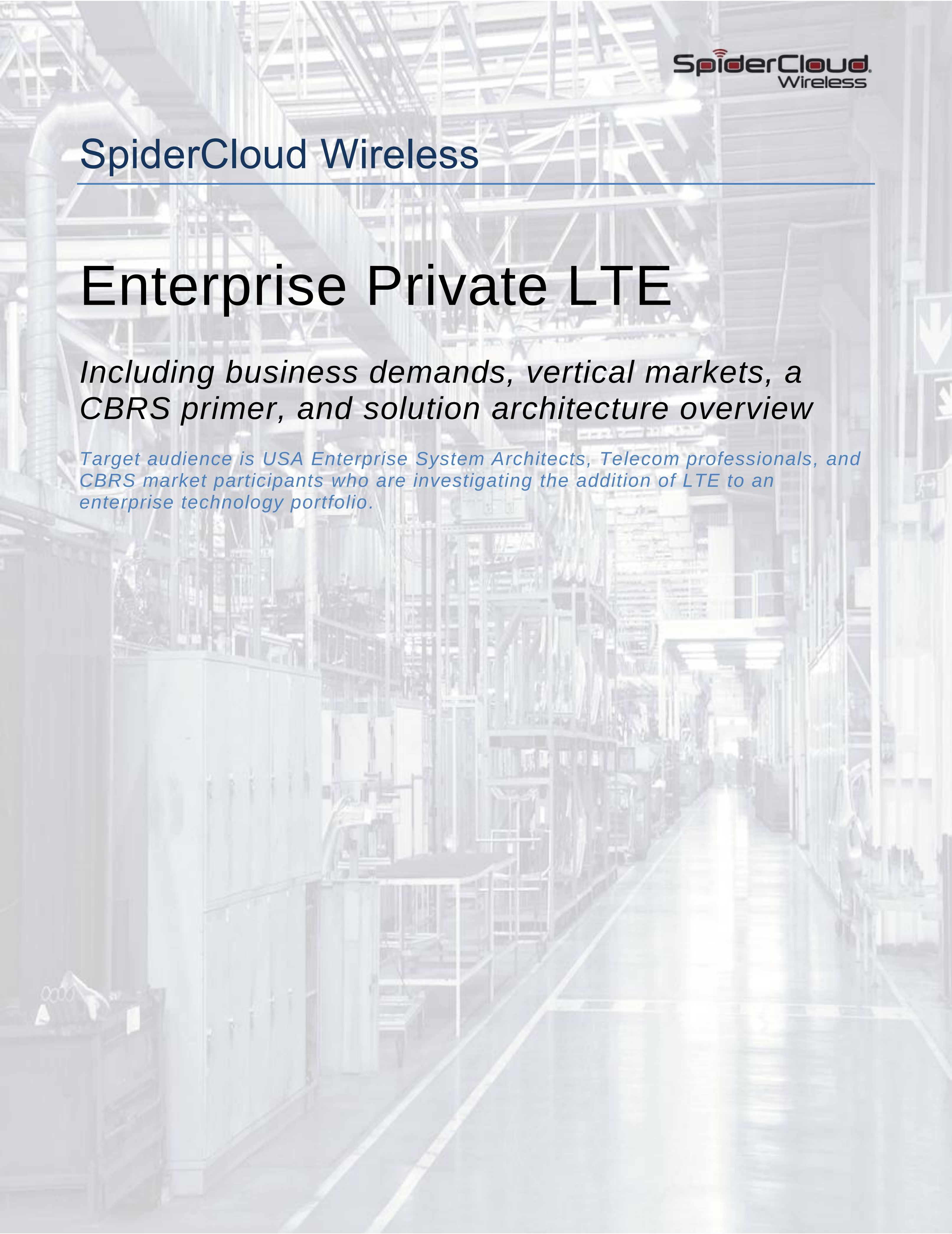

SpiderCloud Wireless

SpiderCloud Wireless

Enterprise Private LTE

Including business demands, vertical markets, a CBRS primer, and solution architecture overview

Target audience is USA Enterprise System Architects, Telecom professionals, and CBRS market participants who are investigating the addition of LTE to an enterprise technology portfolio.

Table of Contents

Executive Summary

LTE is the mobile broadband technology of choice for mobile service providers around the world, powering 1.7 B devices at the end of 2016 and expected to serve over 4.6 B devices by the end of 2022[1]. LTE offers high bandwidth connectivity with predictable latency. It is extremely secure, has a large ecosystem of suppliers, and offers a robust roadmap. Yet, enterprises have been generally unable to use LTE for their private wireless networks because LTE requires licensed spectrum.

This is about to change in the United States with the availability of Citizens Broadband Radio Services (CBRS) spectrum. Enterprises will be able to use this spectrum, from 3.55 GHz to 3.70 GHz, to deploy private wireless networks based on LTE without obtaining licenses from the Federal Communications Commission (FCC).

Private LTE networks can increase productivity and reduce operating costs in many industries. A manufacturing plant with a private LTE network will be able to replace wired connections to machines and robots with wireless connections. A hospital will be able to use LTE to connect clinical devices to its network. Commercial aircraft will be able to start uploading gigabits of data collected during their flight to servers as soon as they land. Some enterprises may offer to share their private LTE networks as neutral host onsite radio solution for the mobile service providers. Some of the mobile service providers may take this offer to deliver better cellular service indoors for their mobile subscribers at that site. The possibilities are endless.

Private LTE networks will be deployed using the same system architecture that is used for the public LTE networks. However, over the last few years, companies such as SpiderCloud Wireless have dramatically reduced the cost and complexity of building high-capacity LTE radio access networks inside buildings and campuses, making the price per sq. ft. of deploying LTE comparable to Wi-Fi. Partner companies have reduced the cost and complexity of LTE core network equipment. Many companies are building low-cost LTE mobile device modules that can be easily integrated into machines and to many kinds of Internet of Things devices.

This paper begins by explaining the benefits of LTE to enterprises, followed by examples of how it can be used in several large industries, from healthcare to manufacturing and transportation hubs. It provides a primer on CBRS spectrum rules, and then explains how an enterprise can build a private LTE network, provision client devices, and create new services. Finally, it provides a short overview of SpiderCloud's solution for private LTE networks.

[1] Ericsson Mobility Report, Nov 2016

1. Business Demands for Private LTE

Let's unpack LTE and its potential attractiveness to enterprises as a platform.

- LTE offers predictable latency, necessary for many Internet of Things (IOT) applications that rely on time-bound communications. In such applications a missed or delayed transmission can result in a catastrophic failure.

- LTE is designed for supporting large number of bandwidth hungry devices. Not only do LTE access points (called "small cells") offer data rates as high as 300 Mbps, but, unlike Wi-Fi, they are able to do so, without sacrificing predictability, even when the small cell is shared by large number of users.

- LTE offers seamless mobility. This means that whether an enterprise is a manufacturing plant with forklifts, or a hospital with doctors on the move, an LTE network can provide them reliable connectivity throughout the building or campus.

- LTE has over-the-air encryption and integrity protection built in along with the strong SIM based authentication. LTE's security mechanisms are proven to work on billions of devices, and are maintained by a large community of security developers and white hat hackers on behalf of the mobile industry.

- LTE is power efficient. It delivers a long mobile battery life because it has been engineered and optimized to operate over an extended period while communicating with radios that are a long distance away.

- Large enterprises and campuses can be covered with a relatively small number of small cells. Several commercially available indoor small cells easily cover over 10,000 ft^2. CBRS spectrum rules allow outdoor small cells to transmit at as high as 50W[2], sufficient to cover few km^2. Each small cell can simultaneously service 64 to 128 client devices without degradation in aggregate throughput

Though enterprises can access all the benefits of LTE on a public mobile operator LTE network, the public LTE network comes with strings attached. When enterprises use the public LTE network, they have to rely on operators to provision devices and provide adequate network capacity, in places where the enterprise needs it. Enterprises don't have the ability to easily connect devices to enterprise applications and they have to pay per MB and per device connected.

The public LTE network still makes sense for applications where enterprises want to access a wide-area mobile network, e.g. when the IOT device is outside of the enterprise premises. However, when the IOT device is on the enterprise campus, the device could very well connect via enterprise owned Private LTE network. This is where enterprises already rely on private networks, such as Ethernet LANs and Wi-Fi. As discussed in the next section, there are several applications that can benefit from being untethered from an Ethernet LAN but cannot be suitably addressed by Wi-Fi. This is where private LTE networks in CBRS band come in.

2. Vertical Market Use Cases for Private LTE

Healthcare

This market has a significant amount of high tech devices that are used throughout both clinics and hospitals. In the past, while IT system architects and operations people have desired LTE, they have only been offered Wi-Fi because it has been the lowest common denominator. The advantages of LTE were outweighed by the decision of which mobile service provider's radio to put into a clinical device.

CBRS enabled Private LTE solves this by delivering mobile service provider independent spectrum that is nationally available. This is of critical importance as every clinical device must go through an FDA certification process and CBRS spectrum enables one certification to be attained that will be good for any Private LTE

[2] 50W is effective isotropic radiated power (EIRP) including antenna gains.

instance. We envision that future generations of USA targeted, FDA approved devices will offer an integrated CBRS and Wi-Fi radio subsystem that can satisfy both Wi-Fi and CBRS enabled venues. According to MDDI, the market for medical devices is worth billions of dollars[3] and quality connectivity has a high value.

Manufacturing Plant

There are many industrial machines and applications that are still connected to wires today as Wi-Fi is not suited for the deterministic demands between process control computers and Programmable Logic Controllers (PLC). Timing windows in a manufacturing ecosystem are very critical because an action that happens too late or not at all disrupts system wide operations.

Consider the example of welding robots used along an automobile assembly line. All the robots operate in a synchronized and precise manner. If the communication between a robot and assembly line sensors or controls platforms is delayed, the slow robot risks slowing down the assembly line or colliding with another robot that has had no delays. Today, robots, assembly line sensors, PLCs, and so forth are still hardwired to remove the potential risk of variations in communications delay/jitter and availability out of the equation.

In a distribution center, picking robots place products on conveyor systems, PLC’s read each bar code on the products as they go by, and another PLC is instructed to switch each box to the correct conveyor to route them to the point where the total order is being packaged for outbound shipment. Today, the bar code reader and switching PLC’s are both hardwired because a delay in communications will result in the box in motion not being routed to its correct outbound shipping point.

In both, the assembly line and the distribution center, every cable run is costly and may have to be done with rugged cables or protected in conduit. But without deterministic communications, use of cabling is the correct decision to assure trouble free operations every day. In both environments, private LTE networks can offer an alternative to hardwired connections.

Transportation Hubs

Employee communications are a key need across transportation hubs. Because of the need for security, the systems are closed environments and the devices in use are both expensive and limited in function. LTE is viable in large open areas indoors (commercial jet hangers) and outdoors (ramp areas away from the terminals/buildings) as the range between a cell and a mobile device can be quite far. Private LTE brings a closed system with a long signal reach that provides great coverage and unprecedented capacity.

Private LTE enables remote diagnostics, for example, if something looks wrong, an employee can perform a quick video consultation with a remote specialist and allow them to solve the problem right now under direction of the specialist. Further, the capability to report an incident with multimedia enables personnel responding to an issue to assess it, equip themselves fully, and arrive ready to work instead of having to make one additional trip for tools and parts after they arrive and assess. This “first visit” capability is especially attractive in HazMat remediation.

Surveillance cameras that only require a connection to a power source provide great agility. Where cameras might be needed only for an event or seasonally, it is expensive to put in a network cable and then abandon it. With Private LTE, even wideband 4K cameras can be supported.

IoT in the baggage handling area is very similar to the Distribution Center needs of many PLCs handling routing of baggage/cargo to the transport equipment that moves it to the aircraft for loading. There are many other needs for IoT, for example, weather sensors (instrument the micro-climates across an airport), intrusion detection (fences, gates, doors, windows), badge readers, and employee locators.

IoT at the ramp is an especially interesting area of exploration. Modern aircraft collect a significant amount of data each time they fly. This data must be uploaded from the aircraft each time it lands. To illustrate the problem, domestic flights have a 40 minute window to turnaround an aircraft where turnaround is the time frame from

[3] http://www.mddionline.com/article/top-40-medical-device-companies

pulling up to gate, unloading passengers, servicing aircraft, loading passengers, and departing gate. In this same 40 minute window, a Private LTE infrastructure can support the aircraft's transmission of the collected data.

Finally, for many types of operations that must collect money, Point of Sale terminals are required. While this could be handled just fine on a service providers LTE infrastructure, because the PoS devices never leave the facility, Private LTE is ideal to enable across the facility as a measure to eliminate unneeded mobile subscriptions and Wi-Fi concerns around SSID chaos, security configuration, and audit compliance required by retail PCI regulations.

Oil Exploration & Production

Many of the use cases explored in prior vertical markets are similar for exploration and production (E&P) and also refining. These apply here:

- PLC for sensors, instrumentation, and control
- Surveillance
- Mobile devices
- Apps that provide "total visibility" to platform operations

The obvious benefits of Private LTE are greatly amplified in this market. The difference in E&P platforms and Refineries is the harsh physical environment and presence of explosive gases. The cost of running low voltage cabling in rated conduits and providing equipment either "intrinsically safe" or installed in a compliant enclosure is high. Standards that are followed are IEC 60079 Series Explosive Atmosphere and IEC 60529 Degrees of Ingress Protection where housings are typically IP66 rated.

3. CBRS Spectrum Enables Private LTE Networks

Today, if an enterprise wants to build a private wireless network, it must do so using unlicensed spectrum in 2.4 GHz or 5.8 GHz bands. The de-facto standard for wireless connectivity in this spectrum is Wi-Fi. However, as discussed earlier, Wi-Fi cannot provide predictable latency, quality of service or high bandwidth once Wi-Fi access points are heavily loaded. Also, it is very difficult for the enterprise to control what other Wi-Fi devices (e.g. Mobile Wi-Fi Hotspots) may be brought on premises, what channels they use and what kind of interference they generate for the Enterprise Wi-Fi deployments. LTE is designed to avoid all these pitfalls, and the FCC is now making spectrum in the 3.5 GHz band available to enterprises for private LTE networks.

LTE is already being deployed in the 3.5 GHz band by mobile operators in countries such as Japan where it is available as licensed spectrum. As a result, many LTE network infrastructure suppliers and device chipset manufacturers already offer products in the 3.5 GHz band. This band was not licensed to wireless operators in the US because it has several incumbent users, such as the US Navy, that are difficult to relocate. However, the typical utilization is very low. In many geographical areas there is no incumbent use at all. This underutilization offers plenty of opportunities to use the band for Private LTE deployments as long as it is ensured that operating a specific LTE network in a specific location does not endanger any nearby incumbent usage in the same spectrum (if any).

The FCC is now making this spectrum flexibly available under a new set of licensing rules that protects the incumbents while making the spectrum broadly available for a wide set of users[4]. This regulatory framework, called Citizens Broadband Radio Service (CBRS), establishes a three-tier approach for the use of this spectrum. At the top tier are the incumbents such as radars, fixed satellite stations and wireless Internet service providers (WISP)[5]. On the second tier are entities that purchase exclusive use licenses for their LTE deployments. Such licenses are called Priority Access Licenses (PAL) and are defined at the county level. On the third-tier are users that have non-exclusive use rights called General Authorized Access (GAA) at the location where their deployment resides.

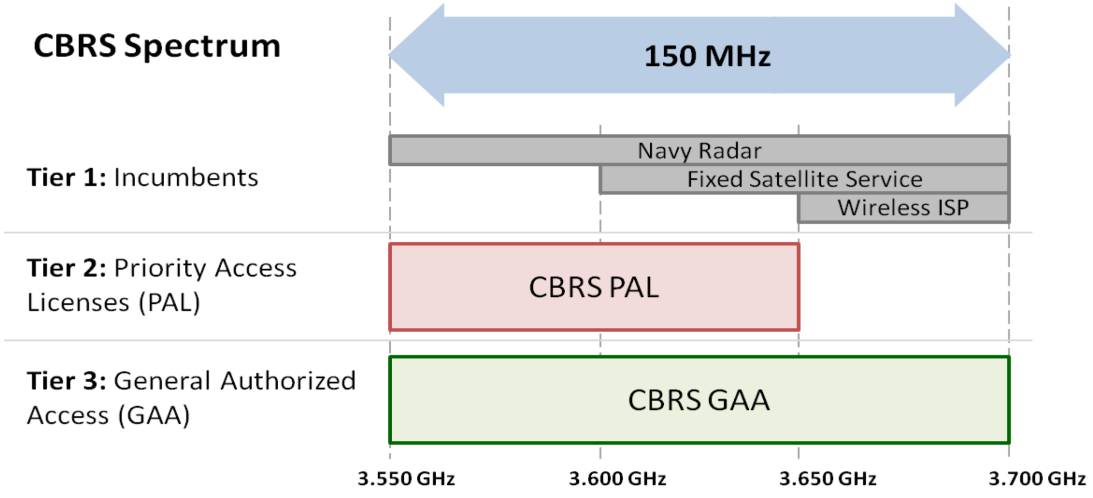

Figure 1: Three-tiered model for CBRS Spectrum Access

A cloud-based Spectrum Access Server (SAS) is responsible for protecting incumbents from harmful interference from the new users of this spectrum (PAL users and GAA users). Every CBRS base station, called a Citizens Broadband Radio Service Device (CBSD), must first connect to a SAS when the CBSD is powered on, and provide its coordinates (latitude, longitude, altitude) and globally unique CBSD identifier to the SAS. Based on this information, the SAS provides the CBSD with the CBRS channels available for the CBSD at the CBSD location.

[4] https://www.fcc.gov/document/35-ghz-order-recon-and-2nd-ro

[5] WISPs will lose their incumbent status in 6 years.

Multiple entities are building SAS systems that use the standard interface between SAS and CBSDs. Also, there is an interface between the SAS entities so that they can provide consistent service to their CBSD customers in the same geographic area.

Technically, CBRS rules allow the SAS to change the channels available to a CBSD any time to protect higher-tier users. E.g. if an incumbent system, like a Navy radar, in a given location starts to use a specific portion of CBRS spectrum, the SAS becomes aware of this via the SAS distributed Environmental Sensing Capability (ESC) network. The ESC system consists of a set of sensors distributed into areas called "exclusion zones" where incumbent use may occur. When such incumbent use is detected, SAS reassigns all CBSDs operating in that area and using the impacted part of the CBRS spectrum to other CBRS spectrum within five minutes. Well-designed network infrastructure products can minimize the impact of this kind of channel reassignment for enterprises that are geographically close to incumbent users. The vast majority of enterprises will be located far away from incumbent users where incumbent activity will not influence them at all.

If an enterprise wants to have priority over other deployments for use of CBRS spectrum, they can also acquire PAL licenses in an auction. The FCC is expected to start auctioning PAL licenses in late 2019. The PAL rules award licenses on a per county basis and are valid for ten years with rights to renew the license. Acquiring the rights to use PAL licensed CBRS spectrum for an enterprise CBRS deployment could also be achieved by partnering with a mobile operator who already has a PAL license in the county where the enterprise site is located. The flexibility for an enterprise to build an onsite CBRS radio access network that uses the mobile operator provider licensed CBRS spectrum with the onsite Radio Access Network (RAN) being configured to allow both enterprise specific Private LTE devices and partner mobile operator subscriber devices to connect via the on site CBRS RAN infrastructure (neutral host RAN sharing as illustrated in Figure 8). However, acquiring PAL licenses is not necessary for private LTE networks; in most cases using GAA based CBRS spectrum should be fully sufficient.

FCC rules require that a significant share of the CBRS spectrum is reserved for GAA use. CBRS rules do not allow portable or mobile CBSDs, ensuring that an entity controlling access to a facility controls the CBSD installed in it. Even if some entity has acquired a PAL license in a certain census tract, an enterprise may be able to use the same spectrum via GAA if the PAL licensee is not using it within the enterprise facility. The requirement that CBSDs are able to obtain their location, report it to a cloud-connected server, and then control all its clients make CBRS ideal for deploying private LTE networks on the 3.5GHz spectrum.

The GAA framework to access CBRS spectrum offers enterprises reliable and high quality LTE spectrum without the prohibitive cost of traditional licensed spectrum. Since mobile operators plan to use CBRS as well, enterprises that deploy private LTE will benefit from the economies of scale of the mobile industry. As of February 2017, more than 37 companies representing different parts of the mobile value chain had joined the CBRS Alliance, an industry alliance focused on making LTE in CBRS band a success. The next section discusses how an enterprise can build a private LTE network in CBRS spectrum.

4. Technical Architecture: Self contained Private LTE Solution

Network Infrastructure

The network infrastructure for a private LTE network is a scaled-down version of the standard 3GPP infrastructure used to realize nationwide public mobile networks. This infrastructure typically consists of the RAN and an Evolved Packet Core (EPC)[6].

Using the 3GPP framework as the logical architecture allows enterprises and other entities considering deployment of LTE based private networks to simply refer to existing specifications when soliciting infrastructure vendors for network equipment. Enterprises just need to characterize the desired deployment environment and the desired scale for their use case and then leave it to the infrastructure vendors to offer a cost efficient, 3GPP standards compliant and multi vendor interoperable solution for the enterprise.

In recent years it has become common to deploy small cell based LTE RAN solutions in venues, enterprises, and other commercial premises. Small cells are low-power cellular base stations. These small cell based RAN solutions can be adapted to serve the Private Network use case. All that is needed are small cells that support the CBRS radio band as specified in 3GPP (LTE band 48) and have a CBSD to communicate with the SAS.

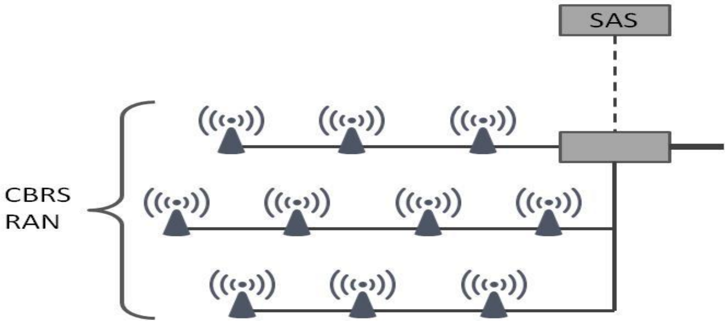

Figure 2: Illustration of CBRS radio access network (RAN) infrastructure

In addition to CBRS-capable small cells, a private LTE network requires a private EPC. An EPC offers 3GPP specific routing and signaling functionality as well as maintenance of 3GPP specified subscriber database contents. With an EPC in place, the private LTE network becomes just another way to gain IP connectivity to the enterprise IP network and services, exactly in the same way as Ethernet or Wi-Fi are used. Devices gain access to the CBRS based Private LTE network by installing enterprise managed SIM cards in the authorized devices. Devices without enterprise issued SIM cards will not be able to access the Private LTE system. Several companies now offer 3GPP compliant EPC functionality as software running on single physical or virtual server (called a “virtual EPC”). When selecting an EPC supplier, an enterprise will also verify that the EPC integrates with the enterprise’s existing management and provisioning systems, and develop enterprise specific operations processes.

[6] The EPC is also commonly known as the “Core Network”

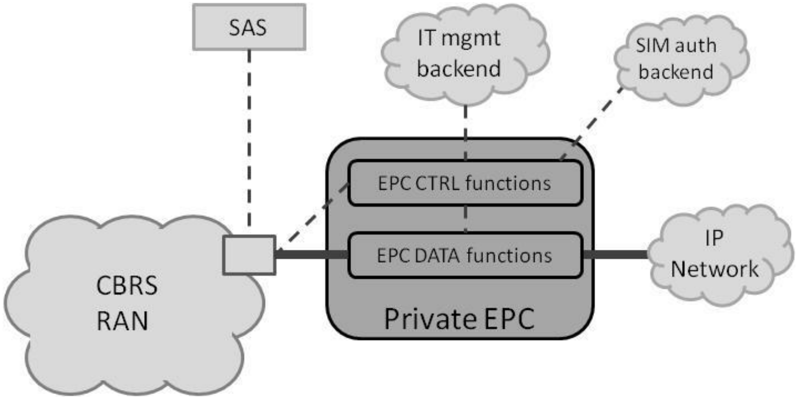

Figure 3: Illustration of CBRS Private Core Network Infrastructure

Client Devices or User Equipment (UE)

In LTE, a client device is called User Equipment (UE). Enterprises can use any UEs that support the new 3GPP band for CBRS, called Band 48, on their private LTE network. Since mobile operators plan to use Band 48 as well, it is expected that there will be wide range of off-the-shelf CBRS UEs for private LTE networks, ranging from smart phones to Internet of Things (IoT) modules.

An enterprise will be able to self-provision its client devices on its private LTE network, without involving a mobile operator. An enterprise will install its own private SIM card on the device. Subsequent sections discuss how this SIM card will identify the private LTE network and join it. The EPC will be responsible for connecting to the SIM authorization system to authenticate the client device. If an enterprise wants the device to work on both the private LTE network and on a mobile operator's network, it will need devices that support two SIM cards (a "dual-SIM device").

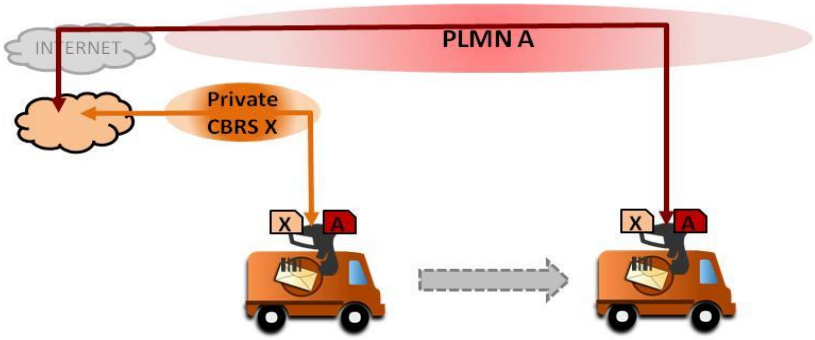

Figure 4: Devices on private LTE network need private SIM. Devices that connect to private and public networks need two SIMs

In addition to benefiting from the economies of scale in the LTE UE market, enterprises will benefit from the LTE roadmap. As an example, 3GPP has specified multiple enhancements to support low-power Internet of Things (IoT) devices. LTE UEs with these enhancements use orders of magnitude less power than what is used by typical Wi-Fi devices. All these enhancements are directly applicable to CBRS both public and private network deployments.

Network Identification

An LTE network is identified using a Public Land Mobile Network Identifier (PLMN-ID). Each mobile operator has a globally unique PLMN-ID and their LTE RAN broadcasts the supported PLMN-ID, so that devices know whether to attempt to connect.

It is not practical to assume that every enterprise would obtain its own globally unique PLMN-ID. To avoid this, a special PLNM 315-010 has been created, called the Shared Home Network Indentifier (HNI), for use in Private LTE deployments.

The Shared HNI is administered at a national level by iconectiv (http://imsiadmin.com). iconectiv assigns each enterprise applicant a unique IMSI Block Number (IBN) within the Shared HNI. Finally, each enterprise assigns the available pool of User Identification Numbers (UIN) to their devices attaching to the Private LTE network.

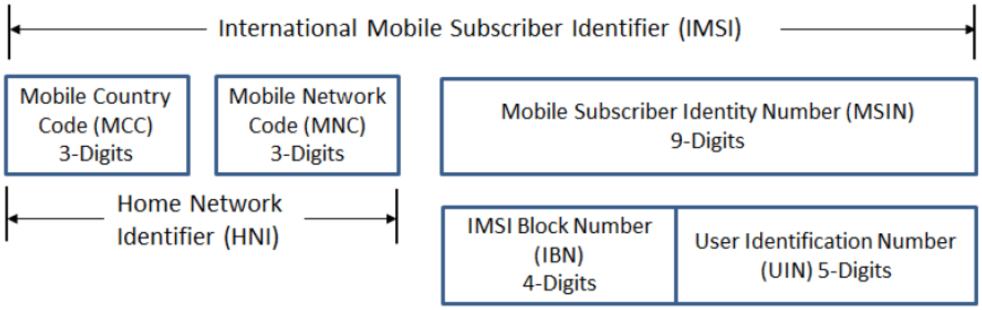
International Mobile Subscriber Identifier (IMSI)
Mobile Country Code (MCC) 3-Digits
Mobile Network Code (MNC) 3-Digits
Mobile Subscriber Identity Number (MSIN) 9-Digits
Home Network Identifier (HNI)
IMSI Block Number (IBN) 4-Digits
User Identification Number (UIN) 5-Digits

Figure 5: IMSI Structure

Subscriber Identification & Authentication

An LTE subscriber is identified using an International Mobile Subscriber Identifier (IMSI). A subscriber's IMSI is stored on the SIM card that is tied to the PLMN-ID associated with entity that issued the SIM card. When a subscriber's device connects to a LTE network, the IMSI and associated credentials within the device's SIM card are authenticated against the Home Subscriber Server (HSS) operated by the same entity who issued the SIM card for the mobile device.

As discussed in the previous section, it is expected that private LTE networks in CBRS band will primarily use the Shared HNI with assigned IBN and locally administrate the UIN pool to create their IMSI numbers.

Once the enterprise has its IMSIs, it can procure the SIM cards and the associated authentication backend solution for the private LTE network. The SIM cards can either be traditional plastic SIM card or be software based. When the SIM card provider produces them, each one is configured with an IMSI value and associated shared secret Key (called K_i in the 3GPP specifications). The K_i configured into the SIM card is not readable from outside, but is solely used within the SIM's secure computing environment to calculate authentication responses based on the authentication challenges received from the network. When an enterprise orders private SIM cards, the vendor provides the physical SIM cards and a list of IMSI and K_i pairs associated with each SIM card. The IMSI/ K_i pairs are imported into the subscriber authentication database to authenticate the private SIM card when connecting the Private LTE network. The IMSI/K_i list needs to be treated with utmost care and cannot be made available to any 3rd party.

The SIM subscriber authentication backend can either be a cloud-based managed service or a solution deployable by the enterprise itself ("Authentication Center (AuC) on a USB stick").

Services & Applications

The use of 3GPP-compliant network infrastructure, client devices, and authentication methods allows the private LTE network to use scaled-down version of 3GPP-specified mobile service infrastructure such as IP Multimedia Services (IMS) as well as the widely used mobile operating systems like Android and iOS. If the enterprise chooses to do so, it can reuse the built-in dialer and messaging applications on smart phones and tablet style devices.

However, the enterprise is not constrained to using IMS or mobile operating systems. As discussed earlier, the private LTE network appears as just another way to gain IP connectivity to the enterprise and any applications can be loaded on client devices.

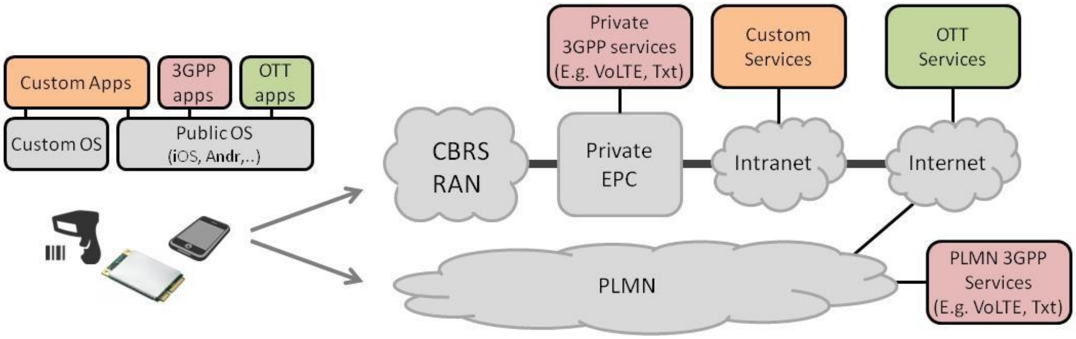

Figure 6: Illustration of various usable Services and related Client Device Applications.

Private LTE Network as Neutral Host for Public LTE Networks

Many enterprises have employees and guests who use their smartphones on public LTE networks. Once a private LTE network is up and running, it can be configured to also operate as an onsite RAN for public LTE service for these smartphones. Of course, this is only possible if these smartphones support the CBRS band. At the time of writing this paper, CBRS-capable smartphones are expected to emerge soon in the US market. SpiderCloud expects that by 2022, as many as 67% of smartphones will be CBRS capable[7].

YEAR	Handset penetration at Year-End
2018	1%
2019	7%
2020	27%
2021	47%
2022	67%

To support this use case, a private LTE RAN can be configured with 3GPP compliant RAN sharing (called MOCN in 3GPP specifications), allowing it to simultaneously advertise its own private LTE Shared HNI as well as public LTE PLMN-IDs of mobile operators. CBRS RAN sharing is enabled by the RAN being connected to multiple core networks. E.g. the same CBRS LTE RAN can be connected to a private EPC on-site and up to five public mobile service provider EPCs at the corresponding mobile service provider data centers. Recent Release 14 changes to the 3GPP LTE specification make it easier for enterprises and mobile service providers to share a LTE RAN by allowing each service provider to assign its own cell identities and tracking area codes to the RAN, removing the need for coordinating these identifiers between the participating service providers.

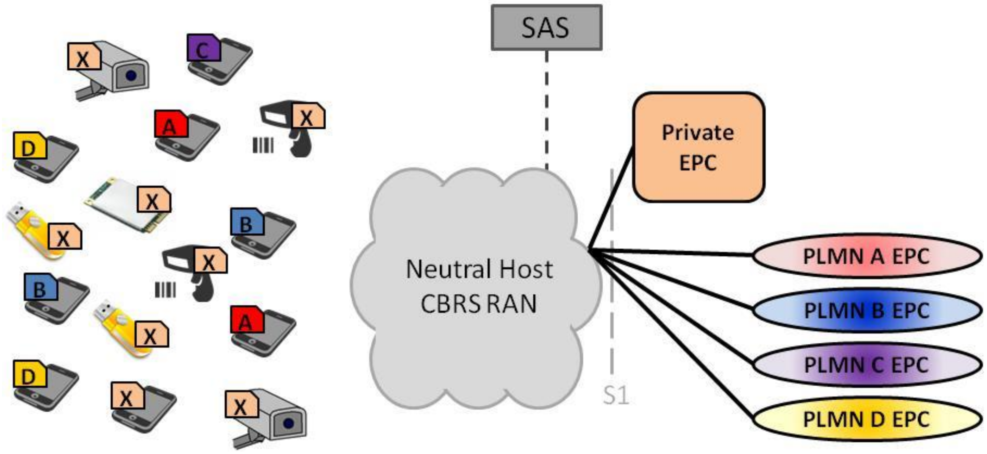

Figure 7. Evolution from pure Private CBRS Network into a Neutral Host CBRS Deployment

Using the same network infrastructure for both private and public LTE networks can create new business models. For instance, a large mobile operator can offer to build and manage private LTE networks (possibly using CBRS spectrum for which the mobile operator holds a license for) for enterprises if it gets the right to share this network also for its own subscribers. This secondary use of a private LTE RAN as a neutral host for mobile service providers is particularly straightforward if the network infrastructure used for the private LTE RAN has been certified for use in major mobile service provider networks.

[7] Handset replacement cycle is 2.5 years, Gartner, www.gartner.com/newsroom/id/3339019

5. Corning CBRS Radio Access Network

Corning is a leading supplier of LTE small cell systems for enterprises. It was the first company to make it possible to deploy LTE in medium to large buildings, commercial venues and campuses in the same way that Wi-Fi is deployed. Major mobile services providers such as Verizon, Vodafone and Telcel have deployed its solution, called Enterprise Radio Access Network (E-RAN), since 2012.

The E-RAN supports CBRS spectrum. The CBRS solution includes indoor and outdoor access points (called Radio Nodes) that connect over Ethernet to the E-RANs small cell controller (called Services Node). The Services Node then connects to an enterprise's Evolved Packet Core (EPC). The EPC is either co-located with the Services Node in the enterprise or hosted in the cloud, depending on the enterprise's desired deployment model.

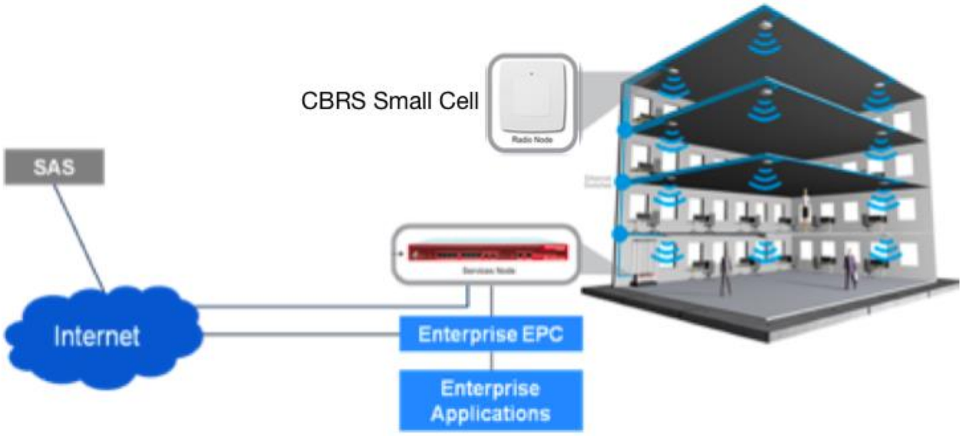

Figure 8. *E-RAN private LTE network solution.*

It is easy to deploy E-RAN in an enterprise because its architecture is similar to contemporary enterprise Wi-Fi. Each installed Radio Node requires a PoE+ Ethernet switch port and leverages existing Ethernet for both data transport and power source.

E-RAN systems are designed to deliver seamless performance throughout a large building or campus, without extensive manual intervention or optimization. Software running on the Services Node is responsible for configuring all the Radio Nodes and managing handovers as client devices move from one Radio Node to another.

CBRS rules require that the location of every CBRS base station (aka CBSD) is known and reported to the SAS. The LTE protocol used in CBRS bands, TDD-LTE, requires that all base stations are synchronized with each other in time and phase. Industry norms expect that GPS is used as the master clock for synchronization. As a result, many CBRS small cells include a GPS receiver. However, it is impractical to expect every small cell in a large enterprise to get GPS signal or individually communicate with the SAS. The Services Node, with a built-in GPS receiver, is responsible for ensuring that CBRS small cells are synchronized with GPS. The Services Node also communicates with the SAS on behalf of all small cells and ensures that available channels are used in a manner that maximizes throughput.

Corning is continuously enhancing E-RAN to meet the requirements of its service provider customers and to keep up with the 3GPP roadmap, and enterprises deploying private LTE networks can benefit from this investment.

6. Summary

Enterprises in a wide range of industries need wireless connectivity that offers high bandwidth and predictable latency, cost-effectively supports a high density of client devices, is secure and reliable to support critical business operations and is fully controlled by the enterprise. Private LTE networks operating in CBRS spectrum can meet these requirements.

Private LTE networks utilize the same standards, network architecture, and supplier ecosystem that are used by mobile operators today. Recent advancements, such as the development of enterprise small cells that can be deployed over existing Ethernet LAN, software that can automatically configure small cells, virtualized core network products that run as software on off-the-shelf hardware, and the availability of CBRS spectrum, make it possible for enterprises to own and operate private LTE networks.

Enterprises are not mobile operators and they never will be. Corning and its partners have internalized this message and it’s our key to approaching the market. We assume that there will not be any LTE or cellular experts within the enterprise to operate the private LTE. Instead, we see enterprise IT operating successful enterprise-wide communications infrastructure that is composed of many technologies and operations partners.

Corning looks forward to discussing the potential of private LTE networks in CBRS spectrum with enterprises. Please learn more at http://corning.com/go-cbrs