GSMA

Exploring Private 5G Networks Through the Lens of MNOs

Whitepaper

November 2025

GSMA

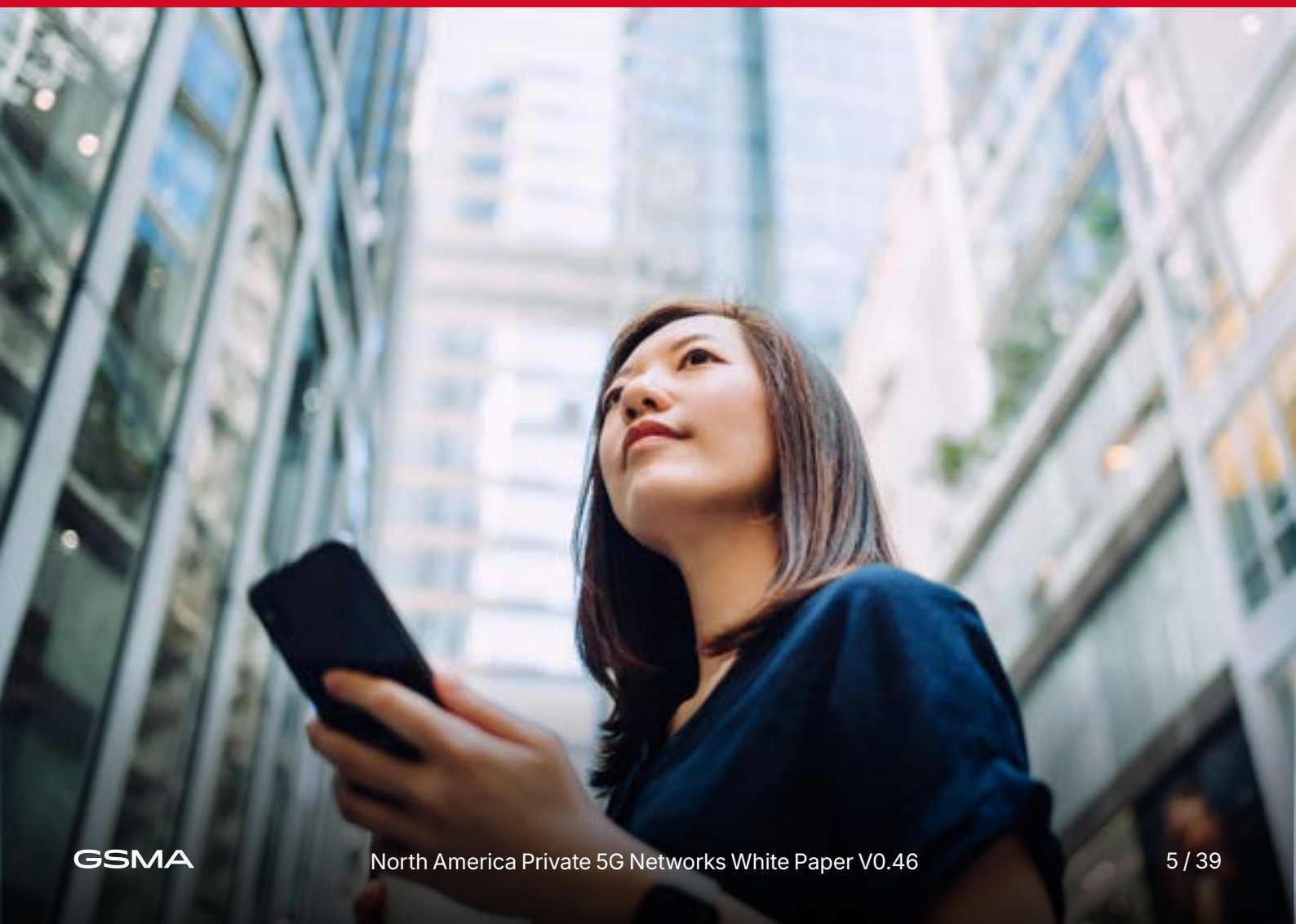
The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive. Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at gsma.com

Contents

Contents (continued)

1. Introduction



1.1 Overview

Cellular mobile connectivity has become the technology of choice for their wide area mobility coverage, standardized eco-system for interoperability and the established operational service assurance & control framework. Cellular Private networks are gaining traction with the ease of cellular spectrum availability for enterprise use and the evolution of cellular infrastructure to support flexible, modular deployment options with 4G and cloud native 5G architecture. As stated in [1], the global private 5G network market was 1.38 billion USD in 2021 and is forecasted to expand at a compound annual growth rate (CAGR) of 49.0% 2022-2030.

A Private network provides connectivity services and optionally other services (e.g. device location) for a private entity such as an enterprise which may designate the authorized users. Private networks may be provided using physically isolated network elements or virtual elements on shared infrastructure. They can be standalone networks that do not rely on the public network infrastructure and hence may be deployed without the participation of a mobile network operator. Alternatively, they can be fully or partially integrated with public networks, and the service is provided by mobile network operators or their partners.

1.2 Scope

The scope of this whitepaper is to provide a comprehensive view of the private network use cases from the point of view of public mobile network ecosystem stakeholders. This whitepaper will cover the overview along with the reference to the work from other industry partners, discuss private network use cases with focus on interaction with public mobile networks, discuss aspects of 3GPP standardization to realise these use cases and identify gaps if any. Additionally, this will help in potentially creating a PRD in collaboration with global GSMA working groups.

1.3 Acronyms

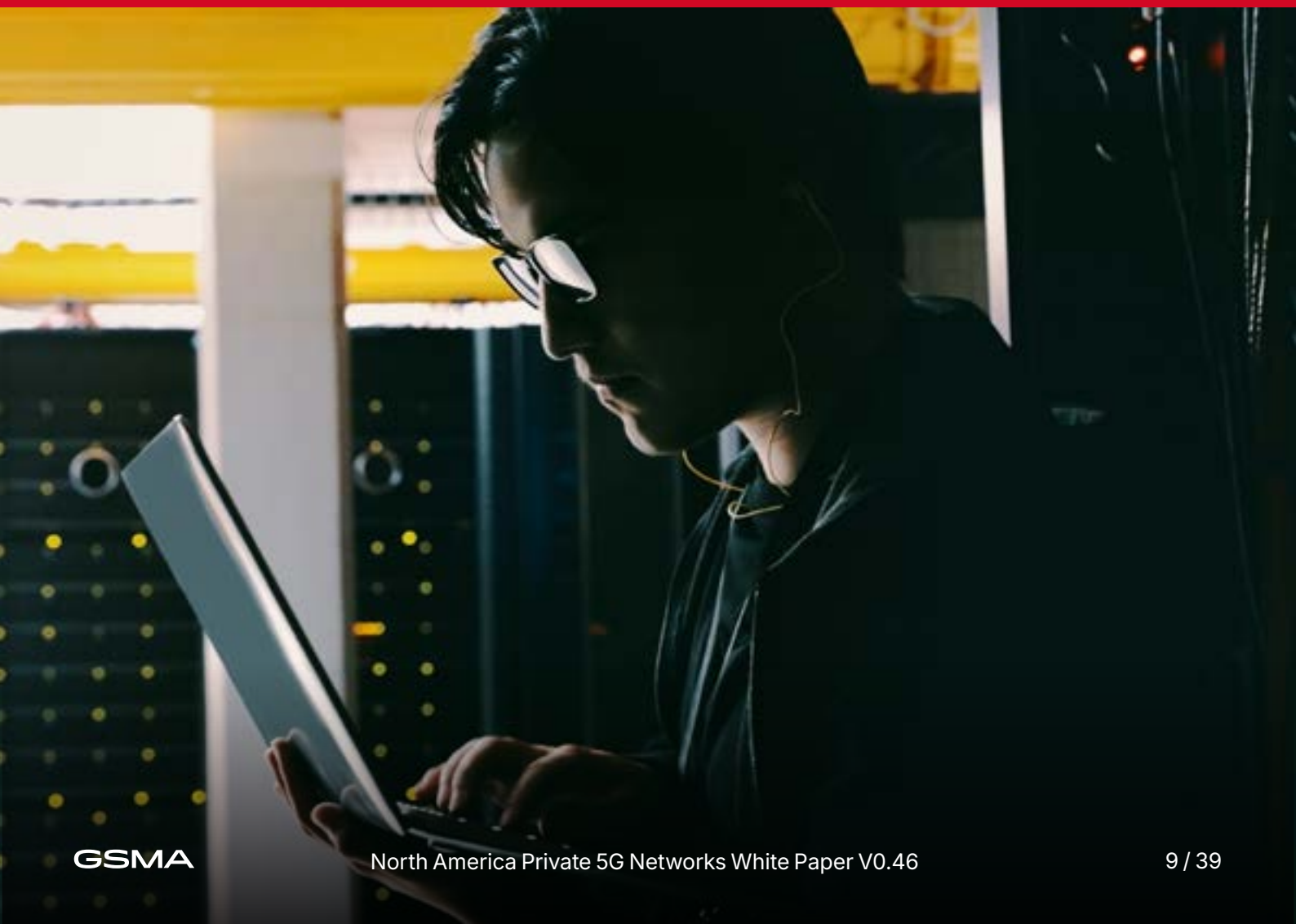
Acronym	Description	Acronym	Description
3GPP	3rd Generation Partnership Project	**NB-IoT**	Narrow Band IoT
5GC	5G Core	**NID**	Network Identifier
5GS	5G System	**NG-RAN**	Next Generation Radio Access Network
5QI	5GS QoS Identifier	**NPN**	Non-Public Network
AF	Application Function	**NR**	New Radio
CAG	Closed Access Group	**NR-U**	NR Unlicensed
CBRS	Citizens Broadband Radio Service	**PLMN**	Public Land Mobile Network
CIoT	Cellular IoT	**PNI-NPN**	Public Network Integrated NPN
CSG	Closed Subscriber Group	**PSP**	Participating Service Provider
DN	Data Network	**QoS**	Quality of Service
DNN	Data Network Name	**RAT**	Radio Access Technology
DRX	Discontinuous Reception	**RF**	Radio Frequency
DSS	Dynamic Spectrum Sharing	**RRC**	Radio Resource Control
EPC	Evolved Packet Core	**SAS**	Spectrum Sharing System
GBR	Guaranteed Bit Rate	**SD**	Slice Differentiator
IoT	Internet of Things	**SNPN**	Standalone NPN
LAA	License Assisted Access	**SSID**	Service Set Identifier
LADN	Local Area Data Network	**SST**	Slice Service Type
LTE	Long Term Evolution	**SUPI**	Subscriber Permanent Identifier
MCC	Mobile Country Code	**TSN**	Time Sensitive Networking
MICO	Mobile Initiated Connection Only	**UE**	User Equipment
MNO	Mobile Network Operator	**URLLC**	Ultra Reliable Low Latency Communication
MOCN	Multi Operator Core Network	**V2X**	Vehicle to Everything
N3IWF	Non-3GPP Inter-Working Function		
NAS	Non-Access Stratum		

1.4 Terminology

The following table clarifies the terminology related to private network as applied in this whitepaper.

Term	Description
Interconnection	Interconnection is the physical linking of a carrier's network with equipment or facilities not belonging to that network. The term may refer to a connection between a carrier's facilities and the equipment belonging to its customer, or to a connection between two or more carriers. [1] IP interconnectivity is the physical linking of an operator's IP network with the IP equipment or facilities that belong to another operator's network. It will allow customers to make an IP call, enabling all the features of enriched calling, to another subscriber on another IP network. It is the linking of two or more operators' networks, either domestically within a country or internationally, so that the calls remain entirely on IP network infrastructure and do not fall back to older legacy services during call routing. [2]
Interoperability	Interoperability in telecommunications refers to environment where different services can operate and accept services from other systems. Examples of aspects relevant to compatibility of telecommunication systems include signal, network scale, and radio frequencies. Interoperability testing (IOT) benefits mobile network operators, device manufacturers, and service providers, among other ecosystem stakeholders, in the efforts to ensure adequate level of functioning of interoperability. An example of this is the GSMA's Interoperability Test Platform, joint end-to-end test environment, to test interoperable mobile money solutions. [3]
Network sharing	As stated in [4], network sharing may take many forms, ranging from passive sharing of cell sites and masts to sharing of radio access networks (RANs) and other active elements such as network roaming and the core.
non-public network	A network that is intended for non-public use. [5] Note: In this whitepaper, this is also referred to as a Private Network
Private slice	Private network slice (NS) is a dedicated network slice deployment for the sole use by a specific third-party. [5]
Roaming	As stated in [6], international mobile roaming is a service that allows mobile users to continue to use their mobile phone or other mobile device to make and receive voice calls and text messages, browse the internet, and send and receive emails, while visiting another country. National roaming refers to the ability of the subscriber to move from one mobile operator to another within the same country. In scenarios involving private network, roaming can refer to both international and national roaming, and the roaming entities can cover both private and public networks.

2. Quick Survey of Private Networks Landscape



2.1 OnGo Alliance

The OnGo Alliance, formerly known as the CBRS Alliance, is a coalition of over 185 member companies, including mobile operators, cable operators, managed service providers, and enterprises. Its primary mission is to promote the development, commercialization, and adoption of LTE and 5G technologies within the 3.5 GHz Citizens Broadband Radio Service (CBRS) band in the United States. The OnGo Alliance's white paper on 5G private networks outlines the advantages and deployment strategies for leveraging private LTE and 5G networks using the Citizens Broadband Radio Service (CBRS) spectrum.

2.1.1 Types of Private Network

The OnGo Alliance's white paper on private networks outlines several types of private network deployments, each tailored to different enterprise needs and use cases. These deployments leverage the Citizens Broadband Radio Service (CBRS) band, allowing for flexible and cost-effective private LTE and 5G networks. The types of networks discussed in the white paper are Standalone, Hybrid, Neutral host and Managed private networks. Each of these types supports various applications and industries, ranging from industrial IoT and smart manufacturing to educational campuses and healthcare facilities. The white paper highlights the flexibility of CBRS-based solutions to meet diverse connectivity needs while ensuring robust performance, security, and cost efficiency.

2.1.2 Business Model and Deployment

The business model for OnGo private 5G networks centres around providing tailored solutions that meet the specific needs of various enterprises. It emphasizes several key components including monetization opportunities, cost efficiency, scalability, greater control and customization. OnGo Alliance white paper provides a comprehensive guide for deploying private 5G networks, detailing the steps necessary to set up these networks which includes understanding the specific requirements of the organization, the benefits of network slicing, virtualization, and edge computing, which enhance the capabilities and flexibility of 5G networks.

2.1.3 Use Cases and Business Benefits

The white paper discusses various use cases for private 5G networks, such as smart buildings, industrial IoT, healthcare, smart cities and campus networks. It explains how private networks can deliver improved performance, reliability, and control over network resources, which are essential for mission-critical applications. The white paper also provides technical insights into the use of CBRS spectrum for private networks, including the regulatory framework, spectrum access mechanisms, and the role of the OnGo Alliance in promoting and certifying devices and solutions for CBRS deployments.

2.1.4 Regulatory and Spectrum Management

Managing spectrum within the CBRS band involves navigating regulatory requirements and ensuring efficient spectrum use. The white paper indicates that more work is needed to streamline these processes and provide enterprises with the tools to manage spectrum effectively.

2.1.5 Challenges

The OnGo Alliance's white paper on 5G private networks outlines challenges that need to be addressed for broader adoption and effective implementation. Listed here are the key gaps identified.

2.1.5.1 Interoperability and Standardization

While the OnGo Alliance has made strides in defining standards, there remain issues with interoperability among different vendors' equipment and software. This is crucial for seamless integration and operation of private networks across various devices and platforms.

2.1.5.2 Roaming and Mobility

The paper highlights the challenges related to roaming between different CBRS networks. Efficient roaming is critical for devices to maintain connectivity as they move between network boundaries, particularly in large enterprise or industrial environments. The need for advanced geofencing and seamless handoff mechanisms is emphasized to improve user experience and network reliability.

2.1.5.3 Security

Security remains a paramount concern. While the OnGo Alliance has outlined security protocols for private LTE and 5G networks, there is a continuous need to enhance these measures to address evolving threats. Ensuring robust security across all network layers is essential for protecting sensitive enterprise data and operations.

2.1.5.4 Scalability and Deployment Complexity

Deploying private 5G networks involves significant complexity, particularly in terms of planning, setup, and ongoing management. Enterprises need clear guidelines and support to scale these networks efficiently, especially as they integrate more IoT devices and expand their coverage areas.

Addressing these challenges will be crucial for the successful deployment and operation of private 5G networks. The white paper calls for continued collaboration among industry stakeholders to develop solutions that overcome these challenges and unlock the full potential of private 5G networks.

2.2 GSA

The Global Mobile Suppliers Association (GSA) is a leading organization representing the global mobile ecosystem. GSA defines a private mobile network as a 3GPP-based 4G/LTE-5G private mobile network intended for the exclusive use of private entities such as enterprises, industries, or governments, utilizing dedicated spectrum & excludes non-3GPP networks. The Global mobile Suppliers Association (GSA) has been instrumental in the advancement and adoption of 5G technology worldwide. Their contributions are on market intelligence, advocacy, industry collaboration, and technical support which is significantly shaping the 5G landscape.

2.2.1 Market Intelligence and Research

GSA provides comprehensive market reports and detailed databases, such as the GSA Analyser for Mobile Broadband Data (GAMBoD), which offer invaluable insights into 5G network deployments, spectrum allocations, and device ecosystems globally. These resources help stakeholders understand market trends, technology adoption rates, and the competitive landscape, facilitating informed decision-making and strategic planning.

2.2.2 Advocacy and Spectrum Policy

GSA actively advocates for the efficient allocation and management of spectrum, a critical resource for 5G networks. By engaging with regulatory bodies and policymakers, GSA ensures that sufficient and appropriate frequency bands are made available for 5G, promoting a favorable regulatory environment that supports network deployment and innovation.

2.2.3 Industry Collaboration

The association encourages collaboration among mobile network operators, equipment manufacturers, and various stakeholders. Through initiatives such as the O-RAN Alliance and the Telecom Infra Project (TIP), the GSA advocates for the creation and adoption of open standards and interoperable solutions, thereby advancing a robust and diverse 5G ecosystem.

2.2.4 Deployment Guidance and Use Cases

GSA provides practical guidance on the deployment of 5G networks, showcasing successful implementations through case studies. This guidance includes insights into network architectures, deployment strategies, spectrum utilization, and case studies from various industries. The GSA's resources are designed to help network operators, equipment manufacturers, and other stakeholders navigate the complexities of deploying 5G networks.

2.2.5 Challenges

GSA identifies several key challenges in deploying private 5G networks, including spectrum allocation, high costs, technical complexities, ecosystem maturity, skills shortages, and defining use cases. Overcoming these challenges requires careful planning, investment, and collaboration with experienced partners. The GSA continues to provide valuable guidance and support to help stakeholders navigate these issues and successfully deploy private 5G networks.

2.2.5.1 Spectrum Allocation and Licensing

Obtaining spectrum for private 5G networks can be challenging due to limited availability and high costs. While some regions are allocating dedicated spectrum for private networks, the process can be complex and time-consuming. Also, navigating the regulatory process for spectrum allocation varies by country, and ensuring compliance with local regulations can be a significant barrier for enterprises.

2.2.5.2 Cost and Financial Considerations

The deployment of private 5G networks requires substantial capital expenditure for infrastructure. Ongoing operational expenses, such as network management, maintenance, and updates, can be considerable, particularly for enterprises without existing telecom expertise.

2.2.5.3 Skills and Expertise

Many enterprises lack the necessary in-house expertise to design, deploy, and manage a private 5G network. Ensuring that staff are trained and knowledgeable about 5G technologies and network management is crucial for long-term success and can be a significant challenge.

2.2.5.4 Use Case Identification and ROI

Identifying and validating use cases that justify the investment in private 5G can be challenging. Enterprises need to clearly understand how 5G can improve their operations and provide a return on investment. Quantifying the benefits and ROI of private 5G networks can be complex, particularly for applications where the advantages may not be immediately apparent or are difficult to measure.

2.3 GSMA Digital Industries

The document uses examples from different industrial sectors to illustrate different deployment needs based on local regulatory rules and business requirements. It also discusses the benefits of using 5G networks as a unifying technology which can meet many Industry4.0 wireless networking needs, including wide coverage and interoperability with legacy devices and networks. The GSMA digital industries group has changed their name in early 2024 and now it is called Connected Manufacturing Production.

2.3.1 General idea

GSMA Digital Industries community forum published a 5G Industrial Private Network [38] whitepaper in June 2023. The Whitepaper aims to reflect the industry view from Mobile (MNO) and Operational Technology (OT) operators views of different types of Private networks deployment, possible business models, requirements and use cases in a nutshell. The document also points to the 5G-ACIA Non-Public Networks reference architecture as well for Stand-alone Private networks and a variation of Non-public networks with local data processing. The enterprise operators' use cases vary and in various situations Standalone Non-Public Networks (SNPN), Public network integrated Non-Public Network (PNI-NPN) and Neutral Host Networks (NHN) are used and their usages and 5G major component locations are mapped.

2.3.2 Types of Private Networks

3GPP generally defines two types of Non-Public Networks. SNPN and PNI-NPN. However, the industrial and other enterprise community requires to have their data processed within the premises with privacy while connected to the Public Networks for network management and Control plane management. This scenario has not fully defined in 3GPP architecture, but trial implementation variations and deployment suggestions exist through several industry groups. Thus, the GSMA 5G Industrial Private networks identifies the need for 1) SNPN 2) PNI-NPN with remote control and data planes and 3) PNI-NPN with local data-planes along with optional edge computing.

2.3.3 Business Models and deployments

The Business model section includes the ownership models of Private Networks supplier, operation and management by stakeholder entities and the considerations for planning a Private network suitable for an industry network. This section also introduced the concept of Neutral Host Networks (NHN) and how this model could be used for multi-operator scenarios sharing network and radio resources. Finally, the 'business models' section provides examples of Private networks commercial availability.

The deployment section discusses three types of connection models – single factory, multi-factory and connected factory deployments. Note that originally SNPN was supposed to be disconnected from all other networks including other SNPNs. However, the business gradually experiences need to connect with another SNPN or PNI-NPN for efficiency and distributed manufacturing of products and SNPNs itself may need a fall-back connectivity with Public Networks in the event of regulatory requirements.

In addition, the paper describes the need of Edge computing locally on the premises or very close to the premises to offer options for local processing to satisfy latency, speed, data privacy and application bandwidth requirements on the premises.

2.3.4 Brownfield Considerations

There are many 4G implementations on Private networks today which are deployed, and the users need guidance to move to 5G network without shutting down their existing deployments. The document provides guidance on transitioning from 4G Private networks to 5G Private networks.

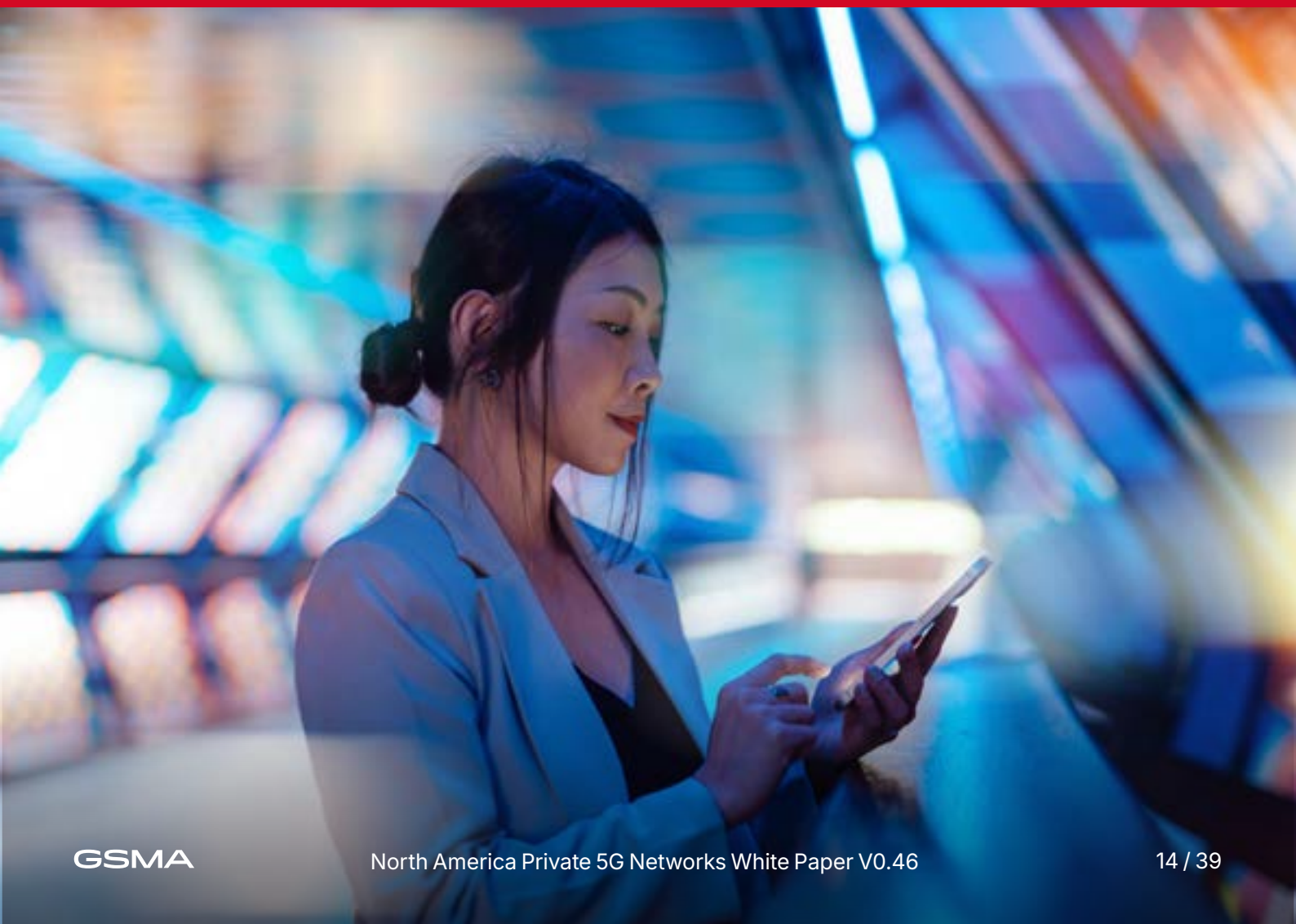
2.3.5 Use cases and Requirements

The 5G Industrial Private Networks whitepaper develops variety of use cases of industrial manufacturing networks, Campus networks, Ports and Airports, Smart tools, Automated Guided Vehicles and Robots, AI/ML and XR application use cases in the Industry 4.0 networks. The use cases are usually planned for commercial use or shown in the part of trial experiments by multiple company efforts.

The network requirement section of the document provides comprehensive guidelines of network requirements for practical considerations such as QoS and SLA management, network slicing options for SNPN and PNI-NPN, network configuration options, Software and network upgrades, vendor interoperability considerations, device access in different kind of private networks and authentications, scalability consideration, Mobility and role of eSIMs in the device identifications. However, this document does not go through any blueprint for 5G Private networks and address allocation schemes in details.

Finally, the document identifies the gaps that other GSMA groups can help address through guidelines to the B2B community, such as mobility and roaming across private networks, device management, auto configuration in batches.

3. Private Network use cases



A wide variety of private wireless network use cases is possible, and several new use cases are in the rise but not all of them of interest to all stakeholders. The intent of this section is to broadly categorize these use cases and focus on the use cases impacting the public mobile network stake holders first.

The key entities, actors and their roles covered in this use case analysis are as follows:

Users:

- Private Network users: Users authorized to use the private network services. Primary users of the private network.
- Public Network users: Users subscribed to the public network offered services.

Network service providers:

- Private Networks: Entity operating private networks for providing access & private network services for the private group of users.
- Public Networks: Public Mobile network providing access to communication services and access to partner services, through external connectivity.
- Neutral host networks: Entity operating network of shared cellular infrastructure in privately owned spaces for providing access to users of multiple public mobile service providers.
- Neutral host network aggregators: 3rd party entity providing network access in privately owned spaces for one or more public or private mobile network service providers.

3.1 UC1: Private network users utilize Private networks for their services

Private networks are purpose-built for a specific set of services for private use and are self-contained. The 3GPP specifications and further deployment guidelines are covered in relevant industry advocacy groups. This use case is not a focus for this whitepaper.

3.2 UC2: Private network users utilize public network to access their enterprise services from outside their private network coverage

A **hybrid private-public network** model combines the advantages of both private and public networks to provide seamless, secure, and flexible connectivity for users. This model allows devices and users to switch between private and public networks as needed, optimizing performance, coverage, and cost-efficiency.

Benefits:

- **Uninterrupted Connectivity** - Seamless transitions between private and public networks ensure continuous service, enhancing productivity and user experience.
- **Enhanced Flexibility** - Users can move freely between locations while maintaining access to necessary applications and data.
- **Optimized Resource Utilization** - Critical operations use the secure and optimized private network, while general communications use the scalable public network.
- **Cost Efficiency** - Reduces the need for extensive private network infrastructure by leveraging public network resources.

Example Application:

Bob runs a large manufacturing & logistics company which uses a private wireless network at its main distribution center to manage automated systems and real-time inventory tracking. Ethan, a delivery driver uses the same network when he is at the distribution center (on-site) for loading and unloading. As Ethan moves away from the distribution center, his devices switch to the public network, allowing him to continue receiving real-time route updates, customer communications, and access to central systems for delivery confirmations. Also, he can access the company's secure applications and data over the public network through secure VPNs or other secure access methods.

By leveraging both private and public networks, Bob's company ensures its operations are efficient, secure, and flexible, providing consistent connectivity, regardless of location.

3.3 UC3: Private network users utilize public network offered communication (Data, Voice & Messaging) services from the private network

This use case involves a **hybrid private-public network** model where users on a private wireless network can seamlessly utilize communication services offered by public networks, both when they are on and off the private network. This approach leverages the strengths of both private and public networks to provide users with consistent and uninterrupted communication services.

Benefits:

- **Operational Efficiency** - Employees use the private wireless network for high-priority and latency-sensitive applications such as real-time monitoring of machinery, automated guided vehicles (AGVs), and augmented reality (AR) maintenance support.
- **Data Security** - Sensitive data and communications related to the manufacturing process are securely transmitted over the private network, ensuring data privacy and compliance with industry regulations.
- **Encryption** - Higher levels of encryption and security protocols can be implemented as per the enterprise requirements.
- Seamless access to communications services – Shoppers enjoy public communication services while they are in the private network premises.

Use Case Scenario:

A large enterprise, such as a manufacturing company, operates a private wireless network within its facilities to support its production lines and employee communication. Employees use smartphones and other devices that are configured to connect to both the private and public networks.

3.4 UC4: Public network users utilize Neutral host (private) networks for the public network offered communication (Data, Voice & Messaging) services

A large underground shopping mall has no public network coverage. The mall wants to enable seamless and secure communication services to shoppers and visitors connected to public networks while they are on the premises.

Benefits:

- **Enhanced Shopping Experience** - Shoppers can access necessary data and applications seamlessly, enhancing their shopping experience with real-time information and offers.
- **Seamless coverage** – Shoppers enjoy public communication services while they are shopping.
- **Increased Engagement** - Facilitates real-time data sharing and engagement between shoppers and the mall, improving customer satisfaction and loyalty.

Example Application:

The Union Mall operates a private wireless network to support its internal communications, security systems, and customer engagement applications. During a busy shopping season, thousands of shoppers and visitors are on-site and connected to public networks. On-site shoppers connect to the Mall's private data network. Once authenticated by the respective public (home) network, the public network users' devices are authorized to access.

- Data services: access internet, including the mall's private data services. Shoppers can then access the Mall's digital directories, shopping apps, special offers, and security alerts. All data transmissions are encrypted, ensuring that sensitive information remains secure. Also, shoppers receive real-time updates on special offers, store information, and navigation assistance within the mall. And the mall meets regulatory requirements for data security and access, ensuring compliance with industry standards.
- Voice services: Ability to make or receive subscribed voice services including the emergency calls.
- Messaging services: Ability to make or receive subscribed messaging services including the emergency messages.

By enabling public network users to utilize data services within the private network coverage, The Union Mall ensures a superior shopping experience for its visitors while maintaining the security and performance benefits of its private network. This integration allows for efficient and secure data communication, enhancing customer engagement and overall operational efficiency.

3.5 UC5: Private network users utilize another private network for their services

In this use case, a private network user utilizes services from another private network for their services. This is not of initial focus for this whitepaper.**Benefits:**

- **Flexibility** - Users can access necessary services across different private networks, enhancing collaboration and productivity.
- **Service Continuity** - Seamless handover and roaming ensure uninterrupted service, critical for critical operations.

Use Case Scenario:

Firefighters (first responders) from California has responded to the call to help with the wild-fire in the east-cost and require the same treatment from the private wireless network operator serving the first responders in Maine.

4. 3GPP architecture models for Private Networks

4.1 General

There is no one 3GPP architecture for supporting private networks. Instead 3GPP specifications support private networks via standardized, interrelated UE and network enablers whose use may be tailored for various use cases and deployment scenarios. Enablers may be combined to support a large number of deployment model options and are specified in 3GPP specifications TS22.261, TS23.501, TS23.502, TS23.503 and TS23.401 among other specifications.

The enablers for a 5G network include:

1. Standalone and Public Network Integrated Non-public networks that provide services to a designated set of subscribers.

2. Network Sharing between private networks, and between private networks and PLMNs.

3. Closed Access Group (CAG) cells which can be used to exclusively provide access to private-network services to a restricted set of UEs.

4. Network Slicing that provides differentiated services via slice types supporting specific service attributes, and multiple isolated instances of a slice type. Network Slicing may also be used to support PNI-NPNs.

5. Service specific features such as URLLC, TSN, Cellular IoT and differentiated QoS.

6. 5G LAN-Virtual Networks and VN Groups which define a set of UEs using private communication for 5G LAN-type service.

7. Trusted and Untrusted non-3GPP access for interworking between a PLMN and SNPN.

8. Secondary Authentication by a DN AAA.

9. UE access to Localized Service (defined by a LADN).

The enablers have expanded in number, capability and scope over subsequent 3GPP generations, and tThe enablers have expanded in number, capability and scope over subsequent 3GPP generations, and their capabilities in many cases extends beyond support for private networks. For example, Network Sharing whereby a single RAN can be used by multiple operators, was supported in 3G, primarily to lower costs by sharing a RAN deployment among PLMN operators. 3G also supports differentiate service using application flow specific QoS. CSGs are supported in 4G, and 5G supports a similar capability with CAGs. 5G introduced network slicing, TSN, URLLC and explicit support for NPNs.

Within each generation, functionality has expanded over subsequent releases. The following sections present 3GPP enablers that may be used to implement private networks based on information available by the Release 18 specifications. Possible business relationships, network ownership, deployment scenarios, roles for offering service and network ecosystem relationships among entities involved in providing the RAN, core network and private network services are described in this section only when they are central to individual enablers (e.g. a PNI-NPN assumes a role for a MNO operating a PLMN).

4.2 Non-Public Networks (NPN)

NPNs, introduced in 5G Release 16 and subsequently enhanced, enable deployment of the 5G System for private use (e.g. by or for an enterprise) by permitting access to services only to designated subscribers within a specified geographic area. The NPN can be deployed as a Stand-alone Non-Public Network (SNPN) or Public Network Integrated NPN (PNI-NPN). An NPN operator manages SNPNs without relying on the functions of a PLMN, whereas PNI-NPNs are hosted by the PLMN.

4.2.1 Standalone NPNs

The SNPN uses a combination of a PLMN Identifier (PLMN ID) and Network Identifier (NID) to identify the SNPN. A 5G UE can register with an SNPN based on the 5G Subscriber's Permanent Identifier (SUPI) and credentials for the SNPN.

The PLMN ID used for an SNPN may be based on the mobile country code (MCC) 999 reserved for private use by the ITU. The RAN of the SNPN broadcasts the combined PLMN ID and NID in the System Broadcast Information and supports network selection and re-selection, load and access control, and barring. The NIDs can be self-assigned individually by the SNPN upon its deployment.

The active NIDs in this case may not be unique, but they use different numbering space to prevent conflicts. Alternatively, coordinated NID-assignment, that can have either 1) globally unique NID-assignment independent of the respective PLMN ID; or 2) globally unique NID/PLMN ID combination may be used.

The SNPN may be deployed to provide access to services using one or more of the following architectures:

- The SNPN is a standalone network with no interaction with a PLMN
- The SNPN acts as an untrusted non-3GPP access, and the UE uses PLMN credentials to register with the PLMN via the SNPN using user plane connectivity.
- The PLMN acts as an untrusted non-3GPP access, and the UE uses SNPN credentials to register with the SNPN via the PLMN user plane connectivity.
- The SNPN is accessed via trusted or non-trusted non-3GPP access.

Access to the services provided by the SNPN and the PLMN is based on registration using separate subscriber credentials for each. The use of trusted and untrusted access for private networks is further described in section 4.8.

SNPN NFs may reside within the operational area where private network services are provided such as factory, or in an operator or 3rd party data center. The SNPN subscriber may have dual subscriptions, one for the NPN and a second for the PLMN.

4.2.2 Public Network Integrated NPNs (PNI-NPN)

A PNI-NPN is realized by using the PLMN to provide connectivity to dedicated data networks (e.g. an enterprise DN) and/or by using PLMN Network Slices that are dedicated to supporting the NPN. A PNI-NPN may use a Closed Access Group (CAG) that designates the cells within the PLMN where the subscribers belonging to the CAG (i.e. the NPN subscribers) are allowed access. UEs that do not belong to the CAG (e.g. PLMN UEs) may not access the CAG cells. UEs that belong to the CAG may be restricted to only CAG-cells, or allowed to access other cells of the PLMN, depending on configuration. UEs that access the PNI-NPN have a subscription to the PLMN and are provided with credentials to enable access to the network slice used for the PNI-NPN, the data network to which the UE may connect and/or CAG information.

4.3 Network Sharing

With 5G Network Sharing as defined by 3GPP, the RAN and optionally radio frequencies can be shared by any combination of PLMNs, PNI-NPNs, and SNPNs. This can significantly reduce the burden of deploying a private network as the cost of the RAN can be shared among the various networks, eliminating the need for multiple dedicated RANs with overlapping coverage.

Multi-Operator Core Network (MOCN and Multi-Operator Radio Access Network (MORAN) are 3GPP defined network features that allow multiple operators and service providers to share RAN systems. In MOCN, the participant operators share the same frequencies for transmission and reception by the RAN, while in MORAN, each participant operator owns and uses its own frequency range but shares the same physical RAN system.

With both MOCN and MORAN, operators of each network, which may be a public or private network, may deploy their own core network (e.g. EPC or 5GC) which connects to the shared RAN. 4G supports both MOCN and MORAN while 5G only supports MOCN. MOCN and MORAN can support Neutral Host deployments whereby the RAN is provided by a 3rd party which establishes agreements with participating network operators. The shared RAN routes traffic of a given UE to the core network of the appropriate operator. From the user's perspective, the connection appears to come from their home network (public or private) since the RAN broadcast of system information includes all available core networks. This allows UEs to transition seamlessly between network dedicated cells and shared cells.

4.4 Closed Access Group (CAG)

With 5G PNI-NPNs, a private network can be realized by designating Closed Access Group (CAG) subscribers that can access corresponding CAG cells of the private network. Membership of a UE in a CAG is configured in UDR/UDM subscription data and is independent of the network slice used by the UE. CAGs and CAG cells enable geographic restrictions on access to an NPN. Cells supporting CAGs broadcast PLMN specific CAG Identifiers so unauthorized UEs do not attempt to select and access the CAG cells and instead select and access cells from the public part of the network. For each CAG, the UE subscription may also specify time validity information indicating periods when access is allowed. Up to 12 CAG identifiers may be supported on a cell, and each may be accompanied by a human readable network name for display to the subscriber. Note CAGs are not supported with SNPNs.

A similar capability exists in 4G with Closed Subscriber Group (CSG) subscribers and cells of a Home eNB (HeNB).

4.5 Network Slicing

Network slicing is used to establish logical 5G networks with defined capabilities and characteristics. QoS can be controlled and protection by isolation between slices can be provided. For example, a network slice may provide eMBB service with includes voice connectivity or it can focus on Internet of Things (IoT) service, including for industrial applications. Today, there are many test projects and commercial setups involving industrial devices. [13]

Network slices are characterized by a Slice Service Type (SST) that references the services and features of the network slice, and a Slice Differentiator (SD) that allows for multiple slice instances of the same SST. Standardized values of SST are specified in 3GPP TS23.501 and shown in table 4.5-1.

Table 4.5-1: Standardized Slice Service Types:

Slice/Service type	Description
eMBB	5G enhanced Mobile Broadband.
URLLC	Ultra-reliable low latency communications.
MIoT	Massive IoT.
V2X	V2X services.
HMTC	High-Performance Machine-Type Communications.
HDLLC	High Data rate and Low Latency Communications.

For Private Networks:

- Network slicing of a PLMN may be used to establish PNI-NPNs, as described in section 4.2.2. A PNI-NPN established via network slicing may provide differentiated service using the SSTs indicted in table 4.5-1 or using a non-standardized SST. An operator may use multiple slices of the PLMN for a given private network customer (e.g. provide eMBB and URLLC slices for an enterprise customer). Private network customers may be each assigned their own SD and hence be served via separate network slices, which may be isolated.

- An S-NPN may be sliced by using the SSTs indicated in table 4.5-1 or by using non-standardized SSTs to provide differentiated services for a private network customer (e.g. provide eMBB and URLLC slices of an S-NPN).

Isolation between network slices may be supported by management plane configuration and independent life-cycle management of slices. This can be achieved using slice dedicated core network function (NF) instances and RAN resources. For each network slice, the NF instances can be configured in a manner suitable for the service type.

In this manner, the network operator can offer suitable characteristics for a variety of different requirements for their subscribed verticals. The means to differentiate the network resources and performance via network slicing can also be used to create new business models. As an example, the operator can offer their customers gold, silver, and bronze service categories, each with their personalized pricing and QoS figures. [32]

The network operator can be an MNO wherein slicing is used to establish PNI-NPNs. The network operator for an S-NPN could be MNO, a 3rd party (e.g. IT provider) or the enterprise if their skillset suffices to manage slices. Network Functions associated with a network slice supporting a private network may be instantiated in a local enterprise network, in the MNO's core network, or a network provided by a 3rd party.

Network slices for private networks are not yet used widely in commercial Standalone (SA) 5G networks, despite the forecast indicating about 25% use base in 5G by 2025. [33] [34] [35] Network slicing beyond the RAN and 5GC is still maturing to cope with the impacts of real-world non-ideal aspects in near real-time orchestration, cross-layer (e.g. transport layer) support and coordination of the overall management of the slices. Nevertheless, Network Slicing can serve the requirements for private networks in an optimal way in many use cases.

4.6 Service Specific Features (URLLC, TSN, Cellular IoT) and differentiated QoS

Since GPRS in 2G, 3GPP has provided features that differentiate service for designated devices or user sessions. These features may be used in the context of private networks to meet specialized requirements demanded by applications, some of which are primarily applicable in private network environments. In the 5GS, the features include:

- QoS differentiation for UE service data flows using Guaranteed Bit Rate (GBR), Delay Critical GBR and non-GBR resource types. 3GPP clusters standardized QoS characteristics under 5G QoS Identifiers (5QI) to support a wide range of standardized application requirements (see 3GPP TS23.501, clause 5.7). 5QIs are defined to support conversational voice, live streaming, buffered streaming, push-to-talk, V2X, augmented reality, electrical distribution, motion tracking, and numerous additional application types.

- Integration of the 5GS with IEEE TSN networks to support deterministic networking. The 5GS can be configured as an IEEE 802.Q compliant ethernet bridge in a TSN data network to provide very low latency communication, typically for industrial applications (e.g. robot and controller communication). An IEEE Centralized Network Configuration (CNC) supporting a fully centralized TSN model receives 5GS bridge management information from a TSN AF and configures the 5GS so that user plane device side TSN Translators (DS-TT) at the UE and Network Side TSN Translators (NW-TT) at the UPF transmit PDUs according to a CNC proscribed schedule.

- URLLC, which may provide redundant transmission over the air-interface and in the 5GC. Dual connectivity from a UE to master and secondary gNBs may be used to establish independent user plane paths to separate UPFs. Alternatively, only redundant user plane transmission between the RAN and UPF may be configured. URLLC also provides QoS monitoring and reporting of packet delay between the UE and the UPF, or between only the RAN and UPF. Low latency QoS for URLLC may be supported by using the Delay Critical Guaranteed Bit Rate resource type with an appropriate 5QI.

- Cellular IoT (including NB-IoT) – When a UE registers for service, it may negotiate with the network for Cellular IoT capabilities applicable on 3GPP accesses. These include:

  - Control Plane CIoT 5GS Optimization, which allows the exchange of user data between the UE and the 5GC using an N1 interface NAS message, and exposure of the user data to the application via the NEF. This enables the exchange of small amounts of user data without the overhead of a user plane connection. A PDU Session may be dedicated to Control Plane CIoT 5GS Optimization.

  - User Plane CIoT 5GS Optimization, which allows exchange of user data via the user plane without the UE sending a Service Request. Instead RRC Suspend / Resume procedures are used.

  - N3 data transfer, which allows the UE or the 5GC to switch from the control plane to the user plane (N3 interface) for transfer of user data, for example based on the volume of data transferred.

  - Header compression for data sent via the Control Plane

  - Service Gap control, which ensures a minimum time gap between UE access of the network.

  - NB-IoT, which provides a narrowband (200 kHz) RAT that facilitates power and cost savings for low data rate IoT devices.

For power saving purposes, the UE may also negotiate Mobile Initiated Connection Only (MICO) mode when network-initiated data transfer is not required. In this case the UE does not need to monitor for paging messages when idle. Alternatively, the UE may negotiate Extended Discontinuous Reception (eDRX) where the UE may sleep for extended periods between checking for downlink data arrival.

CIoT features are supported for both the EPC and 5GC, and the network can direct a UE to either the EPC or 5GC.

4.7 5G LAN-Virtual Networks

5G LAN type service offering private communication is supported in 3GPP using 5G LAN-Virtual Networks. UEs that participate in the service belong to a 5G VN Group. Local switching at a UPF and N19-based forwarding between UPFs allow LAN service traffic to be sent directly between UEs without using the N6 interface to a data network. Unicast one-to-one communication between two UEs of a VN Group or between a UE and a device on the DN is supported. Similarly, one-to-many multicast and broadcast traffic from a UE or device on the DN to other UEs of the VN Group or devices on the DN are supported.

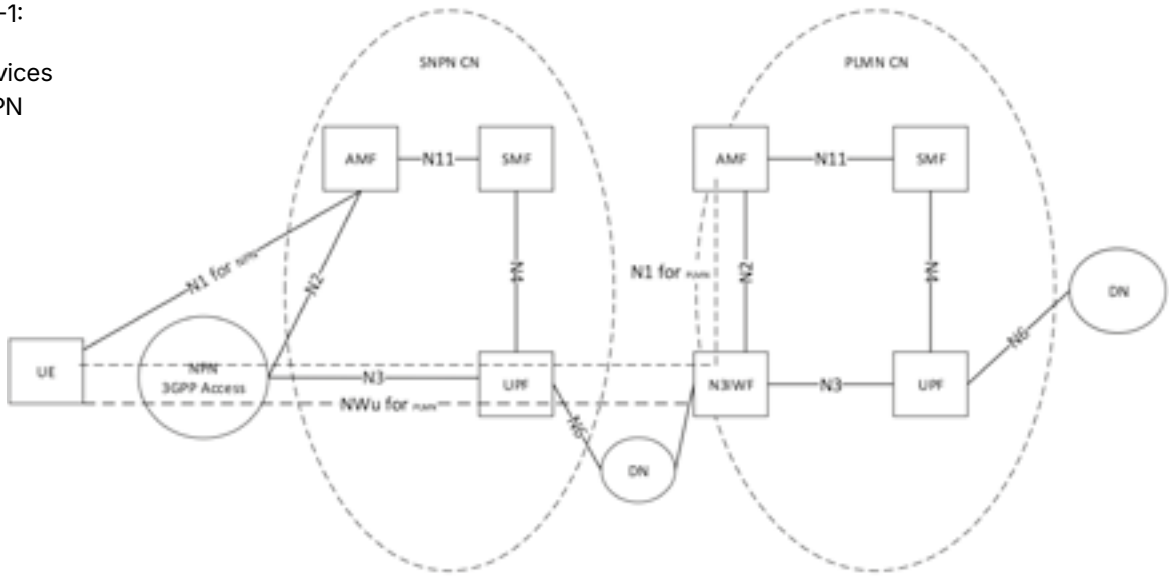
5G VN Group characteristics include VN Group identities (e.g. an external or internal Group ID), VN Group membership, and parameters including DNN, Slice (S-NSSAI), PDU Session type (IP or Ethernet) and secondary authentication / authorization information for accessing the DNN and slice (S-NSSAI) associated with the 5G VN Group.

4.8 Untrusted non-3GPP access for Public / Private Network Interworking

The architecture introduced in 3GPP for untrusted non-3GPP access can be used by UEs registered on an SNPN to obtain the services from a PLMN, or for UEs registered on a PLMN to obtain services from the SNPN. To support this, a UE must have credentials for both the PLMN and the SNPN. After a UE has registered on a PLMN, it may send a subsequent registration via the PLMN user plane to the SNPN. Similarly, if the UE has registered in on an SNPN, it may send a subsequent registration via the SNPN user plane to the PLMN. In either case, the network on which the UE first registers take the role of the untrusted non-3GPP access. In addition, both trusted and untrusted non-3GPP access architectures may be used for a UE to obtain SNPN services via non-3GPP access.

The architecture for access to PLMN services via an SNPN user plane acting as untrusted non-3GPP access is illustrated by 3GPP in TS 23.501, Annex D.3 which is reproduced in Figure 4.8-1. The corresponding architecture for access to SNPN services via a PLMN is similar, with the PLMN and SNPN switching roles.

Figure 4.8-1: Access to PLMN services via an SNPN



4.9 UE access to Localized Service (defined by a LADN)

A Local Area Data Network (LADN) may be used to provide access to a DN only in specific geographic areas defined by PLMN or SNPN tracking areas (TAs). The area where service is allowed, may for example correspond to the coverage of gNBs deployed at an enterprise where private network service is to be provided. A DN may be designated as an LADN, and the service area of the LADN configured in the 5GS per network slice (per S-NSSAI). When the UE registers, it may provide an one or more LADN DNN to the network, and the LADN service area(s) are provide to the UE. If the LADN information in the network changes, the UE may be updated via a configuration update. An association between an application and an LADN may be configured in the UE so the application (e.g. an enterprise application) is available only in the LADN.

Access to the LADN is successful only when the UE resides within the service area of the LADN. A UE that is outside of an LADN service area should not attempt to send a PDU Session Establishment Request or Service Request for the LADN DNN. If a request is sent, it is rejected by the 5GS. If UE mobility results in it residing outside of the LADN, the user plane connection for the PDU Session is deactivated or the PDU Session is released.

4.10 Secondary and Network Slice Specific Authentication / Authorization

Secondary authentication/authorization allows a AAA server associated with the DN being accessed by the UE to authenticate the UE and authorize access to services in the DN, separate from authentication and authorization for access to the 5GC via the AUSF. For the case where the DN is a private network (e.g. an enterprise network), secondary authentication and authorization provides a separate layer of access control for the private data network. The DN-AAA server may be deployed in the 5GC and belong to the PLMN operator, or it may be deployed in a DN and belong to a separate DN operator.

Secondary authentication and authorization may be performed when PDU Sessions are established, as determined by SMF policy for the DN. For AAA servers deployed in the DN, credentials are passed from the UE to the 5GC via NAS (N1) signaling are sent from the 5GC to the DN-AAA via the 5GC user plane. If secondary authentication fails for a PDU Session, the PDU Session setup is aborted.

The 3GPP network also supports Network Slice Specific Authentication and Authorization at UE registration. This uses a AAA server provided by the H-PLMN or a third party. For the case when a private network is implemented using network slicing (e.g. a PNI-NPN), this capability can be used (e.g. by the MNO or a third-party private enterprise) to control access to the network slice rather than the DN to which the network slice provides connectivity.

4.11 LTE / EPC (EPS) Enablers for Private Networks

While previous sections focus on 3GPP specified 5GS enablers for private networks, the EPS also supports enablers that may be deployed alone or in combination to support a variety of private network use cases. Note 3GPP EPS standards do not explicitly support non-public networks (PNI-NPN or SNPN) as has been defined for the 5GS. However similar capability can be configured using enablers defined for the EPS. In this section we provide a brief summary of these enablers.

They include:

1. Network Sharing - As described in section 4.3, MOCN and MORAN can be used to share the RAN between core networks belonging to different 4G network operators. Shared eNBs broadcast the PLMN IDs of each network operator. When a UE access the RAN, the RAN routes the traffic to the EPC of the network operator associated with the UEs HPLMN. For private networks, network sharing may be combined with DCNs for dedicated private networks within the selected PLMN and with CSGs to provide cell access for only designated UEs.

2. Closed Subscriber Group (CSG) – CSGs and CSG cells in 4G are similar to their 5G counterpart, CAGs and CAG cells described in section 4.4. The CSG subscribers in a PLMN are provided exclusive access CSG cells of a Home eNB (HeNB). In addition, Hybrid cells may be designated that provide access to both CSG members and non-CSG members, where admission and rate control may be different for the two groups. Membership in CSGs for a UE is indicated in subscription data. Note to support a private network, a HeNB may be deployed with or without a local gateway (L-GW) that provides local user plane traffic off-load to a data network (e.g an enterprise network).

3. Data Networks for private network subscribers – Whereas the 5GS provides a UE with connectivity to a DN via a PDU Session, where the DN may be a private network hosting for example enterprise applications, the EPS similarly provides a UE with connectivity to a Packet Data Network (PDN) via a PDN Connection. When a UE attaches to the network, it can request a PDN connection by providing the EPC with an Access Point Name (APN) that represents the PDN. If the APN is allowed by HSS subscription information, the HSS provides the PDN subscription contexts for the APN. When the APN indicates a private (e.g. enterprise) network, connectivity is established between the UE and the private data network. 3GPP standards allow a UE to establish simultaneous PDN connections to different PDNs, allowing access to the services offered by those PDNs.

4. Dedicated Core Network (DCN) – DCNs may be used by a network operator to deploy private networks within a PLMN. DCNs may be dedicated to specific subscribers such as M2M subscribers or subscribers associated with an enterprise. Within the EPC, a DCN is composed of an MME and may also include dedicated SGW, PGW and PCRF. Multiple DCNs may share the same RAN and a default DCN may be used for UEs that are not otherwise assigned to a specific DCN. DCNs may be deployed in specific coverage areas, for example a coverage area associated with an enterprise. For each UE, the eNB selects the MME associated with the DCN based on the "UE Usage Type" subscription information obtained from the HSS. The dedicated MME in turn may select a dedicated SGW and PGW. The UE may assist the RAN with DCN selection by providing a PLMN specific DCN-ID when the UE registers or does a Tracking Area Update (TAU). In this case the DCN-ID is provisioned in the UE by the HPLMN. DCNs may be supported for roaming UEs based on operator policies in the VPLMN. If MOCN is used for network sharing, the CN operator is selected first, followed by selection of a DCN supported by the selected operator.

5. Ethernet PDN Connections – Ethernet PDN connections provide connectivity between a UE and an Ethernet network, which may be a private (e.g. enterprise) network. Ethernet PDN Connections can be supported with LTE access using the 5GS / EPS interworking architecture specified by 3GPP, which uses a combination PGW-C and SMF, and the 5GS UDM for subscriber subscription records.

6. Service specific features such as differentiated QoS and Narrow Band IoT (NB-IoT). – The EPS supports features that differentiate service based on device or application, and as with the 5GS, this differentiation can be used in the context of private networks. GBR and non-GBR EPS bearers of a PDN Connection provide QoS differentiation. Different EPS bearers may have different QoS characteristics as identified by a QoS Class Identifier (QCI). QCI characteristics include attributes such as priority, packet delay budget and packet error loss rate (see 3GPP TS 23.203, clause 6.1.7). Similar to 5G 5QI, standardized QCI are mapped to services such as conversational voice, live streaming, buffered streaming, push-to-talk, and V2X. QoS parameters for GBR bearers additionally include a Guaranteed Bit Rate (GBR) and a Maximum Bit Rate (MBR).

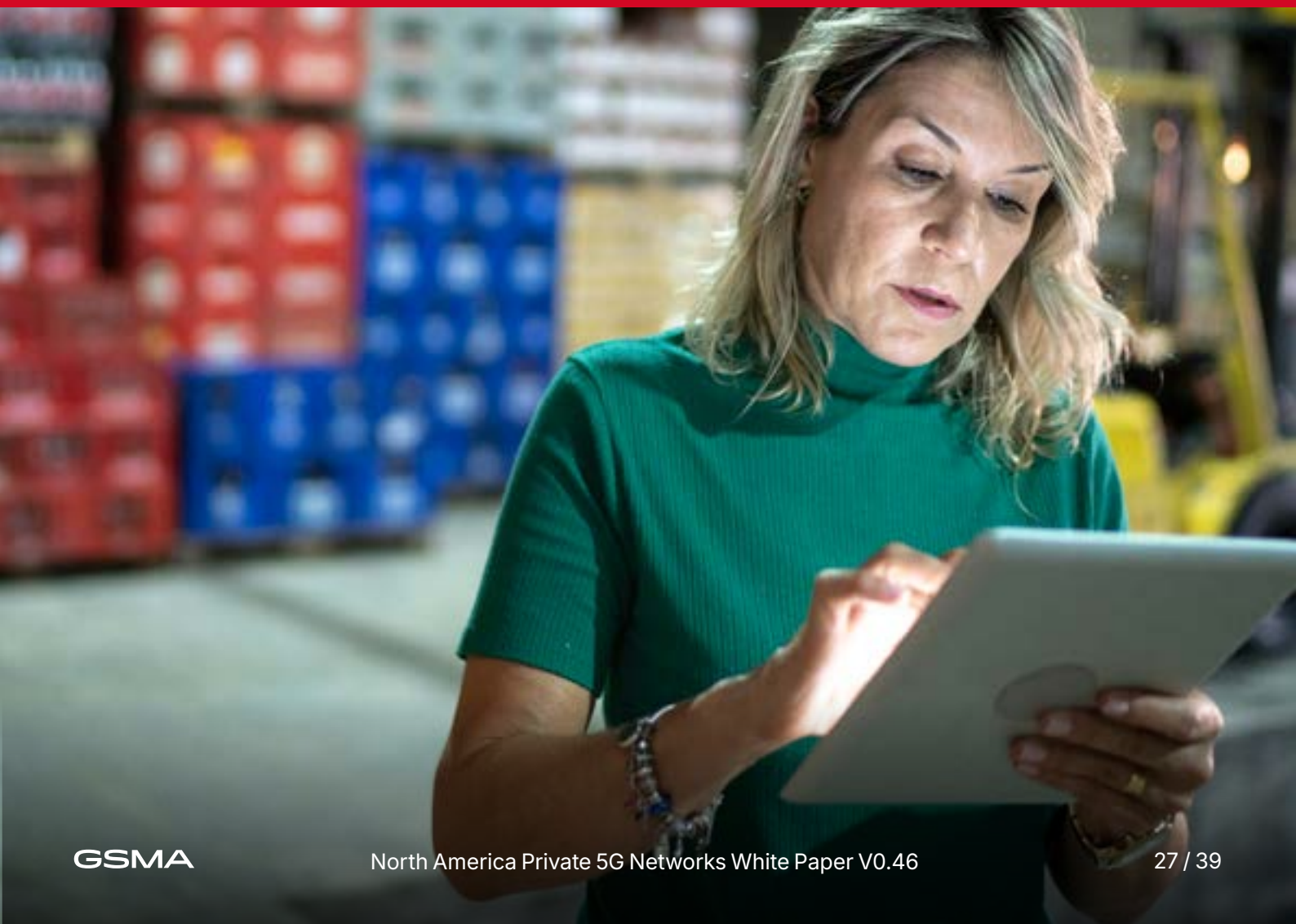
   Cellular IoT, including NB-IoT, described in section 4.6 similarly apply in LTE to support service specific functionality.

7. Local IP Access (LIPA) – LIPA allows traffic from a UE connected to a home eNB (HeNB) - e.g. femto cell, to be directed via a local gateway (L-GW) to a local network (e.g. an private network for a residence or enterprise) without the traffic transiting the operator core network. The L-GW is co-located with the home eNB that serves a local coverage area. For an APN for which LIPA is allowed, LIPA may be enabled per user according to subscription data in the HSS. Mobility is not supported for LIPA PDN connections. If the UE moves outside the coverage area of the HeNB, the LIPA PDN connection is released and the UE may initiate setup of a new PDN connection on the target HeNB.

   Note Selected IP Traffic Offload (SIPTO) can provide similar off-loading of user traffic at an L-GW which may be standalone or co-located with an eNB. However SIPTO is intended only for off-loading internet traffic from the operator core network, and is therefore less suitable for directing private network traffic to a local (e.g. enterprise) PDN.

8. MulteFire – MulteFire is based on 3GPP standardized LTE and was developed by the MulteFire Alliance, an industry consortium. MulteFire supports LTE in unlicensed spectrum using listen-before-talk to prevent interference and enable co-existence with other technologies such as Wi-Fi operating in the same spectrum. It can provide high capacity in the 5 GHz band and is intended to provide Wi-Fi like deployment simplicity. MulteFire may be used in a neutral host access mode to share the unlicensed spectrum among multiple participating service providers. It also supports a traditional access mode for interworking (e.g. mobility) with a 3GPP MNO network.

5. 3GPP Network Enablers for use cases



5.1 General

This section explores examples for how the 3GPP enablers described in section 4 can be used for the use cases described in section 3. Multiple enablers may be appropriate for each use case, and different combinations may be used depending on operator objectives and desired private and public network functionality.

Note a given enabler may be used in different ways depending on what other enablers are used and the use case.

5.2 UC1: Private network users utilize Standalone Private networks

Standalone, self-contained private networks do not require a PLMN, and may be deployed by an enterprise, an independent private network operator, an IT provider or a PLMN operator that wishes to offer private service separate from their PLMN. Applicable 3GPP enablers include:

- SNPNs, which allow private network deployment independent of the PLMN.
- Network Slicing to offer different types of service (e.g. eMBB and IIoT) within the SNPN.
- Service specific features to meet QoS, device (e.g. mIoT) and reliability requirements.
- 5G LAN Service, when a virtual network is needed to provide private service to a group of users. Untrusted non-3GPP access for a UE registered on an SNPN to also register and obtain services from a PLMN, or a UE registered on a PLMN to also register and obtain services from an SNPN.

LTE (EPC) variant -

Standalone private LTE using a Dedicated Core Network (DCN), dedicated MME (and optionally SGW/PGW/PCRF) per enterprise or user group. Deployed on-prem or in operator/third-party DCs.

A private operator may deploy a standalone private LTE with on-prem EPC (MME/SGW/PGW) and SIM-based access. Production tablets and AGVs (automated guided vehicles) use a private APN with local breakout to on-prem servers for security/latency. Dedicated QoS (QCI) bearers prioritize control traffic for consistent, low-latency delivery.

5.3 UC2: Private network users utilize public network to access their enterprise services from outside their private network coverage

PNI-NPNs have two components that make them well suited for this use case:

- A PNI-NPN may be implemented using a network slice of the PLMN. After registering and being authorized for service using one or more network slices configured in the UE subscription record, a UE needing private network service may request a PDU Session using a slice associated with the NPN. The 5GS control and user plane resources allocated for the network slice may be dedicated to the private network users. These resources may be deployed in an enterprise, at the PLMN edge, or within the PLMN. When dedicated resources are used, a separate NPN service provider may manage the network slice.
- A PNI-NPN may provide access to a data network where services for the private network are available (e.g. an enterprise network). Alternatively, a UE receiving NPN service via a network slice of the PLMN may connect to a DN provided by the PLMN (e.g. for IMS services) that is also used for public network users.

In this use case, subscribers use a private 5G network when in the geographic area of an enterprise and they use the PLMN when they move away from the enterprise. In both cases they can access enterprise services such as real-time inventory tracking cited in the example application in section 3.2, where these enterprise services may be provided from applications in a private enterprise DN. To support this, a PNI-NPN network slice may be configured to provide a private 5G network in the geographic area of the enterprise. This can be accomplished by configuring the Network Slice Area of Service (NS-AoS) for the PNI-NPN slice as the cells or Tracking Area(s) in the enterprise geographic area.

A separate network slice is used to provide broadband access to users in the PLMN coverage area, including the enterprise users when they are outside of the geographic area associated with the PNI-NPN slice. The private network users are provided with credentials to access both the PNI-NPN and the PLMN. They are also provided with credentials to access the private enterprise DN from either the PNI-NPN slice or the PLMN broadband network slice. For each DN, the UE establishes a PDU Session. To ensure secure access to the enterprise DN, the DN operator may use an enterprise DN AAA to provide secondary authentication. With this configuration:

- When subscribers are in the geographic area of the enterprise, they establish a PDU Session in the PNI-NPN network slice (if not already established) and access the enterprise DN via that slice.

- When subscribers are outside of the geographic area of the enterprise, i.e. outside of the PNI-NPN NS-AoS, they establish a PDU Session in a PLMN network slice used for broadband access (if not already established) and access the enterprise DN via that slice.

The network operator may provide the UEs with a Network Slice Selection Policy (NSSP) in the UE Route Selection Policy (URSP) to instruct the UEs to preferentially route traffic to the PNI-NPN when the UEs are in the enterprise geographic area.

If the operator wants to prevent public access within the geographic area of the enterprise, cells that provide coverage in the enterprise may in addition be configured as CAG cells, restricting access to only enterprise authorized UEs associated with the CAG.

Note in an alternative configuration, the PNI-NPN network slice may be established without the NS-AoS restriction. Subscribers may then remain on the PNI-NPN network slice and access the enterprise DN applications independent of whether they reside within the geographic area of the enterprise.

LTE (EPC) variant -

- **Off-site continuity via PLMN:** When users leave the private LTE footprint, they continue to access enterprise apps using the PLMN through enterprise APNs/PDNs authorized in HSS (same identity/policy). Simultaneous PDNs allow continuous app sessions.

- **On-site optimization:** Inside the campus, the private LTE DCN (dedicated MME/SGW/PGW) handles traffic locally; DCN selection based on “UE Usage Type” and/or DCN-ID keeps enterprise flows in the private core.

- **Shared RAN options:** MOCN/MORAN can be used to share the eNBs, letting devices move seamlessly while hitting the correct (private vs public) core.

A private network subscriber leaves the coverage area of the private network and roams onto the MNO’s macro-LTE. The device establishes an enterprise APN on the PLMN to reach line-of-business apps securely, preserving identity/policy from the HSS. Within the private network, the same SIM hits the private EPC for low-latency access; off campus, services continue through the PLMN APN.

5.4 UC3: Private network users utilize public network offered communication (Data, Voice & Messaging) services from the private network

In this use case, subscribers can use services available from the public network (PLMN) independent of whether they are using a private 5G network or the PLMN. Like UC2, the private (e.g. enterprise) 5G network can be supported using a PNI-NPN network slice from which a PDU Session is established to the enterprise DN. If the NS-AoS is not restricted, access to private network services in the enterprise DN via the PNI-NPN may be available independent of whether the subscriber is in the geographic area of the enterprise.

To access public network services available via the PLMN, the UEs may be provided with credentials to access the DNs accessible from the PLMN via the PNI-NPN network slice, the eMBB network slice, and/or optionally service specific network slices such as that used for IMS. Scenarios for private network users to access public network services via the PLMN are the same as for public network users, and may include for example, one or more of the following.

- A dedicated network slice for IMS services offered from an IMS DN.
- An eMBB network slice for broadband access to data services available from 3rd party providers (i.e. on the internet).
- Messaging services provided either via a user plane connection to a DN where applications offering messaging services are hosted, or via the 3GPP control plane whereby messages are delivered from an SMSF via an AMF to the UE using Non-Access Stratum (NAS) signaling (see 3GPP TS 23.040 and TS 23.501).
- For the case where messages are sent via the user plane, a dedicated network slice that provides connectivity to the DN where messaging applications reside may be used.
- For the case where messages are sent via the 5GC control plane, a dedicated network slice that includes SMS-related network functions (e.g. SMSF, IP-SM-GW, etc.) in addition to 5GC NFs (e.g. AMF, SMF, NRF, PCF, UDM, etc.) may be used.

If the PLMN operator offers services via additional DNs, separate PDU Sessions may be setup in the broadband access network slice, the IMS slice or the messaging slice to access those DNs and the associated services.

LTE (EPC) variant -

From the private LTE network, users establish an additional PDN connection to PLMN DNs that host public services (e.g., broadband/data and operator communications services). QCI profiles enforce appropriate QoS. With MOCN, the shared RAN routes each UE to its “home” EPC, so public services feel native even while on the private footprint.

On a private network with shared RAN (MOCN), subscribers attach to the operator PLMN access public services (e.g., VoLTE/IMS and messaging) normally, while a parallel PDN/APN provides reach into the enterprise DN. Mission apps stay local; public comms run in the MNO core with appropriate QCI mapping.

Voice/SMS → typically only works when the SIM is attached to MNO’s public PLMN.

Data (enterprise apps, IoT, low-latency control) → handled locally by the private EPC when on campus.

5.5 UC4: Public network users utilize Neutral host (private) networks for the public network offered communication (Data, Voice & Messaging) services

In this use case, a neutral host (e.g. for a large shopping mall) provides 5G infrastructure to support private networks for a large number of companies / tenants. The neutral host may deploy an NG-RAN that is shared among the various companies or tenants. The neutral host also deploys a 5G core network and a DN where tenant applications are hosted, or alternatively individual tenants or the neutral host may deploy dedicated 5G core networks for establishing connections to tenant dedicated DNs where tenant specific applications are hosted. The neutral host also shares the NG-RAN with one or more MNOs to allow access to public network communication services provided by those operators. Two options for configuring this are:

1. The neutral host is a 3rd party such as an IT provider. The 3rd party provides an NG-RAN that is shared using MOCN (see section 4.3) with MNOs and optionally tenants that wish to deploy their own 5G core network and DN. The private network(s) may be configured as SNPN(s), or if the 3rd party has partnered with an MNO, as PNI-NPN(s) with CAGs, where the CAGs provide service on designated cell sites or tracking areas in the geographic area of the private network(s).

2. The neutral host is an MNO that configures one or more network slices of the PLMN as PNI-NPN(s). A single PNI-NPN network slice may be configured for all tenants, or tenant specific PNI-NPN network slices may be configured. Each PNI-NPN can provide connectivity with a tenant specific private DN or with a DN shared by multiple or all tenants. The NG-RAN may also be shared with other MNOs using MOCN to allow access to public network communication services from other operators.

Public network users with credentials to access the public network services can do so directly from the NG-RAN if the NG-RAN is shared using MOCN. Subscribers that use the private network are provided with credentials that allow access to the SNPN or PNI-NPN network slice(s). Credentials are also provided to allow access to the PLMN and the communication services available in the PLMN DN(s). For an SNPN the private network may use credentials owned by an independent Credentials Holder, or the subscriber may obtain credentials from a provisioning server in an Onboarding Network (see TS 23.501, clause 5.30). Similarly for private networks configured using PNI-NPNs, credentials to access the network slice (S-NSSAI) associated with the PNI-NPN may be provided by the MNO. In addition, secondary authentication may be used for Tenant specific authentication and authorization to access tenant specific DNs.

LTE (EPC) variant -

Neutral Host network provides a shared LTE eNB RAN using MOCN or MORAN. eNB broadcasts multiple PLMN IDs; traffic is steered to each operator's EPC and users see their normal PLMN service. For Unlicensed option, MulteFire can implement a neutral-host-like access layer over 5 GHz where licensed spectrum is constrained.

A neutral-host LTE RAN network broadcasts multiple PLMN IDs via MOCN. Visitors within the neutral host coverage area connect with their usual SIMs and receive their operator's native services (VoLTE, messaging, data). And operations staff on the same RAN use the private APN for private connectivity, isolated from public traffic.

MOCN → lets one shared RAN serve multiple MNOs and a private enterprise network at the same time.

Visitors → Connect with their normal SIM, use operator services (voice, messaging, data).

Operations → Use a private APN for private connectivity, isolated from public traffic, even though it's the same physical RAN.

5.6 UC5: Private network user utilizes another private network for their services

For this use case, there is more than one private network, and users that receive services on a first private network can also receive services from a second private network. As described in the use case scenario, the users may be first responders that temporarily need access to services in a jurisdiction that is different from where they normally operate. Ways this may be supported include:

- An MNO may configure a single PNI-NPN network slice for all first responders, and the private networks may be distinguished by the DN where services are provided. MNO provides the DNN and credentials that allow users of the different private networks to access their respective private DN(s). Additional credentials may be provided to authorize the use of a DN when users are temporarily deployed in a different jurisdiction, and optionally secondary authentication may be used in the DNs to authorize the users.

- An MNO may configure different PNI-NPN network slices for the users in different jurisdictions. In this case the MNO needs to in addition provide PNI-NPN network slice (S-NSSAI) information and authorization for users that move to a different jurisdiction.

LTE (EPC) variant -

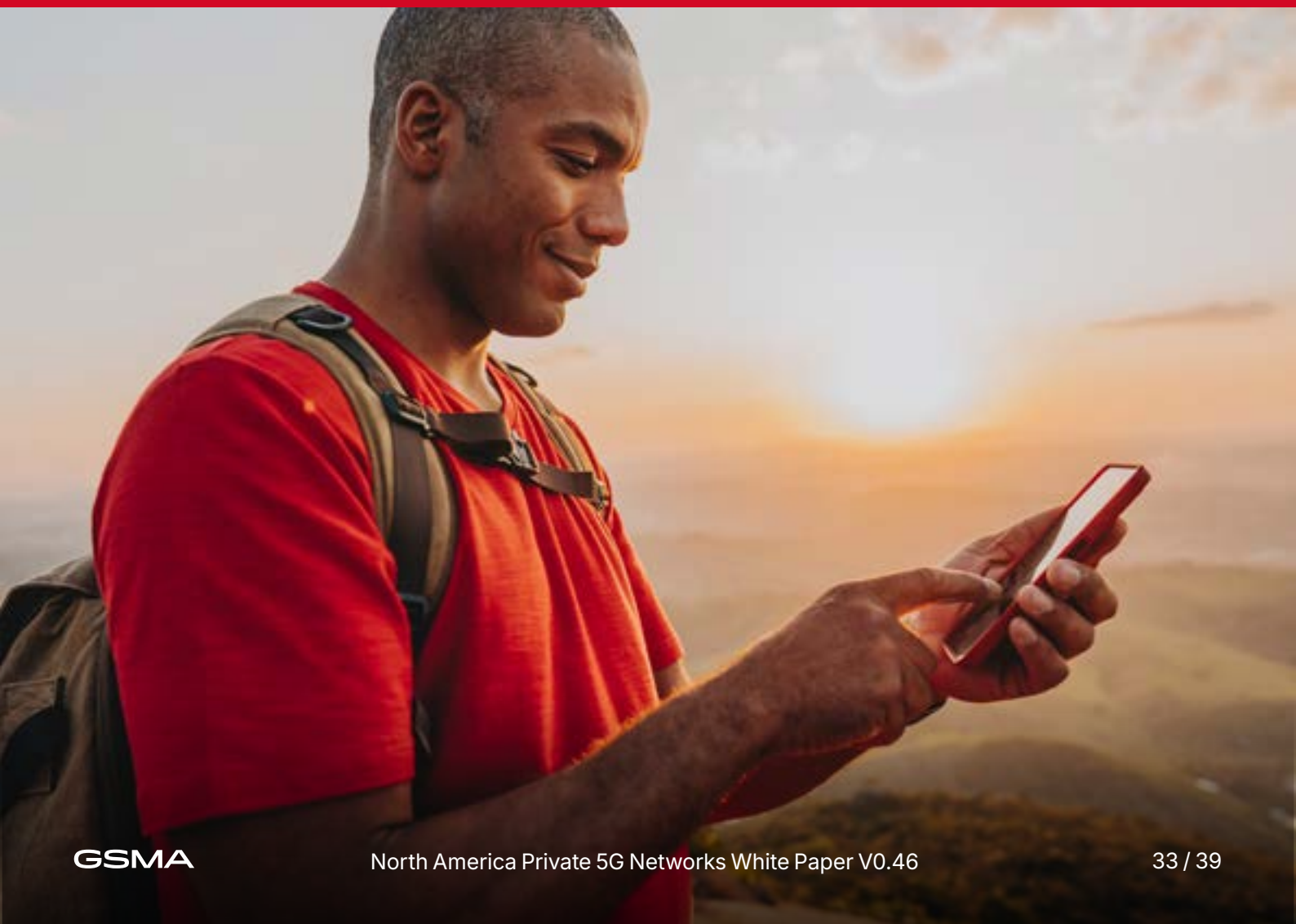
- **Core separation with DCNs:** Multiple DCNs per jurisdiction/agency keep policies and DNs separated. DCN selection (via "UE Usage Type"/DCN-ID) enables temporary authorization for visiting users.

- **Shared RAN:** MOCN lets different private operators (or private + public) share the same eNBs while routing each user to the correct EPC/DCN.

- **Enterprise DNs & APNs:** Visiting users can be granted APN/PDN credentials to the host enterprise DN for the mission window, then revoked post-event.

Using MOCN and DCN selection, visiting subscribers SIMs can be temporarily authorized on the host's private EPC and APN to access the network via local breakout for low latency, security and operational efficiency.

6. Conclusions



The rapid evolution of private and public wireless networks, driven by 3GPP enablers, provides a flexible and robust framework to meet the diverse needs of enterprises and public users. As mentioned in the use cases, 3GPP-enabled networks offer multiple configuration options that allow organizations to deploy private networks in isolation or integration with public networks for extended reach and functionality. The ability to blend private and public networks provides a spectrum of benefits, from seamless connectivity to operational efficiency.

For standalone private networks, 3GPP enablers such as SNPNs and network slicing help enterprises to maintain control and offer tailored services for different enterprise needs, ranging from enhanced mobile broadband to IoT. Meanwhile, PNI-NPN configurations allow private network users to benefit from public network services, enabling seamless transitions between private and public coverage and ensuring continuous access to essential enterprise services. This is especially vital for industries like logistics, where real-time updates and secure access to enterprise systems are essential for operational continuity.

Similarly, the integration of public network services within private network environments enables both communication capabilities and data security. Enterprises benefit from a secure, dedicated network for high-priority applications, while still leveraging the scalability and broader reach of public networks for communication services. This ensures not only productivity and efficiency but also the protection of sensitive information.

For public network users, the neutral host model demonstrates the potential for private networks to enhance the user experience in areas lacking public network coverage. By providing access to data, voice, and messaging services through private networks, operators can improve customer engagement and satisfaction, while ensuring compliance with security and regulatory standards. And the flexibility of private networks leveraging other private networks points to an emerging landscape where neutral hosts and shared infrastructure models become increasingly prevalent, enabling multiple enterprises to leverage common network assets while maintaining separate network identities and data security.

These various use cases demonstrate the potential of 5G/LTE networks in supporting both highly customized private network solutions and seamless integrations with public networks. As the deployment continues to expand, the interoperability, flexibility, and innovation made possible by 3GPP enablers will play a crucial role in driving further industry growth and delivering enhanced connectivity across sectors.

7. References

[1] GSMA, “Glossary,” GSMA, [Online]. Available: https://www.gsma.com/futurenetworks/all-ip/glossary/. [Accessed 29 November 2023].

[2] GSMA, “Interconnectivity,” GSMA, [Online]. Available: https://www.gsma.com/futurenetworks/ip_services/interconnection/. [Accessed 29 November 2023].

[3] GSMA, “Mobile for development: interoperability test platform,” GSMA, [Online]. Available: https://www.gsma.com/mobilefordevelopment/mobile-money/interoperability-test-platform/. [Accessed 29 November 2023].

[4] GSMA, “Mobile infrastructure sharing,” GSMA, September 2012. [Online]. Available: https://www.gsma.com/publicpolicy/wp-content/uploads/2012/09/Mobile-Infrastructure-sharing.pdf. [Accessed 25 October 2023].

[5] 3GPP, “Service requirements for the 5G system, Stage 1,” 3GPP, December, 2022.

[6] GSMA, “International roaming explained,” GSMA, August 2012. [Online]. Available: https://www.gsma.com/latinamerica/wp-content/uploads/2012/08/GSMA-Mobile-roaming-web-English.pdf. [Accessed 25 October 2023].

[7] Apple, “Wi-Fi network roaming with 802.11k, 802.11r, and 802.11v on iOS, iPadOS, and macOS,” Apple, [Online]. Available: https://support.apple.com/en-us/HT202628. [Accessed 28 April 2023].

[8] STL, “Redefining Connectivity with LTE – WiFi Interworking,” 22 July 2014. [Online]. Available: https://stl.tech/blog/innovating-connectivity-with-lte-wi-fi-interworking/. [Accessed 3 May 2023].

[9] 3GPP, “TS 23.261. IP flow mobility and seamless Wireless Local Area Network (WLAN) offload; Stage 2,” 3GPP, 2022.

[10] 3GPP, “TS 23.402. Architecture enhancements for non-3GPP accesses, V18.2.0 (Release 18),” 3GPP, 2023.

[11] 3GPP, “TS 33.501. Security architecture and procedures for 5G system, V18.3.0 (Release 18),” 3GPP, 2023.

[12] 3GPP, “Private Mobile Networks,” 3GPP, 19 December 2022. [Online]. Available: https://www.3gpp.org/news-events/partner-news/gsa-private-mobile-networks. [Accessed 12 March 2023].

[13] GSMA, “Internet of Things,” GSMA, [Online]. Available: https://www.gsma.com/iot/manufacturing/private-networks/private-networks/. [Accessed 18 December 2022].

[14] H. Koorapaty, “3GPP technologies in unlicensed spectrum: A contributor to the common good,” Ericsson, 16 September 2020. [Online]. Available: https://www.ericsson.com/en/blog/2020/9/3gpp-technologies-unlicensed-spectrum. [Accessed 20 November 2023].

[15] N. Rastegardoost, “3GPP: The Unlicensed Journey,” Ofinno, November 2020. [Online]. Available: https://ofinno.com/wp-content/uploads/2020/11/OFNO_White_Sheet_112320.pdf. [Accessed 20 November 2023].

[16] OnGo Alliance, “https://ongoalliance.org/wp-content/uploads/2020/12/OnGo-Private-LTE-Deployment-Guide-2.1.0.pdf].

[17] OnGo Alliance, “OnGo Private 5G Deployment Guide,” OnGo Alliance, April 2022. [Online]. Available: https://ongoalliance.org/wp-content/uploads/2022/05/OnGo-Private-5G-Deployment-Guide-1.0.0.pdf. [Accessed 20 November 2023].

[18] 3GPP, “NR Dynamic spectrum sharing in Rel-17,” 3GPP, 8 August 2022. [Online]. Available: https://www.3gpp.org/technologies/nr-dynamic-spectrum-sharing-in-rel-17. [Accessed 20 November 2023].

[19] S. S. B. B. M. Dominik, “Spectrum Sharing: Licensed Shared Access (LSA) and Spectrum Access System (SAS),” Intel, October 2015. [Online]. Available: https://www.intel.com/content/dam/www/public/us/en/documents/white-papers/spectrum-sharing-lsa-sas-paper.pdf. [Accessed 20 November 2023].

[20] OnGo Alliance, “Roaming Whitepaper,” OnGo Alliance, 11 September 2023. [Online]. Available: https://ongoalliance.org/resource/ongo-roaming-whitepaper/. [Accessed 13 November 2023].

[21] Celona, “Product brief. Private Wireless and Celona 5G LAN Overview,” Celona, 2023. [Online]. Available: https://www.celona.io/resources. [Accessed 21 November 2023].

[22] C&T RF Antennas Inc, “ITU Approves LoRaWAN as Global IoT Standard,” LinkedIn, 8 December 2021. [Online]. Available: https://www.linkedin.com/pulse/itu-approves-lorawan-global-iot-standard-ct-rf-antennas-inc/?trk=articles_directory. [Accessed 28 November 2023].

[23] DECT Forum, “The New DECT Standard NR+,” 2023. [Online]. Available: https://www.dect.org/nrplus. [Accessed 28 November 2023].

[24] D. C. A. S. A. R. A. A. Ralf Keller, “Roaming in the 5G System: the 5GS roaming architecture,” Ericsson, 17 June 2021. [Online]. Available: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/roaming-in-the-5g-system. [Accessed 20 November 2023].

[25] D. Chandramouli, “5G for Industry 4.0,” 13 May 2020. [Online]. Available: https://www.3gpp.org/news-events/3gpp-news/tsn-v-lan.

[26] 3GPP, “Private Mobile Networks,” 3GPP and GSA, 19 December 2022. [Online]. Available: https://www.3gpp.org/news-events/partner-news/gsa-private-mobile-networks. [Accessed 29 November 2023].

[27] GSA, “Private-Mobile-Networks December-2022 Summary Report,” GSA, December 2022. [Online]. Available: https://gsacom.com/paper/private-mobile-networks-december-2022-summary-report/. [Accessed 29 November 2023].

[28] 5GACIA, “5G Non-Public Networks for Industrial Scenarios,” 5GACIA, July 2019.

[29] H. J. Son, “7 Deployment Scenarios of Private 5G Networks,” NetManias, 21 October 2019. [Online]. Available: https://www.netmanias.com/en/?m=view&id=blog&no=14500. [Accessed 22 January 2023].

[30] Syniverse, “Managing the Complexities of Connectivity for Enterprises and Operators,” Syniverse, 24 March 2022. [Online]. Available: https://www.syniverse.com/blog/connectivity/managing-the-complexities-of-connectivity-for-enterprises-and-operators/. [Accessed 24 January 2023].

[31] Samsung, “Technical whitepaper: network slicing,” Samsung, 2020.

[32] GSMA, “Network Slicing: North America’s Perspective V1.0,” GSMA, 3 August 2021. [Online]. Available: https://www.gsma.com/newsroom/wp-content/uploads//NG.130-White-Paper-Network-Slicing-NA-Perspective-1.pdf. [Accessed 18 December 2022].

[33] GSMA, “5G Global Launches & Statistics,” GSMA, [Online]. Available: https://www.gsma.com/futurenetworks/ip_services/understanding-5g/5g-innovation/. [Accessed 11 January 2023].

[34] GSA, “5G Market Snapshot 2021 – end of Year,” GSA, [Online]. Available: https://gsacom.com/paper/5g-market-snapshot-2021-end-of-year/. [Accessed 11 January 2023].

[35] GSMA, “Mobile economy report 2022,” GSMA, 2022. [Online]. Available: https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/02/280222-The-Mobile-Economy-2022.pdf. [Accessed 11 January 2023].

[36] Celona, “Private LTE Networks for Enterprise: Overview & Solutions,” Celona, [Online]. Available: https://www.celona.io/cbrs/private-lte. [Accessed 22 November 2023].

[37] GSMA Public Policy Position “Licensed Shared Access (LSA) and Authorised Shared Access (ASA)”, February 2013

[38] GSMA , “Private 5G Industrial Networks: An analysis of Use cases and Requirements

“,Available: https://www.gsma.com/solutions-and-impact/industries/connected-manufacturing/gsma_resources/private-5g-industrial-networks-2023/, June 2023

GSMA

About the GSMA

The GSMA represents the interests of mobile operators worldwide, uniting more than 750 operators with over 350 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organizations in adjacent industry sectors. The GSMA also produces the industry-leading MWC events held annually in Barcelona, Los Angeles and Shanghai, as well as the Mobile 360 Series of regional conferences. For more information, please visit the GSMA corporate website at www.gsma.com.

About the GSMA North America Team

Headquartered in Atlanta, Georgia, USA, GSMA North America represents and leads mobile network operators in the United States, Canada, Greenland and the Caribbean. Working alongside some of the mobile industry's most influential companies, GSMA North America aims to increase the region's commercial opportunities and develop a collaborative and socially responsible and ecosystem. In this mission, GSMA North America convenes several leading annual industry events, provides regulatory expertise and technical knowledge to support network optimization.

Document Editor

GSMA Staff

For further information, please visit:
https://www.gsma.com/northamerica

GSMA NORTH AMERICA
Armour Yards
165 Ottley Drive
Atlanta, GA 30324
USA

GSMA Head Office
1 Angel Lane
London, EC4R 3AB
U.K.
Tel: +44 (0)207 356 0600
Email: info@gsma.com