The Security of Verizon's 5G Network

Network Security Planning Version 1.0

verizon

August 2020

Table of Contents

List of Figures

Executive Summary

At Verizon, security is a driving factor in how we build and operate our 5G network. Our goal is to make sure every element of our 5G network implements security controls that deliver confidentiality, integrity, and availability so the overall network provides subscribers with a secure communications channel, and security is yet another factor that makes our wireless network best in class.

Verizon has structured our approach for securing our 5G network around four pillars:

- Leveraging Verizon's global security capabilities;
- Deploying security features from 5G standards;
- Enhancing security via features specific to Verizon's 5G implementation;
- Inserting customer-facing security services.

1.1 Global Security Capabilities

The first pillar of Verizon's approach to securing our 5G network is leveraging the existing global security capabilities that we have in place. These include:

- Enterprise Protections such as physical security of our facilities, penetration testing of key systems, an enterprise vulnerability management program, global security operations centers, supply chain security practices, and security governance programs.
- Partnerships with industry groups such as the Communications Information Sharing and Analysis Center (Comm ISAC), the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), and the Alliance for Telecommunications Industry Solutions (ATIS).
- A Global Backbone network providing visibility into worldwide threat-actor behavior that Verizon uses to inform the defense of its networks.

1.2 Features in 5G Standards

The second pillar of Verizon's approach to securing our 5G network is leveraging new security features that are part of 3GPP's 5G standards. Verizon's 5G network will implement numerous optional features to enhance security, and 3GPP's new trust model and security architecture has influenced our implementation decisions.

- User Equipment (UE) security features include protecting information that could be used to identify and track a subscriber, preventing attackers from modifying user traffic, and ensuring subscribers only connect to trusted cell sites.
- Radio Access Network (RAN) security features provide secure communications on all RAN interfaces and include extra protections at places that are vulnerable to physical attacks.
- Core Network security features include specialized Network Functions (NFs) and enhanced protections for the new Service-Based Architecture (SBA) that NFs will use to communicate.

1.3 Unique Verizon Capabilities

The third pillar of Verizon's approach to securing our 5G network is enhancing security by building in unique features. We take advantage of the flexibility in 5G standards to design, implement, and deploy our network with this heightened security posture.

- Design decisions include building upon Verizon's robust 4G LTE security principles as well as tailoring redundancy models and security protections for each NF based on functionality.
- Implementation aspects include a robust device certification process, hardening key infrastructure services and network interfaces, and securely provisioning and booting NFs.
- Deployment capabilities involve utilizing core services such as PKI, access management, security analytics, vulnerability scanning and software scanning.

1.4 Enabling Customer-Facing Services

The fourth pillar of Verizon's approach to securing our 5G network is using 5G's new capabilities to enable new customer-facing security services. 5G provides unprecedented flexibility and agility to create services on demand at locations throughout the network. We will leverage this to offer customers new services that were otherwise not possible.

- Network Slicing will provide various levels of isolation and resource guarantees to customers.
- Orchestration will dynamically instantiate security services for customer applications and devices.
- Edge Computing will host latency-sensitive, network-based security services that are tailored for customer applications and devices.

1.5 Key Examples

We highlight some key examples of the security capabilities in Verizon's 5G network:

- UEs on Verizon's network will automatically use an encrypted identifier, called the Subscription Concealed Identifier (SUCI), when authenticating to the network. The SUCI is generated using cryptographically strong encryption keys that come preconfigured in a tamper-resistant hardware element on the device, and it encrypts metadata that could otherwise be used to track a user and compromise their privacy.
- 5G networks break down large, multi-purpose NFs from 4G LTE into smaller, single-purpose NFs that are deployed in a distributed manner. Verizon 5G leverages this disaggregation to deploy NFs in a way that eliminates single points of failure and minimizes the blast radius of an NF outage or security issue. In other words, a malfunctioning NF will impact a smaller number of customers than a similar failure would in 4G LTE.
- The distributed 5G RAN will have NFs at the edge of the network, potentially at unmanned locations or sites with minimal physical security. Verizon's network will ensure these distributed NFs cannot access cryptographic keys protecting subscriber traffic thereby protecting the traffic from an attacker physically compromising the site.
- The SBA in Verizon's 5G Core will cryptographically authenticate the identities of any NFs trying to communicate, encrypt all NF communications, and cryptographically authorize communications between NFs using modern security standards such as X.509v3 certificates, TLS 1.2, and OAuth.
- Verizon 5G devices go through a rigorous certification process to ensure they are not introducing vulnerabilities into our network, including penetration testing by a specialized team that has deep understanding of how cellular networks work.
- 5G NFs will be deployed as Virtual NFs (VNFs) or Containerized NFs (CNFs) that run on top of a cloud platform. In Verizon's 5G network, these VNFs and CNFs run on the Verizon Cloud Platform (VCP), Verizon's internal cloud. Verizon is hardening VCP using a defense-in-depth approach such as trusted boot for VCP's physical servers, host-based security monitoring tools to protect the OS, and SELinux controls to protect the VNFs/CNFs. We are also building security capabilities natively into VCP that VNFs and CNFs can seamlessly leverage as they deploy (e.g., firewalling, DoS protection).
- The network interface providing subscribers with Internet access has significant attack exposure since attackers anywhere on the Internet can access it. As a result, the Verizon 5G network will have considerable protections on this interface to include packet filtering, rate limiting, DoS protection, and detection/prevention of malware.
- All NFs in Verizon's 5G network will leverage a common PKI for identity. The PKI will include a CA hierarchy designed specifically for 5G, and it will provide full lifecycle management of the 5G identity certificates.

Since 5G is an evolution of 4G LTE, these four pillars and their associated features build upon 4G security, improve it in key areas, and provide an overall higher level of security in 5G than in 4G LTE. Verizon's 5G implementation goes further by building in additional capabilities to make our 5G security a differentiator in the marketplace. Combined together, these things make Verizon's 5G a network more secure than what was possible before and ultimately enable the 4th Industrial Revolution.

Overview

To fully realize their potential, 5G networks must be secure. 5G is an evolution of 4G LTE, and from this perspective, 5G provides more security than 4G LTE since 5G builds upon 4G LTE security and improves it in key areas.

At Verizon, security is a driving factor in how we build and operate our 5G network. Our goal is to make sure every element of our 5G network implements security controls that deliver confidentiality, integrity, and availability so the overall network provides subscribers with a secure communications channel. We also incorporate features that enhance subscribers' security above and beyond just securing the communications channel; for example, by protecting their devices from Denial of Service (DoS) attacks. In doing so, we believe security will continue to be yet another factor that makes our wireless network best in class.

Our approach to 5G security is structured around the four pillars shown in Figure 2-1: leveraging Verizon's global security capabilities; deploying security features from 5G standards; enhancing security via features specific to Verizon's 5G implementation; and inserting customer-facing security services. The rest of the paper discusses each pillar in detail.

Figure 2-1: Four Pillars of Verizon's 5G security approach

Scope

We describe Verizon's approach for building and operating a secure 5G network, the security features we implement, and key attacks we mitigate. Instead of providing an exhaustive list of 5G security capabilities, we focus on specific items in Verizon's network that provide an extra level of security.

As illustrated in Figure 2-1, we use the term "5G network" to include the 5G Radio Access Network (RAN) and 5G Core Network (5GC) as defined by 3GPP [1]. We also include the procedures and mechanisms end-user devices (called User Equipment, or UE) use to connect to the network. We do not cover general security for UEs (e.g., security of the UE's operating system) nor the security of other network components such as the IP Multimedia Subsystem (IMS) and Packet Data Network (PDN).

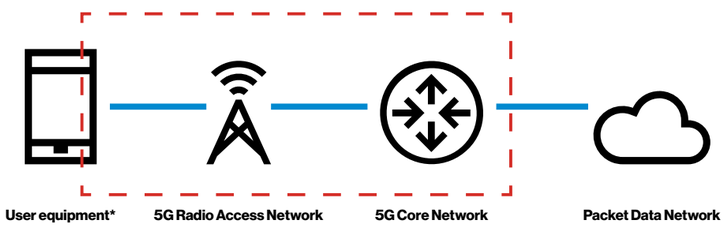


Figure 3-1: Scope covered by this paper.
*Only the procedures and mechanisms the UE uses to connect to the network are in scope.

Scope

5G is a complete overhaul of 4G LTE network components, so Verizon will deploy 5G in a phased approach. However, 4G LTE's large installed base means it will exist for a long time. As a result, 4G LTE and 5G networks must coexist for the foreseeable future, and there are many deployment models for doing so. Figure 3-1 shows the standardized deployment models. This paper will describe the security features associated with Option 2 and Option 3x.

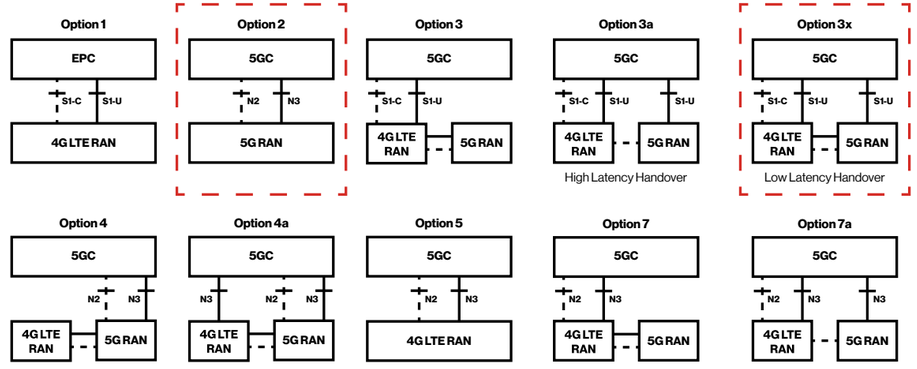


Figure 3-2: 5G deployment models.
This paper will focus on Option 2 and Option 3x. Note that 3GPP is negotiating with the International Telecommunication Union (ITU) as to which RAN technologies will qualify for the "5G" designation, so this figure may change as those decisions are made.

In both 4G LTE and 5G, the Evolved Packet Core (EPC) and 5GC, respectively, dictate which standards-based security features are available. As shown in Figure 3-2, Option 3x uses the EPC. Therefore, the standards-based security features available in Option 3x are essentially the same as those available in 4G LTE. Because this paper is focused on security features unique to 5G, we will not cover the EPC-based security aspects of Option 3x in detail.

5G will be deployed in a phased approach, so the security features described in this paper will become available as various 5G components are deployed. This paper is not meant to provide a 5G deployment timeline, so the security features described here will represent the end state environment when 5G elements are fully deployed instead of representing a specific point in time during 5G deployment.

We also do not provide a formal threat analysis of new risks in 5G or risks carried over from 4G LTE since other works already discuss these things; see for example [2]. Instead we focus on specific security capabilities Verizon's 5G network will implement and the attacks they mitigate.

Finally, we will not describe the general 5G architecture or functionality, the 5G standards development process, or Verizon's overall security programs.

Global Security Capabilities

The first pillar of Verizon's approach to securing our 5G network is leveraging the existing global security capabilities that we have in place. We only outline these capabilities since they are not specific to 5G.

- Enterprise Protections: Verizon has many enterprise capabilities to protect itself as a company and to protect its network. These include things such as physical security of its facilities, penetration testing of key systems, an enterprise vulnerability management program, global security operations centers, supply chain security practices, and security governance programs.
- Partnerships: Verizon participates in groups such as the Communications Information Sharing and Analysis Center (Comm ISAC), the FCC's Communications Security, Reliability, and Interoperability Council (CSRIC), and the Alliance for Telecommunications Industry Solutions (ATIS) to promote security and leverage best practices and lessons learned from the industry.
- Global Backbone: Verizon's global backbone network provides visibility into worldwide threat-actor behavior, and Verizon uses this visibility to inform the defense of its networks.

Features in 5G Standards

The second pillar of Verizon's approach to securing our 5G network is leveraging the new security features that are part of 3GPP's 5G standards.

3GPP designed 5G security around the trust model shown in Figure 5-1 where network functions (NFs) in the inner circles of the figure are more trusted that network functions in the outer circles. The trust model influenced decisions in the design of 5G security; for example, by ensuring sensitive data and encryption keys from higher-trust network functions are not available to lower-trust ones.

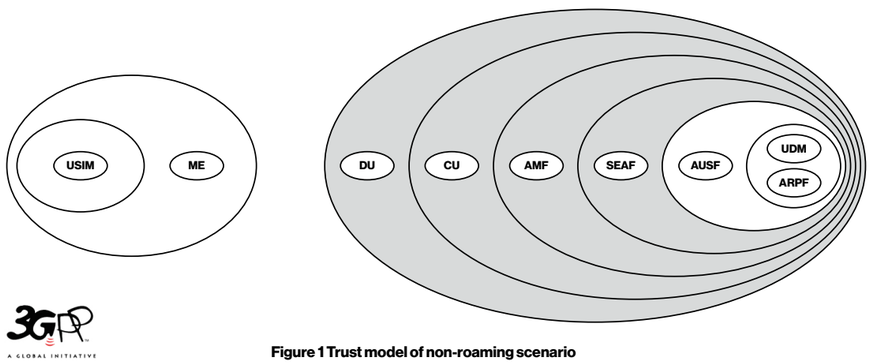


Figure 5-1: 5G trust model.
Source: https://www.3gpp.org/news-events/1975-sec_5g.

3GPP also organized 5G's security features around a new security architecture shown in Figure 5-2. Security features provided by each architectural domain enable the interactions in the figure.

Features in 5G Standards

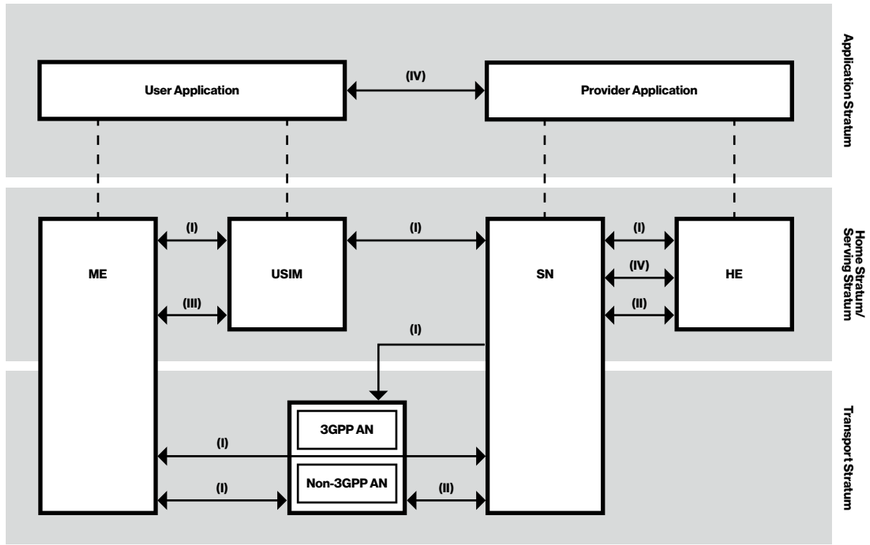


Figure 5-2: Six Domains of the 5G Security Architecture:
Network Access Security (I); Network Domain Security (II); User Domain Security (III); Application Domain Security (IV); Service-Based Architecture Domain Security (IV); Visibility and Configurability of Security (VI).
Note that Domain VI is not shown. Source: [2].

Verizon's 5G network implements this trust model and security architecture. However, since 5G's new security features require the 5GC, they are only applicable to 5G Option 2 deployments.

Many of 5G's new security features are optional, so we provide an overview of key features that Verizon will implement along with relevant details on how Verizon will implement the feature. We do not provide a comprehensive list of every security feature in the 5G standards, especially those that are mandatory or existed in 4G LTE. The full list of security features and detailed specifications for each feature can be found in [3]. We organize our descriptions around different parts of the network: UE; 5G RAN; and 5G Core

5.1 UE

5G enhances security by adding new protections for communications between the UE and the network and strengthening the authentication procedures the UE uses to connect to the network.

5.1.1 Enhanced Subscriber Privacy

A UE must identify itself and the subscriber using it when connecting to a cellular network. This allows network operators to restrict network access to only authorized devices and subscribers. 3GPP-based networks such as 5G identify subscribers by assigning a globally unique identifier to each subscriber and having the UE send the subscriber's identifier to the network during the connection process. In 5G this identifier is called the Subscription Permanent Identifier (SUPI). 5G specifications add a new security feature that requires UEs to identify themselves during the network connection process using a different identifier, called the Subscription Concealed Identifier (SUCI), instead of the SUPI. This increases security because UEs can create the SUCI by encrypting the parts of the SUPI that could identify a subscriber. This prevents attackers from observing the connection procedure, capturing the subscriber's identifying information (e.g., by using a Stingray), and then tracking the subscriber's location

UEs in Verizon's 5G network will by default create the SUCI using a public encryption key from Verizon's network in combination with a unique ephemeral key generated by the UE upon each connection attempt. This means that neither passive attackers (i.e., eavesdroppers) nor active attackers (e.g., spoofed base stations) will be able to follow a UE's SUCI over multiple connections – the ephemeral key causes the SUCI to change for each connection. Furthermore, attackers will not be able to obtain details in the SUPI that identify the subscriber since Verizon is the only entity with access to the private key needed to decrypt the SUCI. As a result, attackers cannot track or identify subscribers on Verizon's 5G network using the SUCI.

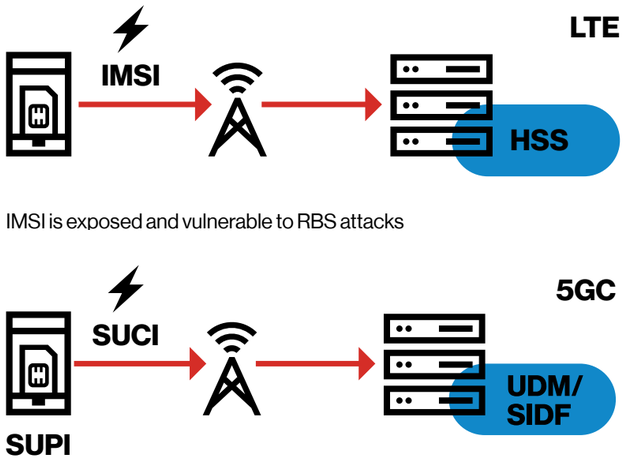


Figure 5-3: UEs send the SUCI to the 5G network during the connection process to protect against Rogue Base Station attacks (RBS).

5.1.2 User Plane Integrity Protection

A UE transmits user traffic (e.g., photos, web traffic, text messages) to the cellular network via the User Plane. This is in contrast to the Control Plane, which transmits network management and scheduling messages. Both 4G LTE and 5G allow the UE to encrypt the User Plane to protect users' privacy. However, researchers have shown that attackers can exploit a lack of User Plane integrity to maliciously redirect traffic; for example, to send a UE's DNS queries to a malicious server [4].

5G adds a new security feature that gives UEs the option to provide integrity protection for the User Plane in addition to encrypting it. UEs in Verizon's 5G network will by default provide integrity protection for the User Plane using the 128-NIA1 and 128-NIA2 algorithms. UEs in Verizon's 5G network that use these algorithms will also provide bidding down protection to ensure attackers cannot cause the UE to use less secure algorithms.

5.1.3 Stronger Roaming Authentication

Allowing UEs to roam onto partner networks creates multiple opportunities for attack: attackers can trick UEs to connecting to malicious networks; partner networks can pretend UEs are currently roaming on their networks when they are not; or a rogue UE can trick a partner network to allow it to connect.

5G's new authentication procedure, called 5G Authentication and Key Agreement (5G-AKA) and illustrated in Figure 5-4, improves security by cryptographically guaranteeing two things. First, it ensures the subscriber's home network operator authenticates the UE and the roaming network the UE is joining instead of having only the roaming network perform authentication. This prevents UEs from being tricked into joining unauthorized partner networks. Second, it incorporates procedures to ensure that a UE is actually connected to the roaming network. This prevents billing fraud against the home network operator. It also ensures information about the UE and subscriber needed to establish a network connection (e.g., SUPI) are only shared with authorized partner networks. Verizon's 5G network will implement these authentication procedures by default.

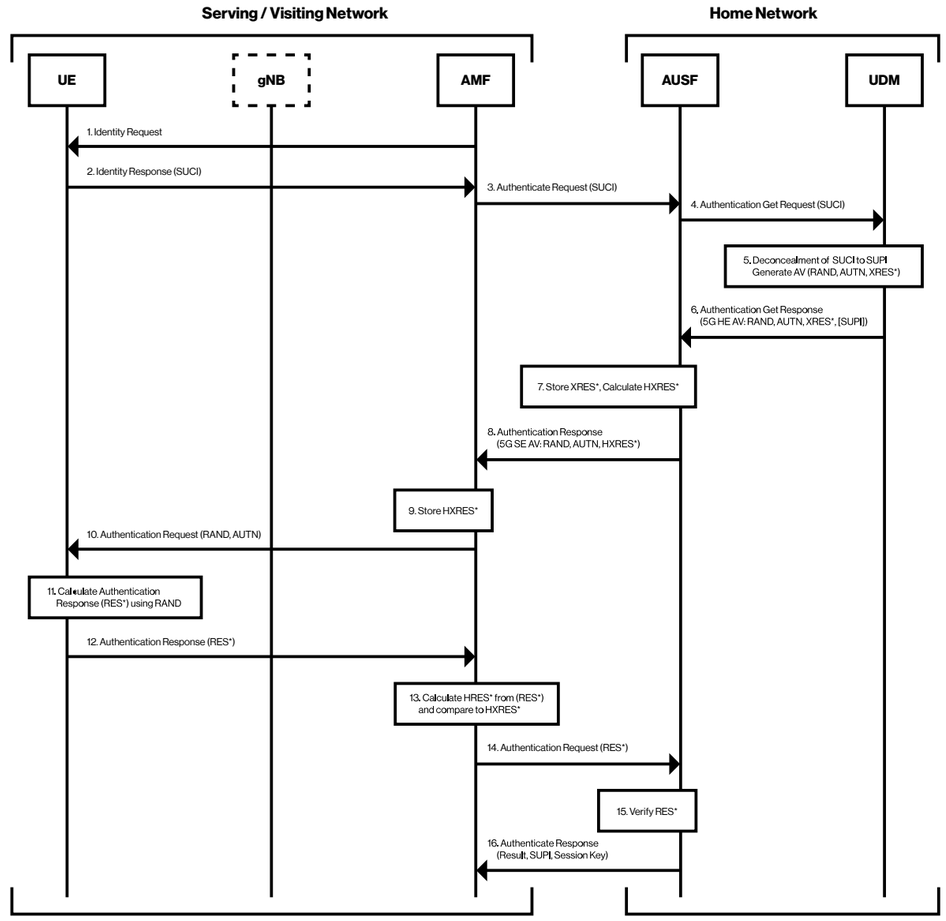


Figure 5-4: 5G-AKA authentication during UE roaming.
The subscriber's Home Network operator must authenticate that both the UE and the roaming network (Visiting Network) are valid in order for a connection to be established and any subscriber information shared with the roaming network. Source: [3].

5.1.4 Authentication Flexibility

While not a direct security improvement per se, 5G also adds features that make it easier to strongly authenticate a UE. In particular, UEs can use 3GPP-specified authentication protocols, 5G-AKA from above and the Extensible Authentication Protocol (EAP) Authentication and Key Agreement (EAP-AKA'), to authenticate to both 3GPP networks and non-3GPP networks such as Wi-Fi. Prior to 5G, UEs could only use 3GPP-specified authentication protocols with 3GPP networks. 5G networks also inherently support UE authentication via an external network and the associated credentials on that network (e.g., an enterprise network can authorize its corporate-owned UEs using its corporate LDAP server).

5.1.5 Secondary Authentication and Authorization

Verizon's 5G network will further expand this flexibility so that external network operators can perform an independent level of authentication and/or authorization (e.g., separate authentication/authorization server and credentials) before the Verizon 5G network allows a UE to connect to the external network. In this use case, the Verizon 5G network will perform the primary authentication when the UE tries to connect to the 5G network. Then, when the UE tries to access the external network, the 5G network will use EAP to request the external network perform a secondary authentication/authorization and only permit connectivity after the external network approves.

5.2 RAN

The 5G RAN provides secure communications on all RAN interfaces and include extra protections at places that are vulnerable to physical attacks.

5.2.1 Restricting Sensitive Data

As shown in Figure 5-5, the 5G RAN, often referred to as a gNodeB (gNB), could be composed of Radio Units (RUs), Distributed Units (DUs), and Central Units (CUs) that may be collocated or distributed in various configurations. Note the DUs and CUs may be deployed as Virtual Network Functions (VNFs), in which case they will be denoted vDU and vCU, respectively. The RUs and DUs sit the edge of the network, and therefore network operators could deploy them in unmanned locations or sites with minimal physical security. This leaves sensitive data vulnerable to physical attacks if they are sent through the RU/DU unencrypted or if the RU/DU possess keys used to decrypt them.

Because of this threat model, the 5G key hierarchy ensures that, when the network activates confidentiality protection for UE communications (i.e., encryption), the network operator can distribute encryption keys such that the RU and DU cannot view the confidentiality-protected data. In other words, the RU and DU do not have the encryption keys. To prevent these attacks, Verizon's network will implement confidentiality protection and ensure the RU/DU do not have access to the encryption keys.

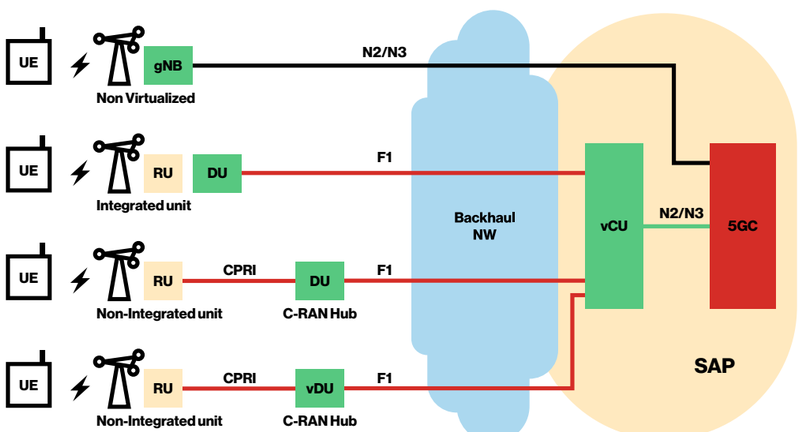


Figure 5-5: 5G RAN architecture. When confidentiality protection is enabled, the 5G key hierarchy allows the network operator to ensure the RU and DU cannot decrypt UE communications

5.2.2 RAN Interface Protection

Both 4G LTE and 5G networks can implement a RAN that is disaggregated into RU, CU, and DU components. However, the split is natively part of the 5G specifications, and, as shown in Figure 5-5, native disaggregation introduces a new standardized F1 interface for both the Control Plane (F1-C) and User Plane (F1-U) as well as new interfaces N2 and N3 to the 5GC. Although not shown in the figure, the architecture also introduces a new E1 interface between multiple CUs. All of these interfaces carry sensitive traffic, and attackers modifying or reading that information can cause significant network disruptions.

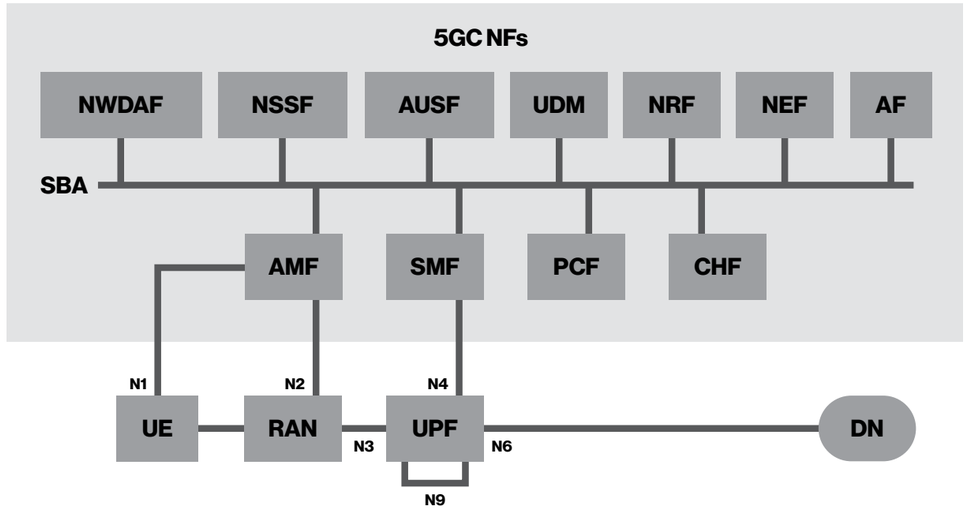
The 5G standards mandate confidentiality, integrity, and replay protection for the F1-C and E1 interfaces, and network operators have the option to use those capabilities on the F1-U, N2, and N3 interfaces. Verizon's 5G network will use IPSec to implement confidentiality, integrity, and replay protection on all these interfaces when equivalent protections are not provided by the underlying transport networks.

5.3 Core Network

The 5GC enhances security by adding specialized NFs for security within an operator's network and with roaming partners and introducing a Service-Based Architecture (SBA) for NF-to-NF communications.

5.3.1 Security-Enhancing NFs

Figure 5-6 shows some of the NFs introduced by the 5GC. Many of them including the AUSF, NRF, and UDM are specifically focused on improving the 5G network's security posture. It is beyond the scope of this document to describe each of these NFs in detail, so the reader is referred to the relevant 3GPP documents.



AF	Application Function	**NSSF**	Network Slice Selection Function
AMF	Access & Mobility Management Function	**NWDAF**	Network Data Analytics Function
AUSF	Authentication Server Function	**PCF**	Policy Control function
CHF	Charging Function	**SMF**	Session Management Function
DN	Data network	**UDM**	Unified Data Management
NEF	Network Exposure Function	**UPF**	User plane Function
NRF	Network Function Repository Function		

Figure 5-6: 3GPP Release 15 5G Architecture, Services-Based Representation.

5.3.2 SBA Protection

5G standards introduce a new architectural option for NF-to-NF communications in the 5GC: the Service-Based Architecture (SBA) shown Figure 5-6. Because the 5GC NFs communicate network-critical messages and process the network's most sensitive data, implementing the correct security capabilities on the SBA is critical for ensuring the overall 5G network is secure.

5G standards mandate that all 5GC NFs validate incoming messages according to protocol specifications and network state. The standards also dictate that network operators have the following options: provide confidentiality, integrity, and replay protection for messages on the SBA; require NFs to request authorization and hide sensitive data (e.g., service topology) during registration, discovery and service request; and implement mutual authentication when two 5GC NFs communicate.

Verizon's 5GC will implement mutual-authentication between NFs using client X.509v3 certificates, and it will protect SBA messages using TLS 1.2 (and TLS 1.3 in the future). Our 5GC will also use OAuth-based JSON Web Tokens issued by the NRF to authorize access to NF services, and it will securely transport the tokens using TLS 1.2.

5.3.3 Inter-Operator Security

5G allows providers other than the subscriber's home network operator to deliver network services. Roaming onto another operator's network when the subscriber is outside the home network operator's coverage area is a common example of this. However, 5G also enables other use cases where providers might offer value-added services directly into the home operator's network. Interfaces to external providers (who might be at lower security levels) opens up a likely avenue for attackers.

The 5GC adds specific NFs to securely communicate over and protect these external interfaces. As above, a detailed description of these NFs is outside the scope of this document, but we do highlight that one NF, the SEPP, plays a key role here by negotiating secure external connections using TLS and providing application layer security using JSON Web Encryption.

Unique Verizon Capabilities

The third pillar of Verizon's approach to securing our 5G network is enhancing security via specific features that are unique to Verizon's 5G implementation. While 5G standards specify security features and options that network operators may implement, the standards do not address many details/decisions needed when building a network. Because Verizon views security as a key component of our best-in-class network, we use this implementation flexibility to build in unique security features to our 5G network. Below, we describe how we do this in terms of secure design, secure implementation, and security services.

6.1 Design

The security of Verizon's 5G network begins with a mindset that security is a critical feature of the network that contributes to our superior network performance. This is reflected in key areas.

6.1.1 4G LTE Security

Verizon's 4G LTE network was designed with security and reliability in mind, and it is one reason our 4G LTE network is best in class. 4G LTE security designs support 5G security in two ways. First, they are directly used in 5G Option 3x deployments. Second Verizon is carrying over the design and operational principles used for the 4G LTE to 5G.

6.1.2 Smaller Blast Radius

A key feature of the overall 5G network architecture is breaking down large, multi-purpose NFs from 4G LTE into smaller, single-purpose NFs that are deployed in a distributed manner. The splitting of the 5G RAN into RU, CU, and DU components described above is an example of this, and similar disaggregation has occurred when moving from the EPC to the 5GC. Verizon is taking advantage of this disaggregation to enhance the security of its network by structuring NF deployment to minimize the blast radius of a NF that has an outage or other security issue. In other words, our network is designed such that malfunctioning NFs will impact a smaller number of customers than they would in 4G LTE. Examples of this include isolating critical NFs at the network layer using of IP subnets or VLANs or at the compute/storage layer by using dedicated resources.

6.1.3 NF Redundancy

Related to the item above, Verizon will leverage the disaggregated nature of 5G NFs to efficiently tailor our deployments such that critical NFs have higher redundancy than non-critical NFs. For example, we can use 2N redundancy for critical NFs and N + 1 redundancy for non-critical NFs. We can also tailor this redundancy on-demand as network and threat conditions change so our risk level is always constant.

6.1.4 NF Protections

Continuing with the theme of disaggregation, Verizon will use the disaggregated nature of 5G to efficiently tailor our network-based security protections such that critical NFs are protected with more capabilities than non-critical NFs. For example, we can provide sophisticated Denial of Service (DoS) protections, network-based Intrusion Detection Systems (IDS) protections, or enhanced monitoring for critical NFs. We can also tailor protections on-demand as network and threat conditions change to actively manage our risk level.

6.2 Implementation

We will implement Verizon's 5G network using secure supporting infrastructure components such as a device certification program, private cloud, and orchestration systems as well as supporting processes such as auto-provisioning. We have built these infrastructure systems and processes specifically with 5G in mind. Below we provide highlights and examples of how these things enhance the security of Verizon's 5G network.

6.2.1 Device Certification

5G devices will go through a rigorous certification process to ensure they are not introducing vulnerabilities into our network. This process includes multiple levels of risk assessment and testing, to include penetration testing by a specialized team that has deep understanding of how cellular networks, especially Verizon's network, function. Furthermore, Verizon has specific technical requirements with which devices must comply before they are allowed on our network. These requirements include industry standards and best practices (e.g., using a dedicated processor, called a baseband or modem processor, to perform all network operations related to establishing 5G network connectivity) as well as Verizon-specific requirements (e.g., using an atomic procedure for firmware update failures, cryptographic certificate management) that improve security. Verizon works closely with device vendors to ensure any issues that are uncovered are fixed within predefined timelines.

6.2.2 Verizon Cloud Platform

Most 5G NFs will be deployed as VNFs or Containerized Network Functions (CNFs) that run on top of a cloud platform. In Verizon's 5G network, these VNFs and CNFs will run on the Verizon Cloud Platform (VCP), Verizon's internal cloud. Verizon is hardening VCP using a defense-in-depth approach such as trusted boot for VCP's physical servers, host-based security monitoring tools to protect the OS, and SELinux controls to protect the VNFs/CNFs. We are also building security capabilities natively into VCP that VNFs and CNFs can seamlessly leverage as they deploy (e.g., firewalling, DoS protection).

6.2.3 Secure Storage

The 5G security architecture depends on keeping many pieces of information private (e.g., subscriber credentials and encryption keys). Our infrastructure includes specific secure storage environments for these purposes. For example, we will use a Hardware Security Module (HSM) when storing subscriber credentials in the network and a Universal Integrated Circuit Card (UICC) when storing subscriber credentials on the UE. We will also tightly control access to these environments. For example, the UDR NF leverages an HSM that provides secure storage of credentials and other subscriber data that can only be accessed by the PCF, NEF and UDM NFs using resource-based access control procedures so the NFs only have access to the data for a defined period of time.

6.2.4 Management Interfaces

Any person or system accessing the management interface of a 5G NF (e.g., OA&M functions) will communicate with the 5G NF using secure connections that provide mutual authentication, integrity protection, and confidentiality protection with TLS 1.2 or SSH.

6.2.5 Internet Protection

Since the 5G network needs to transfer user-plane traffic to/from the Internet, a 5G NF called the UPF will be Internet-accessible via the N6 interface defined by 3GPP. This is shown in Figure 6-1. The N6 interface has significant attack exposure since attackers anywhere on the Internet can access it. The N6 interface also provides a critical service because the majority of subscriber functionality is not available without it. As a result, the Verizon 5G network will have considerable protections on this interface.

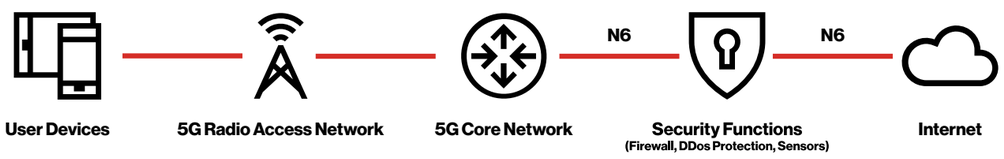


Figure 6-1: Protecting the N6 interface from Internet-based attacks.

6.2.6 Protecting Internal Network Connections

Each component of the 5G network (i.e., 5G RAN, 5GC) and the outside components that connect to it (e.g., OA&M systems, 4G LTE EPC) will use a dedicated and tailored security function with packet and URL filtering and DoS protection on the interface connecting the components. This will mitigate attacks such as a DoS flood from IoT devices over the N3 the interface.

6.2.7 Secure Auto Provisioning

The 5G network will need to auto-provision NFs as well as security features within an NF. For example, a gNB may be deployed at a remote site, and the 5G network must ensure that it comes online securely. As another example, the UICC in the UE needs to be provisioned with specific privacy attributes (e.g., the home network operator's public key) even when the UE is shipped to the subscriber directly from the UE manufacturer. In all of these scenarios, we are carefully designing the provisioning and boot procedures to mitigate security risks.

6.3 Deployment

Verizon has a number of core security services available to all elements within our network. Our 5G network will leverage these services as another mechanism for enhancing its security. We only provide an overview of each service and leave the specific details of the services' designs and capabilities to other documents.

6.3.1 Access Management

Securing access to an NF's management and control plane interfaces is a critical step for deploying 5G securely. Verizon's 5G Network will do this via 2 mechanisms: access managemnent systems using industry-standard protocols such as TACACS+; and a PKI whose CA hierarchy is built specifically for 5G.

6.3.3 Analytics

The disaggregated nature of 5G NFs means there will be many more elements in a 5G network than in 4G LTE, and network operators will need a way to deal with the tremendous amount of telemetry and logging data these 5G elements generate. Every element in Verizon's 5G network will send its telemetry and log data to a centralized big data platform that supports security operations by using everything from basic analytics to sophisticated machine learning models to look for and prioritize security issues.

6.3.4 Vulnerability Scanning

Verizon's 5G network will leverage a centralized Nessus deployment to scan for vulnerabilities in the NFs and supporting infrastructure as well as prioritize vulnerability remediation. We will also take advantage of the fact that VNFs and CNFs exist as software images to scan them with automated tools that look for vulnerabilities and unknown software.

Enabling Customer-Facing Services

The fourth pillar of Verizon's approach to securing our 5G network is using 5G's new capabilities to enable new customer-facing security services. 5G provides unprecedented flexibility and agility to create new services on demand at locations throughout the network. We will leverage these abilities to offer customers new services that were otherwise not possible. In this section, we provide an overview of the mechanisms that enable the agility and flexibility, but we will not describe specific customer-facing services as those have not been defined yet.

7.1 Network Slicing

Network slicing is the network's ability to automatically configure and run multiple logical networks as virtually independent business operations on a common physical infrastructure. The network may be sliced according to applications or devices. Slices enhance security because they allow the network to provide various levels of isolation and resource guarantees to customers.

7.2 Orchestration

Verizon's 5G network will leverage orchestration capabilities to dynamically instantiate NFs based on network conditions such as traffic load and security levels. This orchestration infrastructure is being built so it can also dynamically instantiate security services for customer applications and devices.

7.3 Edge Computing

Since 5G NFs will be virtualized on a cloud platform, there may be times where the cloud platform has extra capacity that can be used for non-network workloads. Using a network operator's cloud platform in this manner is called Edge Computing. Edge Computing will enhance security by offering a location to run latency-sensitive or bandwidth-heavy security functions that either cannot run in other locations (e.g., a public cloud environment or on a UE) or that achieve superior performance from running close to the UE. As above, these security functions can be tailored for customer applications and devices.

Summary

Verizon has structured our approach for securing our 5G network around the four pillars and associated elements shown in Figure 8-1. Since 5G is an evolution of 4G LTE, these things build upon 4G security, improve it in key areas, and provide an overall higher level of security in 5G than in 4G LTE.

Security is a driving factor in how we build and operate our 5G network. Our goal is to make sure every element of our 5G network implements security controls that ensure confidentiality, integrity, and availability so the overall network provides subscribers with a secure communications channel and security is yet another factor that makes our wireless network best in class.

Global Security Capabilities	Features in 5G Standards	Unique Verizon Capabilities	Enabling Customer-Facing Services
• Enterprise Protections • Partnerships • Global Backbone	• UE • RAN • Core	• Design • Implementation • Deployment	• Network Slicing • Orchestration • MEC

Figure 8-1: Verizon's approach to securing our 5G network.

References

[1] 3GPP TS 23.501: "System Architecture for the 5G System".

[2] "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE", S. R. Hussain et. al, Network and Distributed System Security Symposium (NDSS), 2018.

[3] 3GPP TS 33.501: "Security architecture and procedures for 5G system" (2018, Dec.).

[4] "Breaking LTE on Layer Two", David Rupprecht et. al, 2019 IEEE Symposium on Security & Privacy.

verizon