate UCU procedure is required if it is considered as an overhead by the network. The E-URSP along with the proposed alternative slice information for slice unavailability case is shown in the table 3.

Table 3

Example E-URSP rules		Comments
Rule Precedence =1 Traffic Descriptor: Application Identifiers=App1	Route Selection Descriptor Precedence=1 Network Slice Selection: S-NSSAI-a Alternate Slice Selection if Slice a unavailable: S-NSSAI-x (any number of slice information can be added as required) SSC Mode Selection: SSC Mode 3 DNN Selection: internet Access Type preference: 3GPP access	This URSP rule associates the traffic of application "App1" with S-NSSAI-a or S-NSSAI-x, SSC Mode 3, 3GPP access and the "internet" DNN. It enforces the following routing policy: The traffic of App1 should be transferred on a PDU session supporting S-NSSAI-a, SSC Mode 3 and DNN=internet over 3GPP access. If this PDU session is not established, the UE shall attempt to establish a PDU session with S-NSSAI-a, SSC Mode 3 and the "internet" DNN over 3GPP access. If this PDU session is not established because of slice unavailability, the UE shall re-attempt to establish a PDU session with S-NSSAI-x, SSC Mode 3 and the "internet" DNN over 3GPP access.
Rule Precedence =2 Traffic Descriptor: Application Identifiers=App2	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-a Alternate Slice Selection if Slice a unavailable: S-NSSAI-x (any number of slice information can be added as required) Access Type preference: Non-3GPP access	This URSP rule associates the traffic of application "App2" with S-NSSAI-a or S-NSSAI-x, and Non-3GPP access. It enforces the following routing policy: The traffic of application App2 should be transferred on. a PDU session supporting S-NSSAI-a using a Non-3GPP access. If this PDU session is not established, the UE shall attempt to establish a PDU session with S-NSSAI-a, over Access Type=non-3GPP access. If this PDU session is not established because of slice unavailability, the UE shall attempt to establish a PDU session with S-NSSAI-x, over Access Type=non-3GPP access.

	Route Selection Descriptor Precedence =2 Non-seamless Offload indication: Permitted (WLAN SSID-a)	If the PDU session cannot be established, the traffic of App2 shall be directly offloaded to WLAN, if the UE is connected to a WLAN with SSID-a (based on the 2nd RSD)
Rule Precedence =3 Traffic Descriptor: DNN=DNN_1	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-a Alternate Slice Selection if Slice a unavailable: S-NSSAI-x (any number of slice information can be added as required) Access Type preference: Non-3GPP access	This URSP rule associates the traffic of applications that are configured to use DNN_1 with DNN_1, S-NSSAI-a or S-NSSAI-z, over Non-3GPP access. It enforces the following routing policy: The traffic of application(s) that are configured to use DNN_1 should be transferred on a PDU session supporting S-NSSAI-a, over Non-3GPP access. If this PDU session is not established, the UE shall attempt to establish the PDU session with S-NSSAI-a, over Non-3GPP access. If this PDU session is not established because of slice unavailability, the UE shall attempt to establish the PDU session with S-NSSAI-x, over Non-3GPP access.
Rule Precedence =4 Traffic Descriptor: Application Identifiers=App1 Connection Capabilities="internet", "supl"	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-a Alternate Slice Selection if Slice a unavailable: S-NSSAI-x DNN Selection: DNN_1 Access Type preference: Non-3GPP access	This URSP rule associates the application "App1" and the Connection Capabilities "internet" and "supl" with DNN_1, S-NSSAI-a or S-NSSAI-x over Non-3GPP access. It enforces the following routing policy: When the "App1" requests a network connection with Connection Capability "internet" or "supl", the UE establishes (if not already established) a PDU session with DNN_1 and S-NSSAI-a or S-NSSAI-x over Non-3GPP access. After that, the UE routes the traffic of "App1" over this PDU session.

Rule Precedence =5 Traffic Descriptor: Application Identifiers=App3 Connection Capabilities="ims"	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-c Alternate Slice Selection if Slice a unavailable: S-NSSAI-y DNN Selection: DNN_1 Access Type preference: Multi-Access	This URSP rule associates the application "App3" and the Connection Capability "ims" with DNN_1, S-NSSAI-c or S-NSSAI-y and multi-access connectivity. It enforces the following routing policy: When the "App3" requests a network connection with Connection Capability "ims", the UE establishes (if not already established) a MA PDU Session with DNN_1 and S-NSSAI-c or S-NSSAI-y. After that, the UE routes the traffic of "App3" over this MA PDU Session by using the received ATSSS rules.
Rule Precedence = lowest priority Traffic Descriptor: *	Route Selection Descriptor Precedence =1 Network Slice Selection: S-NSSAI-b Alternate Slice Selection if Slice a unavailable: S-NSSAI-z SSC Mode Selection: SSC Mode 3 DNN Selection: internet	This URSP rule associates all traffic not matching any prior rule a PDU Session with S-NSSAI-b or S-NSSAI-z, SSC Mode 3 and the "internet" DNN. It enforces the following routing policy: All traffic not matching any prior rule should be transferred on a PDU session supporting S-NSSAI-b or S-NSSAI-z, SSC Mode 3 and DNN=internet with no access network preference.

Use of E-URSP - Variant 1 (Re-active approach):

During a PDU session establishment procedure, if the SMF finds that specified s-NSSAI in the PDU session request message is unavailable (temporarily or permanently), then the network can send in the PDU session reject message with a suitable clause value to indicate that the slice corresponding to the requested NSSAI/S-NSSAI is unavailable and an indication for the UE to retry the PDU session establishment procedure with the alternate s-NSSAI configured for the same Rule ID in the NSSP of the E-URSP rule.

Use of E-URSP - Variant 2 (Proactive approach):

If the NSSF and/or SMF identifies that any of the s-NSSAI configured in the UE is unavailable, the notification can be sent to AMF in any NAS SM message to trigger alternate s-NSSAI usage notification along with the Rule ID to the UE.

The AMF can send the notification “select alternate S-NSSAI” along with the suitable cause value for slice unavailability in any of the NAS message to trigger the UE to use the alternate S-NSSAI in the future service request message.

On receiving the slice unavailability notification or related cause value along with the “select alternate S-NSSAI” IE from the network the UE uses the alter s-NSSAI configured in the NSSP of the E-URSP for further PDU session requests.

Following the NSRP configuration in the PCF according to the disclosure, the NSRP for various NF service consumers like AMF, NSSF, SMF, NRF or any NF can be provisioned using procedures which will now be described. Furthermore, the NRSP base network slice configuration for UE can be done as described below.

NSRP provisioning procedure

The PCF may provide NF service consumer specific NSRP and related network slice status to NSSF, SMF, and/or any NF whenever it receives a new NSRP from OAM (based on slice SLA) or is configured by the operator or when it derives by itself based on the network slice analytics provided by the NWDAF. The PCF can also provide the NSRP to NSSF, SMF, and/or any NF when the PCF request NSRP with Npcf_NFSlicePolicyControl_Create message.

Fig. 9 shows NSRP and slice availability information provision by a PCF 100 to a NF service consumer 300 according to an embodiment of the disclosure. In step I in Fig. 9, the (V)-PCF 100 may be configured with the NSRP information related to the agreed slice SLA and may contain the network slice status of various NF service consumers provided by the NWDAF 140.

In step II in Fig. 9, the NF service consumer 300 such as e.g. NSSF, SMF, AMF, NRF, any NF may decide to establish slice related policy association with the PCF 100, e.g. when a new slice is instantiated for a NF or during any phase of a network slice lifecycle.

In step III in Fig. 9, the NF service consumer 300 may send a service operation 560 to the PCF 100. The service operation 560 may be for example a Npcf_NFSlicePolicyControl_Create service operation or existing related PCF service operation message containing the NF ID, NSI ID, NSSAI/S-NSSAI(s), service type.

On receiving the service operation 560, the (V)-PCF 100 may, in step IV in Fig. 9, check the NSRP information stored locally and may further check the related network slice status and availability information to filter the NSRP information specific to the NF service consumer 300.

In step V in Fig. 9, the (V)-PCF 100 may send a response service operation 570 to the NF service consumer 300. The response service operation 570 may be for example an Npcf_NFSlicePolicyControl_Create response service operation containing the NF service consumer specific NSRP with slice status and/or availability information and the slice related policy ID.

On receiving the slice policy, the NF service consumer 300 may, in step VI in Fig. 9, enforce the policy in corresponding service operations such as network slice selection, e.g. NSI selection by the AMF during SMF selection, and slice information, e.g. configured NSSAI and allowed NSSAI, determination for UE.

Access and mobility management (AM) NSRP establishment procedure

The PCF may use for example the existing AMPolicyControl_Create service operation or the proposed Npcf_NFSlicePolicyControlCreate service operation messages to provision the NSRP information to the AMF and similar procedure can be used for any NFs to associate the NSRP from PCF.

Fig. 10 shows the AM NSRP establishment procedure according to an embodiment of the disclosure. In step I in Fig. 10, the AMF 300 may decide to establish AM policy association with the (V-)PCF 100. The AMF 300 may decide to establish AM policy association with the (V-)PCF 100 based on local policies or when a new AMF instance is instantiated.

Upon deciding to establish AM policy association with the (V-)PCF 100, the AMF 300 may send a service operation 580 to the (V-)PCF 100 to establish an AM slice policy control association with the (V-)PCF 100 in step II in Fig. 10.

The service operation 580 may be for example an Npcf_AMPolicyCreate or a Npcf_NFSlicePolicyControl_Create service operation. The service operation 580 may include the following information: network function and slice identification information, subscription notification indication and, if available, service area restrictions and may include access type and radio access technology (RAT), and serving network.

In step III in Fig. 10, the (V-)PCF 100 may respond to the service operation 580 with a response service operation 590. The response service operation 590 may be for example an Npcf_AMPolicyCreate or Npcf_NFSlicePolicyControl_Create response service operation.

The (V-)PCF 100 may respond based on the available NSRP, the slice analytics information provided by the NWDAF and slice status and/or availability information computed by the PCF 100.

The (V-)PCF 100 may provide network slice related policy information, e.g. slice related policy ID and NSRP information specific to the AMF 300. In addition, (V-)PCF 100 may provide policy control request trigger of slice policy association to the AMF 300. The AMF 300 may be implicitly subscribed in the (V-)PCF 100 to be notified of changes in the policies.

In the conditional step IV in Fig. 10, the AMF 300 may deploy the slice related policy information which includes storing the NSRP along with slice policy ID(s) and uses the NSRP in determining the slice selection, allowed NSSAI and/or configured NSSAI and any slice related information.

Following the NSRP configuration in the PCF according to the disclosure, the NRSP base network slice configuration for UE may further be performed as described below.

The NRSP based network slice configuration procedure for UE

According to TS 23.501, the UE can be pre-configured with the default configured NSSAI. The UE can be provisioned and/or updated with the default configured NSSAI, determined by the UDM in the HPLMN considering the proposed NSRP (related to the s-NSSAI(s) of the NSSAI or to any corresponding slice information), using the UE parameters update via UDM control plane procedure defined in TS 23.502.

a. Each S-NSSAI in the default configured NSSAI may have a corresponding S-NSSAI as part of the subscribed S-NSSAI(s). Consequently, if the subscribed S-NSSAI(s) which are also present in the default configured NSSAI are updated the UDM should update the default configured NSSAI in the UE by also considering the proposed NSRP.
b. When the subscribed S-NSSAI(s) are updated, e.g. some existing S-NSSAIs are removed and/or some new S-NSSAIs are added, and one or more are applicable to the serving PLMN the UE is registered in, as described in TS 23.501, or when the associated mapping is updated, the AMF may also consider the PCF provided NSRP to update the UE with the configured NSSAI for the serving PLMN and/or allowed

NSSAI and/or the associated mapping to HPLMN S-NSSAIs (see TS 23.501). When there is the need to update the allowed NSSAI, the AMF may also consider the PCF provided NSRP to provide the UE with the new allowed NSSAI and the associated mapping to HPLMN S-NSSAIs.

c. Upon successful completion of a UE's Registration procedure over an access type, the UE obtains from the AMF based on the NSRP available at AMF, and/or local slice usage statistics and/or the slice based analytics information, an allowed NSSAI for this access type, which includes one or more S-NSSAIs and, if needed (see TS 23.501for when this is needed), their mapping to the HPLMN S-NSSAIs.

d. In general, any NF including UDM/UDR, SMF, AMF, NSSF, NRF etc. in the above mentioned cases can also makes use of the proposed NSRP along with the NWDAF provided slice related analytics information, e.g. load information and/or resource status to identify the real time slice availability, i.e. slice limitation versus slice load status.

Usage of the NRSP will now be described.

NRSP to assist NSSF:

- Nnssf_NSSelection_Get service operation of NSSF may consider slice related policy information to provide to AMF / NSSF in a different PLMN allowed s-NSSAI(s) / NSSAI / NRF used to select the NF/services within the selected network slice instance accordingly.
- Nnssf_NSSAIAvailability service operation of NSSF may consider slice related policy information in addition to per tracking area (TA) to update the AMFs and the NSSF on the availability of s-NSSAIs.
- Nnssf_NSSAIAvailability_Notify service operation of NSSF may consider slice related policy information for restrictions while updating the AMF with any S-NSSAIs restricted per TA.
- Nnssf_NSSAIAvailability_Subscribe service operation of NSSF may enable a NF Service Consumer, e.g. AMF, to subscribe to a notification of any changes in status of the NSSAI availability information based on slice related policy information, e.g. S-NSSAIs available per TA and the restricted S-NSSAI(s) per PLMN in that TA in the serving PLMN of the UE, upon this is updated by another AMF.

NRSP to assist AMF for UE network slice configuration:

- During the registration procedure, after the successful registration process, the AMF may take into account the slice related policy information for sending the allowed NSSAI in the registration accept message to the UE.

NSRP assisted SMF based network slice operations

NSRP association establishment/modification during registration procedure

This section explains how the proposed NSRP may be used by the network for slice related decision during the UE registration procedure. During the registration procedure, the AMF may take into account the slice related policy information provided as part of the NSRP for determining the allowed NSSAI to be sent in the registration accept message to the UE.

For example, in the UE registration procedure during the AM policy association establishment/modification, the (new/v-AMF) AMF may perform a NSRP association establishment/modification using the proposed network slice related policy (NSRP) provision/update procedure. If the (V-)PCF identified by the (V-)PCF ID included in UE context from the old AMF is used, the new AMF may perform NSRP association modification with the (V-)PCF as follows:

- The new AMF may send a Npcf_NFSlicePolicyControl Create Request to PCF with the slice identification information such as request s-NSSAI if provided and/or the mobility restrictions, e.g. UE location.
- The PCF may send a Npcf_NFSlicePolicyControl Create Response to the new AMF with one or more NSRP(s) related to the network slice(s) along with the corresponding slice policy ID(s).
- The PCF may trigger UE configuration update procedure.

The (new) AMF may further determine the allowed NSSAI to be sent to UE considering the NSRP received from the PCF in the NSRP association establishment/modification step and any other locally handled NF operational statistical information.

NSRP assisted slice selection during PDU session establishment procedure

This section describes one scenario of how the proposed NSRP may be associated between the PCF and the SMF and used by the network, e.g. SMF, to support efficient PDU session establishment to the available slices based on NSRP, e.g. not fully loaded slice, and/or UPF selection. The procedure assumes that the UE has already registered on the AMF thus unless the UE is emergency registered the AMF has already retrieved the user subscription data from the UDM.

During the PDU session establishment procedure, the AMF may determine that the message corresponds to a request for a new PDU session based on that request type indicates "initial request" and that the PDU session ID is not used for any existing PDU Session(s) of the UE.

If the NAS message does not contain an S-NSSAI, the AMF may determine a default S-NSSAI of the HPLMN for the requested PDU session either according to the UE subscription, if it contains only one default S-NSSAI, or based on operator policy, considering the NSRP if available and further, in the case of LBO, an S-NSSAI of the serving PLMN considering the NSRP if available which matches the S-NSSAI of the HPLMN.

If dynamic PCC is to be used for the PDU session, the SMF performs PCF selection as described in TS 23.501.

The SMF may perform NSRP policy association establishment procedure to establish an NSRP policy association with the PCF and get the NSRP related slice availability information for the PDU session along with the NSRP. The GPSI shall be included if available at SMF.

If the request type is "existing PDU session", the SMF may provide information on the policy control request trigger condition(s) that have been met by an SMF initiated NSRP policy association modification procedure. The PCF may provide NSRP policy information defined in to SMF. The purpose of this step is to receive PCC rules before selecting UPF. If PCC rules are not needed as input for UPF selection, this step may be performed after UPF selection.

In the UPF selection, if the request type is "initial request", the SMF may select an SSC mode for the PDU Session as described in TS 23.501. The SMF also selects one or more UPFs as needed as described in TS 23.501. The SMF may consider the received NSRP and/or UPF availability based on analytics during UPF selection.

The SMF may perform an SMF initiated SM policy and NSRP association modification procedure as defined in TS 23.502 to provide information on the policy control request trigger condition(s) that have been met.

If request type is "initial request" and dynamic PCC is deployed and PDU session type is IPv4 or IPv6 or IPv4v6, the SMF may notify the PCF, if the policy control request trigger condition is met, with the allocated UE IP address/prefix(es). Regarding the network slice limitations, if the SMF based on the analytics information finds that slice limitations are about to be reached,

the SMF may update the PCF with the SMF slice specific availability, which supports the PCF to update the corresponding NSRP.

The PCF may provide updated policies to the SMF including the NSRP, excluding or including slices for the NSRP. The PCF may provide policy information defined in TS 23.502 and in TS 23.503 to SMF.

If request type indicates "initial request", the SMF initiates an N4 session establishment procedure with the selected UPF, otherwise it initiates an N4 session modification procedure with the selected UPF.

The PCF may perform an NSRP policy association establishment procedure to establish an NSRP policy association with the UPF and get the NSRP related slice availability and/or limitation information for the PDU session, if the NSRP is not available at the UPF or obsolete. The slice identification, TAIs and DNN information can be included if available in the UPF. The UPF may provide information on the policy control request trigger condition(s) that have been met by an UPF initiated NSRP policy association modification procedure. The PCF may provide NSRP policy information defined in to UPF.

The SMF sends to AMF for example the Namf_Communication_N1N2 MessageTransfer (PDU Session ID, N2 SM information (PDU Session ID, QoS flow ID(s) (QFI(s)), QoS Profile(s), core network (CN) Tunnel Info, S-NSSAI from the Allowed NSSAI considering the NSRP, Session-aggregated maximum bite rate (AMBR), PDU Session Type, User Plane Security Enforcement information, UE Integrity Protection Maximum Data Rate, Redundancy Sequence Number (RSN), N1 SM container (PDU Session Establishment Accept ([QoS Rule(s) and QoS Flow level QoS parameters if needed for the QoS Flow(s) associated with the QoS rule(s)], selected service and session continuity (SSC) mode, S-NSSAI(s), DNN, allocated IPv4 address, interface identifier, Session-AMBR, selected PDU Session Type, [Reflective QoS Timer] (if available), [P-CSCF address(es)], [Control Plane Only indicator], [Header Compression Configuration], [Always-on PDU Session Granted], [Small Data Rate Control parameters], [Small Data Rate Control Status], [Network Slice Related Policy - Optionally]))). If multiple UPFs are used for the PDU Session, the CN Tunnel Info contain tunnel information related with the UPF that terminates N3.

NSRP assisted AMF based network slice operation

UE configuration update procedure for access and mobility management related parameters considering NSRP

The AMF may determine the necessity of UE configuration change due to various reasons, e.g. UE mobility change, network policy, reception of subscriber data update notification from UDM, change of network slice configuration, need to assign PLMN-assigned UE radio capability ID, and the AMF need to consider the NSRP configured by the PCF during every slice related UE configuration change to configure a slice identification information in the UE corresponding to any relatively available network slice considering the network slice limitation and/or control aspects.

The AMF may check whether network slice configuration needs to be updated by using for example the Nnssf_NSSelection_Get service operation and in such case the AMF compares the stored NSRP vs the NSRP information with the output from the NSSF to decide whether an update of the UE is required.

The AMF may determine the slice information based on the proposed NSRP when there is a need to change the slice related UE configuration.

The AMF may send UE configuration update command containing one or more UE parameters such as configuration update indication, 5G-GUTI, TAI list, slice information based on the available NSRP, e.g. PCF provided NSRP, including allowed NSSAI, mapping of allowed NSSAI, configured NSSAI for the serving PLMN, mapping of configured NSSAI, rejected S-NSSAIs and other parameters. In case of roaming scenario, a derived NSRP can be shared between the serving and the home PCFs to enable available slice selection.

The UE may store the updated slice information and use it in the upcoming service request messages. For example if the UE configuration update indication requires acknowledgement of the UE configuration update command, then the UE shall send a UE configuration update complete message to the AMF.

The AMF may also use for example the Nudm_SDM_Info service operation to provide an acknowledgment to UDM that the UE received the network slicing subscription change indication, if this was indicated, and act upon it. Further, steps may be performed according to the steps 2c to 4 in TS 23.502 UE configuration update procedure for access and mobility management related parameters.

NSRP assisted network slice selection by NSSF

UE configuration update procedure for NSRP information update

Whenever the PCF finds any UE associated network slice unavailable based on the self-derived/operator provided NF slice related policy information and through any other means, e.g. analytics information, the PCF may derive the updated/new NSSP with s-NSSAI(s) to provide UE with an alternative available network slice for uninterrupted service.

The PCF may decide to update NSSP based on triggering conditions such as an initial registration, re-registration, and registration with 5GS when the UE moves from EPS to 5GS. The PCF may compare the slice information from the list of available NSRPs with the NSSP configured in the UEs to determine whether s-NSSAI in the NSSP related to the URSP rule need to be updated to use the available slices.

Alternatively, the AMF (NSSF may also initiate the new configured NSSAI to the AMF) may trigger the UE configuration update procedure to provide the new configured NSSAI for the serving PLMN, based on the new NSRP received from the V-PCF.

The PCF may use the following procedure to update the NSSP in case of slice unavailability issues or triggering conditions in the PCF.

The PCF may decide to update UE policy i.e. S-NSSAI(s) in the NSSP of the URSP rule if a slice is considered unavailable based on the NSRP configured in the PCF during the triggering conditions such as an initial registration, registration with 5GS when the UE moves from EPS to 5GS.

Alternatively, UE configuration update procedure may be triggered by the PCF when a configured slice in UE is considered unavailable by the PCF based on the configured NSRP and the generated slice availability information from the NF Slice analytics provided by the NWDAF.

The PCF may invoke for example Namf_Communication_N1N2MessageTransfer service operation provided by the AMF. The message may include SUPI, UE policy container with the new NSSP with rule identification information (Rule ID) and the S-NSSAIs.

If the UE is in CM-CONNECTED over 3GPP access or non-3GPP access, the AMF may transfer transparently the UE policy container, including e.g. new NSSP with rule identification information (rule ID) and the S-NSSAIs, received from the PCF to the UE.

The UE may update the NSSP, with e.g. the rule identification information (rule ID) and the S-NSSAIs, in the UE policy provided by the PCF and may send the result to the AMF.

If the AMF received the UE Policy container with the result of the delivery of updated NSSP rule ID(s) and the PCF subscribed to be notified of the reception of the UE policy container then the AMF forwards the response of the UE to the PCF using Namf_N1MessageNotify along with the delivered rule ID(s).

The PCF may maintain the latest list of policy Set IDs (PSIs) delivered to the UE and updates the latest list of PSIs in the UDR by invoking for example Nudr_DM_Update (SUPI, policy data, policy set entry, updated PSI data) service operation. The policy data may contain the URSP rule identification information (rule ID) and the S-NSSAIs corresponding to the NSSP.

The first network entity 100 herein may be denoted as a policy control function (PCF) and/or a network data analysis function (NWDAF), or any network element which control the enforcement of the network slice based on SLA. The PCF and/or NWDAF may be functions configured for communication in 3GPP related LTE and LTE-Advanced, in WiMAX and its evolution, and in fifth generation wireless technologies, such as new radio (NR).

The second network entity 300 herein may be denoted as an access and mobility management function (AMF), a network slice selection function (NSSF), a session management function (SMF), and/or another network function (NF). The AMF, NSSF, SMF, and/or NF may be functions configured for communication in 3GPP related LTE and LTE-Advanced, in WiMAX and its evolution, and in fifth generation wireless technologies, such as new radio (NR).

The client device 600 herein, may be denoted as a user device, a User Equipment (UE), a mobile station, an internet of things (IoT) device, a sensor device, a wireless terminal and/or a mobile terminal, is enabled to communicate wirelessly in a wireless communication system, sometimes also referred to as a cellular radio system. The UEs may further be referred to as mobile telephones, cellular telephones, computer tablets or laptops with wireless capability. The UEs in this context may be, for example, portable, pocket-storable, hand-held, computer-comprised, or vehicle-mounted mobile devices, enabled to communicate voice and/or data, via the radio access network, with another entity, such as another receiver or a server.

The UE can be a Station (STA), which is any device that contains an IEEE 802.11-conformant Media Access Control (MAC) and Physical Layer (PHY) interface to the Wireless Medium

(WM). The UE may also be configured for communication in 3GPP related LTE and LTE-Advanced, in WiMAX and its evolution, and in 5G technologies, such as New Radio.

Furthermore, any method according to embodiments of the disclosure may be implemented in a computer program, having code means, which when run by processing means causes the processing means to execute the steps of the method. The computer program is included in a computer readable medium of a computer program product. The computer readable medium may comprise essentially any memory, such as a ROM (Read-Only Memory), a PROM (Programmable Read-Only Memory), an EPROM (Erasable PROM), a Flash memory, an EEPROM (Electrically Erasable PROM), or a hard disk drive.

Moreover, it is realized by the skilled person that embodiments of the first network entity 100, the second network entity 300, and the client device 600 comprises the necessary communication capabilities in the form of e.g., functions, means, units, elements, etc., for performing the solution. Examples of other such means, units, elements and functions comprise: processors, memory, buffers, control logic, encoders, decoders, rate matchers, de-rate matchers, mapping units, multipliers, decision units, selecting units, switches, interleavers, de-interleavers, modulators, demodulators, inputs, outputs, antennas, amplifiers, receiver units, transmitter units, DSPs, MSDs, TCM encoder, TCM decoder, power supply units, power feeders, communication interfaces, communication protocols, etc. which are suitably arranged together for performing the solution.

Especially, the processor(s) of the first network entity 100, the second network entity 300, and the client device 600 may comprise, e.g., one or more instances of a Central Processing Unit (CPU), a processing unit, a processing circuit, a processor, an Application Specific Integrated Circuit (ASIC), a microprocessor, or other processing logic that may interpret and execute instructions. The expression “processor” may thus represent a processing circuitry comprising a plurality of processing circuits, such as, e.g., any, some or all of the ones mentioned above. The processing circuitry may further perform data processing functions for inputting, outputting, and processing of data comprising data buffering and device control functions, such as call processing control, user interface control, or the like.

Finally, it should be understood that the disclosure is not limited to the embodiments described above, but also relates to and incorporates all embodiments within the scope of the appended independent claims.

CLAIMS

1. A first network entity (100) for a communication system (500), the first network entity (100) being configured to

receive a network slice information request, NSIR, (510) from a second network entity (300), wherein the NSIR (510) indicates at least one of a network slice information and/or a client device identity, ID;

obtain a network slice information notification, NSIN, (520) in response to the reception of the NSIR (510), wherein the NSIN (520) indicates a network slice control information; and

transmit the obtained NSIN (520) to the second network entity (300).

2. The first network entity (100) according to claim 1, wherein the network slice information is at least one of: a network function ID, a network slice instance ID, a network slice type, a network slice subscription type, and a single network slice selection assistance information.

3. The first network entity (100) according to claim 1 or 2, wherein the network slice control information comprises at least part of the network slice information, and

the network slice control information further comprises a network slice policy information, wherein the network slice policy information indicates at least one of: a network slice status information, slice identification information, a maximum allowed PDU sessions per network slice, a maximum number of allowed client devices per network slice, a maximum uplink data rate supported for a client device, and a maximum downlink data rate supported for a client device.

4. The first network entity (100) according to claim 3, wherein the network slice status information has any of the attributes: available during a validity period, availability level, permanently not available, or temporarily not available.

5. The first network entity (100) according to any one of the preceding claims, wherein obtain the NSIN (520) comprises

fetch network slice related policy information from a policy control function, PCF, or a unified data repository, UDR, upon receiving the NSIR (510) from the second network entity (300).

6. The first network entity (100) according to any one of the preceding claims, configured to

receive a configuration message (530) from an Operation Administration and Management, OAM, previous to receiving the NSIR (510) from the second network entity (300), wherein the configuration message (530) indicates a network slice policy.

7. The first network entity (100) according to any one of the preceding claims, wherein the first network entity (100) comprises: a policy control function, PCF, and/or a network data analysis function, NWDAF.

8. A second network entity (300) for a communication system (500), the second network entity (300) being configured to

send a NSIR (510) to a first network entity (100), wherein the NSIR (510) indicates least one of a network slice information and/or a client device ID;

receive a NSIN (520) from the first network entity (100) in response to the transmission of the NSIR (510), wherein the NSIN (520) indicates a network slice control information.

9. The second network entity (300) according to claim 8, wherein the network slice information is at least one of: a network function ID, a network slice instance ID, a network slice type, a network slice subscription type, and a single network slice selection assistance information.

10. The second network entity (300) according to claim 8 or 9, wherein the received network slice control information comprises at least part of the network slice information, and
the network slice control information further comprises a network slice policy information, wherein the network slice policy information indicates at least one of: a network slice status information, slice identification information, a maximum allowed PDU sessions per network slice, a maximum number of allowed client devices per network slice, a maximum uplink data rate supported for a client device, and a maximum downlink data rate supported for a client device.

11. The second network entity (300) according to claim 10, wherein the network slice status information has any of the attributes: available during a validity period, availability level, permanently not available, or temporarily not available.

12. The second network entity (300) according to any one of claims 8 to 11, wherein second network entity (300) is an access and mobility management function, AMF, or a network slice selection function, NSSF, and further configured to

determine allowed network slice selection assistance information, NSSAI, based on the received NSIN (520).

13. The second network entity (300) according to any one of claims 8 to 12, wherein second network entity (300) is an AMF or a NSSF, and further configured to

determine a configured NSSAI, based on based on the received NSIN (520).

14. The second network entity (300) according to any one of claims 8 to 13, wherein the second network entity (300) is a session management function, SMF, and further configured to

select a user plane function, UPF, for a protocol data unit, PDU, session based on the received NSIN (520).

15. A client device (600) for a communication system (500), the client device (600) being configured to

obtain a first control message (540) indicating a first network slice information;

receive a second control message (550) from a first network entity (100), wherein the second control message (550) indicates a second network slice information; and

select a network slice for a subsequent service based on the first network slice information and the second network slice information.

16. The client device (600) according to claim 15, wherein the second network slice information is a network slice unavailability notification.

17. The client device (600) according to claim 15 or 16, wherein receive the second control message (550) comprises

receive the second control message (550) during initial registration procedure, service establishing procedure, or a location update procedure.

18. The client device (600) according to any one of claims 15 to 17, wherein the second network slice information comprises at least one of: a rule ID with an alternate S-NSSAI, an allowed NSSAI, and a configured NSSAI.

19. The client device (600) according to any one of claims 15 to 18, wherein the client device (600) is configured to any of: an active state, an inactive state or an idle state.

20. The client device (600) according to any one of the preceding claims, wherein the second control message (X) is received in a NAS message, a client device policy container, or a radio resource control message when the client device (600) is in an active state.

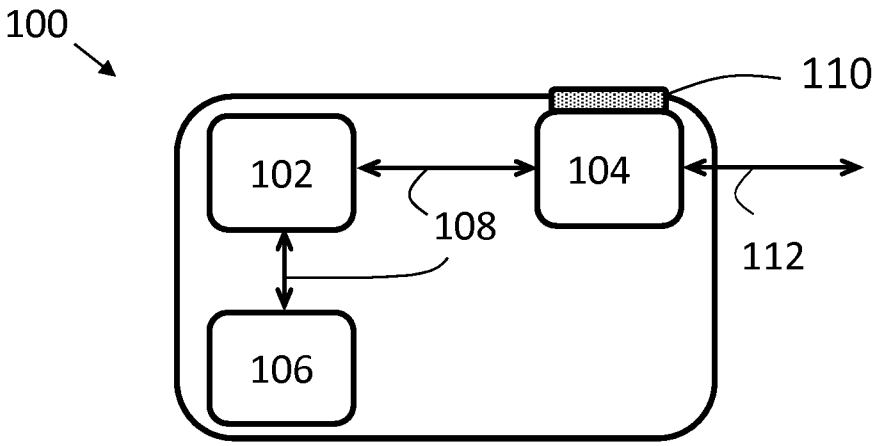

Fig. 1

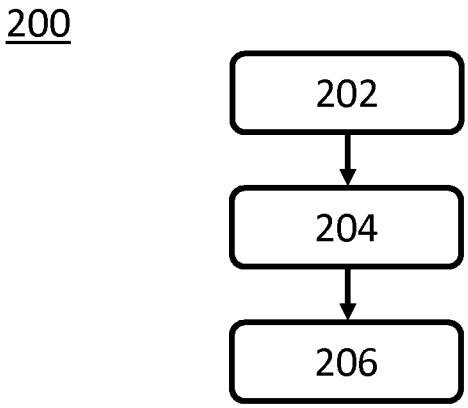

Fig. 2

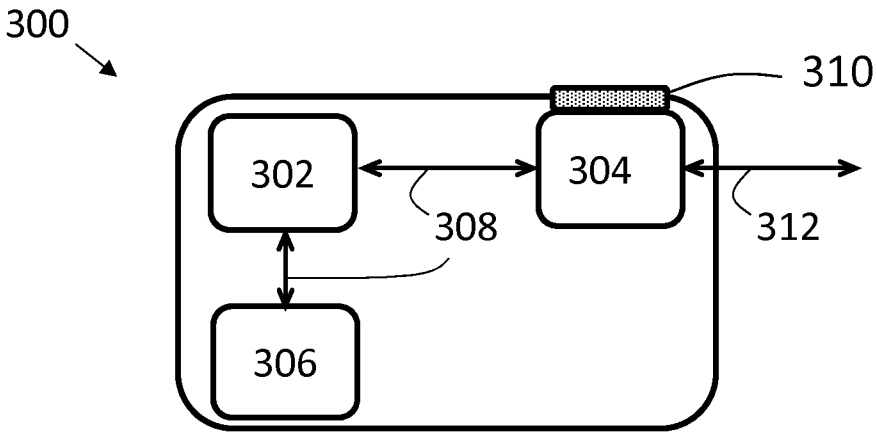

Fig. 3

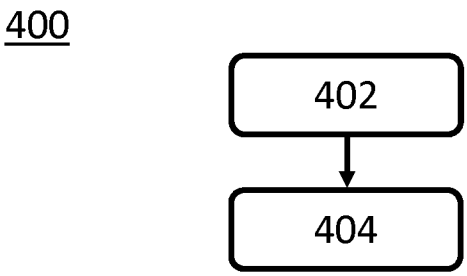

Fig. 4

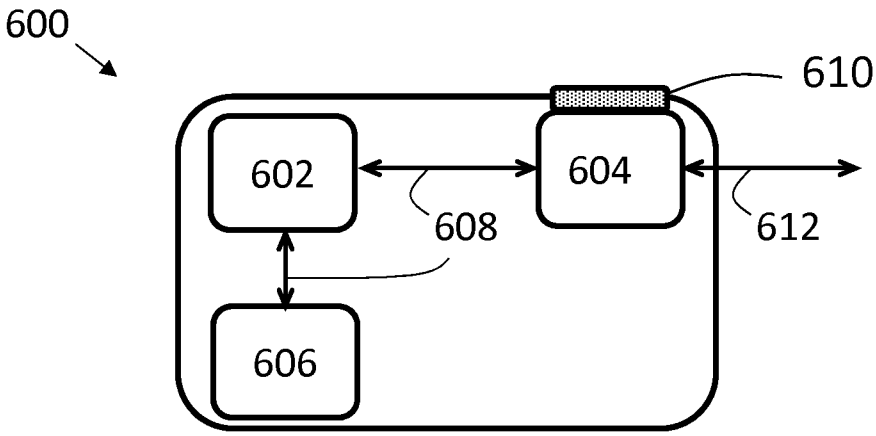

Fig. 5

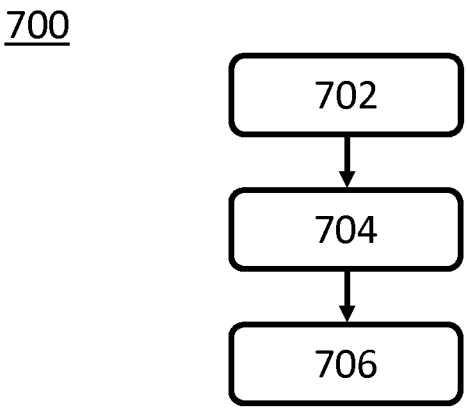

Fig. 6

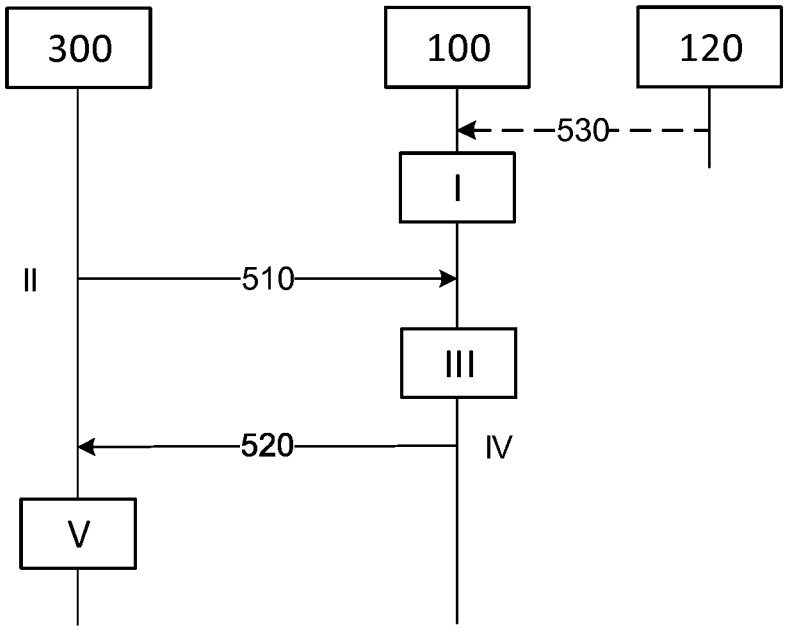

Fig. 7

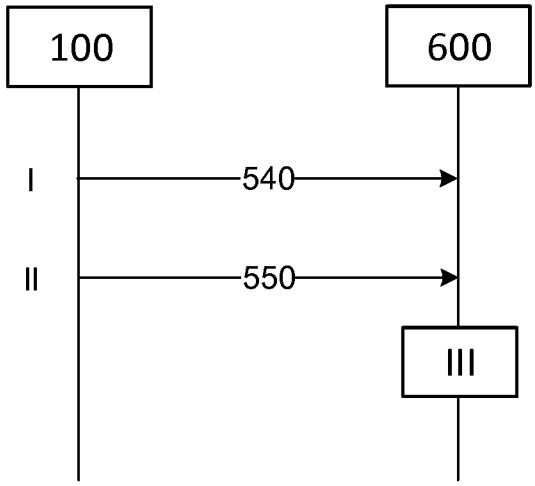

Fig. 8

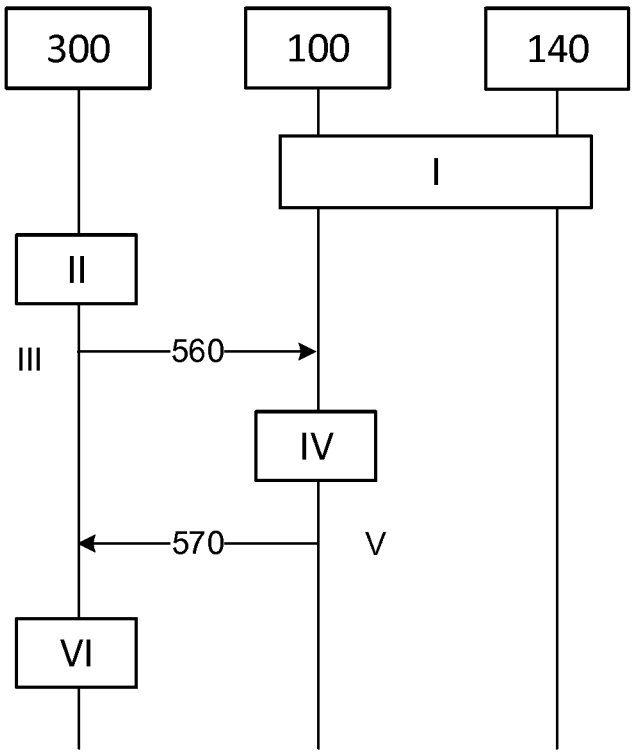

Fig. 9

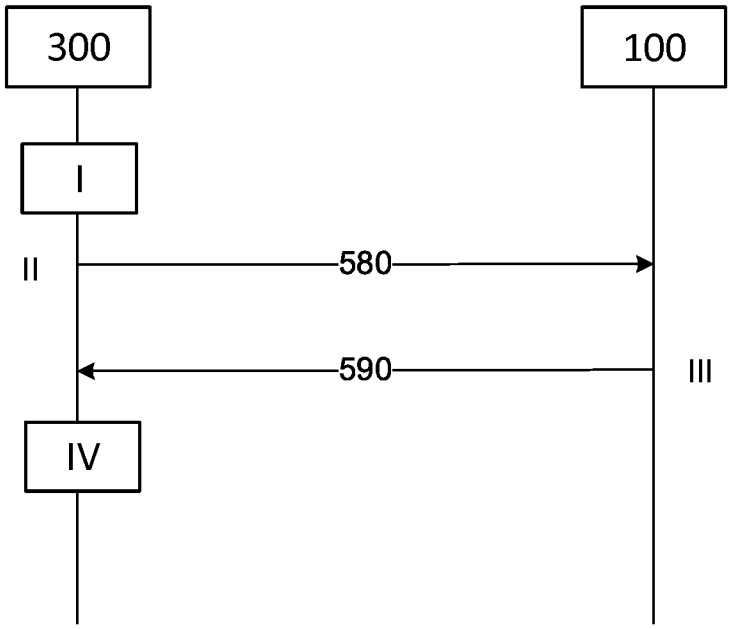

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2019/077107

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W48/18
ADD. H04W60/00 H04W8/18

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 2018/112745 A1 (HUAWEI TECH CO LTD [CN]) 28 June 2018 (2018-06-28) abstract paragraphs [0049] - [0094] -----	1-14
X	US 2018/317157 A1 (BAEK YOUNGKYO [KR] ET AL) 1 November 2018 (2018-11-01)	1-3, 8-10, 12-14
A	abstract paragraphs [0056] - [0074], [0172] - [0190] -----	4-7,11
X	WO 2019/154295 A1 (HUAWEI TECH CO LTD [CN]) 15 August 2019 (2019-08-15)	1-3, 7-10, 12-14
A	abstract paragraphs [0153] - [0202] -----	4-6,11
	-/--	

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 July 2020	21/07/2020

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Valpondi Hereza, F

3

Form PCT/ISA/210 (second sheet) (April 2005)

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	"3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; System Architecture for the 5G System (5GS); Stage 2 (Release 15)", 3GPP STANDARD; TECHNICAL SPECIFICATION; 3GPP TS 23.501, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. SA WG2, no. V15.7.0 24 September 2019 (2019-09-24), pages 1-243, XP051784668, Retrieved from the Internet: URL:ftp://ftp.3gpp.org/Specs/archive/23_series/23.501/23501-f70.zip 23501-f70.doc [retrieved on 2019-09-24]	15,17-20
Y	abstract section 5.15 - pages 136 to 151	16

X	NOKIA ET AL: "Pseudo-CR on general aspects of network slicing in 5GS", 3GPP DRAFT; C1-172370, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; F-06921 SOPHIA-ANTIPOLIS CEDEX ; FRANCE , vol. CT WG1, no. Zhangjiajie, P.R of China; 20170515 - 20170519 14 May 2017 (2017-05-14), XP051270591, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/Meetings_3GPP_SYNC/CT1/Docs/ [retrieved on 2017-05-14]	15-20
Y	the whole document	16

	-/--	

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CHINA MOBILE ET AL: "Solution for Key Issue 4 to assist slice resource allocation and adjustment", 3GPP DRAFT; S2-188031- SOLUTION FOR KEY ISSUE 4 TO ASSIST SLICE RESOURCE ALLOCATION AND ADJUSTMENT - V3, 3RD GENERATION PARTNERSHIP PROJECT (3GPP), MOBILE COMPETENCE CENTRE ; 650, ROUTE DES LUCIOLES ; , vol. SA WG2, no. Sophia Antipolis, France; 20180820 - 20180824 14 August 2018 (2018-08-14), XP051502921, Retrieved from the Internet: URL:http://www.3gpp.org/ftp/tsg%5Fsa/WG2%5FArch/TSGS2%5F128BIS%5FSophia%5FAntipolis/Docs/S2%2D188031%2Ezip [retrieved on 2018-08-14] the whole document -----	1-14
A	KR 2018 0120553 A (SAMSUNG ELECTRONICS CO LTD [KR]) 6 November 2018 (2018-11-06) abstract paragraphs [0024] - [0043] -----	15-20

INTERNATIONAL SEARCH REPORT

International application No.
PCT/EP2019/077107

Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fees, this Authority did not invite payment of additional fees.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.

☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-14

   Second network entity transmitting a network slice information request, NSIR, to a first network entity. The request comprises network slice information and/or a client device ID. Upon reception of the request, the first network entity will obtain a network slice information notification, NSIN, comprising network slice control information (i.e. policies) and transmit it to the requesting second network entity.

   ---

2. claims: 15-20

   Client device receiving two different network slice informations. Based on said information, the client device will select an appropriate network slice for a subsequent service.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/EP2019/077107

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2018112745 A1	28-06-2018	NONE	
US 2018317157 A1	01-11-2018	US 2018317157 A1	01-11-2018
		WO 2018199649 A1	01-11-2018
WO 2019154295 A1	15-08-2019	CN 110120879 A	13-08-2019
		WO 2019154295 A1	15-08-2019
KR 20180120553 A	06-11-2018	CN 110547003 A	06-12-2019
		EP 3574693 A1	04-12-2019
		KR 20180120553 A	06-11-2018