OnGo Alliance Identifier Guidelines for Shared HNI

OnGo-TR-0100

V1.2.2

December 14, 2021

LEGAL NOTICES AND DISCLOSURES

THIS SPECIFICATION IS PROVIDED "AS IS," WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EXPRESS, IMPLIED, OR STATUTORY; AND TO THE MAXIMUM EXTENT PERMITTED BY LAW, ONGO ALLIANCE, AS WELL AS ITS MEMBERS AND THEIR AFFILIATES, HEREBY DISCLAIM ANY AND ALL REPRESENTATIONS AND WARRANTIES, INCLUDING WITHOUT LIMITATION ANY WARRANTIES OF MERCHANTABILITY, TITLE, NON-INFRINGEMENT, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, OR RELIABILITY, OR ARISING OUT OF ANY ALLEGED COURSE OF PERFORMANCE, DEALING OR TRADE USAGE. ANY PERMITTED USER OR IMPLEMENTER OF THIS SPECIFICATION ACCEPTS ALL RISKS ASSOCIATED WITH THE USE OR INABILITY TO USE THIS SPECIFICATION.

THE PROVISION OR OTHER PERMITTED AVAILABILITY OF OR ACCESS TO THIS SPECIFICATION DOES NOT GRANT ANY LICENSE UNDER ANY PATENT OR OTHER INTELLECTUAL PROPERTY RIGHTS ("IPR"). FOR MORE INFORMATION REGARDING IPR THAT MAY APPLY OR POTENTIAL AVAILABILITY OF LICENSES, PLEASE SEE THE ONGO ALLIANCE IPR POLICY. ONGO ALLIANCE TAKES NO POSITION ON THE VALIDITY OR SCOPE OF ANY PARTY'S CLAIMED IPR AND IS NOT RESPONSIBLE FOR IDENTIFYING IPR.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES WILL ONGO ALLIANCE, OR ANY OF ITS MEMBERS OR THEIR AFFILIATES, BE LIABLE FOR DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, PUNITIVE, OR OTHER FORM OF DAMAGES, EVEN IF SUCH DAMAGES ARE FORESEEABLE OR IT HAS BEEN ADVISED OR HAS CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES, ARISING FROM THE USE OR INABILITY TO USE THIS SPECIFICATION, INCLUDING WITHOUT LIMITATION ANY LOSS OF REVENUE, ANTICIPATED PROFITS, OR BUSINESS, REGARDLESS OF WHETHER ANY CLAIM TO SUCH DAMAGES SOUNDS IN CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), PRODUCT LIABILITY, OR OTHER FORM OF ACTION.

THIS DOCUMENT (INCLUDING THE INFORMATION CONTAINED HEREIN) IS PROVIDED AS A CONVENIENCE TO ITS READERS, DOES NOT CONSTITUTE LEGAL ADVICE, SHOULD NOT BE RELIED UPON FOR ANY LEGAL PURPOSE, AND IS SUBJECT TO REVISION OR REMOVAL AT ANY TIME WITHOUT NOTICE. THIS DOCUMENT IS PROVIDED ON AN “AS IS”, “AS AVAILABLE” AND “WITH ALL FAULTS” BASIS. ONGO ALLIANCE MAKES NO REPRESENTATION, WARRANTY, CONDITION OR GUARANTEE AS TO THE USEFULNESS, QUALITY, SUITABILITY, TRUTH, ACCURACY, OR COMPLETENESS OF THIS DOCUMENT OR ANY INFORMATION CONTAINED HEREIN. ANY PERSON THAT USES OR OTHERWISE RELIES IN ANY MANNER ON THE INFORMATION SET FORTH HEREIN DOES SO AT HIS OR HER SOLE RISK.

IMPLEMENTATION OF A [NETWORK] AND/OR RELATED PRODUCTS OR SERVICES IS OFTEN COMPLEX AND HIGHLY REGULATED, REQUIRING COMPLIANCE WITH NUMEROUS LAWS, STATUTES, REGULATIONS AND OTHER LEGAL REQUIREMENTS (“LEGAL REQUIREMENTS”). AMONG OTHER THINGS, APPLICABLE LEGAL REQUIREMENTS MAY INCLUDE NETWORK OPERATOR REQUIREMENTS UNDER FEDERAL LAW, REQUIREMENTS RELATING TO E-911, ETC. A DISCUSSION OF SUCH LEGAL REQUIREMENTS IS BEYOND THE SCOPE OF THIS DOCUMENT. ACCORDINGLY, NETWORK OPERATORS AND OTHERS INTERESTED IN IMPLEMENTING NETWORKS OR RELATED SOLUTIONS ARE STRONGLY ENCOURAGED TO CONSULT WITH APPROPRIATE LEGAL, TECHNICAL AND BUSINESS ADVISORS PRIOR TO MAKING ANY IMPLEMENTATION DECISIONS.

OnGo Alliance
3855 SW 153rd Drive, Beaverton, OR 97003
www.ongoalliance.org
info@ongoalliance.org
Copyright © 2021 OnGo Alliance, All Rights Reserved

Table of Contents

Table of Figures

Table of Tables

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

1 Introduction and Scope

Successful broad deployment of LTE networks in CBRS spectrum (an OnGo Network) requires proper use of LTE network and device identifiers.

This document is a Technical Report that is intended for OnGo LTE operators that will be using a Shared HNI and not for operators that have their own HNI.

The subject of this document is a network based on OnGo Alliance specifications [2][6] that uses a Shared HNI (SHNI) as the CBRS-I. Such a network deployment is referred to as a "SHNI Network" in this document.

2 References

[1] ATIS IOC. IMSI Guidelines for Shared HNI for CBRS Range, http://www.atis.org/01_committ_forums/ioc/Docs/IMSI-CBRS-Guidelines.pdf

[2] OnGo Alliance. Network Services Stage 2 and 3 Specifications. OnGo-TS-1002.

[3] MulteFire Alliance. Architecture for Neutral Host Network Access Mode Stage 2. MFA TS MF.202.

[4] 3GPP. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3. TS 24.301.

[5] GSMA Embedded Mobile Guidelines - Network Aspects, Version 3. https://www.gsma.com/iot/wp-content/uploads/2012/03/GSMA-Whitepaper- Embedded-Mobile-Guidelines-Release_3-Network-Aspects1.pdf

[6] OnGo Alliance. Network Services Use Cases and Requirements. OnGo-TS-1001.

[7] 3GPP. Numbering, addressing and identification. TS 23.003.

[8] 3GPP. S1 Application Protocol (S1AP). TS 36.413.

[9] MulteFire. Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3. MFA TS 24.301.

3 Definition and Abbreviations

3.1 Definitions

Term	Definition
BSSID	Basic Service Set Identifier.
CBRSA	CBRS Alliance. Former name of the OnGo Alliance.
CBRS-NID	CBRS Network ID (27 bits).
CSG	Closed Subscriber Group. GSM/LTE concept re-used by OnGoA as CBRS-NID. See [2] and [7].
DSC	Diameter Signaling Controller.
ECGI	E-UTRAN Cell Global Identifier, composed of HNI + eNB ID (20 bits) + Cell ID (8 bits). See [8].

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

eNB ID	Portion of ECGI that identifies a group of cells and is assigned by the OnGo Alliance. Also called the Macro eNB ID.
ESQK	Emergency Services Query Key.
GUMMEI	Globally Unique MME ID (48 bits).
HNI	Home Network Identifier: MCC+MNC (6 decimal digits[1]).
IBN	IMSI Block Number (4 decimal digits).
IMEI	Individual Mobile Equipment Identity.
IMSI	Individual Mobile Subscriber Identity. Subscription number (15 decimal digits)., see [7]. For Shared HNI: SHNI+IBN+UIN, see [1].
IMSI-A	US IMSI Administrator. http://imsiadmin.com
MCC	Mobile Country Code (3 decimal digits). Assigned by ITU-T to a country
MME	Mobility Management Entity
MMEC	MME Code (8 bits)
MMEGI	MME Group ID (16 bits)
MMEI	MME ID = MMEGI + MMEC
MNC	Mobile Network Code (2-3 decimal digits). Assigned by national IMSI administrator to one operator or, in the case of Shared HNI, to multiple CBRS-I operators
MNO	Mobile Network Operator. A wireless carrier (e.g., Verizon, T-Mobile, etc.)
NR	New Radio. The 3GPP 5G wireless interface.
OnGoA	OnGo Alliance. Formerly the CBRSA.
PLMN-ID	Synonym for HNI.
PSP-ID	Participating Service Provider ID. HNI, OID, domain name or a 24-bit reduction of a longer identifier.
SHNI	Shared HNI. An HNI designated by ATIS IOC for CBRS operation that is recognized by CBRS systems as shared. The first such assignment is 315-010.
SHNI Network	A network that broadcasts a Shared HNI as its identity (supplemented by a CBRS-NID for uniqueness).
TAC	Tracking Area Code (16 bits).
TAI	Tracking Area Identity. SHNI + TAC
TAU	Tracking Area Update.
UIN	User ID Number within IMSI (5 decimal digits).

[1] Decimal digits are encoded as 4-bit BCD unless otherwise specified.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

4 Goals

One of the purposes of the OnGo Alliance is to coordinate the equipment and activities of manufacturers, operators, SAS providers and other participants in the Citizens Broadband Radio Service (CBRS) shared spectrum ecosystem, to speed time to market, reduce cost, and increase the reliability and interoperability of systems based on LTE standards.

One of the ways these goals can be accomplished is through the development of specifications or guidelines specifically oriented to operation in the CBRS spectrum that are not addressed by 3GPP or other organizations. This document presents background information and recommendations related to the coordination of the following important identifiers for network and user equipment (UE), and explains why they benefit from being globally or locally unique:

- Shared HNI. A specific combination of 3-digit Mobile Country Code (MCC) and 3-digit Mobile Network Code that indicates that the network is using a Shared HNI (SHNI). This code is shared by many operators, and is therefore not unique to a single operator. At present there is just one such number (315-010), but there could be more in the future.
- CBRS-NID. The Network ID is based on the LTE CSG-ID (Closed Subscriber Group ID) and supplements the Shared HNI. Together they can provide a globally unique identity for a single SHNI Network.
- IMSI. An IMSI is the 15-digit globally unique wireless subscription identity and is stored in the SIM/UICC inserted or embedded in a UE. For devices provisioned for an SHNI Network, the Shared HNI will be used in the IMSI as MCC+MNC. Devices with an IMSI based on a non-shared HNI that roam into an SHNI Network (e.g., NHN) could continue to use their existing IMSI [7].
- E-UTRAN Cell Global Identifier (ECGI). Every LTE base station (eNodeB) is intended to be uniquely identified by an ECGI that is composed of PLMN-ID and Cell ID. For an OnGo Network, the Shared HNI is used as the PLMN-ID within the ECGI [7].
- MME ID (GUMMEI). Every Mobility Management Entity in an LTE system requires a globally unique MME ID. Because it contains the Shared HNI as a prefix, GUMMEI values must be coordinated within the Shared HNI [7].
- Tracking Area ID (TAI) needs to be locally unique, with no neighboring systems using the same value [7].

Unique identifiers are important in communications systems because communication systems often do not function correctly with duplicate identifiers. For example, it is possible that two mobile devices with the same IMSI will not work properly and eventually both may be blacklisted (unable to receive service) after failing authentication. Similarly, hardware identifiers like IMEI are required to be globally unique.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

5 Problems with Non-Uniqueness for Key Identifiers

This section examines the uniqueness requirements of several key identifier types that are essential to the operation of OnGo LTE networks.

5.1 [LTE and 5G NR] Home Network Identifier (HNI)

Normally an HNI is assigned to a single operator, and the operator is responsible for managing the uniqueness of IMSI codes and other identifiers constructed using the HNI. However, ATIS IOC has made it possible for the new Shared HNI to be used simultaneously by a large number of operators in the CBRS ecosystem. Coordination of the relevant “CBRS Shared HNI” identifiers described in this document will be administered by the OnGo Alliance [1].

5.2 [LTE and 5G NR] IMSI Block Number (IBN)

Every subscriber has an IMSI stored within their ‘smart card’ (UICC) or embedded in the device (eUICC). It is the 15-digit globally unique wireless subscription identity consisting of HNI+MSIN (Mobile Subscription Identification Number). Normally an operator is assigned an HNI for exclusive use, and is responsible for assignment of the MSIN codes to subscribers.

However, for a Shared HNI (SHNI), MSIN is further broken down into IBN+UIN. An OnGo operator that has subscribers (i.e., ‘smart cards’ or UICC for each subscription, whether removable or embedded) is responsible for obtaining at least one IBN for their exclusive use. The Shared HNI + operator-specific IBN then forms a globally unique operator identifier.

The OnGo operator is responsible for creating unique identifiers by allocating a different UIN to each subscriber/subscription. If the OnGo operator fails to obtain an operator-specific IBN for its subscribers, then the global uniqueness of their IMSIs is no longer guaranteed, and the following problems can occur:

- Authentication of the subscription will fail if the wrong MME is queried based on the non-unique IMSI.
- Network operations will fail when the IMSI is used to route messages (e.g., to an MME).

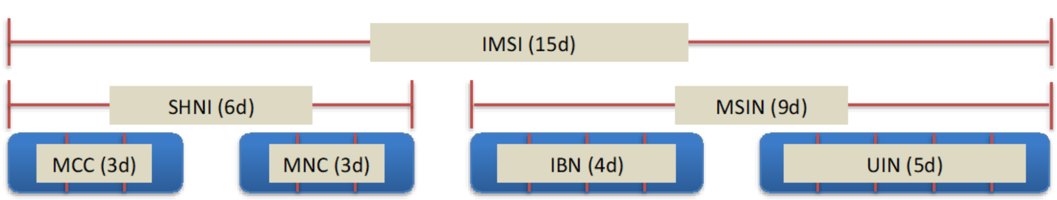

Figure 1: IMSI Components

5.3 [LTE and 5G NR] CBRS-NID – Network ID

The CBRS-NID (the LTE Closed Subscriber Group ID, CSG-ID) is essentially an extension to the Shared HNI that creates a composite, globally unique, operator identity. The use of CSG-ID as CBRS-NID is described in [2].

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

The OnGo Alliance maintains a register of CBRS-NID codes and ensure that any single code is only ever assigned to a single operator[2], thus achieving global uniqueness among operators using the OnGo Alliance CBRS-NID codes.

If a non-unique CBRS-NID is used by one network (Network ‘B’) that is the same as the CBRS-NID assigned to another network (Network ‘G’) then a mobile device from Network ‘G’ encountering Network ‘B’ can attempt to register on this network, and the mobile’s registration will be rejected by Network ‘B’ with e.g., a Cause Value of 3 (Illegal UE) or 8 (EPS services and non-EPS services not allowed). The mobile will then consider its USIM as invalid (see 3GPP TS 24.301 [4] section 5.3.7b and the mobile will not attempt to register when it later encounters its own Network ‘G’. The mobile would return to normal after a power cycle, when the USIM is replaced, or when timer T3245 in the device expires (up to 48 hours) [4][5].

To avoid this problem, OnGo Alliance TS-1002 [2] recommends using Cause Value 15 (No suitable cells in tracking area) when an ATTACH REJECT, TRACKING AREA UPDATE REJECT or SERVICE REJECT is sent to a UE.

Note: An OnGo network using the Neutral Host Network (NHN) architecture defined by the OnGo Alliance in [2], must use a CBRS-NID to identify the NHN.

Note: Few LTE UEs support the CSG-ID mechanism, due to power consumption impacts of supporting CSG-IDs, and lack of demand from the Mobile Network Operators (MNOs). As such, an LTE UE configured to use the CBRS Shared HNI will attempt to connect to any network using the CBRS Shared HNI, regardless of the CBRS-NID broadcast by the network. This will result in OnGo networks using the CBRS Shared HNI having unrecognized devices attempt to connect. This makes the above guidance more critical to ensure that the LTE UE will quickly attempt to connect to the next available network, and find the desired OnGo network by process of elimination.

Unfortunately, an unassociated operator, outside of the Alliance, could use the CBRS Shared HNI without coordination with the Alliance and might select a NID that has assigned to a network by the OnGo Alliance. The OnGo Alliance will take appropriate efforts to avoid conflicts, e.g., by facilitating the assignment of NIDs used by non-OnGo Alliance members.

5.4 [LTE] EUTRAN Cell Global Identifier (ECGI)

The ECGI is a globally unique identifier for an LTE cell or sector, comprised of HNI and Cell Identity. Cell Identity includes the eNB ID. See requirement RAN-Share-005 [6]. The ECGI will not distinguish between multiple CBSDs that broadcast the same system parameters [7][8]. Duplicate ECGIs in different operator networks can cause the following problems:

- **Broken LTE Assumption.** LTE specifications are based upon the assumption that ECGI is globally unique. It is impossible to rule out the possibility that problems will occur with duplicate ECGI that were not known to the authors of this document. Those that are known are listed below.
- **Erroneous E911 call routing and dispatch.** Traditionally, a database of ECGIs is maintained to provide an approximate location and blocks of PSAP routing numbers (ESQK) for 9-1-1 calls when a GPS location is not available (or before a GPS location is available). Duplicate ECGIs could result in the wrong location or wrong routing number being provided to the 9-1-1 call takers at the PSAP if third party or shared

[2] CBRS-NID codes should not be re-used. In the future, the IMSI-A may assign additional HNI codes and there is no way to correlate NID (CSG-ID) with a specific HNI within SIB-1.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

infrastructure is used to interpret the ECGI. Given the complexity of routing to E911 PSAPs it is most likely that the conversion from ECGI to approximate location to routing number is done by a third party.

Slow or inaccurate GPS positioning. GPS positioning significantly benefits in speed and accuracy from an initial 'reference' location (accurate within a few miles) that is normally based on the known location of each base station as identified by an ECGI. Widely used location-based applications (e.g., mapping and navigation apps) rely on a global database of ECGI held by a third party. Through the use of the OMA SUPL protocol and this database, the ECGI is translated to a reference location (e.g., tower latitude and longitude), without operator knowledge or intervention.

- **Failure to meet E911 Mandates.** GPS location is usually used in dispatching E911 calls, and has timing and accuracy requirements imposed by the FCC. Failure to achieve these requirements on a regular basis because of duplicate ECGI information could constitute a violation of FCC rules for operators that are within the E911 mandates.
- **Billing and Accounting Problems.** ECGIs are normally provided in billing information records produced by the AAA. While it will probably not cause billing to the wrong carrier, it could cause confusion over the location of the call when the records are being examined for various purposes, including legal.
- **Difficulty Identifying Interference.** ECGIs may be used to identify an operator when trying to locate the source of an interfering signal. An ECGI that is duplicated will make this more difficult.
- **RF Measurement Exchange Difficulties.** The use of unique ECGIs could facilitate exchange of measurement information between OnGo Alliance systems.

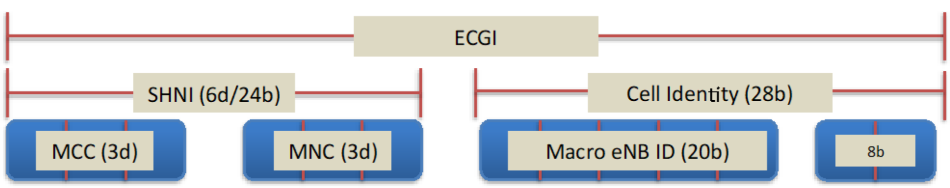

Figure 2: ECGI Components

5.5 [LTE] Globally Unique MME Identity (GUMMEI) [7]

The MME Identity (MMEI), in conjunction with the Shared HNI (MCC+MNC), uniquely identifies a Mobility Management Entity. Lack of uniqueness could prevent operators from supporting roaming of their users to other SHNI Networks, as information related to roaming devices could not be routed to the appropriate MME.

Special routing equipment known as a Diameter Signaling Controller (DSC) could be needed to receive Diameter messages containing the IMSI of the UE (e.g., an attempt to validate the UE by a roaming partner) and use the IBN within the IMSI to determine the network, and then the associated MMEGI.

MME Group ID uniqueness is required if multiple MMEs are using the shared HNI.

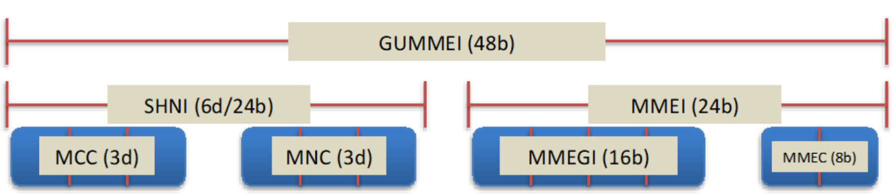

Figure 3: GUMMEI Components

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

5.6 [LTE] Participating Service Provider (PSP-ID)

If Neutral Host Network (NHN) services are provided, the system must broadcast a list of 24- bit PSP-IDs to identify operators whose subscribers are allowed to access service on the SHNI Network.

PSP-IDs come in four types, that originate from different assignment processes:

1. HNI (PLMN-ID). 6 decimal digits (24 bits) formed as the BCD digits of MCC+MNC (HNI).
2. 24-bit OID. One type of OID known as OUI is 24 bits in length. See: http://standards-oui.ieee.org/bopid/opid.txt
3. Other OID. An OID longer than 24 bits is used to create a 24-bit PSP-ID using the SHA- 256 hashing algorithm.
4. Domain name. The domain name is used to create a 24-bit PSP-ID using the SHA-256 hashing algorithm.

The OnGo system also supports three different values of ‘bssid’ to indicate the type of PSP-ID:

- 03:ff:ff:ff:ff:ff indicates type 1 (HNI).
- 03:ff:ff:ff:ff:fe indicates type 2 (24-bit OID).
- 03:ff:ff:ff:ff:fd indicates type 3 or 4 (longer identifier hashed to 24 bits).

Type 1 PSP-IDs will be unique if the HNI is unique, but would not be unique if, for example, the PSP was another OnGo operator using the CBRS HNI.

Type 2 OID PSP-IDs will also be unique as long as a unique 24-bit identifier is obtained from IEEE.

Types 3 and 4 (24-bit hash) will not be guaranteed to be unique.

A non-unique PSP-ID could result in a device attempting to access a network and being rejected. This could result in period of time (e.g., several minutes) during which the UE might not attempt to access other systems for which it is authorized (see section 5.3.7MF1 of [9]).

5.7 [LTE] Tracking Area Identity (TAI) [7]

The Tracking Area Identity (TAI) is used to coordinate between neighboring OnGo LTE systems. When using a Shared HNI, operators need to coordinate the TAI. The TAI is composed of the HNI plus a 16-bit TAC (Tracking Area Code). Coordination of TACs within the Shared HNI is essential for the UE rejection mechanisms as per OnGo Alliance specification [2] §5.5.3.1 to work properly.

If a UE is rejected when presenting a TAI to the network, the UE might not attempt to access any network broadcasting that TAI for a period of time (e.g., several minutes; see section 5.3.7MF1 of [9]). Therefore, it is important that TAC codes (the only unique part of the TAI within a Shared HNI, i.e., SHNI) are coordinated. In situations where coordination is necessary, it can be done by neighboring OnGo operators. No coordination with MNOs is necessary, because they use a TAI based on their own distinct HNI (not SHNI).

5.7.1 IBN-Derived TACs

The Tracking Area Code is assigned by the operator, not by the OnGo Alliance, and needs to be locally unique (i.e., not used by any other nearby network broadcasting SHNI). The full TAI format is SHNI (6d/24b) + TAC (16b). OnGo Network Operators using the SHNI use the following method to define 6 TAC codes that will produce TAI codes that will not conflict with any other SHNI Network using the same method:

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

1. The first TAC is the 16-bit binary code for the numeric value of the network's assigned IBN.3
2. This code plus 10,000.
3. This code plus 20,000.
4. This code plus 30,000.
5. This code plus 40,000.
6. This code plus 50,000.[3]

For example, for the IBN code 1234, the six TAC values will be 01234, 11234, 21234, 31234, 41234 and 51234.

The highest possible code is 59999 with the above scheme, smaller than the highest 16-bit value of 65535. The TACs above this 59999 ceiling are managed by the OnGo Alliance.

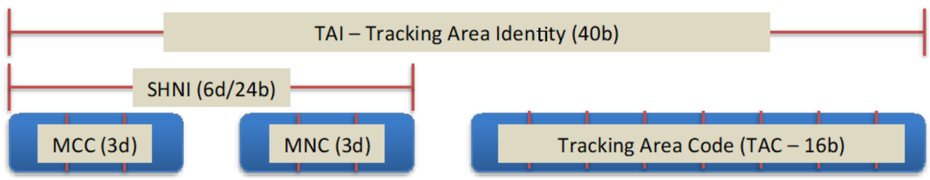

Figure 4: TAI Components

5.7.2 Managed TACs (Optional)

For some deployments, the 6 TACs associated with an IBN will not be sufficient. For example, a network may have multiple isolated "islands" of coverage, which each need their own TAI/TAC. If they do not have a large number of subscribers, acquiring additional IBNs would consume the available domain of IBNs unnecessarily.

To address this circumstance, the pool of TACs between 60,000 and 65,535, which is otherwise unused by the above system of deriving TACs from the IBN, is managed by the OnGo Alliance. OnGo Network Operators may request TACs from this pool when they need or desire additional TACs.

TACs only need to be locally unique. Therefore, re-use of Managed TACs is possible. If the pool of Managed TACs is determined to be depleting too quickly (e.g., faster than the available pool of IBNs is being depleted), the OnGo Identifier Administrator may begin tracking the geographic state or states where the Managed TAC are being used. Managed TACs can then be re-used for networks that will be deployed in geographically distant states. If further re-use is needed, the OnGo Identifier Administrator may begin tracking the counties where the Managed TACs are in use, and re-using those TACs for networks that will be deployed in geographically distant counties. All location information will be treated confidentially.

5.8 [5G NR] 5G NR Identifiers

Within 5GS, private networks can be deployed as Standalone Non-Public Networks (SNPN) or Public Network Integrated Non-Public Networks (PNI-NPN).

In a SNPN, 3GPP introduced new identifiers associated with SNPN, the NID. The NID consists of a 4-bit Assignment Mode (AM) and a 40-bit NID value. Three Assignment Modes are defined (0, 1, and 2).

[3] Note that the IBN is usually encoded as BCD, in which case 9999 would be binary 1001 1001 1001 1001. However, the TAC should be encoded as a binary integer, so 9999 would be binary 0010 0111 0000 1111.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

5.8.1 Assignment Mode 0 – IANA Private Enterprise Number (PEN)

In this mode, a Private Enterprise Number, as assigned by the Internet Assigned Numbers Authority (IANA), is used as the NID to ensure global uniqueness. The IANA assigned PEN is 32-bits, with the remaining 8-bits as NID Code used to distinguish up to 256 networks. Assignment Mode 0 is outside of the scope of OnGo managed identifiers.

The list of PENs can be found here: https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

PENs can be obtained using the form here: https://pen.iana.org/pen/PenApplication.page

5.8.2 Assignment Mode 1 – Self-Assigned

Self-assigned numbers have no guarantee of global uniqueness, and is not recommended by the OnGoA.

5.8.3 Assignment Mode 2 – Globally Unique With PLMN-ID

In AM 2, the NID must be globally unique when combined with the PLMN-ID. For networks using the CBRS SHNI, the CBRS-NID can be used. The CBRS-NID is 27 bits. The remaining 13 bits of the NID are padded with 0's. The CBRS-NID in this context is the same in the CBRS-NID described in §3.3, above, and will come from the same pool.

Table 1: 5G-NR Assignment Mode 2 Network Identifier

Portion	AM	Reserved	Identifier
Content	0010 (2)	0000 0000 0000 0	CBRS-NID
Size in Bits	4	13	27

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

6 Deployment Considerations

6.1 Systems Not Needing Uniqueness

It may be that some OnGo LTE systems will not need identifier uniqueness because when installed they may have most or all of the following characteristics:

- The only OnGo system in a geographical area.
- Do not accept incoming calls.
- Do not provide roaming or Neutral Host Network services.
- Do not allow outbound roaming by their own subscribers.
- Are not required to provide E911 service.
- Do not support third party location-enabled applications.
- Have no other need for unique identifiers.

However, these characteristics may well change over time, and in the worst case, could require later renumbering of the network, the replacement of every SIM card, communication and coordination with third party network elements for roaming and charging, changing the identification of every cell, and so on. Also, devices from a network with non-unique identifiers could attempt to register on another network with the same CBRS-NID (not realizing it is roaming), fail registration, then be unusable for a period of time even back on the home network. Similarly, these networks with non-unique identifiers could impact devices from other networks. The small effort of ensuring identifier uniqueness might not provide an immediate benefit, but could prevent a much larger effort in the future.

6.2 Problems with Self-Assigned Identifiers

Some problems with setting aside a self-assigned block of identifiers are:

- Operators may have no choice but to assign unique IMSI and CBRS-NID codes, in which case self-assigning MME Group IDs and ECGIs are likely unnecessary if, for example, the OnGo Alliance automatically assigns a block of MME Group IDs and ECGIs with every Network ID.
- Operators that do not want to coordinate cannot be relied upon to properly configure their identifiers in the self-assigned address space, and may still conflict with legitimately assigned identifiers.
- Even if the self-assigned address spaces are large, conflicts may be more likely than expected (e.g., if multiple carriers assign ECGIs in sequence starting with zero).
- Loss of a portion of the address space for OnGoA Administration (50% if the first bit is used to distinguished between managed and self-assigned addresses).

6.3 Identity Administrators

Responsibility for administering identifiers important to OnGo Alliance members is shared between the US IMSI Administrator and the OnGo Alliance, as shown in the table below.

This does not consider operators who do not use OnGo Alliance coordination services.

For identifiers that are allocated by the IMSI Administrator (IBN and Shared HNI) the OnGo Alliance database may still need to store this information, at least for some operators.

Table 2: Identifier Administrator Summary Tables

Identifier	Assigned by…			Identifies	Quantity
	IMSI Admin	OnGoA	OnGo Operator		
IMSI	MCC+MNC (SHNI) + IBN	—	UIN	Subscription	10,000 IBN x 100,000 UIN per SHNI
CBRS-NID (LTE & NR[4])	—	CBRS-NID (Conditional[5])	—	Network	2^{27} per SHNI[6]
GUMMEI (LTE Only)	SHNI	MMEGI	MMEC	MME	2^{16} MMEGI x 2^{8} MMEC per SHNI
ECGI (LTE Only)	SHNI	eNB ID	Cell Identity	Cell or sector (eNodeB)	2^{20} eNB ID x 2^{8} Cell Identity per SHNI
TAI/TAC (LTE Only)	SHNI	Optional (see §5.7.2)	IBN-derived TAC (see §5.7.1)	Tracking area	65,534 per region of overlap

6.4 Business Process

If an operator of one or more SHNI Networks needs IMSI codes (i.e., will have UEs homed on the SHNI Network) it can obtain one or more IBNs (IMSI Block Numbers) from the US IMSI Administrator [1]. One IBN can be used for any number of networks controlled by the same account (e.g., OnGo operator). These IMSI codes will be allocated from a Shared HNI designated by the IMSI Administrator for this purpose.

It is beneficial to all industry participants that CBRS-NID, MMEGI and ECGI are obtained from the OnGo Alliance. Any organization wishing to be assigned identifiers for use with an SHNI Network must first establish an account along with a list of contact personnel who are authorized to obtain identifiers on behalf of the organization. One account can be used to establish any number of SHNI Networks.

To obtain an assignment of the identifiers needed for a single SHNI Network the account holder will have to request an assignment of the following from the OnGo Alliance for each network:

- A single CBRS-NID. This number will be broadcast in the CSG-ID field of SIB 1 [7] to uniquely identify the SHNI Network (as the Shared HNI that is also broadcast is not sufficient to identify the network).
- One MME Group ID. Since one MME Group ID can be used to create 256 unique GUMMEI it is unlikely that more than one will be needed by an SHNI Network but if needed, more than one can be allocated to a network.
- One or more eNB IDs. The size and configuration of the network will dictate the quantity of eNB IDs required.

4 5G NR Standalone Non-Public Networks may use the CBRS-NID for the value of the 5GC-NID in Assignment Mode 2, per OnGo-TS-1002 [2].

5 CBRS-NID is mandatory in the support of CBRS NHN architecture as defined per OnGo-TS-1002 [2], but optional for all other deployments including private enterprise deployments and NHN as per 3GPP MOCN

6 It may not be possible to re-use the same CBRS-NID in multiple SHNI, in which case this would be a global quantity.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

- One or more IBNs. Assigned by the US IMSI Administrator, but may be voluntarily stored in the OnGoA database, along with the OnGoA assigned identifiers to facilitate roaming.

6.5 Identifier Management Principles

OnGo Alliance will carefully manage the identifiers to ensure that the limited supply lasts for many years based on the following principles:

- Verify that a new account is a OnGo operator.
- Verify that the quantity of numbering resources requested is reasonable.
- Keep in contact with the OnGo operator to regularly verify that the assigned codes are in use.
- Reclaim codes that are no longer needed.
- Educate the OnGo industry on the need for identifier coordination.
- Document the assignments of SHNI and IBN codes provided to the OnGo Alliance.
- Coordinate the assignment and management of NID, ECGI and MMEGI codes.
- Monitor IBN assignments within CBRS Shared HNI(s) and coordinate as needed.
- Maintain confidentiality of assigned identifiers, only providing aggregate information to the OnGoA, and only publishing information about the identifiers associated with a given company with their permission.
- Aid in resolving identifier collisions and related problems in the field by facilitating communications with other relevant assignees, consistent with maintaining confidentiality as noted above.

6.6 Process Implementation

Assigned identifiers will be stored in a database with a web interface for OnGo Alliance identifier assignments. The relationships between the elements of this system are shown below.

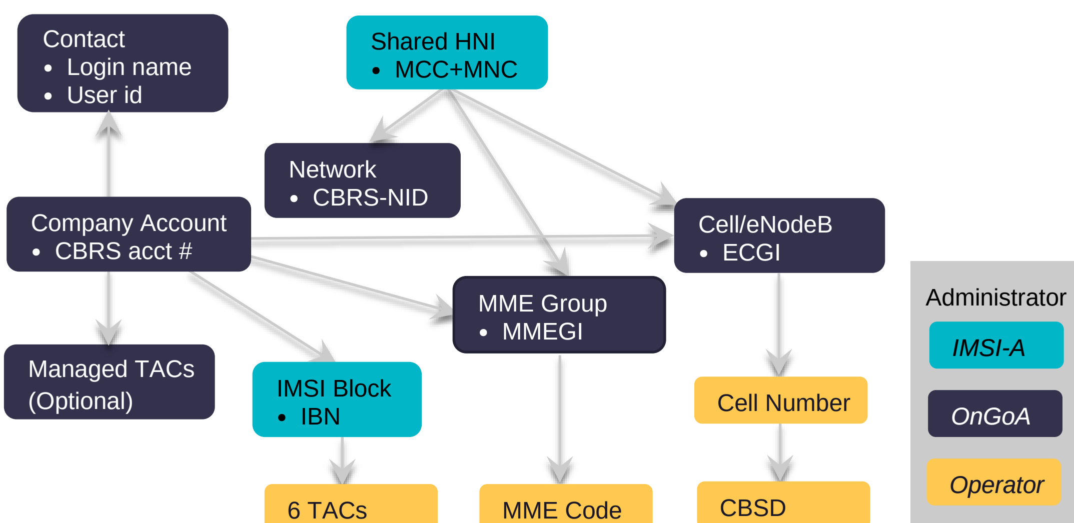

Figure 5: Identifier and Object Relationships

Once an account has been approved, any of the approved contacts for the account can obtain assignments of the three types of identifiers managed by the OnGo Alliance.

The system will also allow accounts to review their current assignments of codes, and will generate an annual invoice for all assigned codes.

Note that the IMSI Block Numbers (IBN) will be assigned by the US IMSI Administrator (IMSI- A). On that basis, a database of IBN may not be needed to be maintained by the OnGoA. However, if the IMSI-A does not provide an easily queried and current list, or if real-time queries are needed, this may need to be maintained by the OnGoA (directly or via an authorized database provider).

Similarly, the Shared HNI is assigned by the IMSI-A. However, to allow the possibility of multiple Shared HNI assignments in the future, a table could be maintained by OnGoA, although at first the table will have only one entry.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

Appendices

Appendix A: ECGI Uniqueness and E911 Detailed Rationale

Geographical location is an important component of Emergency Calling (E911 in North America) that provides two basic location-related functions:

- Identifying the appropriate Public Safety Answering Point (PSAP) to receive the call (e.g., town, city, county, highway patrol).
- Identifying the accurate location for dispatch of public safety assistance (ambulance, police car, etc.).

Geographical location can most rapidly be provided by using the serving cell location (e.g., tower latitude, longitude and perhaps altitude), but this may be inaccurate by several miles in a macro cell. GPS location is much more accurate (several meters) but takes longer to obtain. Therefore, given that US FCC E911 mandates require both speed and accuracy, the PSAP is generally identified using cell location (for speed) and dispatch of an emergency vehicle typically uses GPS location methods (for accuracy, since dispatch is usually initiated several seconds or even minutes after the call is connected to the PSAP).

Various specifications indicate that at times the Cell ID (ECGI) is used to determine the location of a mobile, and depending on the network architecture, this may require the ECGI to be globally unique:

- 3GPP TS 23.167 indicates that, in scenarios where the IMS core needs to retrieve the location information, the Cell ID (ECGI) is included in the SIP invite sent to the emergency call answering center (PSAP).
- 3GPP TS 23.167 also states that, "Location is indicated in network terms, for example using the global cell id [ECGI] in cellular networks...".
- ATIS-0700015.v003 states that the location for IMS-based E911 may be based on the Cell ID. If the LRF or Location Server are outside the OnGo system, then the ECGI would need to be globally unique.

Leveraging national cross-reference tables of ECGI and geographical coordinates, and they do for macro-cells, ECGI is used to derive the cell location (e.g., actual tower location or approximate geographic center of the coverage area) in LTE systems. If this conversion is done within an operator's network, for both PSAP routing and dispatch, the ECGI only needs to be locally unique.

From this approximate location, the Emergency Services location server will obtain a temporary routing phone number (ESQK) that can be used to both route the call to the correct PSAP and provide a key for the PSAP to obtain the now stored approximate location information. It is likely that this function will be outsourced due to the need to maintain a pool of phone numbers for every answering point.

The ECGI is also important for GPS in general (not just E911) because it provides the reference location to make GPS fixes faster and more accurate. This requires a cross reference from ECGI to tower location, which requires uniqueness of the ECGI if the table is maintained by a third party. It is known that industry-wide cross references are maintained by several organizations, including Google, in order to support SUPL-based location services. The SUPL protocol transmits the ECGI from the phone to the server (e.g., supl.google.com), not the cell location. SUPL servers are generally maintained by phone or phone OS manufacturers, and not by individual operators.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org

In the case of outsourced location functions, a globally unique ECGI will probably be necessary because there may not be additional information to be able to resolve the ECGI and location.

Appendix B: Change History

Table 3: Change History

Version	Date	Description
V1.0.0	2018-11-27	Release 1 of this Report
v1.2.0	2021-07-29	Updated to add managed TAC pool. Added confidentiality clauses.
v1.2.1	2021-09-13	Fixed based on comments during voting – Per TS-1002, cause value should be 15, not 12 (changed in the 3.0 release of TS-1002).
V1.2.2	2021-12-14	Formatted to OnGo Alliance template.

Copyright © 2021 OnGo Alliance • 3855 SW 153rd Drive • Beaverton, OR 97003 • www.ongoalliance.org • info@ongoalliance.org