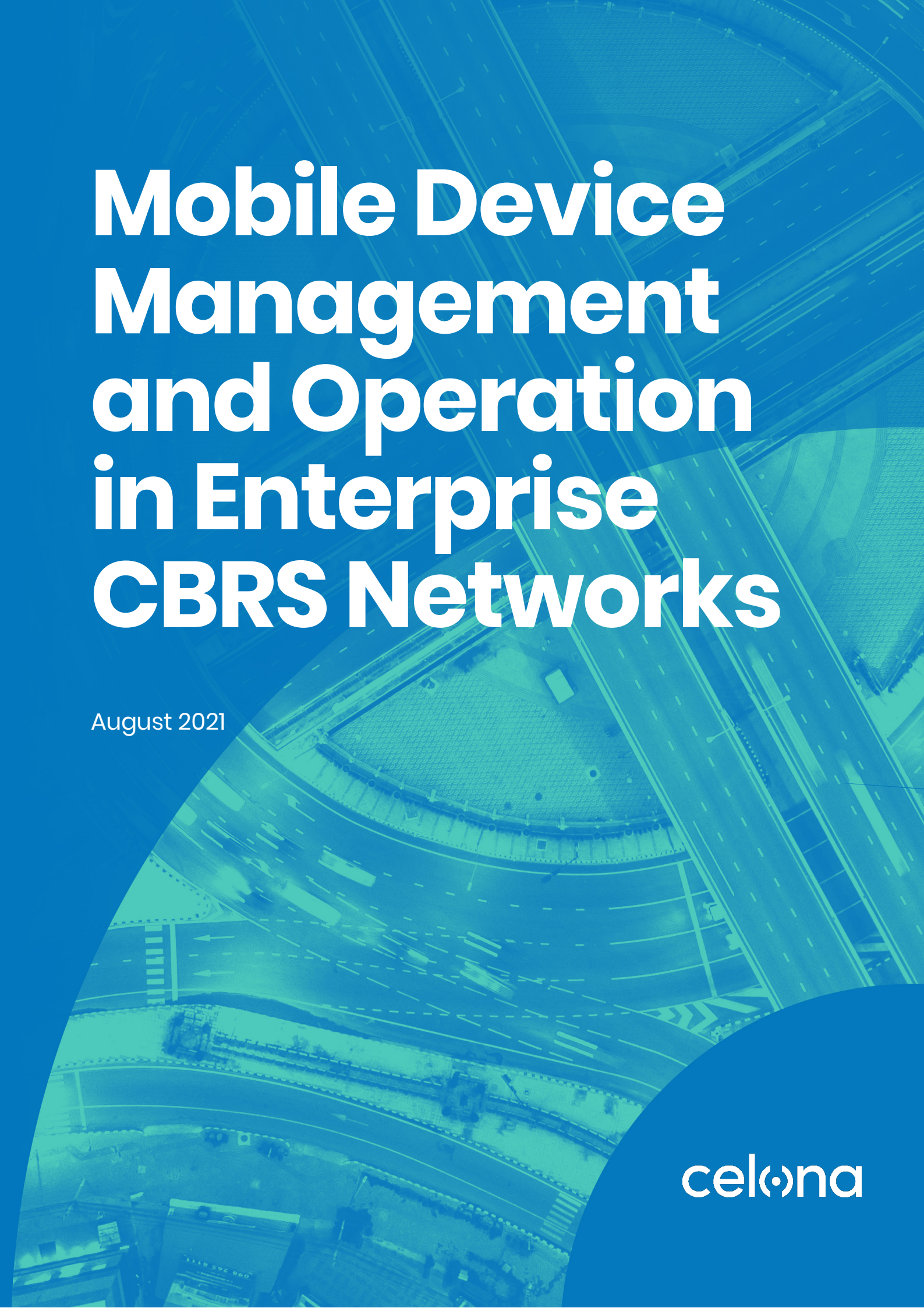
Mobile Device Management and Operation in Enterprise CBRS Networks

August 2021



celona

Contents

Overview

The emergence and innovation of private mobile network technology represents a major opportunity for enterprises to deliver new levels of deterministic wireless service that until now hasn't been feasible.

These private mobile networks are typically deployed, operated, and managed by enterprise IT or in-house network staff. To ensure seamless continuity with existing IT infrastructure, the installation and administration of these new private mobile networks should mimic the deployment ease of Wi-Fi while retaining the functionality and operations of a cellular 3GPP network.

These networks can be used for enterprise only connectivity (i.e., Private networks), for mobile network operator (MNO) only connectivity, such as a neutral host deployment, or can be used for both enterprise and MNO connectivity.

As a result, understanding the intricacies and nuances of mobile device management (MDM) and MDM operation on emerging Citizen's Brand Radio Service (CBRS) over LTE and 5G cellular networks is essential to the successful deployment of enterprise private mobile networks.

The subscriptions and access to the network is regulated by the enterprise IT. The mobile devices operating on the private enterprise network are typically identified, configured, and issued to users.

As with any cellular 3GPP networks, specific identifiers are needed for the mobile device (a.k.a user equipment or UE) to find and associate with the enterprise network. MNOs typically have countrywide footprints and obtain their unique identifiers. Because enterprise deployments are typical in nature, common identifiers are used with the address spaces for the identifiers are shared among different entities.

This paper focuses on enterprise managed devices including their procurement, provisioning, deployment, and operation within CBRS-based private LTE networks.

Device Management

Enabling enterprise campus connectivity requires IT to plan the devices to support and to manage their access and security postures. The choice(s) will dictate the extent of control that enterprise IT has over the devices as well as the costs incurred for supporting the device population.

Independent of the terminology and related acronyms, device management is best approached by addressing the following aspects in developing a clear and concise program for the organization.

TOPIC	ASPECTS TO ADDRESS
Device Management	• Who manages the device and to what extent? • Who is responsible for support? • What, if any, MNO connectivity service is required on the device? Who pays for the service?
The Device	• Who identifies the devices supporting the enterprise? • Who pays for the device? • Who procures the device? • Who provisions the device? • Is support both enterprise and MNO credentials required?
Enterprise Applications	• What enterprise applications must be supported? • How closely do these apps need to integrate with daily workflow?

It's important to note that some form of device protection is needed, and integration of enterprise mobility management (EMM) and mobile device management (MDM) is required.

Locked and unlocked devices

A SIM lock, network lock, carrier lock or subsidy lock is a technical restriction built into mobile phones. These are used by service providers to restrict the use of phones to specific countries and/or networks.

Phones can be locked to accept only SIM cards with certain International Mobile Subscriber Identities (IMSIs); that may be restricted by a:

- **Country based lock**: Mobile country code (MCC;) For example a UE that will only work with a SIM issued in one country.
- **Network based lock**: Mobile network code (MNC). This is the typically employed by the MNOs
- **Pairing UE and SIM lock**: Mobile subscriber identification number (MSIN), This means only one SIM can be used with the phone.
- **MVNO based lock:** Some phones are locked by group IDs (GIDs), that restrict them to a single MVNO of a certain operator. But this is not a common feature employed in the market.

MNO-locked phones do allow for freely adding or replacing with other credentials like enterprise SIM profiles. But enterprise roaming for such devices will be restricted to MNO deployed networks or independently deployed enterprise networks that also support neutral host network (NHN) interworking with that MNO. The roaming is enabled using a single SIM credential provided by the MNO.

Phones that are not locked are called SIM-free or unlocked and do not impose any SIM restrictions. Unlocked devices provide a lot of flexibility because they allow for one or more enterprise credentials to be added to the device. Roaming with the enterprise network with such devices is supported with dual-SIM profiles one for MNO and other for enterprise network(s).

Most UE, when purchased with the operator subsidy, come in a locked state to avoid the user switching over to another MNO.

This allows for recouping the costs for the subsidy provided. Based on the MNO, just completing the required payoff amount for the device will implicitly unlock the device. For other MNOs, the user must call customer service and request the device be unlocked after paying for it.

If the device needs to support enterprise credentials, it needs to be in an unlocked state even if the MNO credential is supported in the device.

COBO, COPE, CYOD

This section details the device types based on the procurement, management, and operational model. Enterprise IT makes a determination on the preferred choice based on their business model and employee engagement aspects involved. It is possible that a given enterprise to use different types based on the user groups within the enterprise that needs to be managed.

TOPIC	COBO	COPE	CYOD
Expansion	Company Owned business only	Corporate-owned, personally enabled	Choose your own device
Devices provided by:	Enterprise	Enterprise	Enterprise provides a set of pre-approved mobile devices; Some flexibility for user to choose amongst approved devices

TOPIC	COBO	COPE	CYOD
Device management	Company-owned, business-only type of device environment, the devices are procured by the company, provisioned, secured, and monitored at all times.	Enterprises have the most control on these devices. Given the devices are owned by the enterprise, they can be regulated for specific types of access and even lock down the devices as needed	Configured with security protocols and business applications before assigning device to employee.
Device maintenance	Owned, maintained, and managed by the enterprise	Owned, maintained, and managed by the enterprise	Enterprise policy dependent – can be shared responsibility between enterprise and employee
Security policy	Devices are pre-configured to maintain device and data security	Devices are pre-configured to maintain device and data security	Managed by enterprise. With restricted set of devices, the security feature is installed prior to assigning to user
Costs	Wholly managed by the enterprise	Wholly managed by the enterprise	Partly managed by the enterprise and the employee
Comfort of device use	These devices are strictly business only- preventing employees from accessing any apps for entertainment or personal use. These devices are locked down to a kiosk mode- single or multi-app depending on the use case. The COBO environment allows the employees to keep their work devices separate from their personal devices and the companies can enforce any policies, make changes and track the performance of the device in real-time.	Restrictive given that the enterprise assigns device of their choice to each employee; Employees still provided the option to customize their device and potentially use it for non-work-related functions. Employees can use the devices as required for personal use while being in a secure framework giving the employees the complete liberty without putting the corporate data and device in jeopardy while also providing enterprises the ultimate control over the devices.	The enterprises publish a list of devices that are approved for the business work and meet the criteria for the management of the same. Can be restrictive based on the device choices made available by the enterprise. CYOD is most commonly used for knowledge workers. Allows for employees to leverage the latest tech for work, but however not necessarily be cost-effective. Device leasing is hence gaining momentum on the enterprise level, making the tech upgrade easy and affordable.

Enterprises need to make the appropriate choices weighing in the trade offs involved. Trade-offs between enterprise security needs and incurred costs with the employee satisfaction, flexibility of device control and productivity should be considered. Some compromises may need to be made based on the employees and the enterprise types involved.

The rest of this white paper describes provisioning, deployment, and operation with the CBRS enterprise private LTE networks for all the three device types: COBO, COPE and CYOD.

SIM Provisioning Methodology

Credentials can be defined as SIM or eSIM that are provisioned in the UE. SIM and eSIM require specific formatting and need to be prepared as independent profiles even if they contain the same information. The credential itself can be put into a physical SIM (removable) or embedded SIM (non-removable). Each of the physical SIM and embedded SIM modules can support one or more credentials. The physical-SIM can be UICC (4G versions as opposed to the 2G/3G SIM). The GSMA specification enhanced the physical SIM to support multiple credentials – referred to as eUICC (embedded UICC). The eUICC terminology can be applied to a physical SIM or embedded SIM.

With the GSMA specification, to support dual SIM operation, one of the SIM credentials has to be in the physical-SIM slot and the other an embedded-SIM. Essentially, both credentials cannot come from physical SIM or embedded SIM. However, each of the physical or embedded SIMs can host multiple credentials with at most one credential active at a time.

From a UE device capability perspective, additional credentials can be added to the embedded SIM. The physical SIM cannot be updated to add newer credentials. The UE can support switching across credentials already provisioned within the physical SIM. Given that a UE needs to potentially support multiple enterprise credentials on the device and also support adding them dynamically, hosting the enterprise credentials as embedded SIM seems most suitable for devices like handheld mobile devices. If static provisioning is sufficient, physical SIMs with enterprise credentials can be supported such as security cameras deployed on campus.

The preferred configuration is to support MNO credentials as physical SIM and CBRS credentials will be as embedded SIM so that one or more enterprise credentials can be provisioned in the UE. This will keep the certification for MNO operation independent from the CBRS credentials being added to the UE dynamically. Figure one, below, describes two methods for dynamic provisioning of credentials on to the UE: the consumer model and the IoT model as per GSMA definitions.

The consumer model supports two methods. The first is for the UE to scan a Quick Response (QR) code containing the specific eSIM credential, which pulls the eSIM profile to the device. The second method generically sends the UE to a specific SIM provisioning platform that then pushes the requisite credential to the device. In the MDM model the device is provided the SM-DP (subscription manager data preparation) server address to reach.

The eSIM credential to be assigned to the UE is paired in the SM-DP+ with the EID (electronic identification) of the device. When the UE access the server, this credential is pushed to the device. The IoT model is typically intended for headless devices. The device reaches a predefined SM-SR (subscription manager secure routing) server where it can be authenticated. The SIM provisioning platform then pushes a credential pre-assigned to the device when it accesses the server.

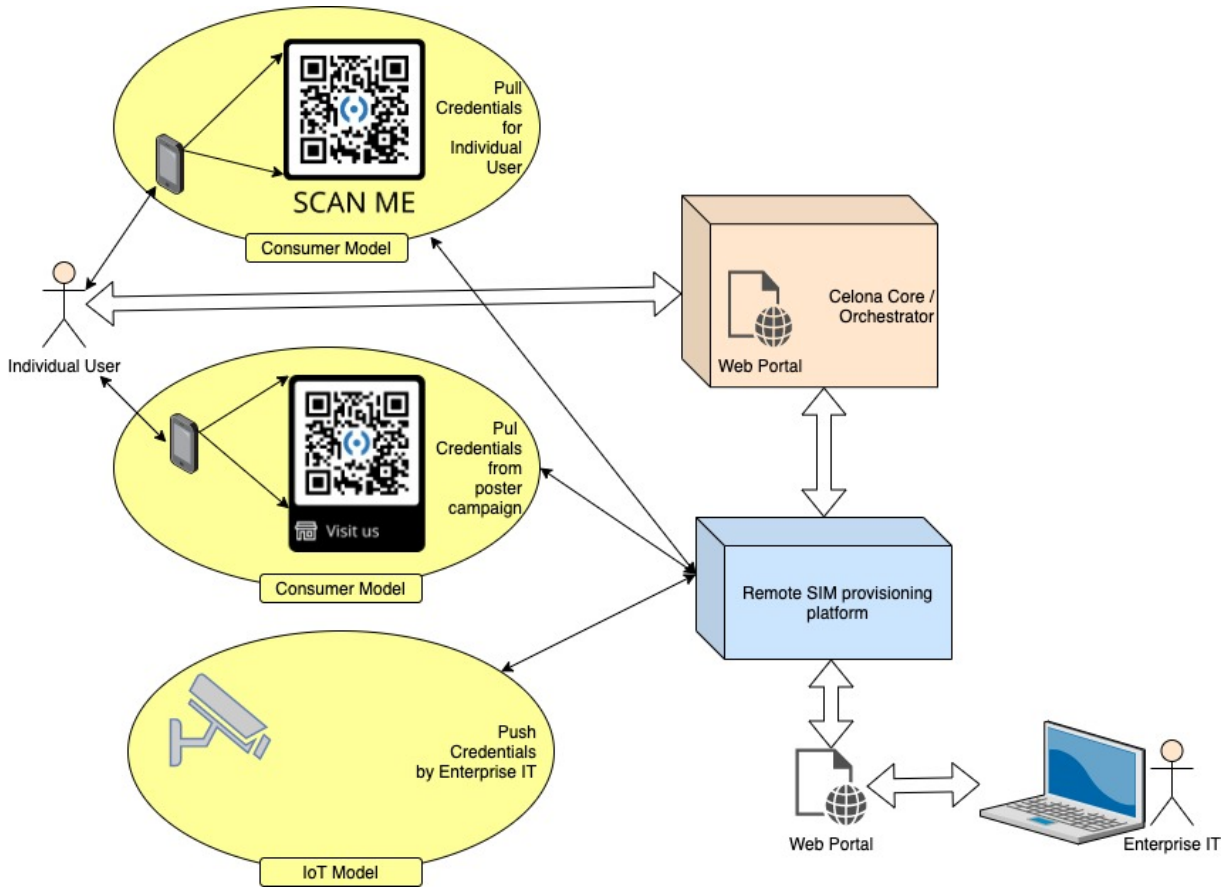


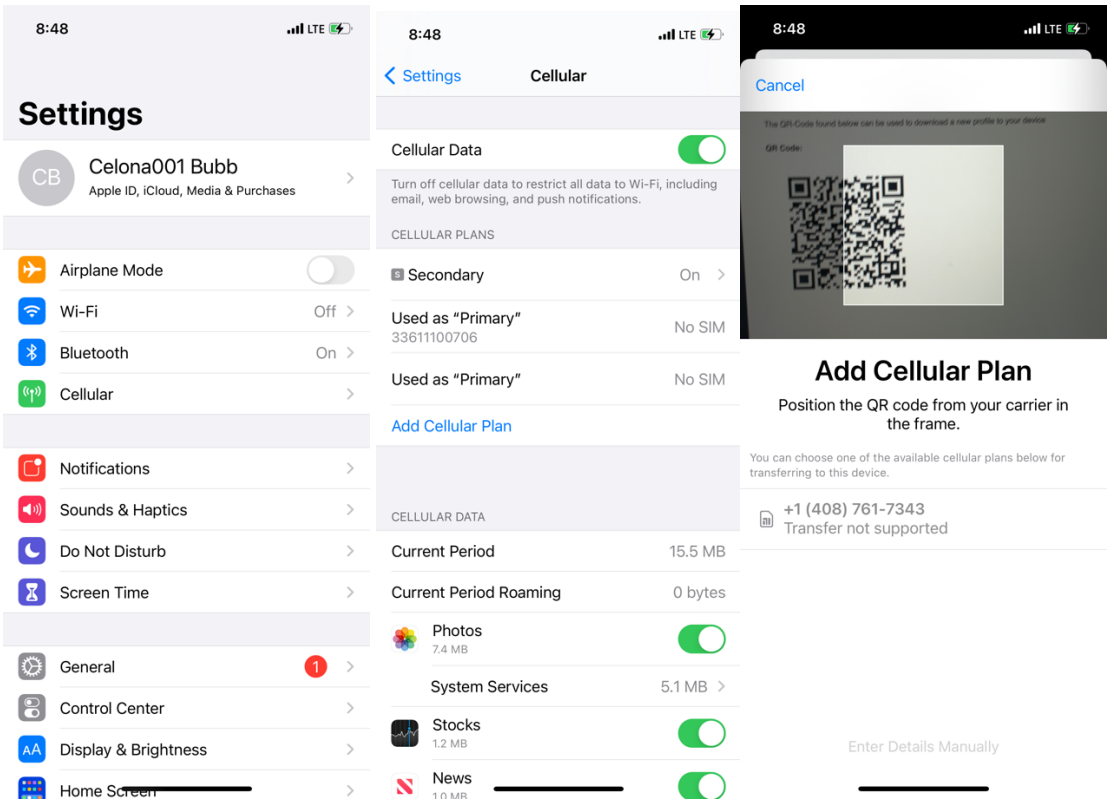
Figure 1 : SIM Provisioning Methodologies

Procedures for installing eSIM credentials on to a mobile device are provided below when using Google Pixel and iPhone. Make sure there is a data connection, either Wi-Fi or cellular, on your mobile phone and go through steps below for provisioning the eSIM on to the mobile device.

On iPhone SE and 11+ later models

- Go to "Settings → Cellular → Add Cellular Plan"
- Follow onscreen instructions to download the eSIM profile using QR Code.
- If prompted to select a default line, choose your new Celona service for data only.
- Wait for the installation process to complete.
- Once you see "Your Cellular Plan Added", begin using your new Celona service.

The images below are screen captures and illustrate the steps involved in provisioning an eSIM on an iPhone.



On Google Pixel 4 and later models

- Go to "Settings → Network & Internet → Mobile Network +"
- Select "Download your SIM instead".
- Follow onscreen instructions to download the eSIM profile using QR Code.
- If prompted to select a default line, choose your new Celona service for data only.
- Wait for the installation process to complete.
- Once you see "Your Number Is Added", begin using your new Celona service.

SIM Provisioning Workflow

Enterprise IT often orders the UEs through established retail channels. Once the devices are received, the appropriate credentials are assigned to the individual devices. The subscriptions will include enterprise private LTE credentials, enterprise Wi-Fi credentials, and, if required, MNO credentials. Enterprise Wi-Fi credentials are handled per the current procedures using device provisioning tools. When the device is only required to support enterprise LTE credentials, this may be supported as a physical SIM or embedded SIM.

Private LTE credentials are provided by the enterprise private LTE deployment vendor. The private enterprise deployment vendor works with a SIM provisioning platform to prepare the physical SIM and embedded SIMs. The physical SIMs are requested by enterprise IT, shipped to the required site(s) and prepared specifically for UE associating with the deployed private LTE network.

For embedded SIMs, enterprise IT requests a batch of eSIM credentials and for the activation codes to be made available for download. Enterprise IT then provides the activation codes or QR codes for them. These codes can be scanned using the UE camera, which triggers the installing the eSIM credential on to the device. A numbered set of steps involved in eSIM provisioning the UEs are illustrated in Figure two below:

Single SIM and Dual SIM UE Configuration

This section details the UE behaviors using a single enterprise credential and dual SIM credential with enterprise and MNO credentials. These credentials can be stored in a physical SIM card and shipped to the enterprise IT or supported embedded SIM profiles that can be provisioned over-the-air on the device. The devices associate and operate only on the CBRS Enterprise network or both the CBRS Enterprise network and MNO network. Based on the application, the device connects to the CBRS enterprise network or MNO network to service the user.

Single SIM UE configurations

The device is provisioned with the CBRS Enterprise credentials. The operation of the UE is same as what is supported for MNO network. When the UE is within the RF footprint of the enterprise campus, it will find and camp on the network. When it is not in the footprint of the enterprise campus, it will continue to run periodic out-of-service scans. UEs have built in battery power optimizations, including using motion sensing techniques, to avoid scans when not needed.

Dual SIM UE configurations

With dual SIM, the following UE configurations are possible:

- Passive / Dual SIM Single Standby (DSSS): The UE operates with a single transmit (TX) and receive (RX) chain. The UE can be associated with only one network at a time with one credential active while the other remains passive. Switching between the networks / SIM profiles is managed locally in the UE and can be based on functions like geofencing.
- Dual SIM Dual Standby (DSDS) config 1: The UE operates with a single TX and RX chain. When in RRC (radio resource control) connected mode on one of the networks, the UE employs tune-aways in an opportunistic fashion, understanding that the UE will not be scheduled traffic in those slots for the purpose of monitoring the paging channel on the other network.
- Dual SIM Dual Standby (DSDS) config 2: The UE operates with a single TX chain and dual RX chains. When in RRC connected mode on one of the networks, the UE monitors the paging channel on the other network by using the second RX chain to avoid any breaks in connected mode operation on the first network.

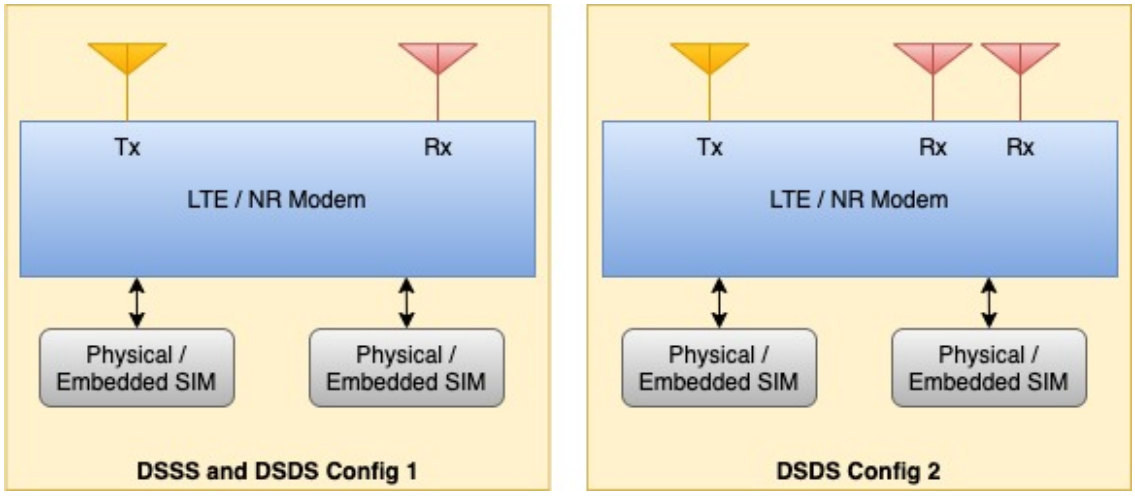


Figure 2 : UE configuration with DSSS and DSDS

The dual SIM Dual Standby (DSDS) UE configuration is the most commonly supported option in the market.

UE Roaming Behaviors

This section details the mechanisms employed in the UE to transition across the MNO and enterprise networks. The transitions are focused on idle mode given that the connected mode transitions will require tighter integration between MNO and enterprise networks. Figure 3 below shows the high-level functions for UE and network sequence of steps involved in UE entering and leaving an enterprise network.

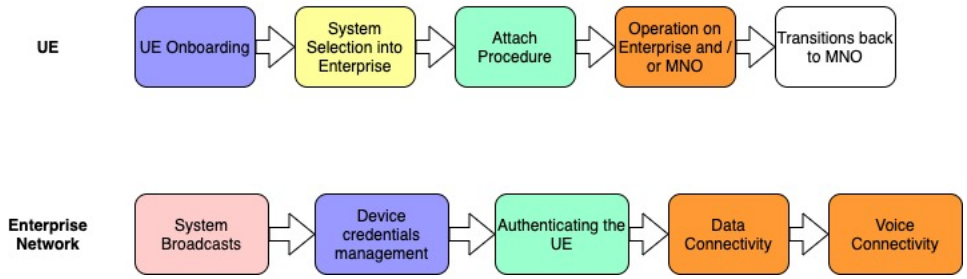


Figure 3 : UE and network sequence of activities for enterprise system operation

UE entering the enterprise network

Using a single SIM credential

Cell Selection: Inter- and Intra-frequency idle mode camping can be supported through system broadcast message from the enterprise access points. This will allow for the UE to find the enterprise systems.

Enterprise networks are typically deployed in very small pockets. As a result. the parameters for the system information blocks (SIBs) that carry broadcast information about the expected AP behaviour must be tuned to avoid power hungry scans. Out-of-service based scanning of the enterprise system can be realized with sufficient backoff when even the enterprise system is not detected.

User initiated manual scans: A manual scan of available systems is requested by the user and the user selects an enterprise system from the list of PLMNs (Private Land Mobile Networks) presented to the user. This scan will be done for all available networks and systems that the UE radio can support.

With dual SIM credential

The UE contains both the enterprise and MNO credentials. The UE has policies that specify when to look for the enterprise network. This is based on periodic scans or by employing other techniques such as radio and geographic signatures to initiate scans. UE offloads the data traffic on to the enterprise network while retaining the voice service on the MNO network. When the MNO footprint is no longer available, the UE uses Wi-Fi calling (WFC) methods to connect to the MNO core network via an IPsec tunnel established over the data connectivity on the enterprise network.

UE leaving the enterprise network

UE transitioning out of the enterprise network is typically handled through idle mobility when the leaving campus coverage. When the UE is in connected mode on the enterprise network, or when dual SIMs are supported, the UE loses the radio connection and transitions the connectivity on to the MNO network. Otherwise, with a single enterprise SIM credential, the UE loses service when not in the RF coverage area of the campus network. With dual SIM, it is typically only data connectivity that is required to be transitioned to the MNO network.

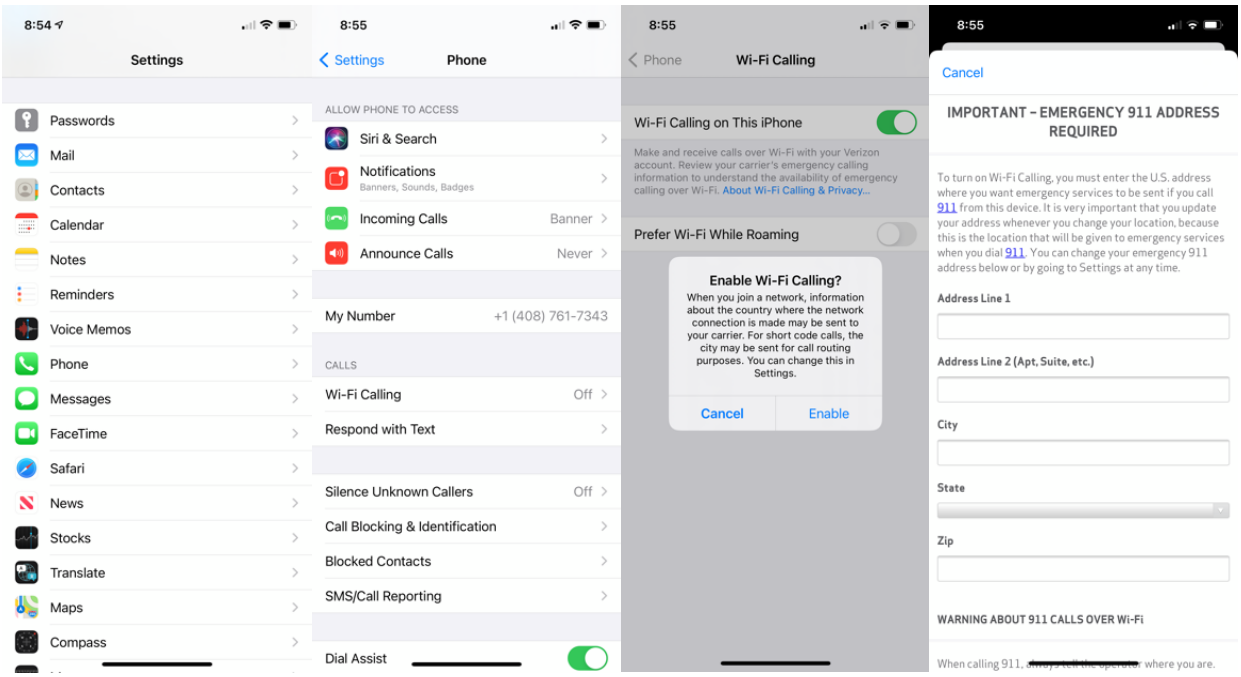
Such transitions will be a break-before-make transitions for packet data connectivity. For instance, with a voice call, when entering the enterprise campus, it is sufficient to continue the service on the MNO network as there typically MNO coverage available even if it may be in weak coverage. It is possible that there is no MNO footprint, and the voice call is supported as “LTE calling”. When leaving the campus network, the Wi-Fi voice call is transitioned to the MNO network assuming there is coverage as the user is leaving the campus.

Enabling LTE calling

Wi-Fi Calling (WFC) is the industry term for enabling VoIP calling with VoLTE procedures with an VPN tunnel established over the internet. The internet connectivity is based on the Internet packet data networks, on an Enterprise LTE network or on Wi-Fi.

Using iPhone as an example, follow the steps below to enable Wi-Fi calling. The images are screen captures to illustrate the steps involved.

- On your iPhone, go to Settings > Phone > Wi-Fi Calling.
- Turn on Add Wi-Fi Calling for Other Devices.
- Go back to the previous screen, then tap Calls on Other Devices.
- Turn on Allow Calls on Other Devices if it's not on.
- Turn on each device that you want to use with Wi-Fi Calling.
- Provide the address for emergency calling



Services Supported on Enterprise Campus Networks

As the UE transitions across the MNO and enterprise Networks, it offloads specific services on the enterprise Network while still being associated with the MNO networks for other services. The transition points for the different services may occur at independent points based on the relative prioritization and the RF footprint of the two networks.

Figure 4 provides a high-level view of the transitions across MNO and enterprise networks and the different available options for data and voice traffic offload.

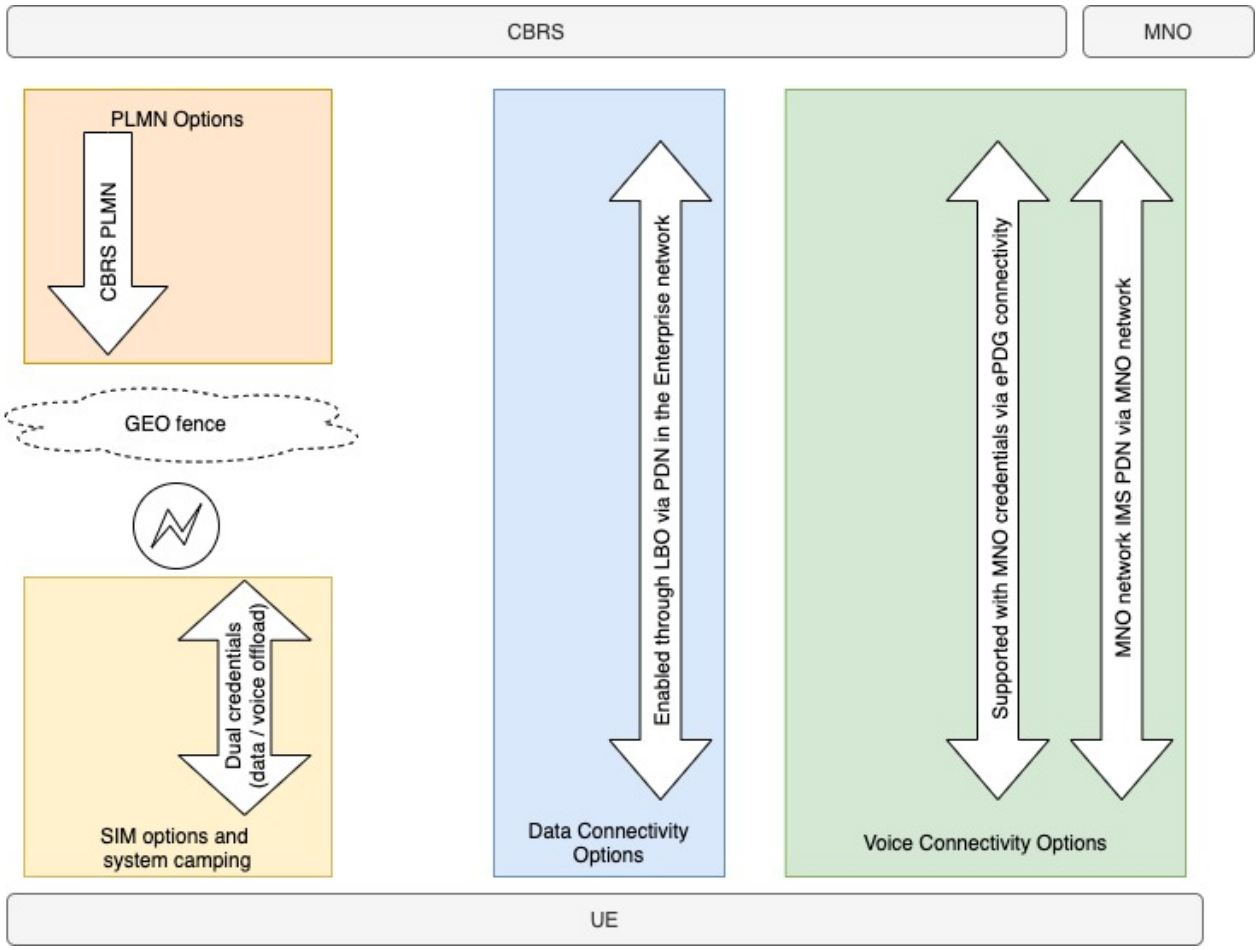


Figure 4: UE transitions into CBRS Enterprise Network

IMS service support on enterprise campus network

From a UE perspective, there are a few viable architectures. Two these are illustrated below. IMS (IP Multimedia System) PDN, based on the operator, is treated as the default PDN. Even for the default PDN, the APN for the IMS PDN is independently set by each MNO.

The GMSA recommendation from IR.92 is used for VoLTE, IR.94 for video telephone and IR.51 for IMS services support over untrusted networks like Wi-Fi/LTE-Internet-PDN and is adopted by all MNOs.

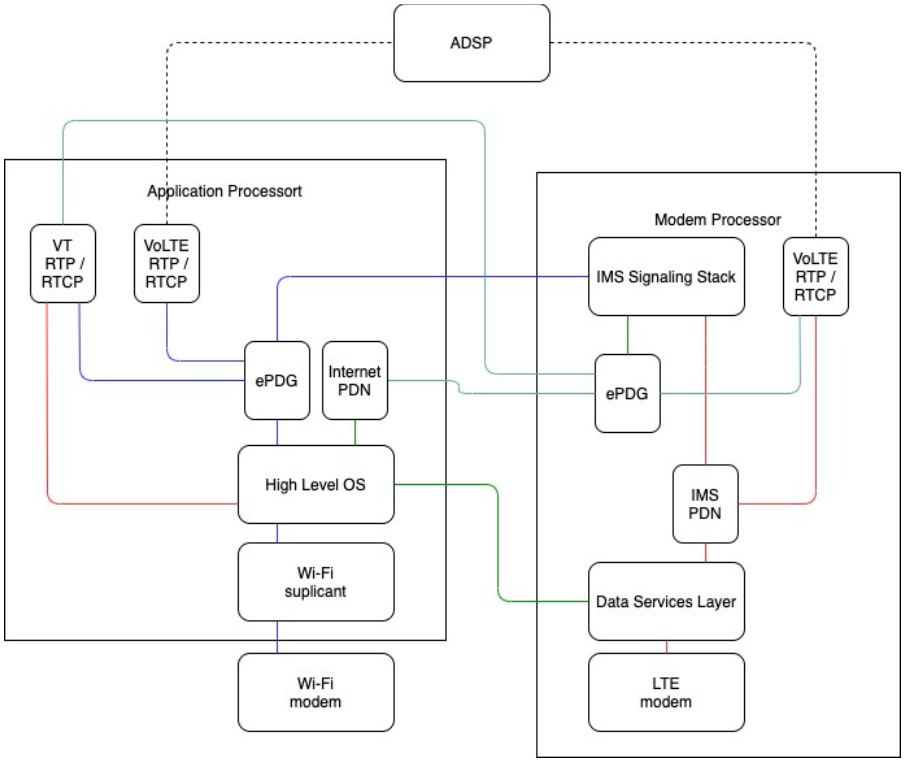


Figure 5: IMS stack running on the modem processor

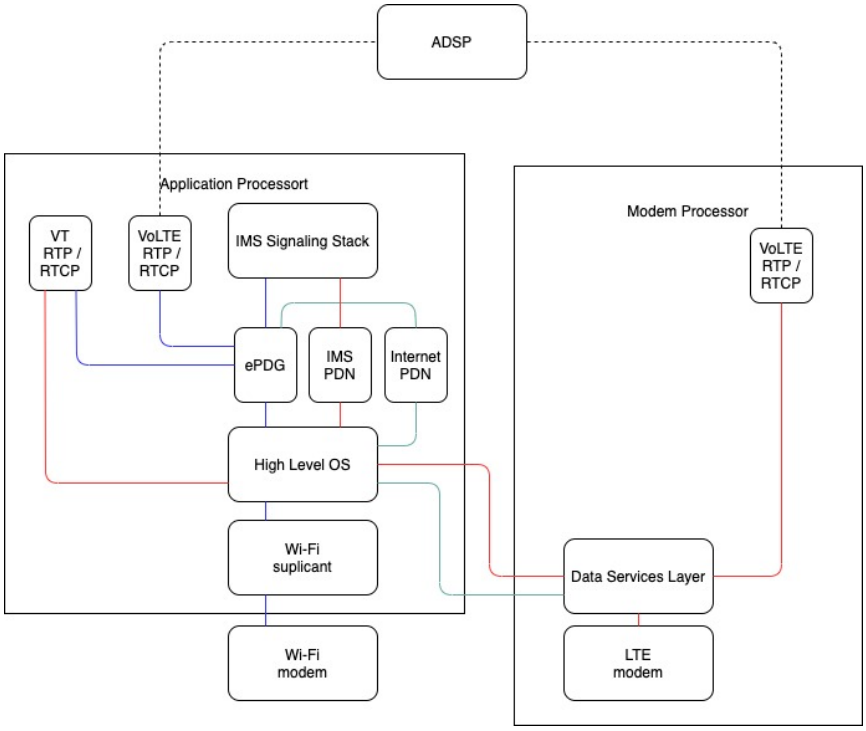


Figure 6: IMS stack running on the application processor

Emergency calling

Emergency calls are supported as VoLTE calls. The key added requirement is location support of the UE. The enterprise deployed eNBs (eNodeBs or cellular access points) for private LTE network deployments do not support emergency calling and the system broadcasts are relegated to the UE. The UE relies on the MNO networks to support emergency calling.

When the UE has only the enterprise credentials, the emergency calling can still be performed on any available MNO network in "limited-service" mode given that the device will not have authenticated identity on the MNO network. The emergency call back mode will not be supported for such emergency calls.

When the UE have both enterprise credentials and MNO credentials, the MNO credentials are used to support emergency calling on the MNO networks.

Other MNO services

This is applicable only when the device has MNO credentials provisioned. There are specific services that currently are supported over the MNO that do transition directly to the enterprise system. The MNO networks have SLAs with content providers and specific services enabled through them with third parties. One possible approach is to obtain similar agreements for the enterprise network and support the service over the RAN or the core of the enterprise network. The more immediate approach will be to have the UE transition to the MNO to support these services. This needs to be a UE-based function to transition when such services are enabled by the user.

A good example of such a service is eMBMS or broadcast and multicast service. The information carried on this channel is based on operator agreements with the content providers and will be carried on the MNO frequencies. When the user enables the application to monitor the service, the UE transitions to the MNO frequency to receive this service. Given that the enterprise network does not broadcast information associated with the eMBMS on the MNO frequencies, when the user activates the application, the UE needs to transition to the MNO frequencies to check if the MNO coverage is available and if the service is active on the channel. When there is no MNO coverage or the service is not active, the UE transition back to the enterprise network as part of the regular procedures of finding the campus network.