OnGo alliance™

Private Cellular Network Security

Considerations for Enterprise

Table of Content

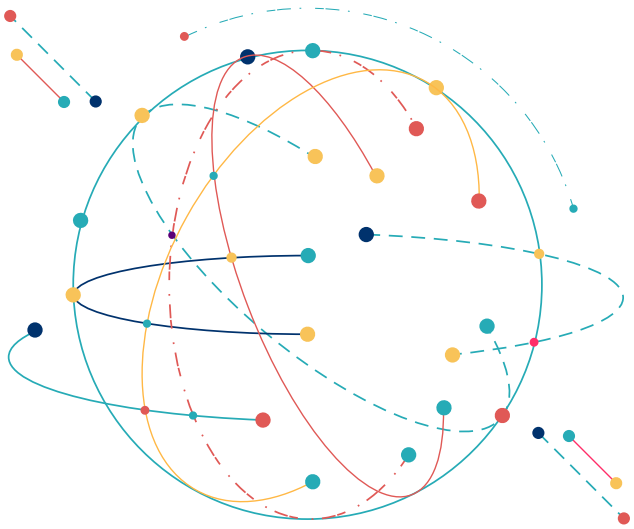
Introduction

Enterprises are expanding their communications infrastructure to include private cellular networks that are physically or virtually separate from public networks, and are used, managed, and controlled exclusively by enterprises. Like 4G/LTE and 5G cellular broadband capabilities in public mobile networks, private cellular networks support high bandwidth, high speeds, high density, and high reliability with very low latency. Unlike public cellular networks, private LTE/5G networks give enterprises deterministic control over how network resources are provisioned.

Based on 4G/LTE or 5G cellular technology, private networks became more accessible in the US when the Citizen Broadband Radio Systems (CBRS) shared spectrum was allocated for private enterprise network use. CBRS, also known as OnGo, is a game-changer for enterprises innovating with advanced technologies such as Internet of Things (IoT), Industry 4.0, robotics, artificial intelligence (AI), machine learning (ML), and autonomous vehicles.

This paper discusses inherent security advantages of 4G/LTE and 5G technology and CBRS-based private cellular networks, along with key elements to include in building a private cellular network threat model. Most of the potential threats are familiar to enterprise risk managers but may occur in new and unfamiliar elements within private cellular networks.

“Based on 4G/LTE or 5G cellular technology, private networks became more accessible in the US when the Citizen Broadband Radio Systems (CBRS) shared spectrum was allocated for private enterprise network use.”



A Bit About Private Cellular Network Components

Private cellular networks for enterprises are based on 4G/LTE or 5G technology, and operate on a variety of licensed, unlicensed, and shared spectrum like CBRS spectrum band.

CBRS-based private cellular networks are made up of the following components:

User Equipment (UE)
includes cell phones, smart monitors, and Internet of Things (IoT) sensors.

SIM/ eSIM cards
that uniquely identify each UE and determine access to the private cellular network.

Radio Access Network (RAN)
includes indoor and outdoor small cell base stations (similar in size to Wi-Fi access points, but with greater range and device density), and network switches/routers.

Core Network
provides authentication and authorization of users, data connectivity, mobility management, subscriber data management, and policy management and controls, and can be on premises or in the cloud.

Multi-Access Edge Computing (MEC)
delivers services and computing functions on network edge nodes, closer to users and thereby reduces latency.

Spectrum Access System (SAS)
allocates frequency channels to base stations (and is unique to OnGo-based networks, not public 4G/LTE or 5G).

Orchestration and Network Management Software
to set up and manage private cellular network components, devices, applications, and services.to users and thereby reduces latency.

Enterprise security policies and functions such as firewalls can typically be extended to include private cellular networks.

Security Advantages with Private Cellular Networks

First and foremost, because private cellular networks are separate from public mobile networks, they are not necessarily subject to the same interference or threats.

Private networks also have these inherent security advantages:

Enterprises can have full control over all aspects of their 4G/5G network, from which devices can gain access, to allocating and partitioning resources for mission critical applications.

Data processing and storage can be separated and protected from the mobile network.

Security policies are designed and controlled by the enterprise, and network configurations can be completely customized to meet enterprise security requirements.

There are essentially three deployment models for private networks, and each have network security implications:

Dedicated wholly owned on-premise model

Enterprises own, manage, and deploy all elements of the private network, including acquiring its own hardware, software, and leverage either an unlicensed General Authorized Access (GAA) CBRS spectrum and/or the licensed Priority Access License (PAL) CBRS spectrum. This gives enterprises maximum control over every aspect of the private cellular network, including security.

Managed/Turnkey model

The private cellular networks are deployed and managed by a third party such as a Mobile Network Operator (MNO), system integrator, or managed service provider. This can include a combination of on-premises or remotely located hardware and software, as well as varying degrees of network management. As such, enterprises would have varying degrees of control over security policies.

Virtual Public Network Slices

Enterprises can secure dedicated virtual network ‘slices’ using public cellular networks with MNOs providing guaranteed service and performance levels. This can be the simplest way to create a private cellular network, but security policies are generally set and managed by the MNOs.

Security as a Design Standard for 4G/LTE and 5G

Since private cellular networks are based on 4G/LTE and 5G cellular technologies, it is useful to understand their inherent security advantages over Wi-Fi wireless networks. 4G/LTE and 5G include native encryption, and while encryption can be added to Wi-Fi, it very often isn't, especially with public hotspots. Furthermore, cellular networks are not open public networks, they only support devices provisioned to run on their networks.

Through 2023, it is expected that 4G/LTE will continue to be the dominant cellular technology, representing 79% of all North American cellular connections . It has been a transformational technology that enabled the massive proliferation of smart devices. The standard for 4G/LTE security is markedly different from 3G and earlier cellular generations, as it was the first standard to include a cross-operator security standard, and user data, control data, and management data are all IP-based.

4G/LTE set the standard for future generations to incorporate the following security principles :

Authentication-the process of identifying, and thereafter trusting, the parties when establishing a communications channel.

Confidentiality-the ability to render information unreadable to those who have not been authenticated on the established communications channel.

Integrity-the ability for all messages to be received by the intended recipient(s) and that the messages are not corrupted or changed in any way.

Availability-the ability for the communications channel to be ready to use whenever the parties need access.

Nonrepudiation-the ability to verify a message has been sent and received.

[1] https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/09/290922-Mobile-Economy-North-America-2022.pdf

[2] https://ongoalliance.org/wp-content/uploads/2022/12/OnGoA-Security-Whitepaper-1.01_Final.pdf

Included in 4G/LTE security principles are the following specific security domains:

4G Security Domains[3]

Network Access Security

- Includes features for user equipment (UE) authentication and secure network access to services.
- Emphasizes encryption, encrypted key management, and use of encrypted keys.
- Support for 3GPP network access as well as non-3GPP network access such as Wi-Fi.
- Protects against attacks on radio interfaces.
- Security context (authentication) delivery from the service network to the access network.

Network Domain Security

Secures signaling data on network nodes and user plane data in the core network.

User Domain security

- Secures user access to the device and mobile network.
- Includes support for physical security mechanisms including smart cards (for tamper resistance) and biometrics (bridging physical and information security).

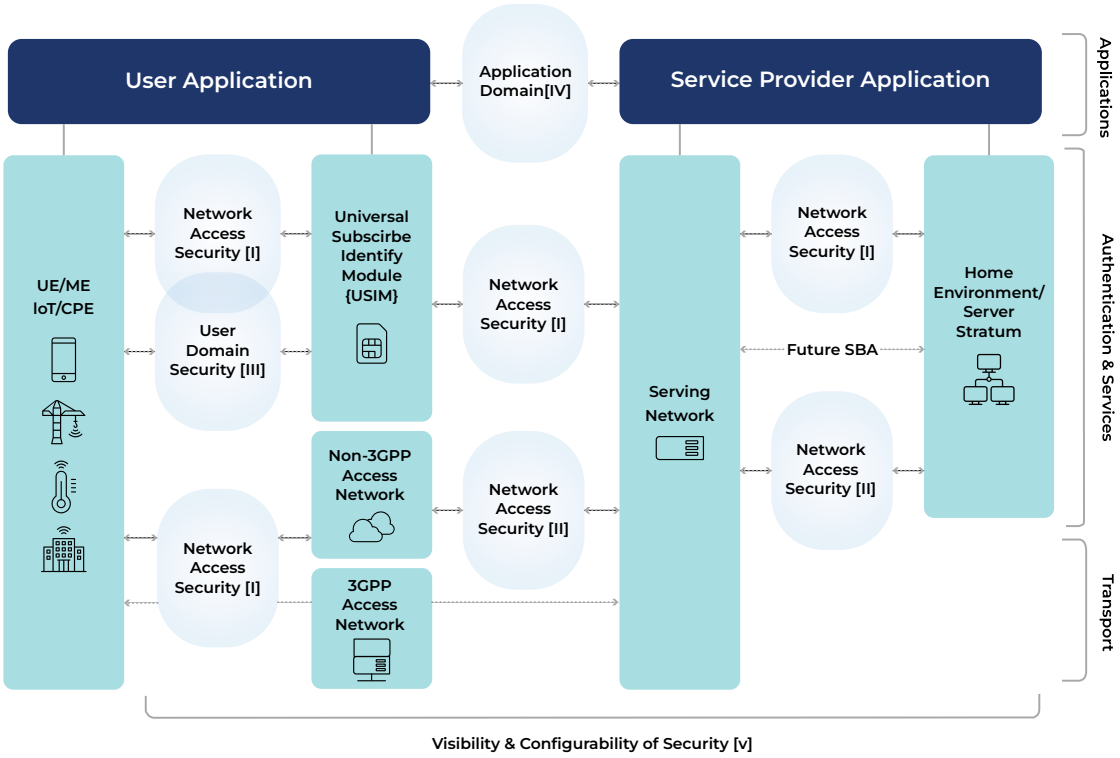
Application Domain Security

Enables applications in the user domain with applications and application providers for secure message exchange.

Visibility and Configurability of Security

Informs users and providers whether security features are functioning.

[3] https://ongoalliance.org/wp-content/uploads/2022/12/OnGoA-Security-Whitepaper-1.01_Final.pdf



5G Security Expansion[4]

While 5G began its roll-out in 2021 and coexists with 4G devices and networks, it is expected to overtake 4G in 2025.[5] Several security-related advancements have been made with 5G, specifically because it is the first generation developed with security protocols specific to unique devices and use cases in mind. The Third Generation Partnership Project (3GPP), the main standards organization that developed 5G standards, developed the following security enhancements to 5G:

Subscriber Security and Privacy

- Encryption of unique device identifiers to mitigate rogue base stations
- Mutual authentication of subscriber and network.
- Confidentiality and integrity protection for control (signaling) traffic and user (data) traffic.
- Ability to restrict radio technologies that a device uses (e.g., turn off 2G/3G).

[4] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

[5] https://www.gsma.com/mobileeconomy/wp-content/uploads/2022/09/290922-Mobile-Economy-North-America-2022.pdf

RAN Security and Privacy

- Use of a massive number of antennas and beamforming techniques to reduce interference and make it harder to conduct over-the-air eavesdropping attacks.
- RAN is separated into distributed units (DUs) and centralized units (CUs), with DUs located near the antenna and CUs, which store sensitive information, placed inside a trusted and physically secure location.

Core Network Security

- Shift to service-based architecture with Transport Layer Security-based authentication and encryption.
- Options for internet Protocol Security and attribute-based security across each interface.
- Service-based discovery and registration to support confidentiality, integrity, and replay protection.

Roaming Security

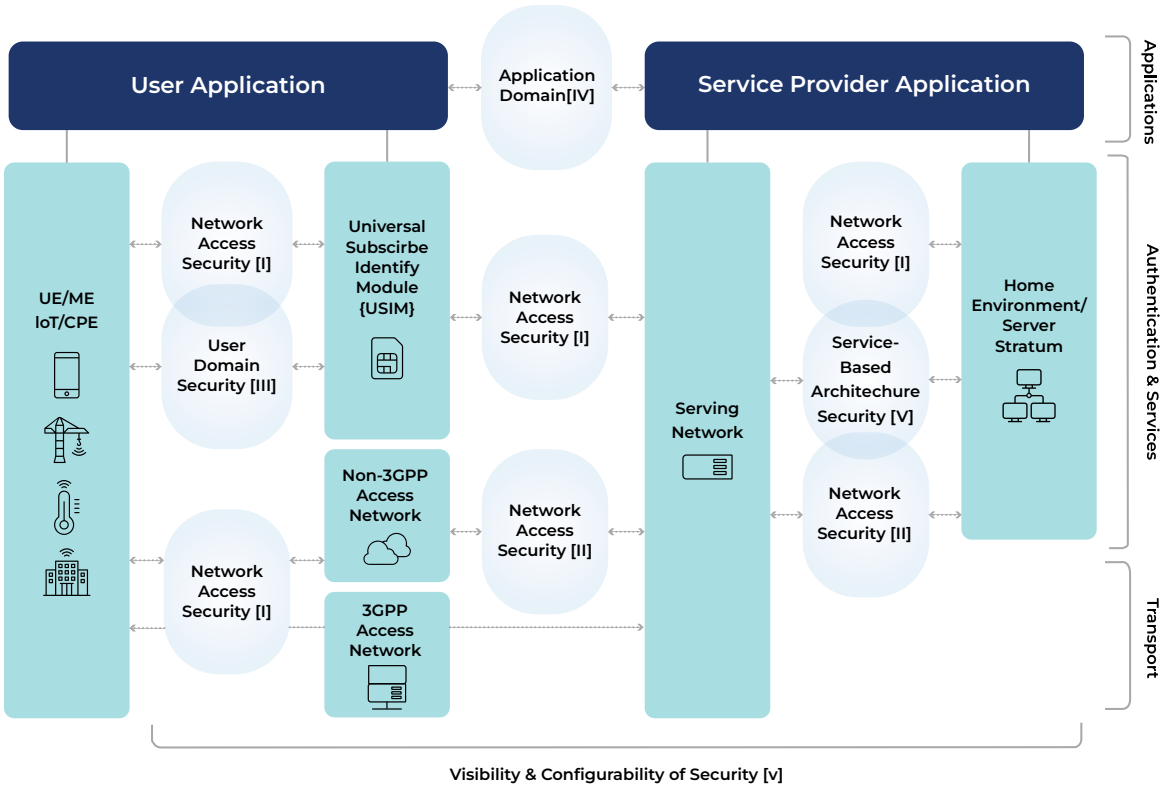
- Security gateway for roaming interconnects to enforce control plane security policies.
- Home network can verify if a device is present in the serving network when it receives a service request from the serving network.
- Protection of user plane traffic between two networks.

Network Slicing and Virtualization

- Network slicing allows isolation of data plane traffic as well as different security attributes for various user classes.
- Software-defined, virtualized network functions allow for rapid reconfiguration to respond to attacks.

Authentication

- Subscriber authentication is completed by the home network (helps protect against false base station attacks).
- Authentication is open and agnostic to the RAN. Both 3GPP and non-3GPP access networks (e.g., Wi-Fi) use the same authentication procedures.



Defining an Enterprise Threat Model for Private Cellular Networks

By expanding an enterprise network's reach, private cellular networks increase possible threat surfaces. As new devices and systems go wireless, there are more opportunities and sources for bad actors to infiltrate. This is especially true with IoT and the mass proliferation of sensors in some verticals where vulnerability to data leaks could exist. As noted earlier, many of these threats are likely familiar to enterprise risk managers, who may already be addressing these threats in their overall network security policies.

The US, the Cybersecurity and Infrastructure Security Agency (CISA), the DHS Science & Technology Directorate (S&T), and the Department of Defense (DOD) published a joint paper[6] that reports on their assessment of possible threats in private mobile networks, to help **"enterprise risk managers prioritize security activities and identify the security capabilities needed to mitigate threats relevant to the 5G systems and subsystems within their 5G-enabled boundary."**

[6] https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf

They outline the following potential threats to private 5G subsystems:

5G User Equipment (UE)

- Malware
- IoT botnet
- Eavesdropping
- User tracking
- Device-to-Device attack
- Radio capability downgrade
- Lost/stolen UE

5G Radio Access Network (RAN)

- Jamming
- Exploit open interfaces (Open RAN open-source standard)
- Rogue base station
- Physical damage
- Eavesdropping air interfaces
- Vulnerable/counterfeit components

5G Core

- Misconfigured functions
- Steal user data/fraud
- Denial of Service (DOS)/Distributed Denial of Service (DDOS)
- Malicious Code
- Outages
- Network function compromise

Multi-Access Edge Computing (MEC)

- Exposure of sensitive data
- User tracking
- Attacks on unsecured apps
- Physical attacks
- Manipulated/deleted data

Network Slicing

- DoS on other slices from insufficient slice resource management
- Data leakage between slices
- Unauthorized access to network slice
- Poorly designed or implemented network slice template

Orchestration and Management

- Modify messages/sessions
- Feed false data to artificial intelligence (AI)/machine learning (ML) algorithms
- Time manipulation
- Compromise software defined networking (SDN) controller
- Policy attacks
- Attack on VM image data store

Cloud/Virtualization

- Virtualization compromise: virtual machine (VM)/hypervisor/container/container platform
- Virtual network function (VNF)/cloud-native network function (CNF) image modification
- Improper tenant isolation
- Attack on application program interfaces (APIs)/Gateways
- Eavesdropping
- Vulnerable open-source code

While many of these threats are common and familiar to enterprise network security experts, the OnGo Alliance's Network Services Task Group and Coexistence Task Group published an in-depth analysis of approaches to augmenting enterprise network security strategies specific to OnGo networks.

OnGo Network Security

The OnGo Network is designed to provide secure wireless communication and support various deployment types such as public, private, neutral host, and fixed wireless access networks. Security is a key consideration in the OnGo system as it is intended to prevent interference with incumbent systems.

The security of OnGo networks is based on the 4G/5G wireless standards and provides a holistic security framework to connect devices from trusted and untrusted networks. The system includes components such as Citizens Broadband Radio Service Devices (CBSDs), Domain Proxies (DPs), Environmental Sensing Capability (ESC), and other SAS members that are vulnerable to attack, and the compromise of these components can impact the confidentiality, integrity, and availability of communication within the CBRS ecosystem. OnGo private networks have non-SIM/eSIM authentication options, and the system requires a minimum of Transport Layer Security (TLS) protocol 1.2 to protect and exchange authorization information and communications between the SAS and CBSDs.

Get access to the comprehensive OnGo Security Framework

The CBRS architecture is designed to protect against DoS attacks and preserve the confidentiality, integrity, and availability (CIA) of information security. The CBRS control plane specifications ensure that communication channels are protected using TLS and entities must acquire a digital certificate from a legitimate CBRS Certificate Authority (CA) to establish a connection. The CBRS Public Key Infrastructure (PKI) infrastructure governs the issuance of digital certificates used to prove the identity of CBRS components when communicating with other components within the CBRS ecosystem.

The OnGo network can incorporate legacy industrial devices such as Supervisory Control and Data Acquisition (SCADA) systems by connecting them to a gateway that aggregates the data for transmission. However, incorporating these devices into the network creates security challenges that need to be addressed in the network planning.

Fault, Configuration, Accounting, Performance, and Security (FCAPS) is a well-known network management framework often used by IT organizations. Each FCAPS management element such as Fault, Configuration, Accounting, Performance, and Security can impact security, and security controls must be in place to protect against data breaches and unauthorized access. Private OnGo networks are more likely to be operated by a single provider using the FCAPS or similar framework, while public and neutral host OnGo networks may require trust mechanisms and security controls consistently applied across multiple providers.

Overall, the OnGo ecosystem will rely more on software security design principles as network functionality moves to virtual network functions at the distributed edge and cloud. Security mechanisms, such as the zero-trust network access (ZTNA) security model and Secure Access Service Edge (SASE) framework for equipment and virtual network functions, and the virtualization and disaggregation of the core network and Open RAN, are necessary, as is securing interconnection between server elements, especially when Open RAN/O-RAN splits are deployed in multiple locations and data centers.

Conclusion

Private cellular networks can transform enterprises by leveraging the intersection of broadband connectivity with high mobility applications to securely realize the potential of advanced technologies. The OnGo Alliance was formed to evangelize CBRS technology, use cases, and business opportunities.

More information about OnGo advancements, including a directory of OnGo partners.

Visit Here

About OnGo Alliance

The OnGo Alliance™ is a coalition of 185+ member companies, including mobile operators, cable operators, managed service providers (MSPs), mobile virtual network operators, enterprises, and more. The mission of the OnGo Alliance is to evangelize 4G and 5G OnGo technology, use cases, and business opportunities while simultaneously driving technology developments necessary to fulfill the mission, including multi-operator capabilities. The Alliance also established an effective product certification program for OnGo equipment in the U.S. 3.5 GHz band, ensuring multi-vendor interoperability. The certification program and specifications enable the commercialization of the OnGo architecture and ensure seamless interoperability for all network components. The certification program ensures all OnGo-Certified Devices reflect the performance and interoperability standards that have been set and promised to customers.

OnGo alliance™