The OnGo SHNI and OnGo Managed Identifiers

June 2023

Contents

Introduction

This whitepaper gives detailed information about the OnGo Alliance's identifier management program. It is intended to explain both why the OnGo Alliance manages identifiers, explain how to get managed identifiers, and how to use them.

At the end, you'll find a glossary defining terms and acronyms used throughout the document and a "checklist" to help drive the planning process.

Who Should Read this Guide?

This whitepaper is intended for people designing and deploying OnGo networks. It assumes that you have some basic knowledge of 3GPP technologies (LTE and 5GS) and wireless networking.

OnGo and CBRS Overview

This section provides background information about OnGo and the CBRS band. If you already know what OnGo is, skip to the next section.

OnGo Overview

OnGo networks are networks deployed in the CBRS Band that use 3GPP technologies – both the 4th generation LTE and 5th generation 5GS (also known as NR). The OnGo Alliance was formed to support and promote deployment of OnGo networks, by defining how 3GPP networks operate in the CBRS Band.

CBRS Overview

In April 2015 the Federal Communications Commission (FCC) formally established the Citizen Broadband Radio Service (CBRS) to address current and future needs for wireless spectrum. Previously reserved solely for military and other government-approved uses, the CBRS band opens up 150 MHz of spectrum at 3.5 GHz band so that private organizations can share this spectrum with incumbent users. The OnGo Alliance created OnGo to promote the use of LTE and 5G in the 3.5 GHz band, although other technologies can also make use of the band. The FCC partitioned 150 MHz of the 3.5 GHz band into 15 x 10 MHz channels. Access to the channels is dynamic and controlled by dedicated spectrum-management services known as Spectrum Access Systems (SAS).

OnGo and CBRS Overview

PAL vs. GAA

Users who operate in the CBRS band have different priority levels. Top priority lies with the Tier 1 incumbent users such as the federal government, fixed satellite users, and grandfathered wireless users. Next in priority are Tier 2, or Priority Access License (PAL), users. These are licensed users who acquire spectrum licenses through an FCC auction. PAL users must not cause harmful interference to Tier 1 users. Third priority is given to Tier 3 General Authorized Access (GAA) users who deploy "lightly-licensed" devices. GAA users must not cause harmful interference to the higher-tier users.

The FCC auctioned PALs on a per-county basis, with sublicensing permitted. Of the 15 channels in the CBRS band, the FCC allocates seven for PAL licensees. Any spectrum not used by PAL holders or the protected incumbents can be used by GAA users. Currently, GAA users are not afforded any interference protection from each other.

Who's Who in OnGo

OnGo is the result of work by many organizations:

- The FCC – The Federal Communications Commission defined the part 96 regulations that opened access to the CBRS band.
- WInnForum – The Wireless Innovation Forum defined the requirements for CBRS- compliant physical devices.
- OnGo Alliance (OnGoA) – The OnGo Alliance defines the requirements for OnGo technologies in the 3.5 GHz band and certifies OnGo-compliant equipment. (The OnGo Alliance was previously known as the CBRS Alliance.)
- 3GPP – The 3rd Generation Partnership Project standards body represents the community of 3GPP equipment manufacturers and service providers, and defines the LTE and 5G NR standards.

CBSDs

Access Points are termed Citizens Broadband Radio Service Devices (CBSDs) in CBRS. CBSDs come in many types – fully integrated small-cells, distributed radio heads, or antenna clusters. CBRS defines a CBSD as a logical entity that radiates RF power, has antenna characteristics and is geolocated. CBSDs come in two classes, defined by their output power, and range. Category A devices must emit less than one watt of power per 10 MHz channel. Category B devices, typically used outdoors, may emit up to 50 watts per 10 MHz channel. In an OnGo network, the 5G gNodeBs (gNBs – base stations) are connected to CBSDs, and are often in the same device.

Table 1: CBSD category summary.

Device Type	Maximum EIRP (dBm/10 MHz)	Limitations
Category A CBSD	30 (1W)	• Outdoor antenna height limited to six meters Height Above Average Terrain (HAAT). • If operation exceeds antenna height or max Category A power limits, the device is subject to Category B limitations.
Category B CBSD	47 (50W)	• Limited to outdoor operation. • Must be professionally installed.

EUDs

In CBRS, End User Devices (EUDs) are the user-facing element. These devices can be either mobile or fixed and their power can't exceed 23 dBm/10 MHz (200 mW). EUDs may operate with permission from a CBSD. In an OnGo 5G network, the EUDs are generally 5G User Equipment (UE) devices.

SAS

All CBSDs must register with an FCC-certified Spectrum Access System (SAS) and obtain a channel grant from the SAS before transmitting in the CBRS band. To prevent interference with incumbent systems, the SAS allocates the spectrum to individual CBSDs and PAL license holders. To coordinate the CBRS band's usage, the SASes maintain a database of CBSDs and incumbent devices to calculate the aggregate interference.

For a SAS to grant access to channels in the lower 100 MHz of the CBRS band, the SAS must have access to an Environmental Sensing Capability (ESC). The ESC is a network of sensors used to detect federal frequency use in the 3550–3650 MHz band where U.S. Navy radar systems can operate, primarily along the Pacific, Atlantic and Gulf coasts. The ESC informs the SAS of radar operations so that the SAS can prevent any CBRS interference with the naval operations by suspending/terminating existing grants and/or rejecting any new grants in that location for those channels. The SASes use a combination of tools to create realistic propagation model to predict potential interference with incumbent systems, and can provide guidance to CBSDs via operating parameters to CBSDs so as to avoid potential interference.

A new CBSD requests access to a range of frequencies from the SAS, and, based on the location of the CBSD, its category, and its antenna characteristics, the SAS grants access to one or more CBRS channels. When higher-priority users need channel access, the SAS can direct the CBSDs to reduce their output power, stop using currently allocated channels, or shut down entirely to avoid interference with PAL users or incumbent systems.

Several FCC-certified SAS systems are deployed across the country. These systems are operated by various companies that share information among each other. Before a CBRS user deploys a CBSD, they need to subscribe to a SAS service from an FCC-certified SAS administrator. Under Part 96 rules, a SAS does not guarantee interference protection among GAA users. However, WInnForum, the OnGo Alliance, and other standards bodies have developed a coexistence framework for GAA users, to help manage GAA operations.

CPIs

Most CBSDs must be registered by a Certified Professional Installer (CPI), who collects and registers information about the CBSD and provides detailed location information to the SASs. The FCC doesn't require a CPI to install CBSDs, but a CPI needs to register each new CBSD with the SAS. CPIs are certified by one of the Training Program Administrators (TPAs) approved by WInnForum. A list of the TPAs is maintained by the WInnForum, and can be found here: https://cbrs.wirelessinnovation.org/cpi-program-administrator.

3GPP Identifiers

This section discussed the identifier used to identify 3GPP (and other) networks, and the limitations of this mechanism in OnGo networks.

HNI Basics

3GPP networks are identified by their Home Network Identifier (HNI) – a 5 or 6 digit number that is continually broadcast by the network. The HNI isn't used just by 3GPP networks; many networks use an HNI to identify themselves..

The HNI consists of two components:

- A 3-digit Mobile Country Code (MCC)
- A 2- or 3-digit Mobile Network Code. Some MCCs use a two-digit MNC, some use a 3-digit MNC. In the United States of America, the MNC is three-digits.

The HNI system is managed by the International Telecommunications Union (ITU), which allocates Mobile Country Codes (MCCs). Assignment of Mobile Network Codes (MNCs) is typically delegated to various regional authorities, who assign the MNCs for their MCCs. In the US, this is the US IMSI Administrator, the Alliance for Telecommunications Industry Solutions (ATIS) (https://imsiadmin.com).

Some countries have multiple MNCs assigned to them (the US has seven – 310 to 316). The MCCs above 900 are reserved for special purposes, like international operators, temporary identifiers, and the like.

Since the number space is limited (1,000 MCCs, and 100 or 1000 MNCs per MCC), the ITU and its delegates do not issue HNIs lightly. New MCCs are only allocated after significant deliberation, and MNCs are typically only granted to those who can demonstrate their intent to use them.

Many of the major network operators in the US have multiple PLMN-IDs, due to a history of mergers and acquisitions, and the need to operate distinct networks. Verizon, for example, has over 40.

The HNI in LTE Networks

In addition to identifying the operator of a 3GPP network, and as the HNI of a subscriber, the 3GPP uses the HNI (PLMN-ID) in a number of other identifiers in their networks. Some network elements in LTE and 5GS need to have globally unique identifiers, particularly where there may be multiple instances of given component in the network. In those cases, the 3GPP ensures global uniqueness by including the PLMN-ID in the identifier. This puts the onus of ensuring that the identifiers are globally unique on the network operator, and if there is an error, it only affects the networks using that PLMN-ID.

> **HNIs and PLMN-IDs**
>
> Within the 3GPP's specifications, the HNI is typically referred to as a Public Land Mobile Network Identifier (PLMN-ID), or just the PLMN. The two terms, PLMN-ID and HNI, are more or less equivalent. In this document, we use the term PLMN-ID when discussing 3GPP-specific uses, while HNI is technology agnostic.

In LTE, the following key identifiers use the PLMN-ID to ensure global uniqueness:

Globally Unique Mobility Management Entity Identifier (GUMMEI)

The GUMMEI is used to identify the Mobility Management Entity within LTE's core network, the Evolved Packet Core (EPC). The MME is responsible for tracking devices as they physically move around the network, and for routing data to and from those devices appropriately. A network can have multiple MMEs, each with their own GUMMEI. They can also be grouped together, with up to 256 MMEs per MME group.

The below table gives the breakdown of the GUMMEI and its components:

Table 2: GUMMEI Components

Component	Length	Description
GUMMEI	48 bits	The Globally Unique Mobility Management Entity Identifier, a globally unique number that identifies a specific MME instance.
PLMN-ID	24 bits	The PLMN-ID of the network.
MMEI	24 bits	Mobility Management Entity Identity
MMEGI	16 bits	Mobility Management Entity Group Identity – the identity of a MME group.
MMEC	8 bits	Mobility Management Entity Code – a code that uniquely identifies an MME within the MME group.

LTE Globally Unique Temporary Identifier (GUTI)

The GUTI is used to identify a specific device (UE/EUD) within a network. While the IMSI identifies the subscriber, LTE avoids using the IMSI as much as possible for security purposes. Instead, the network assigns a device a temporary identifier, the GUTI. The GUTI is assigned by the MME, and is used to notify the device when the network needs to send data to it, and by the device when it needs to update the network as it moves around the network's coverage area.

Table 3: LTE GUTI Components

Component	Length	Description
LTE GUTI	80 bits	The Globally Unique Temporary Identifier is assigned to a device by the MME to avoid using the IMSI.
PLMN-ID	24 bits	The PLMN-ID of the network.
MMEGI	16 bits	Mobility Management Entity Group Identity – the identity of the MME Group that assigned the GUTI.
S-TMSI	40 bits	The Serving Temporary Mobile Subscriber Identity,
MMEC	8 bits	Mobility Management Entity Code – a code that uniquely identifies the MME within the MME group that assigned the S-TMSI.
M-TMSI	32 bits	MME Temporary Mobile Subscriber Identity – the temporary identifier assigned by the MME.

E-UTRA Cell Global Identifier (ECGI)

The ECGI is used to uniquely identify an LTE cell. A given eNodeB (an E-UTRAN base station) can have multiple cells, each with their own cell ID. The ECGI is used several different elements of an LTE network:

- Self-Optimizing Network (SON): LTE networks are able to optimize operation, by continually monitoring the RF environment that the network is operating in. The network can request devices perform measurements of networks operating in other channels and bands. The ECGI is used to uniquely identify a given cell, and allows the eNodeBs to coordinate their operation.
- Location Services: To support emergency services (E911) and other location services, LTE can use the ECGI to help physically locate a given device within their network. (Normally, the network only has an approximate idea of where a device

is using tracking areas – which are described below – but when a more precise location is needed, the ECGI can help.)

Table 4: ECGI Components

Component	Length	Description
ECGI	52 bits	E-UTRAN Cell Global Identifier
PLMN-ID	24 bits	The PLMN-ID of the network.
ECI	28 bits	E-UTRAN Cell Identifier, which identifies the cell within the network.
eNB ID	20 bits	The Macro eNodeB Identifier, which identifies the base station within the network.
Cell ID	8 bits	The cell identifier identifies the cell within the eNodeB.

Note: The division of the ECI between the eNB ID and the Cell ID can "float" – with the eNB ID and Cell ID having a variable number bits – as long as it totals 28 bits. Within OnGo, we have formally defined the eNB ID as being 20 bits, with a Cell ID of 8 bits.

LTE Tracking Area Identifier (TAI)

The TAI is used to identify a tracking area within a network. LTE networks divide themselves into Tracking Areas, each of which covers a geographic area within the network. Each eNodeB in the network broadcasts its TAI. As a device moves around the network, it monitors the TAI being broadcast by the eNodeBs it is connected to. When the TAI changes, it notifies its MME that it has moved to a new tracking area. When the network (MME) needs to connect to a device, the eNodeBs in the tracking area page the device (using the TMSI), and then the MME routes the traffic to the eNodeB that the device responded to. Configuring the tracking areas is a matter of control traffic management: smaller tracking areas results in more tracking area update traffic, but less overhead from paging traffic. Larger tracking areas have less update traffic, but more overhead from paging traffic.

Strictly speaking, the TAI's don't have to be globally unique, as the user devices are looking for changes in the TAI – as long as two physically adjacent cells don't have the same TAI, the system will function. In practice, networks typically make sure that repeated TAIs are separated by as many tracking areas as possible.

Table 5: TAI Components

Component	Length	Description
LTE TAI	40 bits	Tracking Area Identifier
PLMN-ID	24 bits	The PLMN-ID of the network.
LTE TAC	16 bits	Tracking Area Code, which is (locally) unique within the network.

Individual Mobile Subscriber Identity (IMSI)

The IMSI is what uniquely identifies the subscriber to a network. This is what is stored on the USIM – the SIM card that is put in your phone. Various cryptographic techniques are used to authenticate that the IMSI is valid, and LTE avoids broadcasting the IMSI "in-the-clear" to prevent spoofing.

Table 6: IMSI Components

Component	Length	Description
IMSI	15 digits	Individual Mobile Subscriber Identity
PLMN-ID	6 digits	The PLMN-ID of the network that the user is a subscriber of.
MSIN	9 digits	Mobile Subscriber Identification Number, that uniquely identifies a user of the network.

Note: The PLMN-ID can be 5-digits long, with a 10-digit MSIN, but for in the US, it's 6 digits, with a 9-digit MSIN.

The HNI in 5GS Networks

The 3GPP uses the HNI (PLMN-ID) in 5GS networks in a similar fashion as LTE: including the PLMN-ID in identifiers that need to be globally unique. While the names and bit lengths can be different, the basic purpose and design is the same.

Globally Unique AMF Identifier (GUAMI)

The 5GS's version of the MME is the Access and Mobility Management Function (AMF). Where LTE provides two tiers of grouping (an MME Group, and an MME Code), 5GS provides an additional tier of grouping for AMFs: An AMF Region Identity, an AMF Set Identity, and an AMF Pointer. Beyond this changes, the GUAMI is functionally equivalent to the GUMMEI.

The below table gives the breakdown of the GUMMEI and its components:

Table 7: GUAMI Components

Component	Length	Description
GUAMI	48 bits	The Globally Unique AMF Identifier, a globally unique number that identifies a specific AMF instance.
PLMN-ID	24 bits	The PLMN-ID of the network.
AMF ID	24 bits	Access and Mobility Management Function Identifier
AMF Region ID	8 bits	The identity of an AMF Region.
AMF Set ID	10 bits	The identity of an AMF Set within an AMF Region.
AMF Pointer	6 bits	A unique code that identifies an AMF within an AMF Set.

5G Globally Unique Temporary Identifier (GUTI)

The 5G GUTI is used to identify a specific device (UE/EUD) within a network, just like the LTE GUTI. The 5GS avoids using the IMSI as much as possible for security purposes. Instead, the network assigns a device a temporary identifier, the GUTI. The GUTI is assigned by the AMF, and is used to notify the device when the network needs to send data to it, and by the device when it needs to update the network as it moves around the network's coverage area. The only real difference is that the 5G GUTI

Table 8: 5G GUTI Components

Component	Length	Description
5G GUTI	80 bits	The Globally Unique Temporary Identifier is assigned to a device by the MME to avoid using the IMSI.
PLMN-ID	24 bits	The PLMN-ID of the network.
AMF ID	24 bits	The AMF Identifier of the AMF that assigned the GUTI.
AMF Region ID	8 bits	The identity of an AMF Region.
AMF Set ID	10 bits	The identity of an AMF Set within an AMF Region.
AMF Pointer	6 bits	A unique code that identifies an AMF within an AMF Set.
5G-TMSI	32 bits	The Serving Temporary Mobile Subscriber Identity,

New Radio Cell Global Identifier (NCGI)

The NCGI is used to uniquely identify an 5GS cell, and is analogous to the LTE ECGI. A given gNodeB (an 5G NR base station) can have multiple cells, each with their own cell ID. As with the LTE, the NCGI is used as part of the 5GS's self-optimizing network (SON) and E911 systems. The primary differences are that the NCGI is 8 bits longer than the LTE ECGI.

Table 9: NCGI Components

Component	Length	Description
NCGI	52 bits	New Radio Cell Global Identifier
PLMN-ID	24 bits	The PLMN-ID of the network.
NR Cell ID	36 bits	The 5GS New Radio cell identifier, which identifies the cell within the network.
gNB ID	28 bits	The gNodeB Identifier, which identifies the 5G base station within the network.
Cell ID	8 bits	The cell identifier identifies the cell within the eNodeB.

Note: As with LTE, the division of the NR Cell Identity between the gNB ID and the Cell ID can “float” – with the gNB ID ranging from 22 to 32 bits, and the Cell ID ranging from 14 to 4 bits. Within OnGo, we have formally defined the gNB ID as being 28 bits, with a Cell ID of 8 bits – 256 cells per gNB ID.

5G Tracking Area Identifier (TAI)

As with LTE, the 5G TAI is used to identify a tracking area within a network. In the case of 5G, the TAC component is 8 bits longer, allowing for more tracking areas within a network.

Table 10: 5G TAI Components

Component	Length	Description
5G TAI	48 bits	5G Tracking Area Identifier
PLMN-ID	24 bits	The PLMN-ID of the network.
5G TAC	24 bits	Tracking Area Code, which is (locally) unique within the network.

Individual Mobile Subscriber Identity (IMSI)

IMSIs in 5GS are the same as in LTE – there is no change.

HNIs and OnGo Networks

The HNI system was designed to support the ecosystem of a small number of large network operators. It works great in that context, but OnGo enables a large number of small networks – and in the OnGo context, the HNI mechanism doesn’t work as well. There are two major problems:

Not Enough HNIs

The available number space for HNIs is relatively small, with only a million total numbers available. (The total number available is actually smaller, as a several MCCs have been reserved for test purposes.) There simply aren't enough HNIs available for each OnGo network to have its own HNI.

Administrative Hurdles

Largely because there is a limited pool of numbers to assign, the ITU its delegates, do not hand out new HNIs lightly. Some require proof that the requester will be using the HNI in the form of a spectrum license. But the CBRS band has an entirely new licensing model, and while PAL holders do have a license, GAA users are licensed on-the-fly.

The CBRS Shared HNI (SHNI) Solution

This problem was recognized early one, and a simple solution was identified – allocate an HNI for use by networks operating in the CBRS band. Network operators deploying in the CBRS band that don't have their own HNI could use the CBRS Shared HNI (SHNI). The value of the CBRS SHNI is 315-010 (the MCC is 315, the MNC is 010).

While this neatly sidesteps the problem of the limited number space for HNIs, it creates two new problems:

Uniquely Identifying Networks

If multiple networks are using the CBRS SHNI, the HNI is no longer sufficient to uniquely identify a specific network. Put simply, if there are two networks broadcasting the same HNI, how can a device determine which one it should connect to? Solving this problem depends on the networking technology being used, and is thus outside the scope of the US IMSI Administrator and the CBRS specifications. Uniquely identifying networks that use the CBRS SHNI has to be addressed by the specific networking technology that is being used.

Preventing Collisions

In the 3GPP context, there is an additional wrinkle with using an SHNI – preventing identifiers collisions. A collision occurs when identifier which is assumed to be globally unique turns out to not be unique, because two different networks using the same HNI (PLMN-ID) accidentally use the same identifiers. In regular 3GPP networks, it's up to the network operator to make sure that they don't accidentally use the same identifier twice, and if they make an error, it only affects their network, as the PLMN-ID component is unique to them. But when using an SHNI, one operator could cause problems with another network operator. While collisions typically only become a problem when networks have overlapping coverage area, they can be extremely disruptive. Just how bad a collision is depends on what identifier is being duplicated:

LTE GUMMEI Collisions

A GUMMEI collision occurs when two networks using the same PLMN-ID (the CBRS SHNI) use the same MMEGI and MMEC. A GUMMEI collision can disrupt the various mobility systems within LTE. A number of the security and encryption mechanisms will fail as well, as the needed encryption keys will not be correct or available. The end result is that the users will lose service as they move around the network.

5G GUAMI Collisions

GUAMI collisions in the 5GS have the same basic impact as in LTE: loss of service for mobile devices, and security failures.

LTE and 5G GUTI Collisions

GUTI collisions have a similar impact as GUMMEI collisions – with the user device being denied service do to mobility and security failures. These will tend to show up when the devices try and notify the network of their status, or when the network tries to initiate a connection to the device – the wrong device will respond, and the security and encryption mechanisms will fail.

LTE ECGI Collisions

ECGI collisions tend to degrade LTE system operation, rather than prevent operation entirely. The SON mechanisms use the ECGI to identify specific cells, and if multiple cells are using the same ECGI in the same area, measurements performed by devices will not be correct, causing the coordination between eNBs to adjust themselves incorrectly. The net result is that interference between eNBs will increase (or not be decreased as expected), and overall system performance in terms of range and data rates will be reduced.

Location-related services will also be degraded. This is particularly of concern with E911 and other emergency services, which can use ECGI to help determine where a device is located. If multiple cells use the same ECGI, the location will be incorrect.

5G NCGI

NCGI collisions in the 5GS have the same basic impact as in LTE ECGI collisions: increased interference between cells, and degraded E911 location performance.

LTE and 5G TAI Collisions

TAI collisions, like GUMMEI or GUTI collisions, tend to cause problems with mobility. Tracking area updates won't occur correctly as the device moves around the coverage area, and so the network doesn't know which tracking area a device is in. The net result is an increase in control traffic overhead as the network has to start looking for the device in other tracking areas. Due to how certain errors are handled within LTE, there are some circumstances where a TAI collision can cause an extended denial of service, with the device waiting 12 hours before attempting to connect again.

IMSI Collisions

IMSI collisions – when two different SIMs have the same IMSI on them – tends to result in a denial of service. When the device attempts to connect to a network that knows about the *other* IMSI, authentication will fail: the cryptographic keys stored on the SIM for that IMSI will be incorrect.

OnGo Managed Identifiers

In order to make it easier for organizations to deploy OnGo Networks using the CBRS SHNI, the OnGo Alliance has created an identifier management program. This program addresses the two problems with using an SHNI in an LTE or 5GS network: uniquely identifying networks, and preventing collisions. This section provides details on these elements.

CBRS Network ID (CBRS NID)

In order to distinguish between different 3GPP networks using the CBRS SHNI, we have defined a new identifier – the CBRS Network Identifier (CBRS NID). This identifier is 27 bits long, and uniquely identifies the network. The OnGo Alliance assigns and manages this identifier to ensure that no two organizations are assigned the same CBRS NID. How the CBRS NID is used depends on what 3GPP technology you are using, and in the case of 5GS, which release of the specifications:

LTE and the CBRS-NID

Fortunately for everyone, the 3GPP defined a mechanism in LTE that does exactly what we need it to: the Closed Subscriber Group (CSG). This is a feature in LTE that allows a network to define areas of the network that are only accessible to specific users. The CSG is identified by a CSG Identifier (CSG-ID) that is broadcast by designated eNBs, and is stored on the user's SIM. A device will only connect to a cell broadcasting the CSG-ID if it matches the CSG-ID stored on its SIM.

This mechanism is prefect for uniquely identifying networks using a SHNI, and in OnGo we use it by simply having the eNBs broadcast the CBRS NID in the CSG-ID field. The upshot is that no change is needed to the 3GPP specifications, and the CSG mechanism does everything we need it to. There's just one little problem:

CSG-ID Support

Unfortunately, very few user devices in the United States actually support the CSG mechanism. The feature is, strictly speaking, option in the LTE specifications. While most device makers have implemented it in their software, they have disabled it in their active builds. This is largely because the carriers haven't needed it, and the CSG mechanism can increase the idle power consumption by user devices.

Why the CBRS NID and not the OnGo NID?

The reason we call it the CBRS NID and not the OnGo NID is that when this solution was initially deployed, the OnGo Alliance was named the CBRS Alliance. Rather than rename the identifier, we left it "as-is".

The good news is that the impact of not supporting the CSG mechanism is actually quite small. Devices with SIMs containing the CBRS SHNI, and that don't support the CSG mechanism, will try and connect to any network broadcasting the CBRS SHNI regardless of the CSG ID and CBRS NID. If it attempts to connect to the wrong network, the network will reject the connection as it does not recognize the device. The device then immediately tries to attach to the next network it sees broadcasting the CBRS SHNI. It will repeat this process until it tries to connect to the correct network. The net result being a number of unrecognized devices connecting to the incorrect networks, and in increase in the time it takes for a device to acquire service. Since there can be at most 15 networks operating in the CBRS band at once, the overall increase in time is on the order of minutes.

5GS Release 15

The Release 15 of the 3GPP's 5GS specifications was the first to handle stand-alone (SA) 5GS networks – the previous release only allowed for Non-Stand-Alone (NSA) operation, with an LTE network providing the control channel, and using a 5G network to provide additional data capacity.

In release 15, there is no equivalent of the CSG-ID mechanism in LTE, and no way for the network to broadcast the CBRS-NID, and no way for the user devices to know what CBRS-NID to look for. Fortunately, this does not prevent use of Release 15 5GS networks using the CBRS SHNI. Just as with LTE and devices not supporting the CSG mechanism, it takes a little extra time for devices to attach to the correct network, as it will try to connect to all 5GS networks using the CBRS SHNI.

There is an additional shortcoming in release 15, in that roaming into and out of a Release 15 5G network using the CBRS SHNI is not supported by the specifications. Individual implementations could make it work, but would have to be proprietary.

5GS Release 16 SNPN

In Release 16 of the 5GS specifications, the 3GPP added a mechanism for supporting use of SHNIs as part of adding support for Stand-Alone Non-Public Networks (SNPN). SNPNs are identified by a 40-bit NID (called the 5GC NID), and networks can use one of several different assignment modes. Assignment Mode 2 is for use with a Shared PLMN-ID, and is thus perfect for the CBRS SHNI. Since the 5GC NID is 13 bits longer than the CBRS NID, we add 13 leading 0s as padding.

Table 11: The 5GC NID and the CBRS NID

Component	Length	Description
AM	4 bits	Assignment Mode of the 5GC-NID. OnGo uses Assignment Mode 2. (b0010)
5GC NID	40 bits	New Radio Cell Global Identifier
Padding	13 bits	13 leading 0's as padding.
CBRS-NID	27 bits	The CBRS-NID as assigned by the OnGo Alliance.

Note: The other assignments modes use either a Private Enterprise Number (PEN) as assigned by the Internet Assigned Numbers Authority (IANA) (for assignment mode 0), or a self-assigned identifier with no guarantee of uniqueness (for assignment mode 1). We recommend using assignment mode 2.

The Release 16 5GC-NID handles everything needed to make a SHNI like the CBRS SHNI work, including full support for roaming. It also addresses the issue of identifier collisions, as the 5GC-NID is used as part of resolving identifiers, eliminating the risk of collisions of identifiers using a SHNI.

Preventing Collisions – Managing Identifiers

As discussed previously, the other big challenge in using a Shared PLMN-ID like the CBRS SHNI) is making sure globally unique identifiers are actually globally unique. The OnGo Alliance allocates and assigns identifiers to anyone that requests them, and by making sure we don't assign the same identifiers twice, you don't have to worry about collisions. Instead of asking every network operator for which identifiers they use, you can just get an identifier from the OnGo Alliance, and not have to worry about it. To make things even simpler, we only manage a component of each identifier, so you have maximum flexibility, and need to get as few identifiers from us as possible.

The next section of this document will go into details of how to get identifiers, and the processes associated with identifier management. For now, we'll focus on which identifiers we manage

LTE Managed Identifiers

LTE – Mobility Management Entity Group Identifier (MMEGI)

For LTE, the OnGo Alliance assigns and manages the Mobility Management Entity Group Identifier (MMEGI). This identifier is used in both the GUMMEI and the LTE GUTI. By managing the MMEGI component of the GUMMEI, network operators can deploy up to 256 MMEs per MMEGI, as the GUMMEI includes an 8-bit MME Code (MMEC), which should be more than enough for most network deployments.

Likewise the MMEGI is a component of the LTE GUTI, which allows the MMEs to issue GUTIs without worrying about collisions.

LTE – eNodeB Identifiers (eNB IDs)

The eNB ID is the component that uniquely identifies the base station within the ECGI, and is what is managed by the OnGo Alliance. ECGIs also include an 8-bit Cell Identity, allowing for up to 256 cells per eNB ID.

Note: Network operators can re-use the assigned eNB ID across multiple eNBs, using different cell identities to distinguish between the cells on the different eNBs. We still recommend getting 1 eNB ID per base station, in order to prevent potential accidental collisions.

OnGo Managed Identifiers

LTE – Tracking Area Codes (TACs)

The OnGo Alliance does not directly manage the TAC component of the TAI. Instead, we rely on the assigned IMSI Block Number (IBN) to generate a set of TACs that networks can use. (See below for more information on IMSI Block Numbers.) For each IBN, there are 6 associated TACs:

- The IBN is the first TAC.
- The IBN + 10,000 is the second TAC.
- The IBN + 20,000 is the third TAC.
- …
- The IBN + 50,000 is the sixth TAC.

TAC Example – LTE

An LTE deployment gets an IMSI Block Number (IBN) assigned by the US IMSI Administrator – 0046.

From that IBN, they can generate the following six TACs:

- 46 (0x002E)
- 10,046 (0x273E)
- 20,046 (0x4E4E)
- 30,046 (0x755E)
- 40,046 (0x9C6E)
- 50,046 (0xC37E)

Note: Note that for IBNs 6,832 to 7,087 can only derive 5 TACs. See "Reserved TACs" for more information.

For many network deployments, 6 TACs will be more than sufficient. If more than 6 TACs are needed, network operators have two options:

- Obtain an additional IBN OR
- Request a TAC from our pool of managed TACs.

Managed TAC Pool

The above algorithm results in a set of TACs that are not addressed: from 60,001 to 65,536 (2^{16}). These TACs are reserved as a pool of managed TACs. If you need additional TACs, and you aren't issuing enough SIMs to get an extra IBN, you can request how many TACs you need from the managed TAC pool.

Reserved TACs

Neutral Host Networks (NHNs) are networks that provide seamless coverage to multiple public networks. For various technical reasons, TAC collisions are particularly difficult to prevent in the NHN context, and requires coordination between the participating networks. The public network operators are working with the US IMSI Administrator to manage and allocate a pool of TACs for use in NHNs. The current tentative plan is to reserve the range of 0xDE00 to 0XDEFF for use as NHN TACs. The net result being that IBNs in the corresponding range (6,832 to 7,087) will only be able to use 5 TACs. When the final determination has been made, this document will be updated, and management of identifiers modified as necessary.

5GS Release 15 Managed Identifiers

5GS – AMF Region + Set ID

As with LTE and the MMEGI, we manage a component of the GUAMI, rather than the entire identifier. For this identifier we manage the AMF Region + Set ID as a single 18-bit identifier, which can be used for up to 64 GUAMIs. The AMF Region + Set ID also show up in the 5G GUTI, and by managing this component of the GUTI, we prevent collisions for all of the GUTIs that can be assigned by the 5GS.

5GS – gNB ID

The 5GS equivalent of the eNB ID, the OnGo Alliance manages this component of the NCGI. At 28 bits, this leaves 8 bits for the cell ID, allowing up to 256 cell IDs per gNB ID.

Note: Network operators can re-use the assigned gNB ID across multiple gNBs, using different cell identities to distinguish between the cells on the different gNBs. We still recommend getting 1 gNB ID per base station, in order to prevent potential accidental collisions.

5GS – Tracking Area Codes (TACs)

5G uses a TAC that is 24 bits long, 8 bits longer than in LTE. The OnGo Alliance is considering several options for assigning and managing 5G TACs. As an interim solution, 5G TACs can be obtained from the OnGo Alliance for use in 5G networks on a provisional basis. Once the final mechanism is determined, TACs may need to be adjusted. Holders of 5G TACs will be notified, and this document updated.

5GS Release 16 – 5G-NID

As noted above, Release 16 added support for SNPNs, and by defining a 5G NID eliminated the need managing identifiers in release 16. The managed identifiers discussed above (AMF Region + Set ID, gNB ID, TACs) – are only needed for release 15 networks, or release 16 networks that don't support the 5G NID system. You *can* use the managed identifiers for a release 16 network that does support the 5G NID, but the 5G NID option is recommended, as roaming is supported when using the 5G NID.

Note: You still need to generate values for the AMF Region + Set IDs, gNB IDs and TACs, you just don't need to get managed values from the OnGo Alliance when deploying a network that supports SNPN operation.

IMSI Block Numbers

Rather than manage the entire 9-digit MSIN component of the IMSI, which would require OnGo network deployers to need to request IDs for each SIM they want to issue, we have divided the MSIN into a four-digit IMSI block number and a five-digit User Identification Number (UIN). This allows a network operator to issue up to 100,000 IMSIs (SIMS) per IBN. As the IMSI system is the same in both LTE and 5GS, IBNs are needed for both LTE and 5GS networks.

Table 12: IBN Definition Components

Component	Length	Description
IMSI	15 digits	Individual Mobile Subscriber Identity
PLMN-ID	6 digits	The PLMN-ID of the network that the user is a subscriber of.
MSIN	9 digits	Mobile Subscriber Identification Number, that uniquely identifies a network user.
IBN	4 digits	IMSI Block Number.
UIN	5 digits	User Identification Number.

Note: For various administrative and regulatory reasons, the IBNs are actually assigned and managed by the US IMSI Administrator, rather than the OnGo Alliance. This will be discussed further in the next section.

Note: The IMSIs and IBNs occupy the same number space in LTE and 5GS – a 5GS IMSI is the same as an LTE IMSI, and the same IMSI *cannot* used be used once for an LTE SIM and once for a 5G SIM.

Number Spaces – 5G vs. LTE

Except for the IMSI Block Number (IBN), the managed identifiers in LTE and 5G exist in separate number spaces. That is, an eNB ID of 1234 assigned to an LTE network is not also the gNB ID of a 5G network, and cannot be as a gNB ID unless you are also assigned the gNB ID of 1234. Likewise, an AMF Region + Set ID value cannot be used as an MMEGI. eNB IDs, gNB IDs, MMEGIs, and AMF Region + Set IDs all have separate assignment lists.

The exception to this being the IMSI – which is a single number space. There is no difference between an LTE IMSI and a 5G IMSI; they are the same thing, and there is no difference in their number spaces and allocations. By extensions, IBNs work the same way: there is not a list of LTE IBNs, and a different list of 5G IBNs. There is only one list of IBNs.

TACs derive from the IBN, and while they have different lengths in LTE (16 bits) and 5GS (24 bits), they still exist in the same number space. The LTE TACs essentially have the last 8-bits of the 5GS TAC truncated off of them, and are a subset of the 5GS TACs.

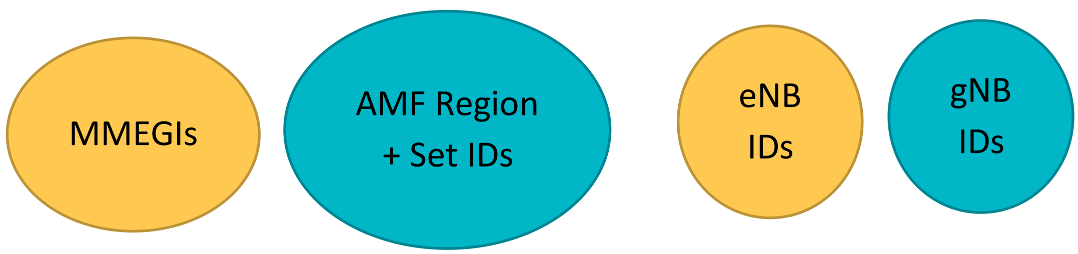


Figure 1: Venn Diagram chart of the separate number spaces.

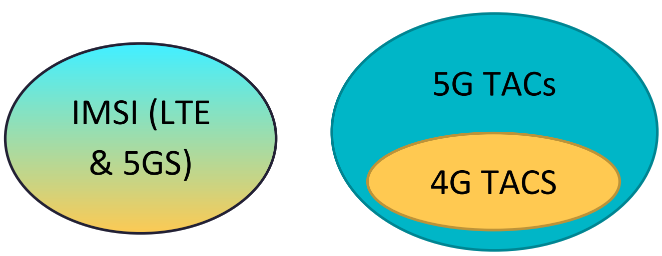


Figure 2: Venn Diagram chart of the shared number spaces.

OnGo Identifier Management

This section describes the processes associated with the identifiers managed by the OnGo Alliance (and the US IMSI Administrator), including how to get identifiers, and how to cancel them if you don't need them anymore.

High-Level Overview

Here are the basics:

- Identifiers can be obtained by anyone – not just OnGo Alliance members.
- We have an online store for reserving identifiers, which can be found here: https://ongoalliance.org/ongo-identifiers/.
- We charge an initial administrative fee to obtain identifiers, and an annual renewal fee to maintain them.
- Getting an IMSI Block Number works the same way, using form G: https://imsiadmin.com/imsi-form-g.
- The OnGo Alliance staff administers the identifier management program.
- Assigned identifiers are kept confidential.
- The primary contact for identifier management can be reached by email at shni@ongoalliance.org.
- The processes are documented in a pair of technical reports maintained by the OnGo Alliance – TR-0100 and TR-0101.

How to Get OnGo Identifiers

Identifiers can be obtained using our online portal, which can be found at https://ongoalliance.org/ongo-identifiers/. There is a link on the main page "Purchase OnGo Identifiers". The process is quite simple:

1. You tell us how many of what identifiers you need, provide basic contact information, and a credit card.
2. We assign the identifiers, record the information in our database, and send an email to you with the with the assigned identifiers.

We can also do manual orders and assignments if you need, though we add a surcharge if you go this route. Just email shni@ongoalliance.org, telling us what you need and who you are, and we'll issue an invoice.

How to Get IBNs

The process is pretty much the same for getting IMSI Block Numbers:

1. Fill out the form G on the US IMSI Administrator's website: https://imsiadmin.com/imsi-form-g.
2. They assign the IBN, and let you know what it is.

They do ask for information about your PAL license (if you have one) and if you have a contract with a SAS admin – mostly as evidence that you will actually be using the IBN they assign you.

OnGo Identifier Fees

We charge fees to obtain identifiers, to cover our administrative costs, and to discourage companies from reserving identifiers that they don't need. We also offer a package of identifiers that provides a complete set at reduced cost.

Component	Initial Fee	Annual Renewal Fee
LTE Identifier Package 1x CBRS-NID 1x MMEGI 100x eNB IDs	$325	$150
5GS Identifier Package 1x CBRS-NID 1x AMF Region + Set ID 100x gNB IDs	$325	$150
CBRS-NID	$40	$15
MMEGI	$125	$50
eNB ID	$2	$1
AMF Region + Set ID	$125	$50
gNB ID	$2	$1
TAC	$0	$0
IBN (to US IMSI Admin)	$325	$325

How to Cancel Identifiers

If you no longer need some or all of your identifiers, we can cancel them, and return them to the pool of available identifiers. Just email shni@ongoalliance.org, and we'll take care of it.

Confidentiality

Assigned identifiers are treated as confidential information, and not published. Summary information about how many identifiers have been assigned is provided periodically to the OnGo Alliance members, but who has been assigned what identifiers is not shared without the express permission of the company that has those identifiers.

Note: IBN assignments are not confidential, and by default get posted to the US IMSI administrator's website: https://imsiadmin.com/cbrs-assignments.

Troubleshooting

If you do run into a problem with your assigned identifiers, such as a collision with another network in your area that is using the wrong identifiers, we will facilitate resolving the issue and provide points of contact where they are known.

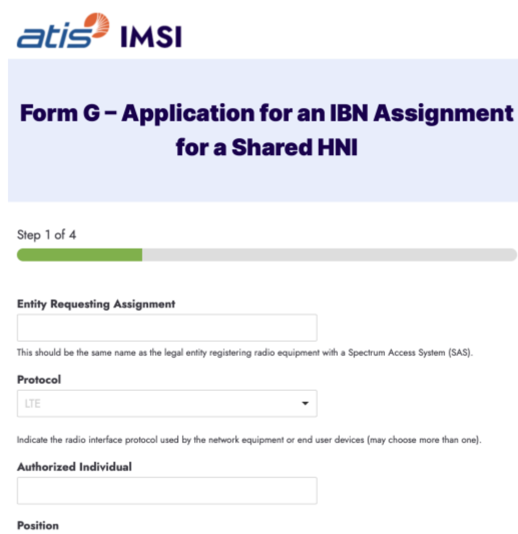
IBN Management

As discussed above, we use a (slightly) different system for managing International Mobile Subscriber Identifiers (IMSIs) – we have divided the 9-digit Mobile Subscriber Identification Number (MSIN) component of the IMSI into a 4-digit IMSI Block Number (IBN) and a 5-digit User Identification Number (UIN). The benefit to you is that you don’t have to get each individual MSIN assigned to you. Instead you get an IBN, and with that, you can generate up to 100,000 UINs, allowing you to issue 100,000 IMSIs.

For various administrative reasons, IBNs are assigned by the US IMSI Administrator – ATIS.

Obtaining an IBN – Form G

Getting an IBN from ATIS is relatively straightforward – you just need to fill out Form G on the IMSI administration website (https://imsiadmin.com/forms/form-g-application-for-an-ibn-assignment-for-a-shared-hni/). Since the available number space is limited, they require that you show evidence of intent to provide services with your IBN. For PAL licensees, you can just provide the PAL License Number from the FCC. For GAA users, you need to provide documentation that you have contracted with a SAS administrator.



Deploying Your Network – Form I

Once you deploy and turn on your network, you need to inform ATIS using Form I (https://imsiadmin.com/forms/form-i-deployment-confirmation-for-ibn-assignment-for-shared-hni/). Formally, until you turn on your network and fill in Form I, the assignment of the IBN isn’t complete.

Changing Information for an IBN – Form J

If there is a change in the information related to an assigned IBN (such as a change in company name or address or anything you provided in Form G) you use Form J (https://imsiadmin.com/forms/form-j-modification-of-ibn-assignment-for-a-shared-hni/) to notify ATIS.

Return an Unused IBN – Form L

If you no longer need an assigned IBN – if for example, you got your own PLMN-ID, and are no longer using the CBRS SHNI – you can return the IBN to the available pool using Form L (https://imsiadmin.com/forms/form-l-ibn-for-shared-hni-return/).

Managing Assigned OnGo Identifiers

Many of the operators of OnGo networks do not have experience in managing the identifiers of 3GPP networks, as this has previously been the domain of the major network operators. This section provides some guidance on best practices.

A note on terms: Assigned Identifiers are the managed identifiers that have been assigned to your organization by the OnGo Alliance (or the US IMSI Administrator, for IBNs). Allocated Identifiers are the Assigned Identifiers that are actively in use in your network.

Assign an Identifier Manager

We recommend that you define a single person as being responsible for managing the identifiers. The Identifier Manager is responsible for requesting new assigned identifiers from the OnGo Alliance, and allocating them to your network.

For particularly large networks with lots of identifiers, it may make sense to have this task handled by a group, rather than an individual.

We also recommend you define backups for the responsible person or group, able to handle the task when the primary is unavailable.

Record Identifier Allocations

Another "best practice" to consider is maintaining a database of which of the Assigned Identifiers have been allocated, and where those Allocated Identifiers are being used. The following elements should be tracked:

For LTE networks:

- For each MME instance:
    - MMEGI assigned (from OnGoA)
    - MMEC assigned
    - Responsible point of contact
- For each CBSD:
    - eNB ID assigned (from OnGoA)
    - Cell ID(s) assigned
    - TAC assigned (from IBN)

  - Where the CBSD is located
  - Other CBSD configuration info – such as category (A or B), manufacturer, etc.
  - Responsible point of contact

For 5G networks:

- For each AMF instance:
  - AMF Region + Set ID assigned (from OnGoA[1])
  - AMF Pointer assigned
  - Responsible point of contact
- For each CBSD:
  - gNB ID assigned (from OnGoA[1])
  - Cell ID(s) assigned
  - TAC assigned (from IBN)
  - Where the CBSD is located
  - Other CBSD configuration info – such as category (A or B), manufacturer, etc.
  - Responsible point of contact

You will also need to track the SIMs that you have issued:

- IMSI Block Number (IBN)
- User Identification Number (UIN)
- Phone number associated with SIM (if any)
- Device (UE/EUD) that the SIM is installed in
- Location of the device, if known/fixed
- User of the device
- Responsible point of contact
- Any other configuration info that may be set for specific SIMs.

[1] For 5GS SNPN's (Release 16 and later), you don't need to obtain the AMF Region + Set ID and gNB ID from the OnGo Alliance. You'll still need generate values for these identifiers, and track which ones you are using – you just don't need to get managed ones from the OnGo Alliance.

Maintaining the database should be the responsibility of the Identifier Manager. Depending on the scale of the network, a spreadsheet may be sufficient, but is not generally recommended.

We recommend that writing information to the database be restricted to the Identifier Manager, but that the information should be visible to anyone in your organization.

Ensuring that the database is backed up is critical – rebuilding the database after corruption or loss can be very painful.

Track Number of Unallocated Identifiers

If you have a large pool of assigned identifiers from the OnGo Alliance, we recommend the Identifier Manager keep track of how many of those identifiers are not currently allocated. Unallocated identifiers can be returned to the OnGo Alliance or held in reserve for future use. If you deploy multiple networks, or your network configuration changes frequently, the Identifier Manager can order new assigned identifiers when the pool of unallocated identifiers gets too low.

Define Identifier Processes

It's rarely a bad idea to define business processes, and handling your managed identifiers is no exception. Key processes to consider:

- Allocating identifiers from the pool of assigned identifiers, including who can request an allocation.
- Updating allocated identifier information.
- Deallocating identifiers.
- Investigating and resolving identifier collisions.
- Requesting more identifiers from the OnGo Alliance.

Frequently Asked Questions

This section addresses those questions that are asked most frequently regarding our identifier management program.

Does my network need identifiers?

If you don't have your own PLMN-ID, and you aren't deploying a Neutral Host Network, you will need to get identifiers.

Who should get the identifiers?

The OnGo Alliance doesn't mandate a particular party get the identifiers. It could be the venue owner, or a third party such as a solution provider or administrator.

Can I get identifiers even if I'm not a member of the OnGo Alliance?

Yes, anyone can request identifiers.

Do device makers need to get identifiers?

No. We have reserved identifiers for testing purposes, if you need them.

How long does it take to get identifiers assigned?

One or two days, typically.

When should I get my identifiers?

We recommend you get the identifiers once you know how many CBSDs you will be deploying. You won't be able to turn on your network without them, so getting them early helps ensure there won't be any problems.

How many identifiers do I need?

It depends on the identifier:

- CBRS NIDs – For most deployments, you just need one (1) CBRS NID. If you are deploying multiple networks, we recommend getting one for each network. Sharing CBRS NIDs across multiple networks is possible, but not recommend.
- MMEGIs – You just need one (1) MMEGI. Each MMEGI allows you to deploy up to 256 MMEs. Since a single MME can handle a lot of users and eNBs, most private

networks only need one MME. If you need more than 256 MMEs, your network is probably big enough that getting your own PLMN-ID would be worthwhile.

- eNB IDs – We recommend one per CBSD in your network. The ECGI includes an 8-bit cell identifier, so while you *could* re-use the same eNB ID across multiple CBSDs, using the different cell identifiers to distinguish them, we don't recommend doing so due to the risk of a misconfiguration. A collision won't typically break your network – things will still work – but it can decrease overall performance as the SON systems will not function well.
- IBNs – You need one of these for every 100,000 SIMs/devices you will be deploying.
- TACs – You get 6 for each IBN you have, which is sufficient for most deployments. The tradeoff with tracking areas is that, if you have lots of tracking areas, you get more signaling traffic overhead as the devices move around the network and notify the MME that they've changed tracking areas. If you have a small number of tracking areas, paging traffic overhead (when the network needs to establish a connection to a device) goes up, as each eNB in the tracking area tries to initiate the connection. In cases where your network has lots of isolated coverage areas, such as different buildings or multiple campuses, you may want to give each area its own TAC.

Why do you charge for identifiers?

Mostly to discourage companies from reserving identifiers that they don't need. The available pool of numbers is relatively limited – MMEGIs are only 16 bits – so we don't want to be wasting any of them by reserving numbers that aren't used.

Can I share IDs across networks?

In general, no – the whole point of managing identifiers is to prevent collisions. MMEGIs are a possible exception, as the 8-bit MMEC further distinguishes individual MMEs. If you are deploying multiple networks, you could use get a single MMEGI, and just make sure that each network uses different MMECs for their MMEs.

Frequently Asked Questions

Why are IBNs managed by someone else?

This is mostly for administrative reasons. The US IMSI Administrator (ATIS) has been given control of HNI assignments in the US, as delegated by the ITU, the IMSI Oversight Council and the US State Department. IMSIs are their domain, so the IBN system falls under their control.

Why does the IMSI Admin want a SAS administrator contract?

This is mostly to demonstrate that you intend to deploy a CBRS network. There aren't a lot of IBNs to hand out – there's only 9,999 IBNs that can be assigned, and we don't want to waste them.

Where do I get temporary or test identifiers?

We've set aside identifiers for testing purposes, at the top of the available range. Anyone can use them at any time. Collisions are not prevented; using on a live network is a bad idea. The reserved for testing identifiers are:

- CBRS NIDs: 134,217,680 to 134,217,711 (0x7FFFFD0 to 0x7FFFFEF)
- MMEGIs: 65,488 to 65,519 (0xFFD0 to 0xFFEF)
- eNB IDs: 1,048,528 to 1,048,559 (0xFFFD0 to 0xFFFEF)
- AMF ID: 262,112 to 262,143 (0x3FFE0 to 0x3FFFF)
- gNB IDs: 268,435,424 to 268,435,455 (0xFFFFFE0 to 0xFFFFFFF)
- IBN: 9,999
- TACs (LTE): 9,999; 19,999; 29,999; 39,999; 49,999; 59,999
    - In hexadecimal: 0x270F; 0x4E1F; 0x752F; 0x9C3F; 0xC34F; 0xEA5F
- TACs (5GS): 2,559,744 to 2,559,999; 5,119,744 to 5,119,999; 7,679,744 to 7,679,999; 10,239,744 to 10,239,999; 12,799,744 to 12,799,999; 15,359,744 to 15,369,999
    - In hexadecimal: 0x270F00 to 0x270FFF; 0x4E1F00 to 0x4E1FFF; 0x752F00 to 0x752FFF; 0x9C3F00 to 0x9C3FFF; 0xC34F00 to 0xC34FFF; 0xEA5F00 to 0xEA5FFF.

What about Physical Cell Identities?

Both LTE and 5GS use a Physical Cell Identity (PCI) in their synchronization signals. As these are not intended to be globally unique, there is no need for management of these identifiers. They are intended to be *locally* unique – different from the PCIs used by other nearby cells – and configuring the PCI is part of the deploying any LTE or 5GS network, regardless of being an OnGo network or not. Several websites track the PCIs used in different locations, such as http://www.cellmapper.net/ or http://www.antennasearch.com/.

Who Do I Go To For Help?

The administrators of the OnGo Managed Identifier program can be reached at shni@ongoalliance.org – if you have any questions that aren't answered here, send us a question at that address, and we'll do our best to answer.

Glossary

Term	Definition
5G GUTI	A GUTI in a 5GS network; 80 bits; composed of the PLMN-ID, AMF ID and 5G TMSI.
5G NR	5G New Radio, the radio interface component of the 5GS. Officially it is just the radio interface, but in practice is often used to refer to the entire 5GS.
5G TAC	5G Tracking Area Code; 24 bits; uniquely identifies a tracking area within a 5GS network; part of the 5G TAI; derived from the IBN for networks using the CBRS SHNI.
5G TAI	5G Tracking Area Identifier; 48 bits; uniquely identifies a tracking area; composed of the PLMN-ID and 5G TAC.
5G TMSI	5G Temporary Mobile Subscriber Identifier; 32 bits; part of the 5G GUTI.
5GC	5G Core, the core network component of the 3GPP's fifth generation wireless standard.
5GC NID	5GC Network Identifier; 40 bits; defined in 3GPP's Release 16 to support SNPNs; used in OnGo for the CBRS NID, with padding 0 bits prepended to be the same length.
5GS	5G System, the 3GPP's fifth-generation wireless standard.
Allocated Identifier	An assigned identifier that is currently in use by your network.
AM	Assignment Mode; 4 bits; indicates how the 5GC NID is assigned for Release 16 SNPNs; OnGo uses AM 2 (b0010) when using the CBRS SHNI.
AMF	Access and Mobility Management Function, the component of the 5GC that handles mobility and access control; 5GS version of the MME.
AMF ID	Access and Mobility Management Function Identifier; 24 bits; uniquely identifies the AMF in a 5GS network; composed of the AMF Region Identity, AMF Set Identity, and AMF Pointer; part of the GUAMI and 5G GUTI.
AMF Pointer	6 bits; identifies a specific AMF instance in an AMF Set; part of the AMF ID.
AMF Region ID	AMF Region Identifier; 8 bits; identifies an AMF Region in a 5GS network; part of the AMF ID; AMF Region + Set ID managed by OnGo Alliance for networks using the CBRS SHNI.
AMF Set ID	AMF Set Identifier; 10 bits; identifies a set of AMFs within an AMF Region; part of the AMF ID; AMF Region + Set ID managed by OnGo Alliance for networks using the CBRS SHNI.
Assigned Identifier	A managed identifier that has been assigned to your company, either by the OnGo Alliance (for most identifiers) or by the US IMSI Administrator (for IBNs).
ATIS	Alliance for Telecommunications Industry Solutions, the US IMSI Adminstator.
CBRS	Citizens Broadband Radio Service
CBRS-NID	A CBRS Network ID, 27 bits, that uniquely identifies a network using the CBRS SHNI.
CBRS SHNI	The CBRS Shared HNI; a PLMN-ID that can be used by multiple OnGo networks (315-010).
CBSD	Citizens Broadband Radio Service Device: Fixed Stations or networks of such stations that operate on a Priority Access or General Authorized Access basis in the Citizens Broadband Radio Service consistent with Title 47 CFR Part 96.
Cell ID	Cell Identifier; 8 bits; uniquely identifies a cell within an eNB; part of the ECI and ECGI.

Term	Definition
CPI	Certified Professional Installer, an individual authorized by the WInnForum to register information about a CBSD with the SAS.
CSG-ID	Closed Subscriber Group Identifier; 27 bits; identifies a closed group for purposes of network selection; used by LTE OnGo networks for the CBRS NID.
ECGI	E-UTRA Cell Global Identifier; 52-bits; uniquely identifies an LTE cell; composed of the PLMN-ID and the ECI.
ECI	E-UTRA Cell Identifier; 28-bits; uniquely identifies an LTE cell in an LTE network; composed of the eNB ID and Cell ID; part of the ECGI.
eNB ID	Evolved Node-B Identifier; 20 bits; identifies an eNB in an LTE network; part of the ECI and ECGI; managed by the OnGo Alliance for networks using the CBRS SHNI.
eNB	Evolved Node-B, an LTE base station
EPC	Evolved Packet Core provides network services to mobile devices in LTE
ESC	Environmental Sensing Capability
eSIM	Embedded SIM, a SIM system without a removable UICC/SIM card
EUD	End-User Device: an LTE or 5GS UE in OnGo (e.g., a smartphone, sensor, etc.).
E-UTRA	Evolved Universal Terrestrial Radio Access; the radio interface of LTE.
FCC	Federal Communications Commission
GAA	General Authorized Access
GHz	Gigahertz
gNB ID	gNB Identifier; 28 bits; uniquely identifies a gNB in an 5GS network; managed by the OnGo Alliance for networks using the CBRS SHNI.
gNB	A next Generation Node-B, a base station in the 5GS, 5Gs version of an eNB.
GUAMI	Globally Unique AMF Identifier; 48 bits; uniquely identifies the AMF of a 5GC; composed of a PLMN-ID and AMF Identifier.
GUMMEI	Globally Unique Mobility Management Entity Identifier; 48 bits; uniquely identifies an MME in an LTE EPC.
GUTI	Globally Unique Temporary Identifier; LTE and 5GS; 80-bits; assigned to a UE by the network to uniquely identify a device without using the IMSI.
HNI	Home Network Identifier; a 6-digit number composed of a MCC and a MNC. (Can be 5 digits, but is 6 digits in the US.) Also called a PLMN-ID.
IANA	Internet Assigned Numbers Authority
IBN	IMSI Block Number; 4 digits; component of the IMSI.
Identifier Manager	The person (or group) responsible for administering your company's Assigned Identifiers, and the associated processes.
IMSI	Individual Mobile Subscriber Identity; 16 digits; uniquely identifies as user/subscriber of a 3GPP network; composed of the PLMN-ID and MSIN (IBN + UIN in OnGo).

Glossary

Term	Definition
ITU	International Telecommunications Union
LTE	Long Term Evolution, the 4th generation mobile technology; used in OnGo
LTE GUTI	A GUTI in an LTE network; composed of the PLMN-ID, MMEGI, and S-TMSI.
LTE TAC	LTE Tracking Area Code; 16 bits; uniquely identifies a tracking area within an LTE network; part of the LTE TAI; derived from the IBN for networks using the CBRS SHNI.
LTE TAI	LTE Tracking Area Identifier; 40-bits; globally unique identifier of a tracking area; composed of the PLMN-ID and an LTE TAC.
LTE UE	LTE User Equipment: a device (mobile or fixed) used by an end-user to communicate (e.g., a smartphone).
MCC	Mobile Country Code; 3 digit component of the HNI/PLMN-ID that identifies the country where the network is located.
MHz	Megahertz
MME	Mobility Management Entity, the network element of an EPC that controls mobile device access to the EPC
MME Group	A collection of MMEs within a given network.
MMEC	MME Code; 8-bits; identifiers an individual MME within an MME Group; part of the GUMMEI and LTE GUTI.
MMEI	MME Identifier; 24 bits; composed of MMEGI plus the MMEC.
MMEGI	MME Group ID; 16 bits; identifies a specific MME Group within an LTE network; managed by the OnGo Alliance for networks using the CBRS SHNI.
MNC	Mobile Network Code; 3 digit component of the HNI/PLMN-ID that identifies the individual network. Can be 2 or 3 digits in general, 3-digits in the US.
MSIN	Mobile Subscriber Identification Number; 9 digits; uniquely identifies a subscriber within an LTE network; composed of the IBN and UIN in OnGo networks using the CBRS SHNI; part of the IMSI.
M-TMSI	MME Temporary Mobile Subscriber Identity; 32 bits; part of the S-TMSI and LTE GUTI.
NCGI	New Radio Cell Global Identifier; 52 bits; uniquely identifies a gNB; composed of the PLMN-ID, and NR Cell ID.
NHN	Neutral Host Network, an LTE network that provides coverage to multiple MNOs.
NR	New Radio, the name of the radio interface of the 3GPP's fifth generation standard.
NR Cell ID	New Radio Cell Identifier; 36 bits; uniquely identifies a cell within a 5GS network; composed of the gNB ID and Cell ID; part of the NCGI.
OnGo	LTE or 5GS networks operating in the CBRS band
PAL	Priority Access License

Glossary

Term	Definition
PCI	A number from broadcast by each cell, to distinguish it from other nearby cells. Value should be locally unique. In LTE there are 503 identities, while in 5GS, there are 1008. The PCI is not managed – configuring the PCI to be locally unique is the responsibility of the network operator.
PEN	Private Enterprise Number; globally unique identifier assigned by the IANA.
PGW	Packet Data Network Gateway, a network element of an EPC that provides connectivity from a UE to external packet data networks by being the exit and entry of traffic for UEs.
PLMN-ID	Public Land Mobile Network Identity; an HNI, as typically used in 3GPP specifications.
RF	Radio Frequency
SAS	Spectrum Access System, manages and assigns CBRS spectrum use on a dynamic, as-needed basis across PAL and GAA users.
SIM	Subscriber Identifier Module; the small card in a LTE/5GS UE device that identifies the subscriber to the network; contains the IMSI.
SNPN	Standalone Non-Public Network; part of 5GS release 16, adds a mechanism for using a shared PLMN-ID (like the CBRS SHNI) in 5G networks.
SON	Self-Optimizing Network; feature of LTE and 5GS networks that enables automatic optimization of adjacent base stations and cells to reduce interference.
S-TMSI	Serving Temporary Mobile Subscriber Identity; 40 bits; part of the GUTI.
TAC	Tracking Area Code; part of the TAI.
TAI	Tracking Area Identifier.
TPA	Training Program Administrator.
UE	User Equipment, a device using the mobile network
UICC	Universal Integrated Circuit Card, a SIM card.
WInnForum	The organization that develops the standards for CBRS system elements that include the SAS, ESCs, CBSDs, and CPI certification.