OnGo Private LTE Deployment Guide

January 2022, v2.1.0

Contents

Contents

Gathering Requirements

Overview

With the opening up of the CBRS band to the public, the FCC removed several key barriers to deploying LTE networks. The new requirements enable you to significantly increase the speed and reduce the cost of deploying an LTE network. This paper is a guide for deploying your own Private LTE networks using OnGo's LTE technology in the CBRS band. It is intended to familiarize you with key aspects of designing and deploying an OnGo Private LTE network, so you're prepared for discussions with equipment makers and service providers. In addition, this guide provides a walk-through of the deployment process and examines many of the major design decisions involved in deploying an OnGo Private LTE network.

What is a Private LTE Network?

A Private LTE network is a network that is only accessible to users that have been granted access by the network's owner. This is in contrast to the public networks operated by the various mobile carriers. Private LTE networks typically cover a specific area, such as inside a building or facility.

Who Should Read this Guide?

We have written this guide for organizations interested in deploying and operating a pOnGo-based Private LTE network to meet their business needs. We want company leaders to learn the current "art of the possible," while also helping network engineers ask the right questions when planning to deploy an OnGo Private LTE network.

Much of the design, deployment, and operational tasks can be addressed in detail by an OnGo system service provider – many of whom belong to the OnGo Alliance. Understanding the scope of services, and the nature of the various tasks involved, will help you define service needs and select an appropriate service provider.

CBRS Overview

Wireless communication has become the "fourth utility." It has become as essential as power, water, and Internet connectivity for most organizations. Yet, while demand for

mobile communication appears limitless, the wireless spectrum — the medium for carrying wireless information — is finite, and increasingly scarce and valuable.

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 so private organizations can share this spectrum with incumbent users. The OnGo Alliance created OnGo to promote the use of LTE 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).

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.

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 – 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 in order to establish the LTE and 5G standards.

The FCC auctions 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 interference protection from each other.

Band 48 Properties

For wireless communications, different frequency bands have different properties. In general, lower frequencies are better for long-range communications, while higher frequencies have larger bandwidths, which allow for higher data rates. At 3.5 GHz, the CBRS Band (Band 48) provides a balanced "mid-band" mix of capabilities – good propagation characteristics, with good data capacity.

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, emit less than one watt of power per 10 MHz channel. Category B devices, typically used outdoors, emit up to 50 watts per 10 MHz channel. In an OnGo network, the LTE eNodeBs (base stations) are connected to CBSDs, and are often in the same device.

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	45 (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 the power can't exceed 23 dBm/10 MHz (200 mW). EUDs may operate with permission from a CBSD. In an OnGo network, the EUDs are generally LTE 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 SAS maintains a database of CBSDs and incumbent devices to calculate the aggregate interference.

OnGo and 5G NR

The CBRS band also supports 5G networks, where the band is identified as band n48. 5G NR networks can be deployed as non-standalone (NSA) networks, augmenting an LTE network in the CBRS band or in another band entirely; or the 5G NR network can be deployed in a standalone (SA) configuration. See our forthcoming OnGo Private 5G Deployment Guide for more information.

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 CBRS interference the naval operation. The SAS uses propagation models to predict potential interference with incumbent systems and transmits 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.

Process Summary

Deploying and operating an OnGo Private LTE network involves multiple steps. They consist of the following stages:

Figure 1: Process sumamry stages.

1. Gather Requirements. Information should include how many people will use the network, what their data service needs are, and what are the key use cases for your network.
2. Survey and Planning. In this stage, you survey the physical space the network needs to cover, identify vendors of the system elements and services, and estimate bandwidth needs and capabilities.
3. Design. Now you begin selecting vendors and refining your network design. During this phase you'll conduct signal measurements and modeling to make sure your network provides the needed level of coverage.
4. Installation. It's time to begin installing your network – CBSDs, radio hardware, backhaul connections, etc.
5. Maintain. Once the network is deployed and operating, you'll need to stay on top of monitoring to ensure that the network is operating correctly.

The rest of this guide walks you through the process, providing further details on each of these steps.

Gathering Requirements

The first step in any successful deployment requires a detailed understanding of your organization's needs and the problems you wish to solve by deploying an OnGo private LTE network. Start by identifying your critical use cases so your networking team, or an OnGo service provider, can design a system to meet your needs.

Understanding Needs, Use Cases, & Problems to be Solved

The first step in gathering requirements is to identify the critical use-cases for your OnGo Private LTE network. Here we provide a list of questions you should consider when defining your network requirements:

- What is the primary purpose of your Private LTE network?
  - For example, will the network need to provide data connectivity for IoT devices, or will it be used exclusively for mobile phones? If for mobile phones, will your mobile devices also require support for data? The answers to these initial questions will drive many decisions and provide the answers to the more detailed questions below.
- Who will be connecting to your Private LTE network?
  - Should access to the network be limited to a static list of users? Employees of your organization only? Or will visitors, external partners, or guests also require access to the network?
  - Will users require privileged access to critical business assets? Will users be members of particular groups requiring constant wireless connectivity, such as executive leadership, IT, security, or development? Understanding roles and access privileges will ensure proper authentication and security, as well as your device and user-provisioning needs.
- What will be connecting to your network?
  - This can include gateways, internal communication channels, and applications, as well as IoT devices, cameras, and various mobile user devices.
  - If you have existing devices that you want to connect via your private LTE network, what interfaces do they have?
- What level of security do you need?

  - To supply enterprise-grade LTE security (e.g., device authentication, traffic encryption), an OnGo network requires little to no extra work. If you need additional protection, you should define your security requirements as early as possible.
- Are the devices connecting to your network going to be mobile or fixed-in-place?
  - Fixed and mobile devices have different network architectures and device-management requirements.
- How many users, devices, or IoT nodes will access the network?
  - Whether you need to support hundreds or thousands of connections, correctly scoping the network is crucial to achieving the required performance.
- What type of traffic will those users and devices be generating?
  - For example, the data requirements of a voice call are very different from a device periodically providing status updates.
- Is latency a significant concern?
  - Some applications require low-latency operations, which will impact your network design.
- What will the devices be connecting to?
  - If devices and users need to connect to other company networks or the Internet at large, you need to make provisions for backhaul communications. However, backhaul support may be unnecessary if the devices will be sending data only among each other.
- Will mobility into and out of the network be needed?
  - If needed, you can configure your Private LTE network to allow devices to roam seamlessly into and out of the network. Arrangements must be made with existing network operators to support roaming to and from their systems.
- In what type of environment will the system be deployed?
  - Given that OnGo Private LTE networks function both indoors and outdoors, your specific environment will determine many aspects of your system.
- What wireless data infrastructure do you already have?

  - If you have an existing WiFi network, you can allocate devices and data traffic to the system that best supports your needs. This can improve the performance of both networks.
  - If you already have LTE systems deployed, such as a Distributed Antenna System (DAS) or a small-cell system, you will need to consider them as you design your deployment.
- How mission-critical is your network?
  - The CBRS band provides multiple levels of licensing, with licensed users having priority when allocating channels. If your deployment requires high availability, you may need to engage the services of a provider with a PAL license.
- What growth do you anticipate over the next one-to-three years?
  - If you expect to add more users, nodes, functionality, or sites, you should plan your deployment accordingly.
- What kind of infrastructure deployment approach do you prefer for the network and management elements – on-premises, cloud, hybrid cloud?
  - If you already have on-premises hosting options, local hosting may make sense. However, if preferred, some or all of the network elements may live in the cloud.
- How do you want to install, operate, and own the network?
  - For example, does your organization want to capitalize some, or all, of the equipment? Or would you prefer subscription services? Will your internal team manage the core network, or do you want a managed services option? OnGo deployments provide the flexibility to match your service deployment needs with your business model.

This guide will take you through the different deployment processes for two separate sites, each with very distinct requirements. Scenario A is a typical new building deployment. Scenario B is for a larger and more complex sports venue. By going through the detailed deployment process of each, we hope to give you clear examples to help guide the planning of your network.

Scenario A: Smart-Building Network Requirements

For our first scenario, we will look at the requirements for an OnGo-based network supporting the needs of a standard office building. Like any new building today, this facility will require several smart devices to monitor the building, specifically various support systems within the building that control security, HVAC, and lighting, among others. In addition, staff members require access to data while working throughout the building. Most devices remain fixed-in-place, with locations known at the time of installation. Employees do not require seamless mobility, and an IT Team will provision devices manually, so dynamic provisioning is not needed. Most sensors and controls have low bandwidth requirements, except for the security cameras, which consume high uplink bandwidth. The total number of sensors is approximately 500, with 10–20 security cameras. Most of the smart devices will be inside the building, with a few around the exterior perimeter of the building. Security is critical, but the system is not genuinely mission-critical – disruption of the network will not render the building unusable.

Figure 2: Smart-Building example scenario.

Scenario B: Sports Venue Requirements

In the second scenario, we will detail the deployment of an OnGo network at a stadium or sports complex, intended to support large event operations. The primary use case is to provide voice and data to staff during events, when the public networks may be saturated. In addition, the network must support a small number of mobile high-definition video feeds from moving camera crews. Since the venue is large and the staff will be moving around the site during the event, the network must support seamless mobility. The total number of staff during games could reach as many as 200 people. Also, teams and coaches will need network access during events. While security is not a top concern, high-availability is. The cost of network failure could harm the reputation of the facility owner and jeopardize future revenue opportunities.

Figure 3: Sports Venue example scenario.

Once you've determined your primary use cases and requirements, the next step is to begin planning your deployment.

Nominal Design

For in-building or venue applications, collect floorplans and do an initial coverage design. Working this out during the initial design will create a proposed blueprint for antenna/CBSD placement. The site survey, described below, offers you the opportunity to verify the design and make changes based on constructability.

Site Survey

To begin, you'll also need to survey the area you intend your network to cover and how many CBSDs will be required, along with their location. The frequency band where CBSDs operate (3.5 GHz) does not propagate in the same way as "regular" LTE signals and operates at a lower power level (<50 watts) than a macro LTE cell. While the actual list of information required to plan a full deployment may be longer, here are some examples of the type of information you'll need to cover the overall dimensions of the area, such as the length, width, height, area usage type, etc.:

- Dimensions of the outdoor coverage areas.
- Dimensions of the indoor coverage areas.
- Wall dimensions and construction materials, such as concrete, wood, metal studs, etc.
- Location and dimensions of structures in the coverage area, including large pieces of furniture, large objects, obstructions, construction materials, etc.
- Locations of power and data sources, as well as inaccessible areas. Note: If the Wi-Fi infrastructure already exists, you can use the Wi-Fi Access Points as a simple way to map out convenient locations for CBSDs.
- The location of Wi-Fi Access Points and other wireless communication infrastructure, such as DAS or small-cells.
- Areas of potential interference (incumbents, radars, cell towers, etc.).

- The current and expected device and subscriber density. You need to understand the expected end use cases, such as IoT device types, mobile users, etc.
- Location and availability for onsite infrastructure elements as required (data center, networking elements, network management systems, controllers, etc.).
- Location and interfaces, including wired and wireless, of any existing devices that will connect to your network.
- Location of equipment closets, fiber point of presence, power and grounding, cable trays, and the conduit between floors, etc.
- Any future planned remodeling or construction.

These questions are here to help you scope out the overall scale of the deployment. During deployment, installers will require special tools for measuring signal strength and propagation to ensure complete network coverage. It's also good to conduct a baseline walk test with a scanner to understand what other signals are present and their relative strength in the planned coverage area so you can determine what design margins are required for co-channel penetration.

If your site already has Wi-Fi infrastructure, you can use a high-level rule-of-thumb to determine your CBSD requirements. For indoor deployments, one CBSD will typically supply the equivalent coverage of two to three Wi-Fi Access Points. For outdoor deployments, one CBSD can replace from 12 to 20 Wi-Fi Access Points depending on terrain and other factors.

Adjacent LTE Networks

It is often helpful to know what other LTE networks are in your area and some basic configuration information about those networks. Although a SAS can provide basic information about other LTE networks in the CBRS band, other LTE networks are also of concern. Information you want to know includes:

- The band/channel those networks are using.
- Signal level penetration of adjacent networks into the proposed coverage area.

- The Tracking Area Codes, Mobility Management Entity Codes and Group IDs (MMEC and MMEGI), and the Physical Cell Identities used by those networks (see the Identifiers section for more information).

You can get some of this information using the Field Test Mode on devices connected to that network. The details on how to activate and use this mode depend on the device. Typically, activation involves dialing a unique code on the phone, which you can find with a basic internet search. Several websites (such as http://www.cellmapper.net/ or http://www.antennasearch.com/) provide tower and network information and can help identify other networks in your area.

CBRS Band Availability

The SASs can provide information about channel availability in the area and potential interference sources, including any PAL operators and other incumbent users with higher access priority.

Planning – Indoor/Outdoor, Use Cases, Spectrum Usage

You can now begin planning where to place your CBSDs. CBSDs have different power limits depending on their class: One watt for Category A devices (indoor or outdoor) and 50 watts for Category B devices (typically outdoor). In general, a one-watt CBSD can effectively cover about 10,000 square feet in a typical office environment. For outdoor applications, a 50-watt CBSD has an average effective range of 1.5 – 2 miles using an isotropic antenna 160-feet above the ground. To avoid interference with any others in the area using the same band, CBSDs may have to lower their power levels. As a result, the range of the CBSDs, particularly outdoors, may be reduced on occasion.

In addition to range considerations, you'll need to estimate the number and types of devices connecting to each CBSD, so you can determine your data bandwidth requirements. This analysis allows you to estimate the capacity needed on a given CBSD. Finally, you'll need detailed modeling of the signal propagation to estimate the worst-case available bandwidth and confirm if there will be sufficient capacity on a given CBSD for different channel configurations.

Survey & Planning

OnGo networks use Time Division Duplexing (TDD), with the CBSDs/eNBs and EUDs/UEs on the same frequency channel transmitting and receiving at specific times. The throughputs can be calculated depending on several parameters such as the TDD configuration, channel bandwidth, downlink and uplink modulation supported, and the MIMO capability of the CBSD. See examples in the table below. The table lists peak rates shared across all connected users. You can use an online calculator (https://www.cellmapper.net/4G-speed) to determine the available bandwidth. The further away you are from the CBSD you can expect throughput to drop. To compensate, we recommend designing your RF footprint to maintain a cell edge that sustains 15/5Mbps DL/UL throughput. The OnGo signal will typically reach longer ranges and perofrm more reliably at the cell edge than a Wi-Fi signal.

TDD Config (with: Normal Cyclic Prefix + Special Config0)	Channel Bandwidth	Modulation	MIMO	Peak DL	Peak UL
1	10	DL – 64 QAM UL – 16 QAM	2x2 4x4	33.48Mbps 66.96Mbps	10.44Mbps 10.44Mbps
1	20	DL – 64 QAM UL – 16 QAM	2x2 4x4	66.96Mbps 133.92Mbps	20.88Mbps 20.88Mbps
2	20	DL – 64 QAM UL – 16 QAM	2x2 4x4	97.2Mbps 194.4Mpbs	10.8Mbps 10.8Mbps
6	20	DL – 64 QAM UL – 16 QAM	2x2 4x4	51.84Mbps 25.92Mbps	103.69Mbps 25.92Mbps
6	20	DL – 256 QAM UL – 64 QAM	2x2 4x4	69.12Mbps 138.24Mbps	38.88Mbps 38.88Mbps
1	20+20 DL-CA 20+20 UL-CA*	DL – 256 QAM UL – 64 QAM	2x2 2x2	178.56Mbps 178.56Mbps	31.32Mbps 62.64Mbps

* In development now.

You should also note where the data streams are going. If your traffic is staying entirely within your private network, any connection to external networks will be unaffected. However, if you are going to send multiple video streams to the Internet, your backhaul infrastructure will need sufficient capacity to handle the load.

Throughput needs of some various applications:

- 480p video (640x480) – 2.5 Mbps
- 720p video call (1280x720) – 3 Mbps (each way)
- 1080p HD video (1920x1080) – 8 Mbps
- 4k HD video – 20-25 Mbps
- Normal voice call – 12 kbps
- HD voice call – 50 kbps

Note: When a device is moving, its effective bandwidth demands go up. If this is the case, we recommend adding 10% to your calculated bandwidth requirements.

Based on your total bandwidth needs, you can estimate the number of channels you'll need. Suppose your scenario needs more data than can be provided in a single channel. In that case, you can deploy multiple channels – either operating as a single 20 MHz channel, or using carrier aggregation to provide more throughput. The network can also allocate downlink and uplink data in different ratios, allocating for more (or less) uplink capacity.

Note: OnGo CBSDs are only required to support TDD Uplink/Downlink Configuration 1 (balanced) and 2 (downlink-heavy). Other configurations may be supported but are not required. EUDs (UEs) support of the configuration is also required.

TDD Synchronization

In the CBRS band, LTE systems must operate in TDD mode. In that mode, CBSDs (eNBs) need to coordinate with nearby LTE CBSDs to prevent interference. Without coordination, the higher power transmissions of the CBSD can effectively drown out the lower power transmissions of UEs in nearby cells, even when they are on adjacent frequency channels. This interference can occur when the CBSDs use different TDD frame configurations or if the timing is not synchronized between the CBSDs to transmit at the same time.

Being in the same TDD configuration and aligning the timing between cells significantly reduces interference. LTE has existing mechanisms for synchronizing timing between eNBs, using GPS or similar signals for a common timing reference, which is critical for

proper functioning. However, the SAS doesn't currently have provisions for coordinating the TDD configurations.

The OnGo Alliance defines an optional coexistence manager system element to help coordinate between OnGo networks and to minimize TDD-related interference within the CBRS band. This system will coordinate between OnGo networks to select an appropriate TDD configuration. That may constrain what TDD configurations your network can use, but you'll experience significantly reduced interference. Until these systems are online, you'll need to coordinate directly with other OnGo networks in your area to determine which TDD configuration won't interfere with those networks or with your network. An integrated solution provider will be able to help with these issues, if needed.

PAL vs. GAA

For most private LTE deployments, you should not require a PAL. However, consider sublicensing a PAL if your implementation meets one or more of the following criteria:

- Large area or outdoor deployment – If your implementation uses Category B (outdoor) CBSDs, or otherwise covers a large geographic area.
- Mission-critical – A PAL gives your network higher priority, increasing the chances of spectrum access.
- Crowded environment – For example, if your network is in a very dense urban environment. As noted earlier, PAL users are afforded protection from GAA users.

The FCC auctioned PALs on a per-county basis. Light-touch leasing rules allow for PALs to be sublicensed within a county, outside of areas where the PAL owner is broadcasting. PAL holders are not required to sublicense. Information on the PAL auction results and winners is here: https://www.fcc.gov/auction/105.

What is a PAL, and Do I Need One?

There are three tiers of access to the CBRS band:

- Tier 1: Incumbent users such as the federal government and fixed satellite users.
- Tier 2: Priority Access License (PAL) users—licensed wireless users who acquire spectrum through an auction. The SAS will ensure PAL users don't cause harmful interference to Tier 1 users and will protect PAL users from interference by General Authorized Access (GAA) users.
- Tier 3: GAA users who deploy "lightly-licensed" devices. The SAS ensures GAA users don't cause harmful interference to Tier 1 incumbents or Tier 2 PAL users.

Of the 15 CBRS channels, PALs are available for up to seven in the lower 100 MHz. Unused channels (and channels not being used by the incumbents) are available for GAA users. PAL users do not receive guaranteed access to a channel but are much less likely to be denied access by the SAS.

If a PAL holder fails to use their allocated channel(s) for more than seven days, the SAS frees up those channels for GAA users.

Whether or not you need a PAL depends on a number of factors:

- How critical your network is to your operations? PAL holders are much less likely to be impacted by other users and can only be denied access when an incumbent user needs access to the channel.
- Are there many other CBRS networks in your area? If other private GAA CBRS users exist in the same area, a PAL will help ensure that you receive preferential access.
- Does your network cover a large area? The more extensive your network, the more likely you will overlap with another CBRS network. A PAL will reduce chances of interference.

If you did not secure a PAL in the auction, you may be able to sublicense from an existing PAL holder. However, given that PAL holders are not required to lease, it may not be possible to get a PAL in your area.

SAS operators can provide guidance on the availability of spectrum in your area.

Carrier Aggregation

LTE supports the bundling of channels to provide additional bandwidth via a mechanism known as Carrier Aggregation (CA). CA can operate within the CBRS band, allowing multiple 10 MHz channels to be combined. These channels can be contiguous or non-contiguous for maximum flexibility.

Vendor Identification

As part of deploying your Private LTE network you will need many vendors. In the planning stage, you should begin to identify potential vendors. Once you reach the design stage, you will need to select your vendors.

As an alternative to contracting with individual vendors, many companies provide integrated solutions services. These vendors can take care of the details of planning, design, installation, and operations support. Many are members of the OnGo Alliance. A list of our members can be found here: https://ongoalliance.org/members/.

SAS Administrators

The FCC has approved several SAS administrators. While the FCC defines the essential functions of the SAS, each SAS vendor offers a variety of additional services and a range of commercial terms. You can view a list of current SAS administrators here: https://cbrs.wirelessinnovation.org/sas-administrators.

CBSD Vendors

Multiple CBSD vendors offer OnGo-certified devices. Differences between vendors include power levels, antennas, number of devices, throughput, and other configuration options. A complete list can be found here: https://www.ongoalliance.org/certification/.

Evolved Packet Core (EPC) Vendors

To function, OnGo CBSDs must connect to an Evolved Packet Core (EPC). The EPC provides mobile device management functions in the control plane and enables data packet exchanges between the mobile device and applications in the packet network on the data plane. You may deploy an EPC on-site, co-locate with the CBSDs, or use a cloud- based EPC service. CBSDs interoperate with the EPC; therefore, it is essential that you select a compatible EPC.

Element and Device Management System (EMS/DM) Vendors

The EMS and DM systems are tightly integrated with the CBSD and the EPC. The EMS typically provides control, configuration, management, and data collection services for the EPC. At the same time the DM handles lifecycle management for the CBSDs, including activation, configurations, and fault and performance management. The EMS/DM may be provided by the CBSD or EPC vendor, or by independent network management vendors that support the necessary management standards.

End-User Devices (EUDs)

Of course, critical to a private LTE deployment are the EUDs, also referred to as user equipment (UE), that will connect to your network. Any LTE UE device that supports Band 48 can connect to an OnGo network. Fortunately, many handsets on the market today already support Band 48.

If you have existing devices that you want to connect to your Private LTE network that do not support Band 48, you will need a bridging device. This can be a USB dongle or similar device that connects to an existing physical interface. If the device supports another wireless technology, the use of an OnGo EUD bridge in this manner can extend your Private LTE network to include multiple devices, effectively using OnGo as a backhaul connection.

The complete list of certified devices can be found on the OnGo website: https://www.ongoalliance.org/certification/.

Note: In 5G NR, Band 48 is referred to as Band n48.

SIM Provisioning

You will also need a system for provisioning SIMs. You can purchase either a dedicated UICC writer, or a software package for eSIMs. The type of SIM provisioning system you need is based on the EUDs that will connect to your network. SIM provisioning is typically part of an EMS/DM solution, but you may need to acquire this capability separately.

Certified Professional Installer (CPI)

The FCC Part 96 rules that define CBRS generally require that CBSDs be registered with the SAS by a Certified Professional Installer (CPI). All Category B CBSDs, and any Category A CBSDs that cannot self-geolocate, must be registered by a CPI. While CPIs are not required to install the CBSDs themselves, they are responsible for the accuracy of the registration data.

There are currently several training options for CPIs. You can find a list of WInnForum-accredited Training Program Administrators (TPAs) here: https://cbrs.wirelessinnovation.org/cpi-program-administrator.

Networking Plan

The primary consideration for IP networking is what type of physical network infrastructure your CBSDs will use to connect to each other and your internal network. Different CBSDs support different interfaces for their backhaul connections – Ethernet, optical fiber, or even wireless links. If your CBSDs use Ethernet for their backhaul, your existing Ethernet infrastructure for your Wi-Fi network may work just fine for your OnGo deployment. However, if your deployment will use a lot of channels to support very high bandwidths, or your network infrastructure already carries significant traffic, make sure your backhaul connection has enough available bandwidth to support your needs. If not, you may need to add additional backhaul capacity.

You also need a backhaul connection if your system interfaces with other networks (such as the public Internet). As with the internal network, ensure that your total backhaul capacity can support the amount of data you will be carrying. The contract often sets the bandwidth, so check to see if you have sufficient bandwidth to meet your needs. Even if your network doesn't provide access to the Internet, the CBSDs and Domain Proxies must be able to connect to the SAS. That's why we recommend installing high-availability or redundant connections wherever possible. Otherwise, your CBSDs will shut down if they can't check in with a SAS periodically.

As a general rule, bandwidth demand rises 30% per year. So, rather than aiming for "just enough," we recommend building in additional bandwidth, particularly in your onsite infrastructure. You can increase backhaul bandwidth relatively quickly, but installing more cables is a lot more difficult. Most plan for twice their current bandwidth needs to provide reasonable headroom for growth.

Customer Premises Equipment and CPE-CBSDs

In the telecommunications world, the term "Customer Premises Equipment" (CPE) is widely used. Unfortunately, the term's exact definition can often vary depending on the segment of the industry and the technology in use. In the OnGo context, the term CPE officially means an LTE UE operating in the CBRS band. However, the term is often applied to any non-mobile device that is part of an OnGo network, especially if the device does not face an end-user, including CBSDs. Therefore, if you see the term CPE, clarify what it menas.

There is also another type of CBSD called a CPE-CBSD. A CPE-CBSD can transmit at a higher total power level (>23dBm EIRP) than other end-user devices (EUDs) but only after it's registered with the SAS. These devices are typically used in Fixed-Wireless Access (FWA) applications, as a CPE-CBSD must be non-mobile. In addition, since they have a higher transmit power level, CPE-CBSDs can connect to a base station at a more extended range than normal EUDs.

In an OnGo deployment, a CPE- CBSD can be an LTE UE (EUD) that can connect to another CBSD over longer distances than other UEs. It may also include an eNB, allowing the CPE-CBSD to extend your coverage area when wired backhaul is impractical.

Security

Any network system must address security. Fortunately, OnGo has LTE security "baked- in" to the system, so achieving enterprise-level protection of the wireless link is relatively easy. All elements of your deployment will need to consider both physical and cyber security in the design to ensure that the overall system is secure. Security needs should be considered in your selection of CBSDs and management systems.

CBRS uses digital certificates for security purposes, authenticating and securing communications between elements of the system, including the SASs, CBSDs, and Domain Proxies. If you have an existing Public Key Infrastructure (PKI), leverage it to generate the certificates used by your system, or rely on the certificates provided by the manufacturers.

Existing Data Infrastructure

When planning your OnGo deployment, consider any existing data infrastructure, particularly other wireless systems such as Wi-Fi. OnGo excels at providing mobility and coverage in complex RF environments; and reliable, consistent connectivity for a large number of connected devices. In a multi-network architecture, assigning devices

(and their traffic) to the most appropriate network can improve the entire network's performance. As a simple example, fixed devices can be placed on a WiFi (or wired Ethernet) network. In contrast, mobile devices and devices in locations with poor Wi-Fi connectivity can be assigned to the OnGo network.

Business Case

When deploying any new system, it is essential to assess both costs and benefits. While the details differ with each system, keep in mind that once you have deployed a private LTE network to address a particular use case, the incremental cost to support additional use cases is much lower. Adding incremental use cases (such as a Neutral Host Network) to the deployed private LTE network can significantly improve the network's ROI.

Scenario A: Smart-Building Network Planning

To provide a more specific example of the planning required for your network, we will illustrate with our first scenario: a smart office building.

The building stands eight stories tall, with dimensions of 70 by 210 feet. The structure is composed of reinforced concrete, with internal partitions of metal studs covered with drywall. Offices and conference rooms line the outer perimeter, with a central stack for the elevator and stairwell. Each floor has been wired for Ethernet, originating in the wiring closets adjacent to the elevator stack, and reaching into the offices and conference rooms. AC power is available throughout each floor.

Given the overall size of each floor, and the obstructions presented by the elevators and work rooms, it is determined that two CBSDs per floor will be needed. Spacing them sufficiently far apart will ensure full coverage.

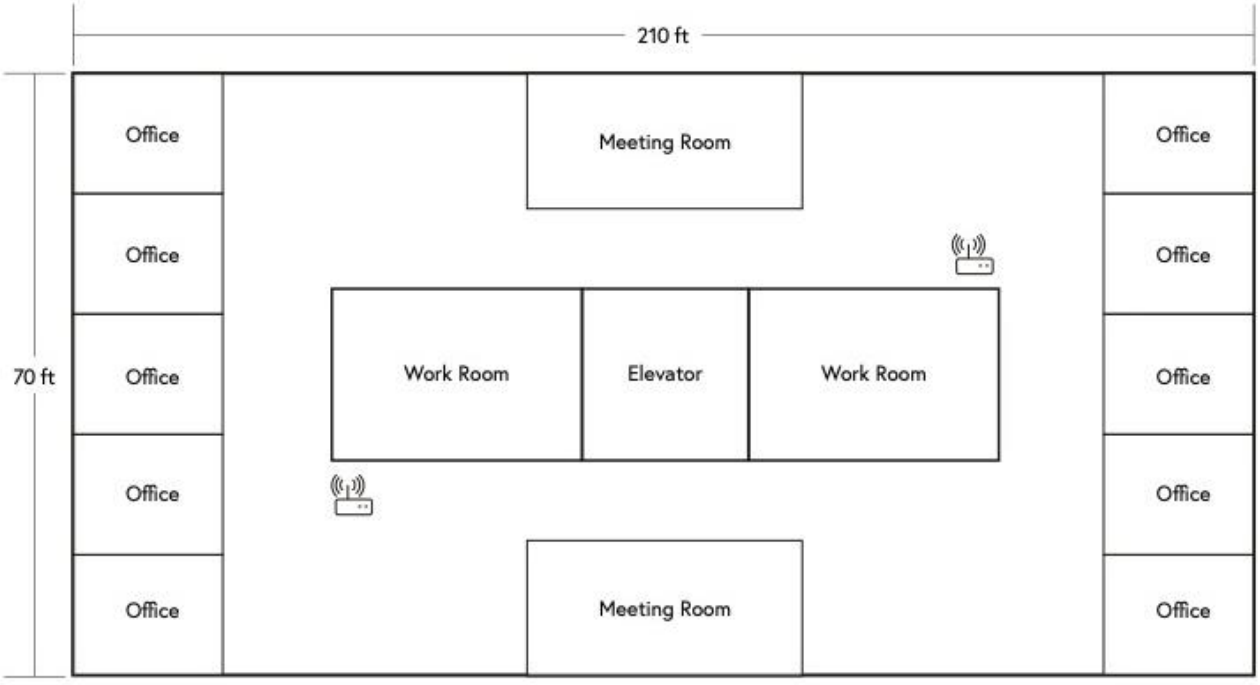

Figure 4: Smart-Building survey floor layout.

Each floor has 50–100 sensors and controls installed, including two high-definition security cameras. The security cameras generate the majority of traffic, with each one continuously sending 8 Mbps of uplink traffic. Given that the sensors and controls

generate only a few kbps total, this infrastructure traffic requires approximately 16 Mbps of uplink per floor. By attaching one camera to each CBSD, one channel will be able to meet these requirements with plenty of bandwidth to spare. If additional cameras are needed, a more uplink-heavy configuration can be used.

Since the deployment covers a relatively small area, and there aren't many other CBRS networks in the area, a PAL is likely unnecessary. However, if the network needs to support a complex of buildings, including outdoor spaces, a PAL may be required. Details from the site survey will help make that determination.

The building already has some wired data infrastructure to support the various tenants, with a shared server room on the ground floor. There is plenty of capacity on the building's ethernet system to support the CBSD, so no new infrastructure is needed.

Most of the traffic from the network will be remain internal; therefore, changes to the backhaul connection to the Internet will not be needed.

The EPC and network management system do not need to be full-featured. Device provisioning will happen infrequently, so the configuration of SIMs as well as the network can be done manually. None of the devices will be roaming to other networks, so agreements with other wireless network carriers are not needed.

When it comes to selecting vendors, the critical consideration is getting a CBSD that can handle the number of device connections anticipated. Given that all CBSDs reside indoors, a high power (Category B) CBSD is not necessary.

Scenario B: Sports Venue Network Planning

Our second scenario, for a large sports and event venue, is significantly more complicated than a single building.

The site covers 72 acres and includes a main stadium, several other athletic fields, and single-level parking to support maximum usage. The main stadium area, built of reinforced concrete, contains locker rooms, offices, and a press box. The total seating capacity of the main stadium is 18,000. The stadium has some wired data infrastructure in the form of Ethernet feeds to the press boxes and offices. A high-definition video screen on the scoreboard has a direct HD video connection to the central controller in the press box, into which several other wired video feeds connect from various locations in the stadium. AC power is available inside the stadium and at the numerous lighting poles around the grounds. There is a small electronics closet in the press-box area for supporting the Audio-Video system that can also be used for any servers needed.

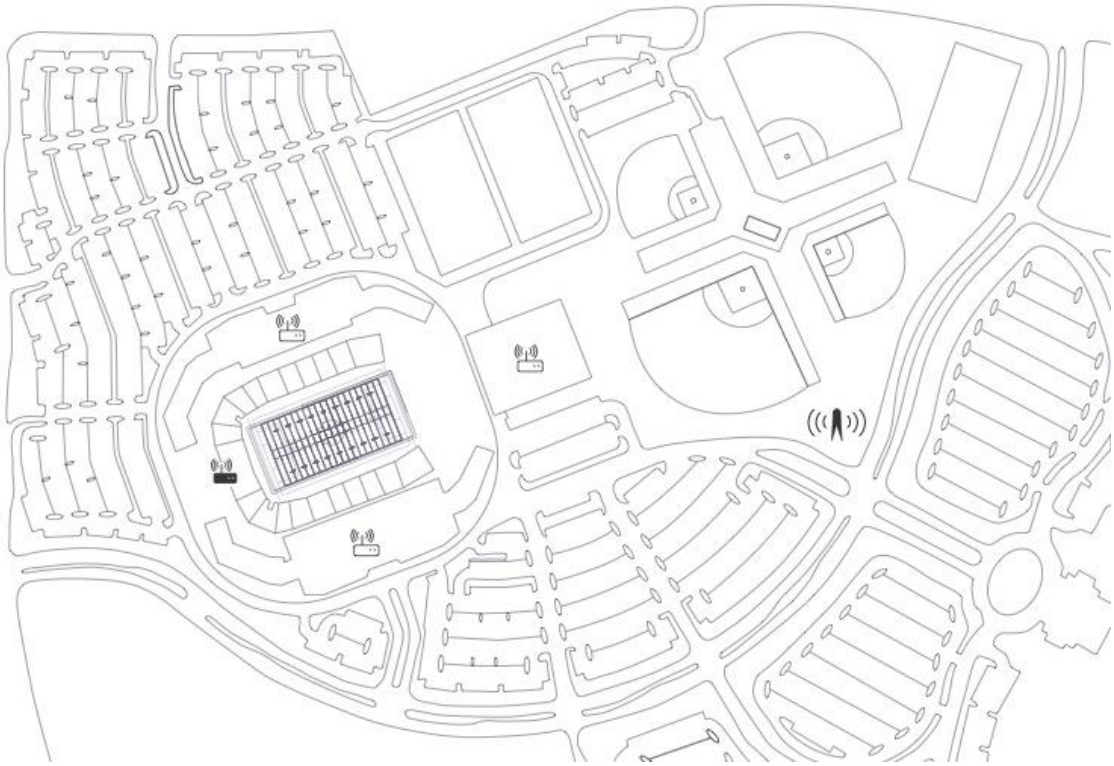

Figure 5: Sports Venue survey layout.

Based on the site map, four Category A CBSDs will be needed: one in the stadium area, one in each of the two locker rooms, and one in the offices. With the parking area lights serving as a convenient mounting position, two outdoor (Category B) CBSDs will provide coverage to the larger grounds and the stadium area.

The device ecosystem consists of the personal phones and tablets of the site staff, the referees, coaches, and staff of the teams playing. The system should therefore support approximately 100 people, each using an average of 1.5 devices, for a total of 150 devices. Also, point-of-sale systems at the various concessions and ticket offices will add another 50 devices. Three mobile HD cameras also require support, with the desire to simultaneously provide live video from all three cameras as they move around the playing area. Based mainly on the number of video feeds needed (three 8Mbps links), that area of the network will need to be uplink heavy, supporting two channels with carrier aggregation to accommodate future growth.

Because of the dense suburban location of the site, the bandwidth need to support the video cameras, and the need for a large amount of outdoor coverage, four channels will be needed. Given these factors, a PAL to ensure channel access will be required.

Devices will regularly move throughout the stadium complex, so the network must support full mobility among the CBSDs within the entire complex.

The system must provide seamless connectivity for authorized devices, giving them full access to voice and data. Therefore, mobility into and out of the network must be supported, which will necessitate roaming agreements with other network carriers.

Given frequent staff changes and the need to accommodate visiting teams, the system must support the ability to add and remove devices easily from the list of authorized devices.

After defining the network capabilities needed for your private LTE deployment, site surveying your location, and selecting vendors, the next step is identifying the network elements best suited for your deployment, including endpoint devices, a radio system, access points, and core network services. The easiest path for many enterprises is to contract with a managed service provider or system integrator. Both can provide design and implementation services, as well as select the appropriate vendors for your deployment.

Vendor Selection

SAS Selection

In this stage, you'll need to contract with a SAS administrator to provide service for your deployment. Different SAS adminisrtators will offer a variety of commercial and contract terms (per CBSD, flat fee, etc.). Select the one that best supports your deployment. Your choice of a SAS administrator will depend on many factors, including:

- Commercial terms for interfacing with the SAS.
- Additional services provided by the SAS administrator, such as spectrum planning and area information.
- Does the SAS administrator have ESC sensors deployed for your area?
- Need for a Domain Proxy (see below).

CBSD Selection

Now you are ready to select the CBSDs. The general requirements that you should consider when choosing a vendor include:

- Indoor and outdoor CBSD options.
- Supported power levels.
  - Category A devices can transmit up to one watt of power, but many vendors offer options with lower power levels.
- The number of devices each CBSD can support.

- Uplink/downlink configuration support.
- Need for a CPI (see below).
- Carrier aggregation support (uplink and downlink) if bandwidth needs require more than one channel.
- Lifecycle management capabilities (activation, provisioning, operating, monitoring).
- Backhaul options.
- Ability to support multiple-location deployments in a single platform.
- Flexibility of adding new CBSD devices from different vendors.
- Integration capability with existing Fault/Performance Management and other systems.
- Integrated Domain Proxy capabilities.
- Ability to use certificates from exsting PKI (if any).
- Price.

EPC Selection

A basic EPC consists of four main network elements: MME, HSS, SGW and PGW. Other EPC network elements may or may not be needed, depending on your deployment needs. The Mobility Management Entity (MME) and Home Subscriber Server (HSS) elements provide mobility and device access controls. The Serving Gateway (SGW) and Packet Gateway (PGW) are the network elements providing actual bearer data transport for mobile devices by routing data packets between CBSDs, your local network, and any connected networks such as the public Internet. The different elements of the EPC can be run on separate devices or integrated into a single device.

EPC network elements can be deployed entirely in the cloud, on-premises together with CBSDs, or in a hybrid mode. The architecture you select depends on your deployment and should include available backhaul, desired latency, and cost considerations. Likewise, your deployment needs (such as seamless roaming to/from the public networks, network slicing, etc.) dictate the features your EPC will need to

support. EPC providers can provide a range of solutions based on your needs. They often offer different management system capabilities, which we will discuss below.

Element Management System (EMS)/ Device Management (DM) Selection

An EMS/DM can be located on the premises or in the cloud. It can also reside side-by-side with the EPC and perform EPC and Device (CBSD) management functions. Key considerations include:

- Standards support (SNMP, TR-069, NetConf, etc.).
- Simplified dashboards of overall status, and key performance indicators, and alarms.
- CBSD Device Management capabilities to enable ease of device deployment and ongoing management.
- Data analytics and reporting of Key Performance Indicators (KPIs) and other performance metrics.
- Fault management and alarming.
- Troubleshooting and diagnostic support.
- Redundancy and resiliency.
- Ability to support multiple location deployments in a single platform.
- Flexibility of adding new CBSD devices from different vendors.
- Integration capability with existing Fault/Performance Management and other systems.

Do I Need a CPI?

For some OnGo deployments, you may not need a CPI. For example, you should be able to skip having a CPI involved if all of the following are true:

- All of your CBSDs are Class A (< one watt).
- All of your CBSD antennas are less thansix6 meters in height above average terrain.
- All of your CBSDs include the capability to automatically determine their location.
- You aren't using a PAL.

CPI Selection

It's also time to select a CPI. Key considerations include understanding the payment terms and additional services the CPI can provide. The CPI can be an internal resource, as long as the person is trained using one of the authorized Training Program Administrators (TPAs), described above.

Note: Some Category A CBSDs have an auto-sensing function that can detect their location using GPS/GNSS and don't require a CPI to register their configuration with the SAS.

CBSD Configuration

The primary element of an OnGo deployment is the CBSDs – the devices that connect with your end-users. Depending on your implementation, you may need one CBSD or many. Exactly how many, where they need to be placed, and how they will be sectored, are functions of the detailed geometry of your site. An RF engineer or solutions provider can ensure that the CBSDs are placed and configured to provide coverage where needed.

Key aspects to consider at this stage include:

CBSD Placement and Sectorization

CBSDs and their antennas need to be placed to provide optimum coverage of the devices using your system with the minimum number of CBSDs. If the area to be covered is large or contains lots of obstructions (walls, trees, and other obstacles), detailed signal measurements and pattern maps may be needed to determine the required coverage.

CBSDs need power and a data connection to the local network (backhaul). The costs of plumbing in power and data feeds can be high and should be considered when planning your CBSD placements. Placing CBSDs where such infrastructure exists (like where there are Wi-Fi Access Points) may reduce the overall cost of deploying an OnGo network.

Configuration

In addition to determining the placement, your CBSDs also need to be configured to support your deployment. For example, you can configure your CBSDs to provide more uplink or downlink capacity by adjusting the number of 10 MHz channels used, and the frame structure of those channels, depending on the kind of data traffic the system

needs. CBSDs can be sectorized as well by segmenting the coverage area into different sectors operating in parallel.

Existing CBRS Networks/Incumbents

The presence or absence of other CBRS networks in the area can affect your deployment and should be checked early in the design process. Your selected SAS may be able to provide this information, or use a spectrum analyzer (or similar equipment) to determine potential interference in the area.

OnGo, LTE, and 5G

OnGo is currently LTE in the CBRS band. However, in the next release we will add 5G NR support. 5G will bring improved data rates, reduced latency, greater device density, and new network management features, including advanced network slicing options, to OnGo deployments.

Design Optimization

Proper placement and configuration of the CBSDs are a critical system component and may go through several revisions during the design process. For example, installing a CBSD in your desired location may be prohibitively costly or impractical, requiring the CBSD to be placed elsewhere. Likewise, signals from adjacent systems and networks may interfere with your network. That's why measuring signal strengths, and benchmark testing, should be performed to ensure that the CBSDs can provide the needed coverage and repeated as the design is updated and modified during installation.

The SASs can also provide guidance on the location of any nearby incumbents, availability of channels, and any likely power restrictions in your area.

Network Design

At this stage, you need to decide on the design of the network infrastructure supporting your Private LTE network. Here are several important topics for you to consider:

Domain Proxies

You can group CBSDs behind a Domain Proxy service that communicates with the SAS. The Domain Proxy aggregates all communications from the CBSDs. It provides a single interface point from the SAS to the CBSDs, reducing your configuration and registration complexity, particularly if you have many CBSDs. Whether or not a Domain Proxy is needed depends on the capabilities of the selected CBSDs, and the terms offered by your selected SAS administrator. The Domain Proxies are generally CBSD-vendor-specific and are part of the EMS, and are often integrated within the CBSD device.

Network Slicing

You can configure your Private LTE network to provide multiple independent virtual networks, each with different configurations, controls, and features. For example, you can slice your network to multiple Private LTE networks, allowing staff to have access to your internal network and voice calls, while guest users can only access the public Internet.

Note: While LTE supports basic network slicing, more advanced capabilities are supported by 5G.

Quality of Service

LTE provides multiple features for prioritizing and shaping data traffic, and those features can be used to prioritize certain data traffic in your network. Difference slices (see above) can have different prioritization rules, allowing for further service customization.

EPC

LTE networks require core network services to manage devices, enable mobility, and support voice, video, data, and application services. EPC solutions can be physically deployed on-premises, contracted as a service, accessed via the cloud, or delivered as a hybrid solution. Because OnGo private LTE deployments are so flexible, organizations can either purchase or subscribe to create a solution that best meets their technical

and budget requirements. (See CBRSA-TS-1002 for details on possible core network configurations.)

The same EPC used for a private LTE network can also enable additional expandability, allowing organizations to move mobile devices seamlessly from private to public connectivity via OnGo. For example, assuming you establish roaming relationships between your OnGo private LTE network and the public LTE mobile network operators (MNOs), users can roam from public networks to OnGo private LTE networks, or from OnGo private LTE networks to public networks.

EPCs can even interoperate with other bands and technologies to provide connectivity failover, expand capacity, and eventually accommodate 5G-based technologies. OnGo ecosystem service providers, system integrators, and vendors can help your organization select the optimal solution for each deployment.

Roaming Agreements

If your use case requires seamless roaming onto the public mobile networks, you will need to execute roaming agreements with the mobile network operators (MNOs). In addition to the commercial terms, the EPC will need to be configured to support such roaming. Depending on your use case you may need to set up a roaming agreement with just a single MNO (e.g., if the mobile devices all use the same MNO for service) or with multiple MNOs (e.g., in a BYOD environment).

IP Exchange (IPX)

IP Exchange (IPX) service providers can also provide roaming capabilities to an OnGo Private LTE network. IPXs provide a business and technical framework for integrating data services across networks, both fixed and mobile. In the private LTE context, they can provide a single point of contact for working with the public carriers (MNOs, MVNOS, MSOs, etc.) so that instead of having to implement roaming agreements with each carrier directly, you just work with the IPX. On the technical side, they also have existing infrastructure for the interconnection between your network and the public carriers, enabling cross-network roaming.

Identifiers

You will need to acquire several unique identifiers from the OnGo Alliance in order to ensure that your private LTE deployment interconnects correctly with (and does not interfere with) other LTE networks.

LTE networks use a Public Land Mobile Network Identifier (PLMN-ID) to uniquely identify themselves. There is a limited number of PLMN-IDs available, so OnGo Private LTE networks typically use the CBRS Shared Home Network Identifier (SHNI) (315-010). This can potentially cause problems, as the various globally unique identifiers used in LTE (GUMMEI, etc.) incorporate the PLMN-ID in them to ensure that they are globally unique. To ensure that these identifiers are globally unique, and prevent collision errors, the OnGo Alliance manages components of those identifiers.

Neutral Host Networks

An OnGo deployment can be configured to function as a Neutral Host Network (NHN). In this configuration, the OnGo network extends the networks of multiple Major Network Operators (MNOs). Subscribers to the supported MNOs are given access to the OnGo network transparently, so that it appears as their home network. They can then roam into and out of the CBRS network completely seamlessly.

This functionality requires special configuration of the OnGo Network and agreements with the MNOs. A separate guide on OnGo Neutral Host Networks provides additional information.

An OnGo network can even be configured to function as a Hybrid Network, providing NHN services as well as a Private LTE network.

The following identifiers can be acquired from the OnGo Alliance:

- A CBRS-NID (Network Identifier). This 27-bit number is used to uniquely identify networks using the CBRS SHNI.
- A Moblity Management Entity Group ID (MMEGI) , which is used to identify the Mobility Management Entity (MME), a component of the EPC.
- Macro eNB Identifiers (eNB IDs), one for each eNB in your deployment. These are used in LTE's self-optimization systems. (This identifier is needed even for microcell deployments, despite the name.)

Identifiers can be obtained from the OnGo Alliance online: https://ongoalliance.org/ongo-identifiers/. Contact SHNI@ongoalliance.org for additional information on identifiers.

In addition to the identifiers obtained from the OnGo Alliance, you will also need to generate several identifiers for use by your network:

- A Mobility Management Entity Code (MMEC) is an 8-bit number used to identify the MME within the MME Group associated with a given MMEGI. For most deployments, you'll only need one, but if you have multiple MMEs, each one in a given MME Group needs a unique number. Any number between 0 and 255 will do, and does not have to be obtained from the OnGo Alliance.

Do I Need to Reserve ID Numbers?

In order to prevent potential interference issues with other LTE networks in your area we generally recommend you reserve ID numbers. However, if your system is physically isolated from other LTE networks, and devices are not going to be moving in and out of your coverage area, then you can probably get by without ID numbers. That said, it is generally a good idea to get them anyway, as you may require ID numbers in the future as new services are added or outside circumstances change.

- Tracking Area Codes (TACs). These codes distinguish tracking areas controlled by a single MME and must be globally unique when combined with the first PLMN-ID broadcast by your NHN. We recommend using your IMSI Block Number (IBN – see below) for your first TAC. If you need additional TACs for large deployments with lots of CBSDs, we recommend you add 10,000 to the value of the previously used TAC (i.e. IBN + 10,000, IBN + 20,000, etc.). This method is not guaranteed to create a unique number, but it should be sufficiently unique to prevent collisions. If you need more than the 6 TACs derived from the IBN, you can request an additional IBN (see below) or obtain managed TACs from the OnGo Alliance. (See below for a discussion of how many tracking areas, and TACs, you will need.)
- Physical Cell Identity (PCI) – This is a number between 0 and 503 and is broadcast by each cell in your network. (An eNB typically can operate multiple cells – Category A CBSDs generally have only one cell, while Category B CBSDs may have eNBs that support several cells.) CBSDs should use Physical Cell Identities different from other nearby LTE cells, including other LTE networks operating in different bands in your area. PCIs are often optimized by the RAN using LTE's built-in self-optimizing network (SON) functionality.

You may acquire a dedicated global unique Home Network Identifier from the US IMSI Administrator, or request a different Shared HNI from other sources, but this process can be significantly more complicated than getting identifiers from the OnGo Alliance.

IMSI Block Numbers

If your network is using devices that connect only to your system, you will need to obtain an IMSI Block Number (IBN), which can be assigned by the US IMSI Administrator (https://imsiadmin.com/imsi-home). If you are going to have more than 100,000 devices, you will need an additional IBN. This IBN can be used to generate IMSI numbers to be assigned to a device's SIM card or an equivalent system such as an eSIM.

About LTE Identifiers and OnGo

In LTE, networks are identified using a five or six digit code, called the Public Land Mobile Network Identifier (PLMN- ID), that consists of a three-digit country code, and a two or three-digit Mobile Network Code. This information is broadcast by the LTE base stations (also called Evolved Node Bs, or eNBs). Devices then compare that PLMN-ID to the Home Network Identifier (HNI) stored in their SIMs to determine if it is part of their home network. eNBs can also broadcast a 27-bit Closed Subscriber Group Identifier (CSG-ID) that allows only devices with that ID to connect with the designated eNBs.

Tracking Areas

LTE network covarage areas are divided into Tracking Areas, each identified by a Tracking Area Code (TAC). These codes are used to track how devices are moving within your network. When the network wants to talk to a device (paging), it asks each CBSD/eNB in the tracking area where the device was last seen to connect to that device. With more tracking areas, your network can page devices more efficiently, at the cost of additional control traffic from the devices notifying the network when they have changed tracking areas. With fewer tracking areas, there's less overhead control traffic of devices notifying the network when they've changed traffic areas, at the cost of more control traffic when the network needs to page the device.

If your deployment consists of multiple coverage areas that don't overlap (for example, a network that provides coverage in multiple office buildings but not the outdoor areas between them), each coverage area can be assigned a separate TAC.

Backhaul

Now is an excellent time to make sure any additional network infrastructure you will need is in place. You'll need to consider providing power and IP connectivity to the

CBSD sites and ensure that the CBSDs have the bandwidth needed to connect to other networks, including the Internet.

End-User Devices (EUDs)

End-User Devices (EUDs) are what connect to your private LTE network. Devices can include mobile phones, tablets, laptops, IoT devices, internal communication systems or applications, modems, cameras, gateways, or routers to other networks and systems. Because OnGo uses LTE as its foundational technology, industry standards exist for security, interoperability, and service provision.

Many existing LTE devices (UEs) already support OnGo. As long as the chipset used in the device supports the 3.5GHz CBRS band (Band 48), the device can use OnGo. In many cases, existing equipment can be converted to the OnGo network without replacement, although some devices may need software updates from operators to enable the CBRS band. You can see the list of FCC-authorized EUDs at: https://ongoalliance.org/certification/fcc-authorized-end-user/.

Some important considerations when selecting EUDs:

- Is Band 48 enabled in the software of the device? (FCC authorization doesn't guarantee that the EUD's software enables use of the band.)
- Does it need to be a consumer-grade or an industrial-grade device?
- Does it support other bands than CBRS?
- Does it support the bandwidth and power levels needed for your deployment?
- Does it support the carrier aggregation configuration of your network?
- Does it support the physical and wireless interfaces you need?
- What kind of SIM does it use? Does it support Dual-SIM operation?

Scenario A: Smart-Building Design

At this point a set of vendors has been selected. A single vendor will provide the CBSDs, EPC, Domain Proxy, and EMS as an integrated solution, making the system easier to configure and maintain. The SAS vendor has been selected as well, with commercial terms based on the Domain Proxy aggregating the CBSD communications. Since the CBSDs on the upper floors are going to be higher than 6 meters off the ground, a CPI is needed.

A specialist has been contracted to check that the desired locations of the CBSDs will provide complete coverage, especially for the security cameras on the perimeter of the building. Based on the detailed measurements, the contractor will recommend where to place the CBSDs and how to configure their antennas best. Two CBSDs will cover each floor.

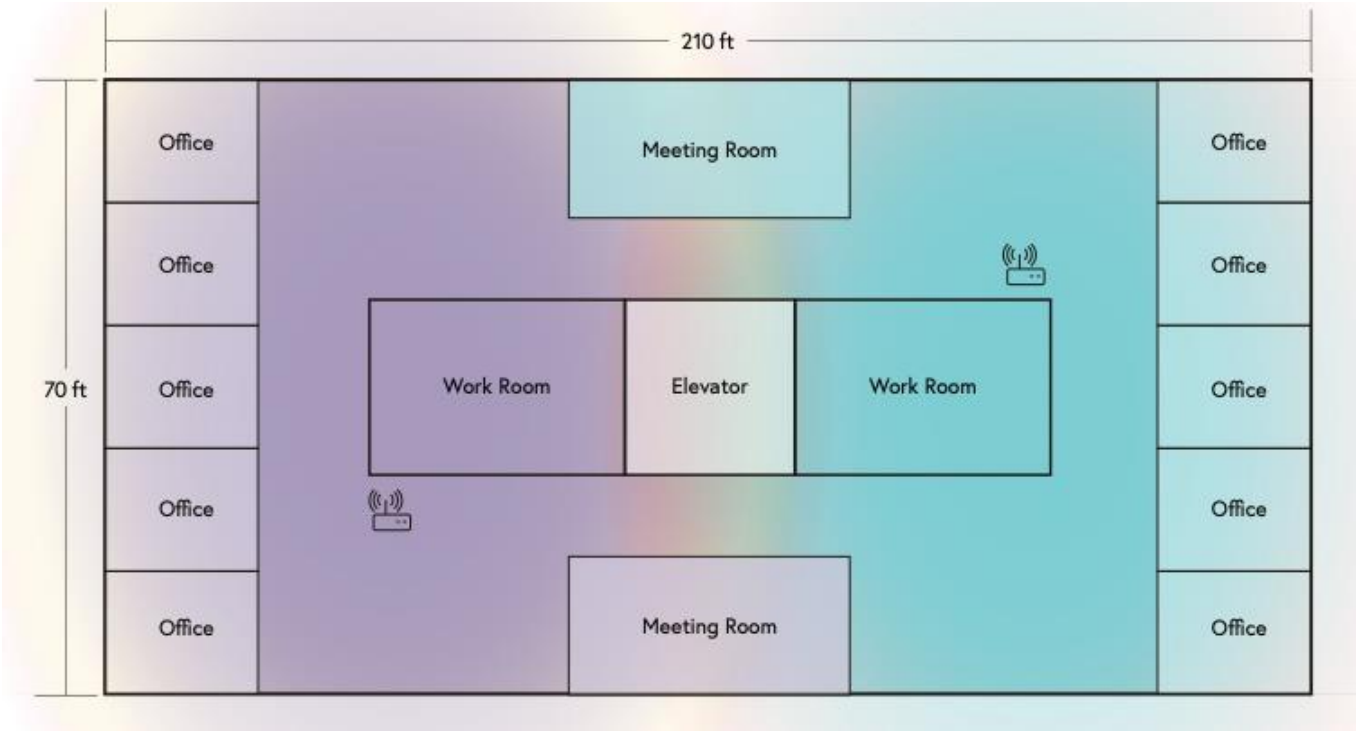

Figure 6: Smart-Building CBSD positioning and coverage map.

The EPC will be located on the site, in a network closet, and will run on a single server along with the Domain Proxy and EMS elements.

While roaming into and out of the public networks is not a requirement, a set of identifiers will need to be reserved to ensure that there are no interoperability problems given that additional networks are deployed in the area. A CBRS-NID and MMEGI, as well as Macro eNB IDs for each CBSD, will need to be reserved.

Scenario B: Sports Venue Design

Vendors are now selected. In this case, two CBSD vendors will be used: one for the indoor Category A CBSDs, and another for the outdoor Category B CBSDs. The chosen EPC is compatible with both CBSD vendors, and also supplies the EMS element. Two different domain proxies are needed, one for each CBSD vendor. The SAS vendor has also been selected, with the commercial terms based on the Domain Proxies aggregating the CBSD communications.

Figure 7: Sports Venue CBSD placement and coverage map.

A specialist service provider has prepared a detailed map of the coverage area to determine the ideal placement of the CBSDs. Two Category B CBSDs will be needed to ensure proper coverage of the stadium area and the parking lots. The Category B CBSD in the stadium will provide coverage of the playing area and stands. It will also be the primary link for the HD video cameras, and will use two 10-MHz channels, in an uplink-heavy configuration, to provide plenty of capacity. Due to interior obstructions, three additional CBSDs will be installed to provide coverage for the offices and indoor training facilities.

To obtain the required PAL, PAL owners in the area have been contacted to discuss sublicensing terms. Also, given that several of the CBSDs are Category B devices, a CPI has been engaged to register the installations.

The EPC will reside on site in the AV closet, and will also host a domain proxy service.

Since users will be roaming into and out of the public networks, the full set of identifiers will be needed: a CBRS-NID and MMEGI, as well as Macro eNB IDs for each CBSD. Roaming Agreements with each of the Major Network Operators (MNOs) have been signed.

Now it is time to start installing your CBSDs, EPC, and the other equipment in your deployment.

CBSD Installation

CBSDs typically need three connections to operate – power, a backhaul data connection, and one or more antennas.

CPI Requirements

All Category B CBSDs must be inspected and registered by a CPI. However, some Category A CBSDs can determine their location automatically via GPS/GNSS and don't always require a CPI. The most critical pieces of information that the CPI provides are the GPS coordinates of the CBSD, the power level, and the environment of the CBSDs (indoor or outdoor).

You can find more information on CPIs at the WInnForum website: https://cbrs.wirelessinnovation.org/cpi-program-administrator.

PAL Configuration & Spectrum License

If you have a PAL or are subleasing from a PAL holder, the SAS needs information about the CBSDs your network uses to add to the list of CBSDs associated with that PAL Protection Area (PPA). In addition, subleasing requires registration and certification with the FCC. If you don't have a PAL and are using GAA for access, no additional configuration information is required.

Each logical CBSD in your system can operate as either GAA or PAL. A physical CBSD device may contain multiple CBSDs, each with its own CBSD-ID, operating on different channels. These are treated as different CBSDs by the SAS, enabling the different logical CBSDs to use either PAL or GAA.

SIM Configuration and Provisioning

Devices that will connect exclusively to your network must be provisioned with SIM cards configured specifically for your network, with a custom IMSI (using your IBN). For

physical SIM cards, you will need to acquire SIM cards in the appropriate form factor, a SIM writer, and the necessary software. Devices with eSIMs can be provisioned using software, which is typically provided by the device manufacturer.

To properly configure your SIMs for connection to your network, you must set the Home Network Identifier (HNI) in the SIM to the Public Land Mobile Network Identity (PLMN- ID) of your network. For most Private LTE deployments using identifiers assigned by the OnGo Alliance, this is the OnGo Alliance's Shared HNI (315-010). Your specific network is identified by the CBRS-NID, which is provided in the SIM's Closed Subscriber Group (CSG) Identity field.

If you are building a standalone network and have not established agreements with any major network operators but want to support your users' personal devices on the system, you will need to provision those devices for dual-network support. This requires that your users have dual-SIM capable devices, and you configure the secondary SIM to connect to your network.

In either case, you will need to register the device with your network services to allow access for the device. The details of how to do this differ by system, but generally involve entering the IMSI or IMEI identification numbers into the management system.

EPC Configuration

At this time, your network's EPC element needs to be deployed and configured correctly to support your deployment. In particular, the system must be configured with the identifiers for your network (SHNI, CBRS-NID, etc.), and to work with your CBSDs.

Commissioning the CBSDs

Once installed, and with the configuration information (location, power level, etc.) recorded by the CPI, you can activate your CBSDs. The CBSDs will connect with the SAS and then request channel access. In most cases, mainly if there are no incumbents in the area, the SAS will grant access to your requested spectrum in near real-time. However, if you are close-by an incumbent, or in an area with possible incumbent

activity (most commonly on the coasts), spectrum authorization can take up to 48 hours.

Commissioning of End Devices

Once the CBSDs are activated, and channel access granted by the SAS, it is time to start connecting your devices to the network. For many devices, it's merely a matter of using a properly configured SIM, turning on the device, and waiting for it to find your network. Others may require manual connection.

Key Performance Indicator (KPI) Verification

Once your network is commissioned and operating, confirm that your deployment provides the needed capabilities – coverage, available bandwidth, etc. CBSDs can be re-configured, moved, added, or removed where there is insufficient or excess coverage or capacity. Many of these changes require the CPI to update the SAS registration information. We recommend performing these checks as soon as you commission the CBSDs.

Specialist service providers can perform detailed coverage and capacity checks as part of their service offerings. They can also offer detailed analysis and recommendations of how to adjust your network to provide the needed capabilities.

Scenario A: Smart-Building Installation

The CBSDs are installed, and use their autosensing capabilities to register their location with the SAS. As a result, a CPI is not required.

The Domain Proxy, EPC and EMS are installed and configured by the vendor. The vendor has also provided a set of SIMs for use in the devices, pre-configured so that the devices may connect to the OnGo network.

Once everything is provisioned, the OnGo network is commissioned. After a few minutes, the CBSDs will be activated by the SAS. Once the system is active, client devices may be turned on and will connect automatically with the CBSDs.

Scenario B: Sports Venue Installation

The CBSDs have been installed, and the CPI has registered their information – along with the information on the sublicensed PAL – with the contracted SAS.

The Domain Proxy, EPC, and EMS have also been installed and configured by their respective vendors. The vendor has provided a set of SIMs for use in the devices connected to the network. The EMS is used to register the device information for the staff's personal devices to allow them to connect to the system.

Once provisioning is complete, the OnGo network is commissioned. The CBSDs are activated by the SAS after several minutes, though it may take up to 48 hours in some circumstances.

Like any system, a private LTE deployment requires support. If there is a problem, it is essential to remember the system's elements that will most likely be the cause. Here are some recommendations for critical things to remember:

Network Operations Center (NOC) Support

A private LTE deployment has an EPC back-end system: the access network that includes CBSDs and end devices as well as the transport between EPC, access, and end devices. All these components require operational support from a Network Operations Center (NOC). Faults in individual CBSDs or end devices may affect specific areas of the network. If there is a problem with the EPC, the performance of the entire private network can be impacted. So it's crucial to have a NOC monitoring the system 24x7, particularly when mission-critical applications are running on the network.

HW/SW Alarms

Individual CBSDs, the EPC, backhaul connections, or EUDs can develop hardware or software faults. These components generate an alarm when an error occurs to alert the NOC support team. Classification of problems, and time requirements for their resolution, are often included as part of the contracts with service providers.

SAS Connectivity

If connectivity to the SAS is lost, the CBSDs will shut down after just a few minutes, which is why we recommend high-availability or redundant communications. If connectivity is lost, the SAS retains the grant for your network for seven days. As long as the link is restored within that timeframe, your network can resume operation immediately.

Channel Access

If an incumbent system becomes active, the SAS may direct your CBSDs to reduce power or even shut down entirely.

Interference from Other Networks

In general, the SAS prevents interference from other networks operating in the CBRS band, so don't worry about other networks. However, the SAS may instruct your CBSDs to reduce their power levels to prevent interference with other networks with higher priority (PAL holders and incumbents). If there is an interference problem that the SAS isn't automatically addressing, work with your SAS to help identify the problem source and resolve it.

Service Level Agreements (SLAs)

To ensure that your network operates at the needed level, you should establish Service Level Agreements (SLAs) with your vendors. The level of service guaranteed depends on how mission-critical your system is.

Key Performance Indicators (KPIs)

There are several pre-defined LTE-related KPIs that you can use to meet SLAs. Severak broad categories of KPIs are typically used, given elow, along with some example values.

- Availability – Used to measure the percentage of time the network is available for users to make full use of the offered services. Example KPIs include:
  - Call (data or voice) success rate >99.0%
  - Data bearer setup success rate >99.0%
  - VoLTE accessibility success rate >99.5%
- Retainability – This measures how often the users lose connectivity to the network typically due to inadequate coverage and quality.
  - Voice dropped call rate <1.5%
  - Data dropped call rate <0.5%
- Integrity – Used to measure the character of the network through metrics such as throughput and latency.
  - Average latency (uplink and downlink) <150 ms
  - Average jitter (uplink and downlink) <30 ms
  - Average downlink throughput >1 Mbps
- Mobility – Used to measure the network's performance while the users move through the system's coverage area.
  - Intra-network handoff success rate >98%
  - Inter-network handoff (hand in) success rate >99%

- Utilization – Used to measure network usage.
  - Downlink traffic volume (in Mbps)
  - Uplink traffic volume (in Mbps)

The source for the metrics for KPIs may come from the EMS of the CBSD vendor, or from the EPC. KPIs can also be custom-designed for specific use cases.

Changes in the environment can impact the network's KPIs. Reporting can include coverage areas that are disturbed when adding or removing walls and partitions, installing large metal objects in the area, or even planting trees or other foliage. Check periodically to make sure your network is still providing capabilities that can detect any changes, which allows you to adjust network operations as needed.

Monitoring

A network monitoring system plays a vital role in any private LTE deployment. This system should continually evaluate key performance metrics continually against your service level agreements (uptime, average throughput, etc.) and provide immediate notification of any problems that could impact critical services.

Priority Access License (PAL)

If system performance does not meet the desired level due to channel access limitations, you should consider acquiring or sublicensing a PAL.

Glossary

Term	Definition
AC	Alternating Current
AP	Access Point, the Wi-Fi equivalent of an eNB
Backhaul	Connection from a network node (CBSD) to other nodes and external networks.
BTS-CBSD	Base Transceiver Station CBSD: Fixed CBSD base station connecting to EUDs or CPE-CBSDs
BYOD	Bring Your Own Device
CA	Carrier Aggregation
CBRS	Citizens Broadband Radio Service
CBRS-NID	A CBRS Network ID, a CSG-ID that identifies the provider of a network
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.
Category A	<30 dBm/10 MHz (<1 Watt/10 MHz) transmit power CBSD
Category B	<47 dBm/10 MHz (<50 Watt/10 MHz) transmit power CBSD
CPE	Customer Premises Equipment
CPE-CBSD	A fixed device that communicates with a SAS via a BTS-CBSD and can exceed the EUD transmit power limit. In an OnGo context, it functions as a non-mobile UE.
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
DL	Downlink
DM	Device Management System (for CBSD)
eNB	Evolved Node-B, an LTE base station
EIRP	Effective Isotropic Radiated Power: the transmitted power level of a wireless device, including antenna gain
EMS	Element Management System
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 UE in OnGo (e.g., a smartphone, sensor, etc.). It can be a fixed or mobile device. Transmit power level must be <23 dBm EIRP.
FCC	Federal Communications Commission

Glossary

Term	Definition
FWA	Fixed-Wireless Access: A wireless telecommunication system where the devices are non-mobile. Often used for providing backhaul for other services.
GAA	General Authorized Access
GHz	Gigahertz
GNSS	Global Navigation Satellite System (e.g., GPS)
GTP	GPRS Tunneling Protocol: a tunneling protocol for managing mobile bearer data between an SGW and a PGW in an EPC
GPS	Global Positioning System
GW	Gateway
HAAT	Height Above Average Terrain
HD	High Definition
HNI	Home Network Identifier, the PLMN-ID of a device's home network
HSS	Home Subscriber Server, the network element of an EPC, contains user-related and subscription-related information in a centralized database
IBN	IMSI Block Number, a block of numbers granted for use by a network operator
IMEI	Individual Mobile Equipment Identity
IMSI	Individual Mobile Subscriber Identity
IT	Information Technology
ITU	International Telecommunications Union
IoT	Internet of Things
IPX	IP Exchange
Kbps	Kilobits per second
KPI	Key Performance Indicator
LTE	Long Term Evolution, the 4th generation mobile technology; used in OnGo
LTE UE	LTE User Equipment: a device (mobile or fixed) used by an end-user to communicate (e.g., a smartphone).
Mbps	Megabits per second
MHz	Megahertz
MIMO	Multiple-Input and Multiple-Output: a method for multiplying the capacity of a radio link using multiple transmission and receiving antennas to exploit multipath propagation

Glossary

Term	Definition
MME	Mobility Management Entity, the network element of an EPC that controls mobile device access to the EPC
MMEC	MME Code. An 8-bit number that identifiers an individual MME within an MME Group
MME Group	A collection of MMEs within a given network
MMEGI	MME Group ID identifies a specific MME Group within a network
MNO	Mobile Network Operator or a wireless carrier
MSO	Multiple System Operator—an operator of multiple cable or broadcast satellite services.
MVNO	Mobile Virtual Network Operator— a wireless carrier that does not own the physical infrastructure that provides services.
NHN	Neutral Host Network, an LTE network that provides coverage to multiple MNOs.
NOC	Network Operations Center
OnGo	LTE in the CBRS band
PAL	Priority Access License
PCI	Physical Cell Identity, an identifier broadcast by each cell in a network.
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.
Physical Cell Identity	A number from 0 to 503 broadcast by each LTE cell. This number should be different from other cells in the area.
PLMN-ID	Public Land Mobile Network Identity
PPA	PAL Protection Area. the geographic area that the SAS protects from interference for a given PAL.
PSP	Participating Service Provider, a network that is using an NHN to provide services to their subscribers.
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
SAS	Spectrum Access System, manages and assigns CBRS spectrum use on a dynamic, as-needed basis across PAL and GAA users.
SGW	Serving Gateway, a network element of an EPC that routes and forwards user data packets to a PGW via GTP sessions while also acting as the mobility anchor for the user plane inter-eNodeB handovers.
SHNI	Shared Home Network Identifier, a common PLMN-ID for use by CBRS systems (315-010)

Glossary

Term	Definition
SIM	Subscriber Identifier Module
SINR	Signal-to-Interference Plus Noise Ratio
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SON	Self-Optimizing Network
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.
UL	Uplink
USB	Universal Serial Bus
VoLTE	Voice over LTE, a packet-based protocol for handling voice calls in LTE.
WInnForum	The organization that develops the standards for CBRS system elements that include the SAS, ESCs, CBSDs, and CPI certification.

Requirements Gathering

What is the purpose of your private LTE network?
Who will be connecting to your private LTE network?
What devices will be connecting to your private LTE network? How many of each? What SIM system do they use?
Which devices will be mobile within your network? Which devices will move into and out of your network?

Survey and Planning

Sketch of coverage area. Note locations of critical devices, existing Wi-Fi Access Points, power outlets, and data access.
How much data capacity do you need?
Is a PAL needed?
SAS Administrators, CBSD, EPC, and EUD Vendors

Checklist

Design

Selected SAS Administrator:
Selected CBSDs:
Number of CBSDs:
Selected EPC:
Selected EMS/DM:
Selected CPI:
Assigned CBRS NID: (https://ongoalliance.org/ongo-identifiers/)
Assigned MME Group ID (MMEGI):
Assigned Macro eNB IDs:
Assigned IMSI Block Numbers (one per 100,000 devices) (https://imsiadmin.com/imsi-home)
Tracking Area Codes:
SIM Provisioning Option:
PAL License:
Network connections to PSPs:

Install Checklist

Install and Configure CBSDs:
Install and Configure EPC:
CPI Registered With SAS:
SIMs Provisioned:
Commission CBSDs:
Commission End Devices:

Maintain & Service Assurance

KPIs:
Defined Alarms:
Internal Contacts (for alarms):
Operations Contact:
CBSD Support Contact:
EPC Support Contact:

About the OnGo Alliance

The OnGo Alliance believes that 3GPP-based solutions in the 3.5 GHz band, utilizing shared spectrum, can enable both in-building and outdoor coverage and capacity expansion at massive scale. In order to maximize the full potential of spectrum sharing, the OnGo Alliance enables a robust ecosystem through the management of the OnGo brand, and the OnGo Certification Program. For more information, please visit www.ongoalliance.org and learn more about the expanded business opportunities OnGo is enabling.