Guidelines on registration and onboarding for media production equipment over 5G NPNs

5G-MAG has studied deployment scenarios for live media production using Non-Public Networks (NPNs), both stand-alone and within public networks.

The 5G-MAG report Towards a comprehensive 5G-based toolbox for live media production presents high-level scenarios involving the use of 5G devices for media applications. Before using them, devices need to first gain access to the 5G network though several registration and authentication procedures. After use, devices should be "de-registered", i.e. have their access rights revoked.

This report provides:

- information on the registration, authentication and onboarding procedures for devices in NPNs; and
- guidelines for users and operators of 5G NPNs in relation to aspects such as network identifiers and storage, and local and remote provisioning of credentials.

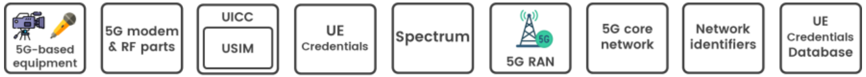
Contents

Characteristics of network equipment and devices

Different types of wireless equipment coexist today. Cameras and audio equipment typically rely on unidirectional links, implying the use of dedicated transmitters and receivers. Wireless cameras have evolved to support modems that enable bidirectional connectivity using LTE/5G.

Commercial smartphones are also increasingly used either for capture or monitoring applications. While some devices have large displays, often with touchscreen capabilities, others may have only a small display or none at all and only simple buttons.

Existing setups that leverage LTE/5G connectivity rely on procedures related to the public network, with traffic treated over-the-top. NPNs, which can be **configured as stand-alone (SNPNs) or integrated with public networks (PNI-NPNs)**, present some challenges and opportunities related to the registration and onboarding of devices.



The following components are relevant on the device side:

1. **5G-based equipment** refers to the media equipment – for acquisition, control, monitoring, and auxiliary processes – that can be connected to the 5G network.
2. **5G modem and RF (radio frequency) parts** refers to the components required to establish 5G mobile connectivity.
3. The **USIM (Universal Subscriber Identity Module)** is the entity that holds subscriber-related information and implements the security function that handles authentication and cryptography aspects on user devices. The USIM can be provisioned and updated remotely. The USIM is hosted in a **UICC (Universal Integrated Circuit Card)**, which may (e.g. a SIM card) or may not be removable (e.g. an eSIM or iSIM).
4. The **UE (User Equipment) credentials** are used by the device for authentication to access a network. They contain information related to the identification of the network as well as the device itself.

The following components are relevant at the network side:

5. The **RAN (radio access network)** consists, in particular, of the nodes providing wireless connectivity.
6. The **core network** allocates a series of network functions, including those relevant for the access and authentication of devices.
7. The **UE credentials database** stores information about the devices authorized to connect to the network.

Deployment scenarios and operational aspects

In the sections that follow we consider some typical media deployment scenarios for non-public networks, whether SNPNs or PNI-NPNs. Scenarios 1 to 4 concern the former, while scenario 5 addresses the latter.

For SNPNs, two deployment types are considered: self-operated networks deployed where there is no public network or where an isolated SNPN is favoured; and multi-tenant networks, such as in venues offering SNPNs that can be used temporarily by different tenants.

For PNI-NPNs, the deployment model considered is by means of configuring network slicing.

Key issues identified

Two key issues have been identified in the processes for onboarding devices in SNPNs**.** They relate to Scenario 4 (multi-tenant installation managed by a third party), and the network configuration and procedures for "device onboarding for SNPNs with UE without pre-provisioned credentials" (with additional details provided in Annex C):

1. Remote provisioning of credentials to UICCs of devices deployed in SNPNs may not be feasible using the GSMA Public Key Infrastructure (PKI) and respective root keys due to the requirement for certification. Coexistence of GSMA PKI root keys and independent eSIM Certificate Authority (CA) root keys is not possible on a single GSMA compliant UICC.
2. There is no standardized provisioning scheme for non-UICC-based credentials (i.e., default UE credentials). This is a gap in the 5G ecosystem, out of 3GPP scope, and currently not addressed by other bodies or interest groups.

Scenario 1. Self-operated fixed or nomadic installation with pre-configured equipment

The following considerations are made:

- **5G-based equipment**: owned by the media company; comes with a UICC module.
- **UICC**: configured by the media company, either by means of pre-provisioned removeable UICCs or by uploading the relevant data in a non-removable UICC.
- **UE credentials**: provisioned by the media company, which has also pre-configured the network so that equipment can be registered, authorized, and authenticated.
- **Network identifiers**: provided by the media company, which has obtained a licence to operate an SNPN.
- **RAN** and **core network**: deployed by the media company.
- **Spectrum**: the media company has acquired a licence to operate the network in a given spectrum band.

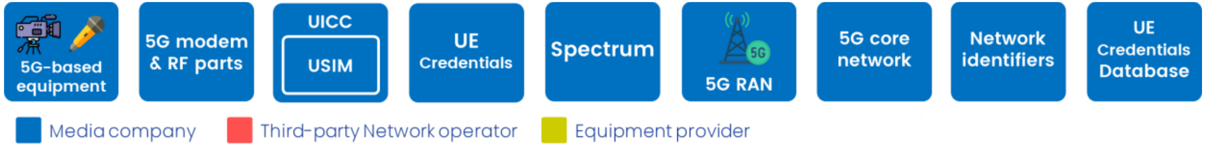
Key aspects to be considered before operation:

- The network is configured by the media company with its SNPN identifiers.
- The network broadcasts the SNPN identifiers, making itself visible to devices.
- Devices are provisioned by the media company with credentials, which include the relevant network identifiers. This can be done either by introducing a removable UICC in the device or via a software download.
- The network is selected either manually (requires a touchscreen or other appropriate interface on the equipment) or automatically.

Key aspects to be considered after operation:

- Equipment may stay registered in the network for future use or can be de-registered by either removing the credentials from the database or removing the USIM from the device.

Details on procedures to address this scenario are provided under Annex A.



5G-based equipment | 5G modem & RF parts | UICC USIM | UE Credentials | Spectrum | 5G RAN | 5G core network | Network identifiers | UE Credentials Database

🟦 Media company 🟥 Third-party Network operator 🟨 Equipment provider

Scenario 2. Self-operated fixed or nomadic installation with third-party equipment

This scenario is an evolution of scenario A with the following considerations:

- **5G-based equipment**: rented by the media company from a third-party provider; the equipment comes with a UICC module.
- **UICC**: can be pre-configured by the media company, either by means of pre-provisioned removeable UICCs or by uploading the relevant data in a non-removable UICC. An alternative whereby equipment could be authorized and authenticated by means of an external server, provided by the media equipment provider, would ease the setup process.
- **UE credentials**: should be provisioned by the media equipment provider by means of an external credentials server.
- **Network identifiers**: provided by the media company, which has obtained an operator licence.
- **RAN** and **core network**: deployed by the media company.
- **Spectrum**: the media company has acquired a spectrum licence.

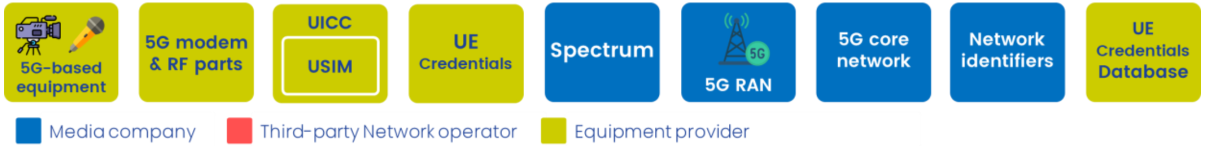
Key aspects to be considered before operation:

- The media company ensures access to equipment credentials from an external credentials server.
- The SNPN is configured so that it can be identified as able to register devices with credentials provided by an external entity.
- The network broadcasts the SNPN identifiers making itself visible.
- Devices should be provisioned by the media company with credentials, which include network identifiers. This can be done by introducing a UICC in the device or via a software download.
- The network should be selected either manually (with a touchscreen or other appropriate interface on the equipment) or automatically.

Key aspects to be considered after operation:

- Equipment should be de-registered by removing access to the external credentials server or by removing the USIM from the device.

Details on procedures to address this scenario are provided under Annex B.



Scenario 3. Multi-tenant installation with shared network infrastructure

A media production company would like to use an NPN already installed at a venue. The venue owner provides connectivity and allows third parties to deploy event-specific RANs while the core network could be deployed in the cloud alongside other processes. The following considerations are made:

- **5G-based equipment**: owned by the media company; comes with a UICC module.
- **UICC**: can be pre-configured by the media company in collaboration with the NPN operator. However, an alternative in which equipment can be authorized and authenticated without the need for pre-provisioning steps is favoured.
- **UE credentials**: The media company has provisioned the credentials but is unable to configure the core network of the SNPN operator. To avoid handing credentials to the network operator, the network will remotely access them from an external server.
- **Network identifiers**: provided by the media company with a licence.
- **RAN**: deployed by the media company.
- **Core network**: deployed by the venue operator.
- **Spectrum**: the media company has acquired a licence that its RAN will use.

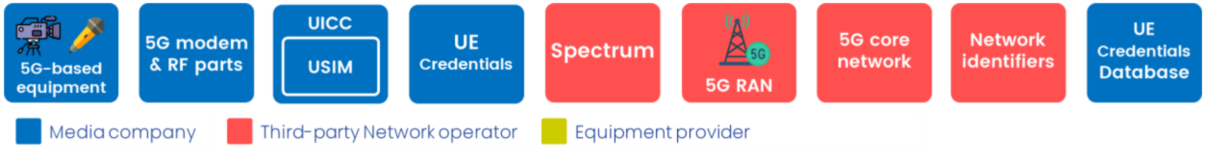
Key aspects to be considered before operation:

- The network is configured with the corresponding SNPN identifiers.
- The network broadcasts the SNPN identifiers making itself visible.
- The media company acquires credentials from the network. Devices shall be provisioned with them, including the relevant network identifiers. This can be done by introducing a UICC in the device or via a software download in agreement with the operator.
- The network shall be selected either manually (with a touchscreen or other appropriate interface on the equipment) or automatically.

Key aspects to be considered after operation:

- Equipment shall be de-registered by removing the USIM from the device.

Details on procedures to address this scenario are provided under Annex A.



5G-based equipment

5G modem & RF parts

UICC

USIM

UE Credentials

Spectrum

5G RAN

5G core network

Network identifiers

UE Credentials Database

🟦 Media company 🟥 Third-party Network operator 🟨 Equipment provider

Scenario 4. Multi-tenant installation managed by a third party

A media production company would like to use an SNPN already installed at a venue. The venue owner allows third parties to use the NPN at specific events. The following consideration are made:

- **5G-based equipment**: owned by the media company; comes with a UICC module.
- **UICC**: does not contain any USIM profile as this is expected to be provisioned by the network during the onboarding process.
- **UE credentials**: are unknown by the media company as details are in the domain of the SNPN operator.
- **Network identifiers**: provided by the venue operator since the network should aid the onboarding of equipment for which credentials have not been pre-provisioned.
- **RAN** and **core network**: deployed by the venue operator
- **Spectrum**: the media company uses spectrum owned by the venue owner.

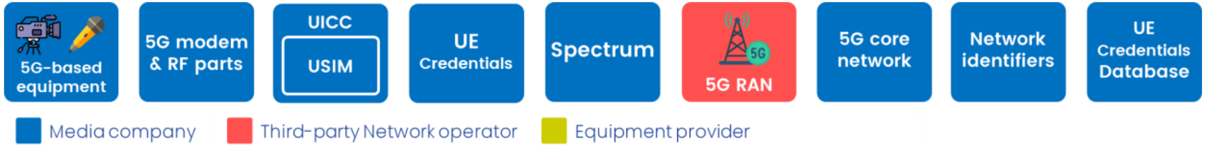
Key aspects to be considered before operation:

- The SNPN operator configures an onboarding network that will be used to provision devices authorized to access the SNPN.
- The SNPN operator enables a provisioning server that contains credentials of the SNPN that will be remotely uploaded to devices.
- The network broadcasts the onboarding network identifiers and the SNPN identifiers making itself visible both during the onboarding process and during access and registration to the SNPN.
- Devices contain default credentials that will be used during the onboarding process.
- The network shall be selected either manually (with a touchscreen or other appropriate interface on the equipment) or automatically.

Key aspects to be considered after operation:

- Equipment may stay registered in the network for future use or be de-registered by either removing the credentials from the database or removing the UICC from the device.

Details on procedures to address this scenario are provided under Annex C.


5G-based equipment

5G modem & RF parts

UICC

USIM

UE Credentials

Spectrum

5G RAN

5G core network

Network identifiers

UE Credentials Database

🟦 Media company 🟥 Third-party Network operator 🟨 Equipment provider

Scenario 5. Media production using a public 5G network (PNI-NPN) with network slicing

A media production company would like to use a public network, taking advantage of network slicing functionalities for relevant operations. The following assumptions are considered:

- **5G-based equipment**: owned by the media company; comes with a UICC module.
- **UICC**: provisioned by the network operator either manually or remotely.
- **UE credentials**: provided by the public network operator.
- **Network identifiers**: provided by the public network operator.
- **RAN** and **core network**: deployed by the public network operator, which is responsible for providing the desired network functionalities in agreement with the media production company.
- **Spectrum**: the media company uses spectrum of the public network operator.

Key aspects to be considered before operation:

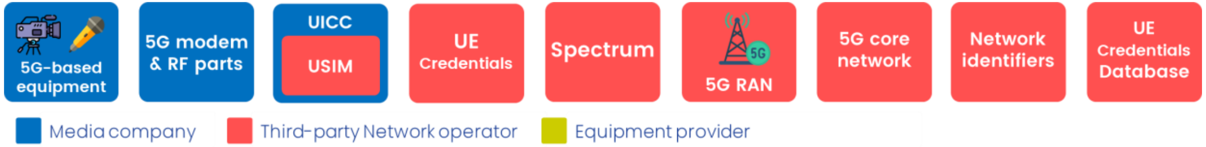
- The public network operator shall provide the media company with the USIM data.
- The public network operator shall provide network slicing functionalities as agreed with the media company.

Key aspects to be considered after operation:

- Equipment may stay registered in the network for future use or be de-registered by either removing the credentials from the database or removing the UICC from the device.

Details on procedures to address this scenario with pre-configured equipment are provided under Annex D.

Details on procedures to address this scenario with remote provisioning of credentials are provided under Annex E.



5G-based equipment

5G modem & RF parts

UICC

USIM

UE Credentials

Spectrum

5G RAN

5G core network

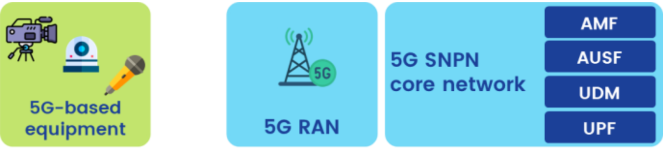
Network identifiers

UE Credentials Database

🟦 Media company 🟥 Third-party Network operator 🟨 Equipment provider

Annexes: Network configuration and detailed procedures

A) Device registration for SNPNs with UE credentials available within the SNPN



This is a list of configuration aspects to be considered before using equipment in an SNPN.

1. Identification of the SNPN

An SNPN is identified by the combination of a Public Land Mobile Network Identifier (**PLMN ID**) and a Network Identifier (**NID**). Refer to 3GPP TS 23.501 [1] Clause 5.30.2.1 for more information.

About the use of PLMN ID

A PLMN ID is a combination of Mobile Country Code (MCC) and Mobile Network Code (MNC).

- A PLMN ID can be one from the selected range reserved by the ITU for private networks. For example, MCC 999 corresponds to a worldwide general assignment without the need for a permit. Coordination may be handled using a directory of operators that use such assignments. More details at: http://handle.itu.int/11.1002/pub/810cad63-en.
- A PLMN ID of an existing operator may be used for SNPN operation.
- New PLMN IDs for SNPNs may be regulated by national Administrations. For example:
  - In Germany, BNetzA has defined MCC 262 and MNC 98 for NPNs. More details at: https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Nummerierung/Campusnetze/artikel.html
  - In Norway, Nkom has established MCC 242 with MNCs 70 to 75 for local, NPN. More details at: https://nkom.no/telefoni-og-telefonnummer/mobile-nettverkskoder-for-ikke-offentlige-nett-og-testformal#gjennomfring_og_sknad

About the use of NID

A NID is a combination of an Assignment Mode (AM) and NID value. It supports different assignment models:

- AM 0 is used in combination with an IANA Private Enterprise Number (PEN) so that the NID is globally unique and managed by IANA.
  - The list of PENs can be found here: https://www.iana.org/assignments/enterprise-numbers/. PENs can be requested using this form: https://pen.iana.org/pen/PenApplication.page

- AM 1 is a self-assignment, with NIDs chosen individually at deployment time. This assignment mode may be subject to clashes at the time of deployment.
- AM 2 makes the combination of a PLMN ID and a NID globally unique. Examples of usage include:
    - Networks using a CBRS-NID. More details at: https://ongoalliance.org/wp-content/uploads/2019/01/ONGO-TR-0100-V1.2.2-.pdf
    - In Germany, the use of AM 2 in combination with PLMN ID 262 98 creates a national number resource managed by the BNetzA. More details at: https://www.bundesnetzagentur.de/DE/Fachthemen/Telekommunikation/Nummerierung/Campusnetze/artikel.html

More details can be found in 3GPP TS 23.003.

2. Network information at the RAN nodes

The network is configured so that the cells providing access to SNPNs broadcast the following information:

- One of multiple PLMN IDs
- A list of NIDs per PLMN ID identifying each SNPN available at that cell

Optionally, a human-readable name per SNPN may be provided, along with other details to prevent non-authorized UE from accessing the cell – further details are available in 3GPP TS 38.300 [2], 3GPP TS 38.304 [3] and 3GPP TS 38.331 [4].

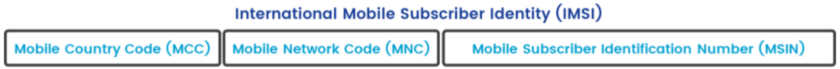
3. UE credentials and configuration

Devices meant to operate in an SNPN are configured with the following details for the SNPNs they can subscribe to:

- PLMN ID and NID of the SNPN
- Subscription Permanent Identifier (SUPI) and credentials for the SNPN. More details at 3GPP TS 23.501 [1] and 3GPP TS 23.003 [5].
- Protection scheme for concealing the SUPI. More details at 3GPP TS 33.501 [6].
- Further configurations as defined in 3GPP TS 31.102 [7].

The SUPI is provisioned in the USIM (for the UE) and in the UDM/UDR function in the 5G Core. In practice the SUPI can be:

- An International Mobile Subscriber Identifier (IMSI) as defined in TS 23.503 [8] for 3GPP RAT


International Mobile Subscriber Identity (IMSI)
Mobile Country Code (MCC)
Mobile Network Code (MNC)
Mobile Subscriber Identification Number (MSIN)

- A Network Access Identifier (NAI) as defined in IETF RFC 754 and clause 28.7.2 of 3GPP TS 23.003 for non-3GPP RAT. The NAI in the form username@realm is specified in clause 2.2 of IETF RFC 7542 [9]. The realm part of the NAI may include the PLMN ID and NID of the SNPN.

About the @realm in an SNPN

Within the realm, the Home Network Domain for an SNPN shall be in the format specified in IETF RFC 1035 [10] and IETF RFC 1123 [11] and structured as:

“5gc.nid<NID>.mnc<MNC>.mcc<MCC>.3gppnetwork.org”

As an example, the Home Network Domain for MCC 345, MNC 12 and NID 000007ed9d5 (hexadecimal: assignment mode = 0, PEN = 00007ed9, NID code = d5) is coded as:

"5gc.nid000007ed9d5.mnc012.mcc345.3gppnetwork.org".

4. Network selection and access control in an SNPN

Once the network has been configured and the devices provisioned with the corresponding credentials, the network selection and access control procedures ensure that the devices can register and access the SNPN.

Access to an SNPN may be managed using regular procedures for PLMN selection (see details in clause 4.4. of 3GPP TS 23.122 [12]). However, when a device is set to operate in SNPN access mode the following procedures apply:

Automatic network selection: the device attempts to register with SNPNs it is allowed to register to, in particular to the SNPN for which it has SUPI and credentials.

Manual network selection: the device provides the user with a list of available SNPNs for which it has SUPI and credentials. The list of SNPNs is provided in numeric form or with human-readable names.

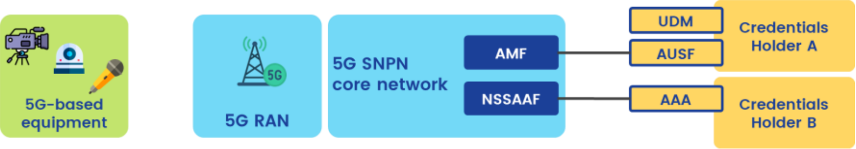
Attempts to register to a network for which there is no subscription for the device will cause registration rejection by the AMF with an appropriate error code. Such devices will be temporarily rejected from automatically selecting and registering to the SNPN. More details in 3GPP TS 24.501 [13].

B) Device registration for SNPNs with UE credentials owned by a credentials holder

A credentials holder (CH) is defined as an entity that authenticates and authorizes access to an SNPN separate from the network operator. In practice, the actual SNPN does not store credentials (e.g., within its UDM/UDR), but the credentials are stored externally. This offers the possibility of using the SNPN as a neutral host while device authentication and authorization is managed using credentials from a third party.

The CH can store credentials by means of:

- The relevant network functions (e.g., AUSF and UDM/UDR) deployed by the CH and connected to the SNPN core.
- An Authentication, Authorization and Accounting (AAA) server connected to the SNPN core



There follows a list of configuration aspects to be considered before using equipment in an SNPN where there is a CH.

1. Identification of the SNPN

The aspects explained in Annex A apply. However, Group Identifiers for Network Selection (GINs) may be used with the purpose of identifying SNPN for which external CHs are provided. This is necessary given the device SUPI is not using the PLMN ID and NID of the actual SNPN but those from the CH. GINs provide a group of third-party CHs with a common network identifier.

About the use of GINs

In a similar way to the NID, GINs can be self-assigned, assigned such that the NID is globally unique (e.g. using IANA PEN numbers), or assigned so that a combination of PLMN ID and NID is globally unique. More details in 3GPP TS 23.003 [5].

2. Network information at the RAN nodes

The aspects explained in Annex A apply. However:

- an SNPN may indicate if access using a CH is supported.
- A list of supported GINs may be provided

3. UE credentials and configuration

The aspects explained in Annex A apply. However:

- The SUPI shall contain identification for the CH, in the form of the @realm when using the NAI, or with the MCC and MNC in case of using an IMSI. Note than when using an AAA server, the identification of the CH is only supported using the NAI.

4. Network selection and access control in an SNPN

In addition to the details provided for regular SNPN network selection, the following apply:

Automatic network selection using a CH: the device attempts to register with the SNPNs that indicate support for registration using a CH.

Manual network selection using a CH: The device provides the user with a list of available SNPNs. Those SNPNs for which a CH is supported are indicated in the list presented to the user.

5. Access to credentials data in the CH

The SNPN may support primary authentication and authorization of UEs that use credentials from a CH by means of:

Network functions (AUSF, UDM) deployed by a CH outside the SNPN

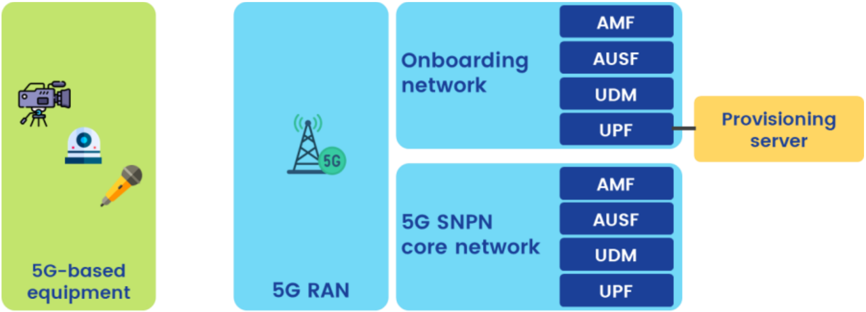
If credentials are stored in a UDM provided by the CH, the AMF in the SNPN forwards requests to the authentication function (AUSF) deployed by the third-party CH.

Authentication, Authorization and Accounting (AAA) server deployed by a CH outside the SNPN

- If credentials are stored in an AAA Server provided by the CH, the AUSF and the UDM of the SNPN can use such credentials for primary authentication and authorization of UEs.
- The AMF may discover and select the AUSF and UDM using the @realm of the NAI. The UDM instructs the AUSF that an AAA server is used for primary authentication. The AUSF selects the NSSAAF to handle the related messages from the device. The NSSAAF selects the corresponding AAA server based on the domain name provided in the @realm of the NAI, relays EAP messages between AUSF and AAA server and performs any related protocol conversion. The AAA server acts as the EAP server for the purpose of primary authentication.
- The UDM is still used for storing subscription information and to decide that the primary authentication is performed by AAA or AUSF. The UDM in the SNPN is pre-configured with information about the need for UEs to use an AAA server for primary authentication. This requires an SLA between the SNPN operator and the CH.

More details are found in clause 5.30.2.9 of 3GPP TS 23.501 [1].

C) Device onboarding for SNPNs with UE without pre-provisioned credentials



Onboarding of UE for SNPNs enables devices that have not been pre-provisioned with credentials to obtain them before they can access a desired SNPN. To enable this procedure, the UE is configured with Default UE credentials.

An Onboarding Network (ONN) is used for the purpose of provisioning devices with SNPN credentials. A provisioning server (PVS) exchanges information with the ONN to provision credentials to the UE. In order to access the PVS, the device may be configured with the PVS IP address or PVS FQDN (Fully Qualified Domain Name).

Procedures when the ONN is an SNPN (ON-SNPN)

The SNPN that enables the onboarding process will indicate this at cell level. The device able to support onboarding should be pre-configured with Default UE credentials and with ON-SNPN selection information (e.g. it can include SNPN network identifiers or GINs). The device will signal to the network its intention to obtain SNPN credentials. After an interaction with the PVS, the device will obtain the SNPN credentials. The provisioning protocol of the default credentials is not standardized by 3GPP and is left to implementers.

The device will de-register from the ON-SNPN and start registration with the actual SNPN.

Procedures when the ONN is a PLMN (ON-PLMN)

The device will use regular PLMN credentials to access the PLMN as the onboarding network. After having registered with the ON-PLMN, the device can be provisioned with the SNPN credentials via the user plane. More details in 3GPP TS 23.122 [12] and 3GPP TS 23.502 [14].

Note that an SNPN may provide functionalities to provision or update the credentials used for secondary authentication/authorization to the UE. Details can be found in clause 5.39 of 3GPP TS 23.501 [1].

In order to enable remote provisioning of credentials for secondary authentication/authorization, UE Configuration Data for User Plane Remote Provisioning are either pre-configured on the UE or provided by the network to the UE (e.g., consisting of PVS IP address(es) and/or PVS FQDN(s)).

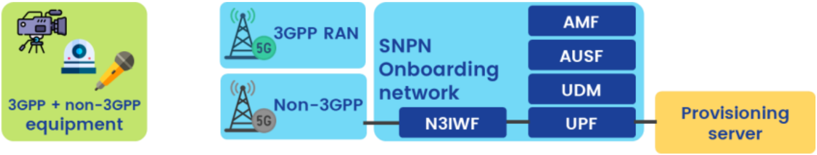
3GPP TS 33.501 [6] makes a distinction between UICC credentials and non-UICC credentials. UICC-based credentials have a well-established ecosystem for provisioning defined by GSMA [15][16][17][18]. Trust in the ecosystem across operators relies on security assurance schemes, certifications and audits of physical locations hosting components taking part in the ecosystem. The GSMA eSIM deployment scenarios are based on fixed locations for hosting components, enabling site certification through audits. This may not be the case for some of the 5G-MAG deployment scenarios described in the 5G-MAG Explainer Deploying Stand-alone Non-Public 5G Networks for media production. The GSMA eSIM specifications allow for the use of an alternative independent eSIM Certificate Authority (CA), but this also implies no reuse of the GSMA ecosystem, i.e. a change of the root certificates in the eSIM no coexistence with GSMA.

The definition of the independent eSIM CA ecosystem and coexistence with the GSMA ecosystem is a gap for isolated SNPN deployments.

There is no standardized provisioning scheme for non-UICC based credentials (i.e. default UE credentials). This is a gap in the 5G ecosystem, out of the 3GPP scope, and currently not addressed by other bodies or interest groups.

Procedures for UE onboarding via non-3GPP access

Access to SNPN services could be performed via non-3GPP access, an example is though Wi-Fi. Even more, onboarding of UEs via non-3GPP access is also supported. Details are in clauses 5.30.2.12 (Untrusted non-3GPP access) and 5.30.2.13 (Trusted non-3GPP access) of 3GPP TS 23.501 [1].

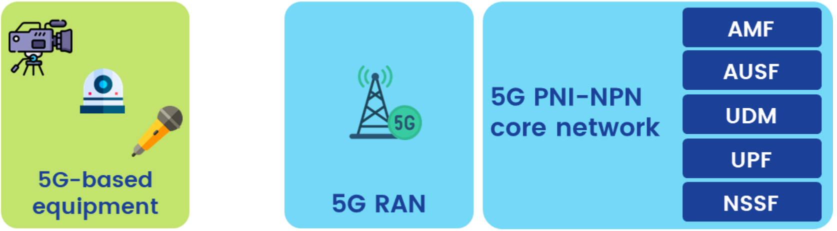


In particular, the UE can register to the SNPN over Untrusted non-3GPP access for UE onboarding. In case the PVS is reachable using local connectivity (e.g. via the internet) SNPN credentials can be obtained directly. However, when this is not the case, the UE may select an N3IWF function (using a FQDN) in the SNPN that supports UE onboarding.

UE onboarding via Trusted non-3GPP access requires that the non-3GPP access network advertises and indication that onboarding is enabled in the SNPN. In this case, the UE will select the SNPN and proceed with the UE onboarding procedures.

D) Device registration for PNI-NPNs with pre-provisioned credentials

A PNI-NPN made available by a PLMN requires subscription to the PLMN. Additionally, as network slicing does not enable the possibility of restricting access to these capabilities to certain UEs, Closed Access Groups (CAGs) may be used to apply access control.



The UE and PNI-NPN may support remote provisioning of credentials to select an appropriate network slice instance.

There follows a list of configuration aspects to be considered before using equipment in a PNI-NPN.

1. **Identification of the PNI-NPN**

Besides the PLMN ID of the public network, a CAG ID identifies the PNI-NPN.

2. **UE credentials and configuration**

A UE that supports CAGs may be pre-configured with the following information:

- A list of CAGs the UE is allowed to access.
- An optional indication of whether the UE is only able to access the 5G system via a CAG cell.

The public network can perform changes to the CAG configuration and provide the necessary updates to UEs.

3. **Network selection and access control in a PNI-NPN**

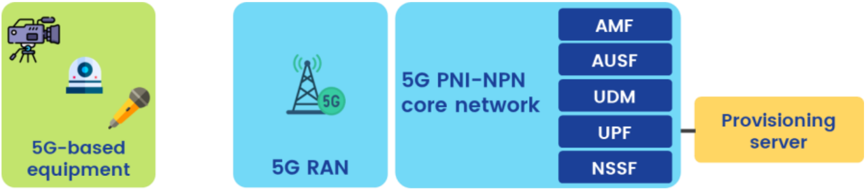
The CAG cells broadcast information that allows UEs supporting the CAG to access the cell.

Mechanisms to prevent access to NPNs from unauthorized UEs are detailed in 3GPP TS 24.501 [13].

Aspects on automatic and manual network selection in relation to CAG are detailed in 3GPP TS 23.122 [12].

E) Device onboarding for PNI-NPNs without pre-provisioned credentials

Note that PNI-NPNs may provide functionalities to provision or update the credentials used for NSSAA to the UE. Details can be found in clause 5.39 of 3GPP TS 23.501 [1]. In order to enable remote provisioning of credentials for NSSAA, UE Configuration Data for User Plane Remote Provisioning are either pre-configured on the UE or provided by the network to the UE (e.g. consisting of PVS IP address(es) and/or PVS FQDN(s)).



According to 3GPP TS 33.501 [6], deployment scenarios addressing the PNI-NPN case are only considered with UICC credentials. This implies that the GSMA ecosystem can be reused for these cases.

Related documentation

[1] 3GPP TS 23.501: "System architecture for the 5G System (5GS)" (Release 17)

[2] 3GPP TS 38.300: “NR and NG-RAN Overall description” (Release 17)

[3] 3GPP TS 38.304: “NR User Equipment (UE) procedures in idle mode and RRC Inactive state” (Release 17)

[4] 3GPP TS 38.331: “NR Radio Resource Control (RRC) protocol specification” (Release 17)

[5] 3GPP TS 23.003: “Numbering, addressing and identification” (Release 17)

[6] 3GPP TS 33.501: “Security architecture and procedures” (Release 17)

[7] 3GPP TS 31.102: “Characteristics of Universal Subscriber Identity Module (USIM) application“ (Release 17)

[8] 3GPP TS 23.503: “Policy and charging control framework for the 5G System (5GS)” (Release 17)

[9] IETF RFC 7542: “The Network Access Identifier”

[10] IETF RFC 1035: “Domain names – implementation and specification”

[11] IETF RFC 1123: “Requirements for Internet Hosts – Application and Support”

[12] 3GPP TS 23.122: “Non-Access-Stratum (NAS) functions related to Mobile Station (MS) in idle mode” (Release 17)

[13] 3GPP TS 24.501: “Non-Access-Stratum (NAS) protocol for 5G System (5GS)” (Release 17)

[14] 3GPP TS 23.502: “Procedures for the 5G System (5GS)” (Release 17)

[15] GSMA SGP.01: “Embedded SIM Remote Provisioning Architecture”

[16] GSMA SGP.21: “RSP Architecture”

[17] GSMA SGP.22: “Remote SIM Provisioning (RSP) Architecture for consumer Devices”

[18] GSMA SGP.31: “eSIM IoT Architecture and Requirements”

5G
MAG

www.5g-mag.com

Published by 5G-MAG | September 2023

5G Media Action Group (5G-MAG) Association
17A L'Ancienne-Route
1218 Grand-Saconnex (Switzerland)

info@5g-mag.com • www.5g-mag.com