Verizon + Wireless + Security

White paper

Multi-pronged strategies to securing mobile networks.

Table of contents

verizon business

Introduction

Wireless networks are everywhere - even where you don't think they are, bringing new possibilities but also serious challenges. Addressing network security needs is paramount to delivering solutions that meet today's expanding demand for mobility and accessibility. Verizon is at the forefront of offering secure wireless solutions, reducing the security risk to personal and corporate information.

Managing the Verizon wireless networks requires innovative proprietary and commercially available methods for securing our network and protecting our customers. Toward that end, Verizon has instituted a multi-pronged strategy, which encompasses our internal engineering teams, external software development partners and external vendors from whom we procure commercial applications and products.

Security has always been one of the top criteria when evaluating wireless access technologies to deploy, and our network security team has developed comprehensive security standards for designing, deploying and managing our networks based on industry practices and established standards from the International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST) and other governing bodies. Internally developed applications and infrastructure are measured by these standards prior to deployment and continuously throughout their production lifetime.

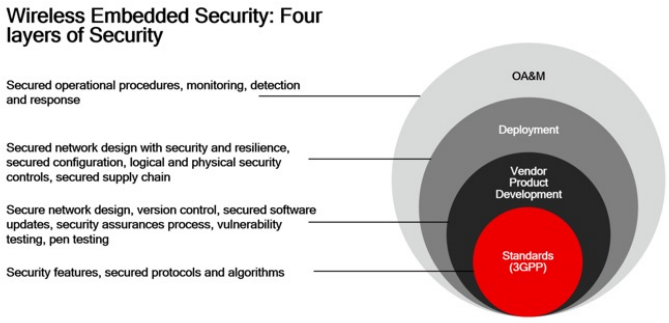
Additionally, all externally developed applications deployed in our network are subject to pre-launch security audits conducted by trusted security experts to verify that these applications have a limited attack surface and do not undermine Verizon's security posture.

In addition to these tactical security projects, we undertake several strategic initiatives such as proactively gathering intelligence and developing security standards proactively for our Original Equipment Manufacturers (OEM) providers. We work closely with our threat detection teams to limit the exposure in the event of a security incident.

This Verizon + Wireless + Security: Multi-pronged Strategies to Securing Mobile Networks white paper focuses on how Verizon addresses all aspects of security to enable mobile users to enjoy secure access. To this extent, the paper explores the embedded security of Verizon's wireless networks in addition to the "above the network" consumer and enterprise security services that enhance the security posture of consumers and enterprises.

1. Embedded Security: Standards, Design, Deployment and Operations

At Verizon, security is a driving factor in how we build and operate our networks. Verizon's goal is to make sure every element of the wireless 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 networks best in class. The embedded security of Verizon's wireless networks are based on adoption of the wireless security standards, secure design and deployment and secure operations and management of the networks.



1.1 Verizon Wireless Networks and Wireless Standards

Many elements in the Verizon wireless networks are similar to components found in a typical corporate IT network, with one key difference – mobile access. The wireless access network is where users are granted entry into the overall mobile network architecture and where implementing and maintaining high security and access protocols become paramount. Verizon operates 4G LTE (Long Term Evolution) and 5G as its primary wireless networks. These wireless access technologies are standards-based and offer robust security based on coding, authentication and encryption. The wireless access network facilitates security by allowing only authorized mobile stations to access the network.

1.1.1 4G LTE Public Access Networks

4G LTE is the fourth generation of wireless technology based on specifications developed by 3GPP, an international standards organization. LTE security architecture is defined in 3GPP TS 33.401. LTE uses an Internet Protocol (IP)-based infrastructure. With LTE, Verizon continues to meet business and consumer demands for higher bandwidth and low latency that will work broadly in the U.S. and globally. Key security enhancements in LTE are discussed below.

Secure storage: The 4G Universal Integrated Circuit Card (UICC) token, which is the next evolution of the Subscriber Identification Module (SIM) card, holds credentials and secure data for accessing services provided by the mobile network. The private key is created when the UICC is manufactured; it is

encrypted with a transport key and shared with Verizon Wireless only via a secure connection, keeping the data from being co-opted. The encrypted key is eventually stored in the mobile user database and only decrypted within a secure element during the authentication process. The Personal Identification Number (PIN) and PIN Unblocking Key (PUK) mechanisms are enforced on the SIM to maintain secure access to data or applications on the Verizon LTE network. In this sense, the SIM offers a hardware Root of Trust for Storage (RTS) for mobile devices; it provides cryptographic primitives and secure storage of key material that cannot be corrupted by the surrounding hardware and software of the handset. The UICC itself is a tamper-resistant compute platform and supports multiple cryptographic algorithms.

Mutual authentication: In LTE networks, the network authenticates the user identity, while the user equipment (UE) authenticates network credentials. The 4G SIM card contains necessary authentication algorithms and certificates, which aid in the secure accessing of the network. The primary algorithm for accessing LTE network services is the 3GPP-defined algorithm, MILENAGE. After initial attachment to the network using the International Mobile Subscriber Identifier (IMSI), a temporary mobile subscriber identity (TMSI) is used instead of the IMSI to protect the subscriber from being identified.

Root key length: The use of 128-bit keys ensures strong security and in so doing requires a greater "level of effort" to attack the algorithm. The security keys in LTE are derived from a Key Derivation Function (KDF). Each key has a different input, and all keys used for crypto-algorithms are 128 bits in length.

Security context: Keys to encrypt signaling and User Plane (UP) data are created for each data session on the Verizon LTE network. The key for UP traffic is retained for the period that the UE is in a valid connected session and keys are deleted on transition to idle mode or on handover to another LTE cell site. Furthermore, handover between LTE cell sites can only be performed after security is activated.

Integrity protection: Integrity protection is used to verify that the signaling has not been modified over the radio access interface and that the origin of signaling data is the one claimed. Each signaling message is appended with an integrity tag and the message is accepted only upon verification of the integrity by the receiving end. The Verizon LTE network supports 128-bit Advanced Encryption Standard (AES) and SNOW3G algorithms for integrity protection.

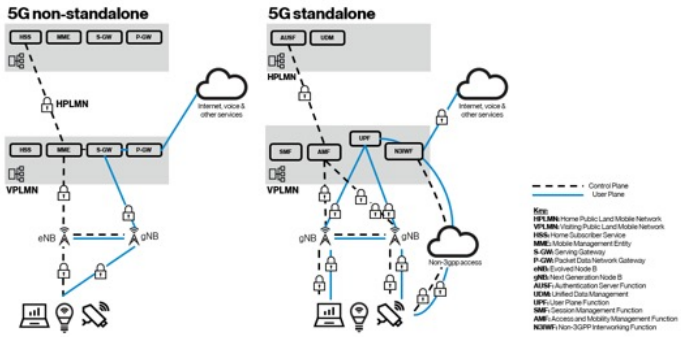
Airlink encryption: Encryption is used to provide confidentiality, so UP data or signaling cannot be overheard on the radio access interface. The Verizon LTE network supports three options for encryption: AES-128, SNOW3G and NULL. One of the options is negotiated between the UE and the LTE Cell site before communication commences. AES-128 is the preferred option in the Verizon LTE network, followed by SNOW3G; if the UE is not capable of either option, then no encryption (NULL) is used.

In addition, the Verizon LTE network fully supports the low power-wide area technologies of Cat-M1 and NB-IoT devices and includes services specifically for Internet of Things (IoT). LTE Cat-M1 and NB-IoT lower the barrier of entry to the IoT world, providing a quick and easy way to develop, deploy and manage machine-to-machine (M2M) solutions.

1.1.2 5G Public Access Networks

5G is an evolution of 4G LTE, with many 5G features being enhancements, improvements or extensions of the equivalent 4G LTE features.

In both 4G LTE and 5G, the Evolved Packet Core (EPC) and 5G Core (5GC), respectively, dictate which standards-based security features are available. Two major 5G deployment alternatives are defined by 3GPP, Non-Standalone (NSA) and Standalone (SA). NSA has the same security features as 4G LTE whereas SA uses new 5G security features.



Key 5G Standalone security differences are:

UE Changes:

1. **Subscriber privacy:** UEs create a Subscription Concealed Identifier (SUCI) by encrypting the parts of the Subscription Permanent Identifier (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.
2. **Stronger roaming authentication:** 5G's new authentication procedure, 5G Authentication and Key Agreement (5G-AKA), 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 rather than relying solely on the authentication performed by the roaming network. This step 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.

3. **Authentication flexibility:** 5G also adds features that make it easier to strongly authenticate a U. In particular, UEs can use 3GPP-specified authentication protocols, the 5G-AKA procedure 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.
4. **Secondary authentication and authorization:** Verizon's 5G network will further expand the above 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.
5. **Protection of user and signaling data:** Confidentiality and integrity protection ciphers for both user and signaling planes are defined for UE. 5G adds a new security feature that gives UEs the option to provide integrity protection for the UP in addition to encrypting it. UEs in the Verizon 5G network will by default provide integrity protection for the UP, using the 128-NIA1 and 128-NIA2 algorithms. UEs in the Verizon 5G network that use these algorithms will also provide bidding-down protection to ensure attackers cannot cause the UE to use less secure algorithms.

Radio Access Network (RAN) Changes:

1. **Restricting sensitive data:** 5G includes extra protections in places that are vulnerable to physical attacks The 5G key hierarchy ensures that when the Verizon 5G network activates confidentiality protection for UE communications (i.e., encryption), the network operator can distribute encryption keys such that the Radio Unit (RU) and Distributed Unit (DU) cannot view the confidentiality-protected data.
2. **Protecting RAN interfaces:** The secure air interface ensures confidentiality and integrity of the traffic between the UE and the RAN. 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. The Verizon 5G network will use Internet Protocol Security (IPSec) to implement confidentiality, integrity and replay protection on all these interfaces when equivalent protections are not provided by the underlying transport networks.

Core Changes

1. **SBA protection:** 5G standards introduce a new architectural option for Network Function (NF)-to-NF communications in the 5GC known as the Service-Based Architecture (SBA).
2. **New security functions in 5G:** 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.

Function	4G LTE	5G (Standalone Architecture)
Privacy and Integrity Cipher	• Encryption on radio path • Control plane ciphering • 128-bit algorithms supported	**In addition to 4G LTE:** • 256-bit algorithms proposed for future release • Integrity implemented preventing unauthorized change of user data.
Authentication Key Agreement (AKA)	• Shared key provisioned • Mutual authentication (UE and network)	**In addition to LTE:** • Access-agnostic authentication (EAP) is used • 5G-AKA and EAP-AKA supported for both 3GPP and non-3GPP • Protects the confidentiality of non-access stratum (NAS) messages
Subscriber Permanent Identifier (SUPI)	Identifier sent in plain text	SUCI is used instead of SUPI
Security Anchor Function (SEAF)	Not Available	Allows re-authentication of the UE when it moves between networks
Home Control	Not Available	• Home Public Mobile Network (HPMN) can verify UE is present • Useful in roaming scenarios with Visiting Public Mobile Network (VPMN) • Assists in fraud prevention
Network Exposure Function (NEF)	Not Available	• NEF securely exposes capabilities to other Application Functions (AF) • Enables secure provision of information in the 3GPP network • Certificate based mutual authentication may be used
Security Edge Proxy Protection (SEPP)	Not Available	• Protects the home network edge, acting as the security gateway • Security between the home network and visited networks

For detailed information, see The Security of Verizon's 5G Network White Paper.

Source: GSMA - Securing the 5G Era

1.1.3 Wireless Private Network

Verizon Wireless Private Network (WPN) is a comprehensive solution that joins wireless devices to an organization's internal IP network using a dedicated connection that isolates data from the public internet. It extends a corporate IP network to wireless devices, while enabling your IT department to maintain the control and manageability it needs. With WPN, organizations can take charge of their evolving networks by:

- Avoiding the exposure of wireless devices and internal networks to the inherent risks of unsolicited public internet traffic.
- Controlling which wireless devices can connect to the network.
- Controlling which network resources the wireless devices and machines can access.
- Leveraging the convenience of mobility and wireless technologies to introduce new opportunities.

With WPN, organizations can add devices to their own internal networks, with their own IP addressing, to be managed by their own support personnel. This empowers them to make wireless solutions part of their infrastructure and extend their core-computing networks farther, faster and easier. Data travels from wireless devices connected to the RAN, through the private network to a dedicated connection to the customer's network. Each customer has its own private network whose traffic is kept isolated from the public internet, avoiding unnecessary risk associated with unsolicited public internet traffic. Only customer-authorized subscribers may send and receive data through that customer's private network. Verizon offers various IP addressing options that provide differing levels of accessibility, protection and manageability.

Private networks support enterprise-owned private IP address assignment to the devices, which essentially makes each device a virtual extension of the wired enterprise network. This allows enterprise IT administrators to manage mobile stations and LAN devices using the same tools and techniques. For example, the same firewall and routing schemes can be used, allowing WPN IT administrators to define which users get internet access through the private network. This makes it easier for enterprise IT administrators to manage and monitor network usage and to enforce their corporate IT policies.

With a private network:

1. Each 4G Private Network is assigned to a unique Access Point Name (APN). Only devices provisioned with the same APN can talk to each other.
2. Each customer APN uses private IP address space, following the standards set by RFC 1918 for Internet Protocol Version 4 (IPv4 IP packets addressed from them cannot be transmitted through the public internet, so if such a private network needs to connect to the internet, it must do so via a Network Address Translator (NAT) gateway, or a proxy server).
3. Each WPN is assigned to a unique set of ingress and egress IP resources in the Packet Gateway (PGW- Enterprise Universal Gateways). Each mobile device provisioned for the customer WPN can only reach their assigned IP resources (ingress/ egress) at the PGW. The PGW is the IP anchor point for the customer's private network devices. The customer-assigned APN can only reach the assigned IP resources on the PGW.
4. Each WPN is assigned to a unique egress routing domain at the provisioned PGW via a unique Virtual Routing and Forwarding (VRF) or VLAN.
5. Each unique egress routing domain is mapped to the customer's connection to their host site (PIP, FES, VPN). This connection is established between the WPN gateway and the customer premises equipment (CPE), which allows access only into the customer's IP network with their hosted applications.
6. The WPN is isolated from the public internet. By virtue of its design, it does not allow access to applications hosted on the public internet. Service Based Access is a specially designed Private Network feature that provides access to a limited set of defined consumer applications.
7. WPN supports IPSec, a protocol for securing IP communications by authenticating and encrypting each IP packet of a data stream. IPSec is compatible with most VPN technologies as well as the Verizon Multiprotocol Label Switching (MPLS) network.
8. The Dynamic Mobile Network Routing (DMNR) option on the WPN advertises the customer's LAN subnet addresses behind a wireless router, thus simplifying connecting LAN subnets like laptops, desktops or other devices located behind those routers to applications hosted by the customer's data center. This option protects sensitive data from traversing public internet space and further enhances the IT administrator's ability to manage individual subnets behind a wireless router by communicating directly with those nodes.

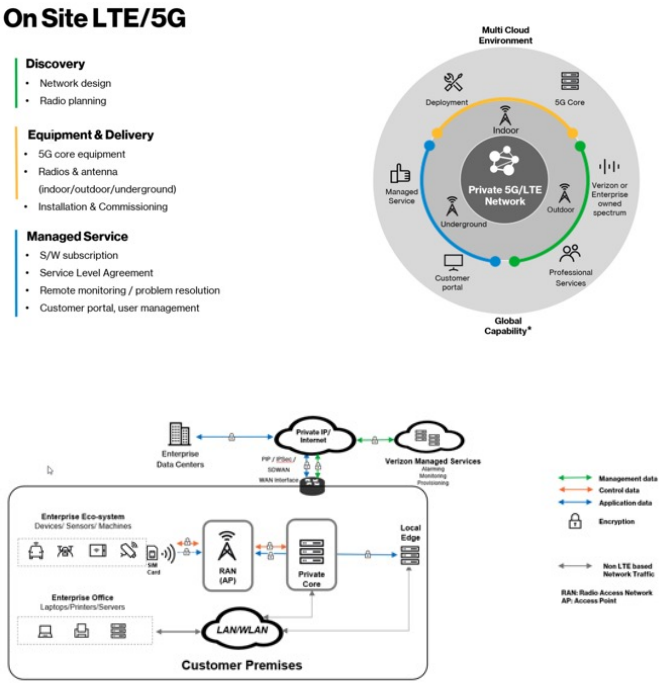
1.1.4 Private Networks - On Site LTE/5G

A distinction between cellular technologies is whether they are public or private. Unlike public networks, private networks often cater for very specific use cases focused on local area coverage that often have more specific requirements than consumer mobile services. Examples include production line management or Automated Guided Vehicle Systems (AGVs).

Verizon's On Site LTE/5G offer a network that is exclusive to the customer, with the bandwidth dedicated to what the organization needs. This provides greater control over the data

and network, meaning data cannot be shared externally. As a result, it becomes a viable option for use cases where IoT devices, such as sensors or cameras, remain on the customer premises and don't need to be roaming.

While the types of cyberthreats remain the same, the fact that the network is being used exclusively in an area that is physically controlled and secured by an organization creates an additional level of protection. For example, for an attacker to get close enough to perform signal-jamming, they would need to be physically on site, which means getting past physical security and remaining undetected.



1.2 Design and Deployment

Security is an integral part of the design and deployment of Verizon's wireless networks. We rely exclusively on trusted network components, managing supply chain security risks through our rigorous supplier vetting processes. We then work with suppliers and engineers to secure these components in the equipment and devices we deploy throughout the network. Further, we leverage all the security capabilities defined in the technical standards, which we helped develop, to deploy secure wireless networks.

1.2.1 Risk Management and Secure Supply Chain

Verizon's trusted supply chain is the foundation of our secure wireless networks. For both hardware and software, Verizon purchases all our network equipment from a small group of sophisticated vendors with whom we have close, trusted relationships developed through vetting and scrutiny, including pre-deployment testing of equipment.

Verizon's contractual supplier security requirements, which are designed to address risk management goals, are based on Verizon's own corporate information security policies as well as open industry standards and control objectives found in NIST guidance and additional security standards regimes such as ISO2700x, SSAE16, PCI-DSS, HIPAA and others.

Verizon has developed its supplier risk assessment and management discipline over many years. Our supplier risk program manages the risk assessments of suppliers and their individual engagements in a methodical and centralized process. Through the program, Verizon identifies, assesses, monitors and manages any risks associated with our suppliers throughout the supplier lifecycle, employing highly trained risk management experts to review and approve each contract request.

Verizon conducts a pre-launch security risk assessment for branded applications and devices, as well as many internal applications and devices. We first evaluate potential risk that may be part of an implementation through a process called Threat Modeling. Based on identified threats, penetration testing is conducted on device and application layers to identify vulnerabilities that could be exploited. Penetration testing is conducted by both Verizon and contracted third party entities. This testing provides insights on two fronts: an "internal" view, (someone with insider knowledge of the device or application) and an "external" view (someone trying to gain access to the device or its application via the internet).

In addition, we work with the product or platform vendor to make sure that identified issues are either resolved prior to commercial launch or, at a minimum, that mitigation plans are in place prior to complete resolution.

1.2.2 Physical Security

1.2.2.1 Partitioned Access Control Systems

As per Verizon established standards, access (either physical or logical) is granted based on what an individual needs in order to do their job – no more, no less.

Verizon's Mobile Switching Centers (MSCs), Network Equipment Centers (NECs) and Network Operation Centers (NOCs) are designed and equipped with access control systems with multiple, layered security access zones such as core equipment spaces, building services spaces, office spaces, public spaces, shipping/receiving spaces, etc. Critical spaces are surrounded and shielded by less critical spaces.

Electronic keys control access to the buildings and interior spaces; mechanical keys are issued only to a few critical personnel as backups. Access to any of those spaces is controlled by the access control system for each individual – employee, contractor, and visitor – according to the legitimate need for their access. Not all employees need access to all spaces all the time. The access control systems are programmed to allow individuals access by time of day, day of the week, per room or space, as required.

Visitors are never to be unescorted at any time in other than designated "public" spaces. Access control systems maintain log files of all access attempts, authorized or unauthorized. If the facility is fenced, the access control system extends to include the whole of the fenced enclosure. Cell sites are similarly equipped with a layered access control system that will – depending on the site configuration – secure the perimeter, the equipment shelter, equipment cabinet and equipment shelf.

1.2.2.2 Intrusion Detection & Alarm

These MSCs, NECs, NOCs and cell sites are designed and equipped with intrusion detection and alarm systems that are tied into their access control systems. The intrusion detection systems include, but are not limited to, door contacts, motion detectors, infrared sensors, cameras with motion detection, glass break sensors, timers, etc., that will generate alarm signals locally and to remote locations such as the NOCs or central station security monitoring points.

1.2.2.3 Systems Surveillance – 24/7

Alarm conditions of all types including those from the Access Control Systems (ACS) and the Intrusion Detection Systems (IDS) are monitored and logged in at least three locations – the system itself, the local control point, and the NOCs fault management system. NOCs are fully staffed and are monitored. In addition, a facility's intrusion detection system may also be monitored by a third-party central station depending on the facility and local assessment of the security environment. Local personnel are on call 24/7 to respond if necessary.

1.3 Operations and Management

Verizon invests heavily in securing all of its networks, against known and potential threats. We continuously monitor our networks to identify and respond to threats. Our networks are monitored 24/7 by a Security Operations Center to identify potential malicious activity. Verizon's corporate governance policies, security monitoring and response capabilities, and software vulnerability management processes have been built upon over the years as the different generations of cellular technologies evolve. To identify issues not prevented by other controls, Verizon also uses detective mechanisms like intrusion detection and network Data Loss Prevention (DLP) to analyze network traffic for malware and unauthorized information transmissions.

1.3.1 Corporate Policy & Governance

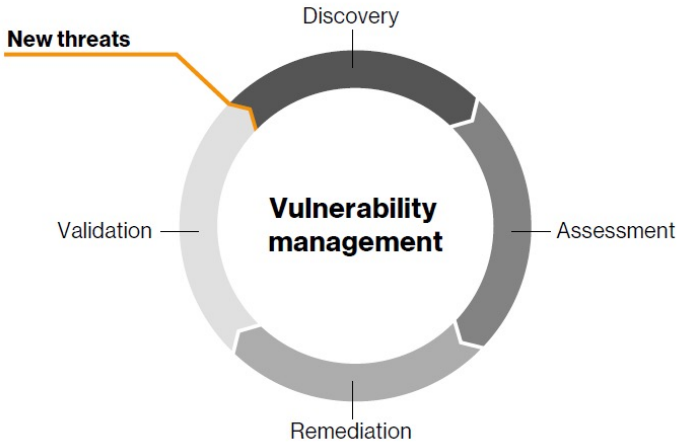
Policy and Governance is the cornerstone of any good security program, and Verizon has a suite of security practices and procedures that align with the NIST Cybersecurity Framework. These formal, internal, corporate-wide policies map to each of the Framework's five Core Functions – Identify, Protect, Detect, Respond and Recover – and each sets forth the individual behaviors and business processes that are required for security, as well as the standards for our infrastructure and its supporting systems and applications. Verizon also internally publishes dozens of detailed corporate information security standards which provide detailed descriptions of the underlying security controls that must be implemented to support each security instruction.

Verizon reviews and updates these policies and standards annually and on an as-needed basis along with evolving regulatory compliance obligations, technology capabilities, improvements to industry best practices, field experience and implementation. Updates are incorporated into the policies after a rigorous review and approval process, and they are communicated to internal stakeholders on roughly a monthly basis.

1.3.2 Vulnerability Management

Vulnerability management is a key aspect to protecting the Verizon wireless networks. We have implemented a four-stage vulnerability management mode:

- **Discovery:** Automated tools that remotely and continuously check for vulnerabilities in operating systems, services, and devices that could be used by hackers to target the customer's private network.
- **Assessment:** Vulnerabilities detected during the Discovery stage are rated and prioritized and documented.
- **Remediation:** Vulnerabilities are addressed based on the priority identified in the previous assessment step.
- **Validation:** After the vulnerabilities are addressed, subsequent scans are used to validate the successful resolution of all identified vulnerabilities.



In addition to these four stages, we regularly monitor various sources to identify trends for potential new vulnerabilities emerging in the hacker community. Tracking vulnerabilities is one measure to determine how well we are performing security assessments, evaluations and resolutions.

1.3.3 Security Monitoring & Response

Verizon monitors all of its network elements for signs of possible intrusions or security breaches, both on the customer facing Wireless Data Network (WDN) and on our management network known as the Engineering Data Network (EDN). We have deployed technologies such as Intrusion Detection Systems (IDS) that detect security issues (e.g., Denial of Service, SYN Floods, Ping Sweeps, BotNets) and Intrusion Prevention Systems (IPS) to automatically block malicious traffic.

When possible, security breaches are detected, we have a dedicated team of certified security professionals (CISSP, GIAC) as part of the Network Security Incident Response Team (NSIRT). The primary mission of this team is to identify incidents and the method by which the breach occurred, and to make all necessary changes to prevent a recurrence of that event. Forensic analyses are also completed on the breach and the appropriate law enforcement agencies are engaged, if needed.

Our security professionals also perform trend analyses on the flow of traffic on our network to detect anomalies that would otherwise go unnoticed – potentially indicating an attack is imminent. The NSIRT team is on call on a 24/7 basis.

Verizon employs experienced security and privacy professionals with several professional certification (i.e., CISSP, CISM, etc) credentials, and maintains organizational memberships (i.e., ICS2, ISACA, etc.).

In addition to IDS and IPS systems which help in identifying intrusion detection and prevention, other preventative controls in place are:

- **Separation of Duties:** The practice of dividing steps in a function among different individuals, to keep a single individual from being able to subvert the overall process.
- **Dual Control:** The process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. No single person is permitted to access or use the materials (e.g., the cryptographic key).
- **Role-based Access Control:** Mechanisms that limit availability of information or information processing resources only to authorized persons or applications.
- **Principle of Least Privilege:** The practice in which a user is granted the minimum level of access to perform actions necessary for the job function.
- **Multi-factor Authentication:** The practice of requiring or more authentications required for remote login.

2. "Above the Network" Security Services

Verizon offers secure wireless data services for its consumer, enterprise and government customers. These services are designed to enhance the mobile experience while maintaining security.

As an award-winning leader in cybersecurity, we keep up with the rapidly changing nature of cyber threats by processing billions of security events each year, analyzing evolving threats at our global security operations centers, performing forensic investigations for companies around the world, and sharing our knowledge through industry-recognized content like the annual Data Breach Investigations Report and Mobile Security Index.

We differ from other security service providers because our substantial risk and incident experience lets us understand the real-world threats customers face and the potential vulnerabilities in each system. And, our years of practical experience in developing and implementing security programs across all industries lets our customers know that our priority is their long-term success.

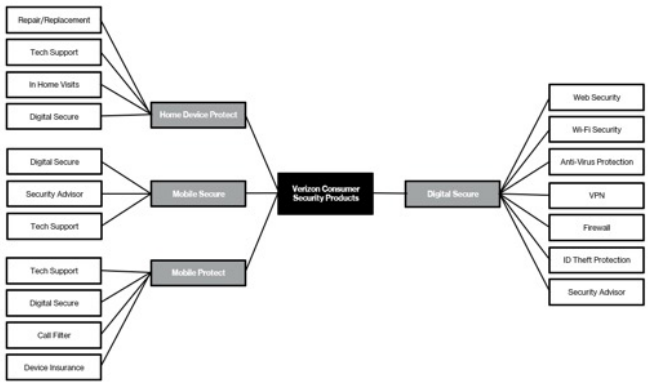
The following sections provide a summary of these services.

2.1 Consumer Security Services

Verizon offers a security suite of applications for smartphones which are designed to protect users from various threats to device and data theft. The basic suite includes antivirus and anti-phishing software that provides protection from malware, and alerts the user when browsing websites that are known to be either malicious or contain phishing or other exploits, as reported by McAfee SiteAdvisor service. Incoming SMS and email attachments are also scanned for potential embedded malicious URLs or malware. Customers that desire even greater protection can find Verizon's Privacy Scan service which notifies users of the risk applications present in

transmitting personal information. Customers are also alerted if connected to an unsecure Wi-Fi connection, or if spoofing is detected.

Verizon-branded apps, such as Verizon Cloud and My Verizon Mobile, authenticate the user in the background, creating a seamless user experience.



2.2 Device Security

Verizon offers services that secure the mobile device to protect user privacy and provide a layer of protection against hazards common to connected mobile computing devices.

2.2.1 Device Access Password & Device Storage Encrypted

Verizon offers devices to its customers that are capable of password protection on the device itself and encryption of information stored on the device. Use of those capabilities is the responsibility of the user and is encouraged by Verizon. Verizon offers a complete suite of managed services in device configuration management.

2.2.2 Device Security Features

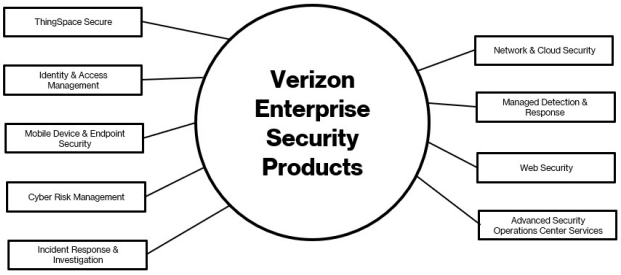
These features are available on most recent devices; however, customers must verify specific feature sets for each device in the device's user manual.

- **Secure Boot:** Helps prevent any OS modification or unauthorized OS software from being executed. During the boot process, secure boot verifies that only signed software is on the device. Also, the device is upgraded with only authorized software.
- **Data at Rest:** Data stored on the device is encrypted.
- **Data in Motion:** Enables over the air encryption and helps prevent interception and alteration of data being transmitted across the network, including via the radio access network (RAN) using transport layer security (TLS) and virtual private network (VPN).
- **Locking:** To combat fraud, all new smartphones are locked to the Verizon network for 60 days after purchase. Smartphones automatically unlock after 60 days as long as the account is not flagged for fraud and the phone is not reported lost/stolen. Both SIMs are locked on a dual/eSIM device. This policy applies to all current and future SIM lock-capable smartphones; the policy does not impact tablets, connected devices, Certified Pre-Owned, Certified Like-New Replacements or Bring Your Own Device phones.
- **Anti-Theft (Kill Switch):** Helps to prevent devices from being used by unauthorized users.

2.3 Verizon Enterprise Security Solutions

In addition to the wireless security solutions mentioned above, Verizon also offers a suite of enterprise security services for wireless and wireline customers that can strengthen an enterprise's security posture. As data and applications move into the customer's Network, WAN and the public cloud, these enterprise security technologies come into play.

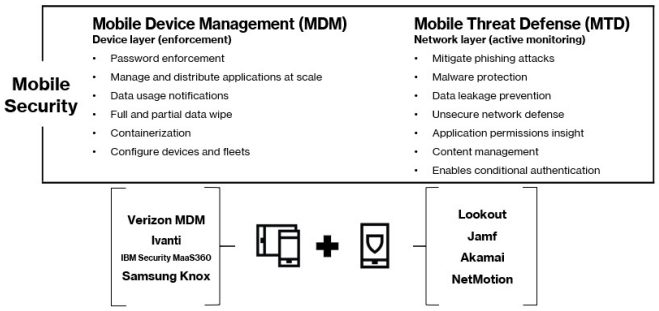
The infographic below provides the security solutions offered by Verizon.



2.3.1 Mobile Device and Endpoint Security

Mobile security is one aspect that should be considered in the context of the overall enterprise security strategy. The key to managing and reducing cyber threats related to mobility is to have strong mobile device management (MDM) and mobile threat defense (MTD) capabilities in place.

Our advanced endpoint protection solutions can help customers keep their policies aligned, while helping prevent malware, ransomware and other dangerous exploits from infiltrating their business. Using malware analysis and artificial intelligence (AI)-based machine learning, it helps customers detect malicious activity and prevent malware from loading and executing. It also facilitates investigation and remediation.



2.3.1.1 Mobile Device Management

Whether customers are looking for ease of use or enterprise-grade unified endpoint management, Verizon makes it easy to find the right technology for them to protect the device. Mobile device management (MDM) solutions allow companies to manage both bring-your-own-device (BYOD) and corporate-liable (CL) devices. Enabling a mobile workforce is a large investment for any enterprise. With CL accounts, an organization has more control over the application policy and more uniformity in the types of devices on the network which can make technical support easier and costs lower.

Mobile Device Management (MDM) and Unified Endpoint Management (UEM) solutions from Verizon and our technology partners can make it easier to control, secure and enforce company policies across all of your devices. They can help a customer's workforce stay productive, while protecting the customer's data and helping streamline device and app deployment, maintain security, and control costs.

Verizon MDM: The Verizon Mobile Device Management (MDM) service suite combines unified endpoint management and broadband hotspot management into a single management portal so customers can manage device app deployment, maintain security policies and more.

Ivanti (formerly MobileIron): Ivanti provides a portfolio of solutions to help secure your mobile infrastructure. Ivanti solutions make it easy to set up devices and protect them with mobile-centric, zero-trust security capabilities such as zero sign-on, multifactor authentication and mobile threat defense.

IBM Security MaaS360: IBM Security MaaS360® with Watson™ Unified Endpoint Management is a single platform to help customers simplify how they manage mobility across their business. Plus, endpoint analytics help them make sense of daily mobile details.

Samsung Knox: Samsung Knox® Manage is a cloud-based mobility management platform designed for enterprise customers to manage and monitor employee devices with flexibility and granularity.

2.3.1.2 Mobile Threat Defense

Securing and managing customers' mobile devices, apps and sensitive data is vital to their livelihood. We have the expertise and leading mobility management offerings to help ensure the solution meets customer security requirements.

Lookout: Lookout leverages its global network of security intelligence to deliver advanced security to mobile devices owned by an organization. Its cloud-first, device-assisted approach to security helps limit impacts on device performance and user experience. Lookout can be quickly deployed for BYOD environments and when combined with mobile device management solutions can provide strong enterprise protection.

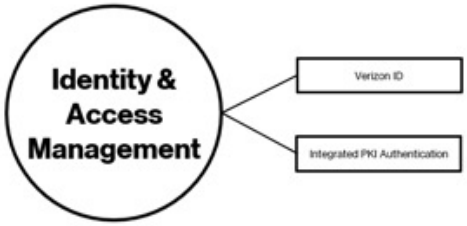
Jamf (formerly Wandera): Jamf is a cloud-delivered security solution that can protect modern enterprises operating beyond the traditional perimeter. When remote users access applications from their smartphones or laptops, Jamf's cloud infrastructure securely connects workers to business applications, and provides real-time threat defense and in-network content filtering to help keep business assets protected.

Akamai (formerly Asavie): Akamai Moda can help customers manage mobile security, productivity and compliance for all customer devices, including smartphones, routers and Wi-Fi hotspots. Akamai SIA Mobile provides private network connectivity on demand for remote sites and IoT devices

Ivanti Mobile Threat Defense (formerly MobileIron): Threat Defense: With advanced capabilities such as multifactor authentication and mobile threat detection that help protect against targeted mobile attacks, these MTD solutions can help protect corporate data accessed by a customer's mobile workforce. Its mobile-centric, zero-trust security approach verifies every user, device, app, network and threat before providing access

Absolute Secure Access (formerly NetMotion): Absolute Secure Access software solutions improve the performance, visibility and security of a customer's mobile enterprise. Absolute Secure Access software gives IT the tools to monitor and dynamically make decisions using real-time data and analytics.

2.4 Identity and Access Management



Many of our enterprise customers choose to utilize their own encryption applications to encrypt voice/data end-to-end. Transport Layer Security (TLS) allows mutual authentication between a client and server, and establishes an authenticated and encrypted connection between the client and the server. Verizon's Application Security delivers layers of security to help thwart cyberattacks.

Application protection enhances security even if the call or data crosses multiple networks. Application protection consists of a number of security tactics working to protect customer data and privacy. The technology used in Application Protection, such as encryption, provides inherent security, to help keep calls, data and applications secure even if intercepted. Verizon's Application Protection solutions provide essential security services needed for establishing trust and privacy in online voice call and application data transactions.

2.4.1 Verizon ID

Verizon ID is a next generation Identity and Access Management (IAM) platform based on identity technologies including BlockChain and Bio-Metrics. Security is significantly enhanced with elimination of User IDs and Passwords.

Verizon ID provides broad range of identity services including:

- Multi-Factor Authentication
- Adaptive Authentication
- Identity Proofing
- Identity Federation
- Trusted Digital Identity Safe

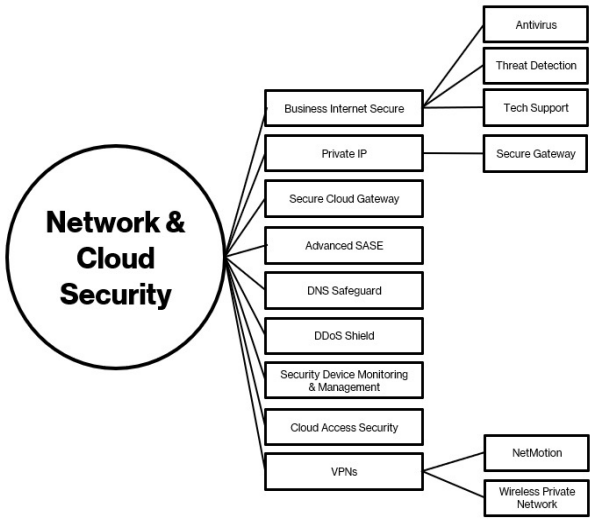
Verizon ID is compliant with major regulations including NIST SP 800-63-3 (Identity Proofing and Validation) and General Data Protection Regulation (GDPR).

2.4.2 Integrated PKI Authentication (IoT SC)

Integrated PKI Authentication (IPA) enhances security by Mutually Authenticating and Encrypting your services, devices, APIs and applications. Verizon's IPA delivers an additional layer of security to help thwart cyber-attacks when traditional security isn't enough or to meet the needs of existing or emerging IoT solutions. The platform consists of many security tactics working together such as trusted credential creation and chaining embedded encryption protecting your data and privacy, and credential validation and secure life-cycle management.

The technology used in Integrated PKI Authentication provides the security services needed for establishing trust in online electronic transactions: confidentiality, integrity, identity authentication and non- repudiation. The establishment and operation of Integrated PKI Authentication certificate authority are governed by their respective Certificate Policies (CP) and Certificate Practice Statements (CPS).

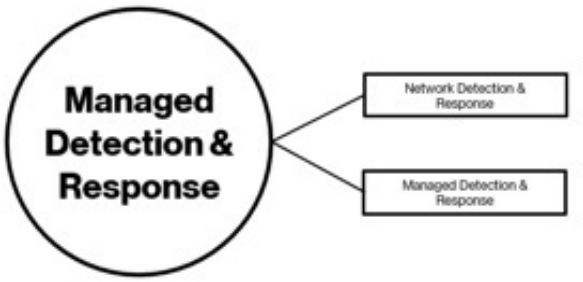
2.5 Network and Cloud Security



As the attack surface expands, protecting critical assets and data from cyber criminals has become increasingly complex. Organizations need to ensure they have the right set of security controls in place to help reduce the chance that an attacker can exploit vulnerabilities within the attack surface. Verizon can help businesses develop and implement appropriate safeguards to ensure delivery of critical services.

We offer a broad range of products and services to secure the cloud, network, endpoints, and help organizations reduce complexity, control costs, and fortify their network infrastructure.

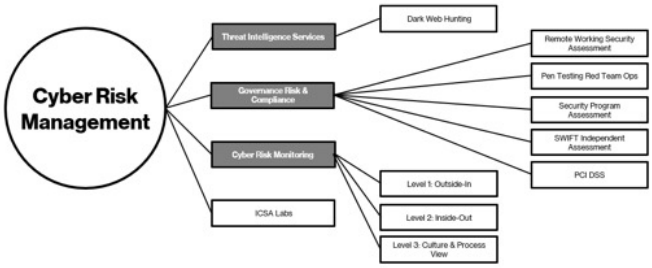
2.6 Managed Detection and Response



Verizon's managed detection and response services help customers identify and contain advanced cyber-attacks. Our broad, rapidly-deployed, cloud-delivered MDR services 24x7 protection by combining people, process and technology. Our deeper dive, stand-alone detection and response technologies help collect and maintain actionable intelligence, identify and alert on major security incidents, and then quickly respond to those that are a potential problem for the organization. Additionally, our Professional Services experts can provide dedicated, proactive threat response.

Using essential technology components including Security Information and Event Management (SIEM) technology, User and Entity Behavioral Analytics (UEBA), and integrations with Network Detection and Response (NDR), Endpoint Detection and Response (EDR), and Deception, Managed Detection and Response helps prioritize and investigate events so an organization can rapidly take direct action to help mitigate threats.

2.7 Cyber Risk Management



Cyber Risk Management helps customers enhance their visibility of their risks and where the threats are both internally and externally. Customers can subscribe to a simple dashboard that provides daily scores and updates on their risk posture and identify areas where their security may be weak. Having more visibility builds confidence and more assurance that programs and resources are appropriately focused on the right things and in the right areas.

From risk assessments and compliance reviews to certifying new solutions and setting up security policies, Verizon also offers a full suite of IT security professional services.

2.8 IoT Connectivity Management Tools

Verizon offers several connectivity management tools as a complete solution for enterprises deploying M2M/IOT applications, as well as M2M vertical solution partners and system integrators. The connectivity management tools provide services in the area of M2M / IOT device provisioning, management, reporting and diagnostics as well as for M2M / IOT application development.

The connectivity management tools can leverage the Verizon Wireless Private Network solution to offer secure device connectivity and application data transport to/from enterprise hosted M2M / IOT applications. The connectivity management tools can also be used with devices on the Verizon public network.

The connectivity management tools can further route such customer specific traffic to individual customer's data centers using VPN/MPLS configurations. Both Static and Dynamic private IP addressing schemes are available to customers using the connectivity management tools.

2.8.1 Machine to Machine (M2M) Management Center

The M2M Management Center provides services in the area of M2M device management, reporting and diagnostics.

2.8.2 ThingSpace Manage Customer Portal

Verizon Wireless offers the ThingSpace Manage Customer Portal as a complete solution for enterprises deploying M2M/IoT applications, as well as M2M/IoT vertical solution partners and system integrators. The ThingSpace Manage Customer Portal provides services in the area of M2M/IoT device provisioning, management, reporting and diagnostics.

2.8.3 Unified Web Services (UWS)

Verizon Wireless offers Unified Web Services as a set of web services APIs (offered via an application software development kit) based on standard SOAP/XML web services API technology. Customers use these APIs to integrate connectivity. management tools services into the applications that they build and host. Access to UWS is provided through a username/password credential that the software application uses. Additional security is provided through web services session time outs and session tokens used in API call invocations. Unified Web Services connections use 1-way Secure Sockets Layer (SSL) (with 128-bit or higher encryption) with white-listing of the customer's application server IP address.

2.8.4 ThingSpace Develop Portal

Verizon Wireless offers the ThingSpace Develop Portal as a developer focused portal, which includes a set of web services APIs based on standard REST web services API technology. Customers use these APIs to integrate connectivity management tools services into the applications that they build and host access to ThingSpace Develop Portal is provided through a username/password credential that the software application uses. Additional security is provided through web services session time outs and session tokens used in API call invocations.

2.8.5 Secure Access Control to Connectivity Management Tools

The connectivity management services are hosted on both the Verizon National Network Operations Data Centers and Verizon IT Data Centers in a highly redundant, failover-capable configuration. Customer access to the connectivity management tools is provided through a formal process of on-boarding which provides access credentials to customers. Customers can use the methods to access the connectivity management tools:

- **Customer Portals:** Access control to the customer portals is provided via username/password credentials provided to users belonging to the customer's organization. SSL based connections for browsers with 128-bit (or higher) encryption are required.
- **Web Services:** A set of web services APIs based on standard SOAP/XML or REST web services API technology.

Customers use these APIs to integrate connectivity management tools and services into the applications that they build and host. Access to the web services is provided through a username/password credential that the software application uses. Additional security is provided through web services session time outs and session tokens used in API call invocations.

3. Summary

Verizon complies with and exceeds industry, statutory and regulatory requirements applicable to wireless networks in the U.S regarding safeguards and controls of protected information. Verizon prides itself as a security leader in the telecommunications industry. We are confident that the confidentiality, integrity and availability of the data will be maintained consistent with our customer expectations, because we have instituted a multi-pronged strategy to security, offering both embedded security in the networks and above the network security products and services.

- **Wireless Standards & Services:** Verizon operates 5G, LTE and CDMA standards based wireless access technologies, which offer robust security-based encoding, authentication and encryption. Also, wireless services are enabled and designed to enhance the mobile experience while maintaining security.
- **Policy & Governance:** Verizon has created enterprise-wide policies that align with ISO 27002 and NIST standards for the protection of customer and employee information.
- **Vulnerability Management:** Verizon has implemented a four stage (Discovery, Assessment, Remediation and Validation) vulnerability management model to guard against vulnerabilities.
- **Risk Management:** Verizon conducts penetration testing by both Verizon Wireless employees and contracted third party entities. The results of the security risk assessment are used to decide whether or not to move forward with a commercial launch of the product.
- **Security Monitoring & Response:** Verizon has a dedicated team of certified security professionals (CISSP, GIAC) as part of the Network Security Incident Response Team (NSIRT) to identify incidents and the method by which a breach occurred, and to make all necessary changes to prevent a recurrence of that event. The NSIRT team is on-call on a 24x7 basis.
- **Physical Security:** Verizon has implemented a partitioned access control system, by which access is granted based on individual needs. Network centers and cell sites are designed and equipped with intrusion detection, alarm systems and alarm conditions of all types, including those from the access control systems (ACS). Intrusion detection systems (IDS) are monitored and logged in at least three locations.

Overall information security is an integral part of Verizon's corporate strategy. We recognize that planning and enforcing a strong multi-pronged security program is a key to protecting sensitive customer data, and we have implemented a thorough process to maintain operations at an acceptable risk level.

Glossary of Terms

1xEV-DO (One times Evolution Data Optimized)
A CDMA2000 technology optimized for packet data services.

1xRTT (One times Radio Transmission Technology)
A CDMA2000 technology with traditional circuit voice and data support that has maximum downlink speeds of 307 Kbps and uplink speeds of 144 Kbps.

2G (second generation)
The second generation of cell-phone technology introduced during the 1990s This generation added data capabilities to cell phones, including internet and email access.

3G (third generation)
Third-generation cellphone technology appeared in the 2000s and forms the foundation of our current cell- phone capabilities 3G technology offers even faster internet access, plus enables worldwide roaming capabilities.

3GPP (3rd Generation Partnership Project)
A collaboration between six international telecommunications organizations that is developing standards for the ITU's IMT-2000 project for the evolution of GSM technologies. It has recently completed the standard for LTE.

3GPP2 (3rd Generation Partnership Project 2)
A collaboration between telecommunications associations to make a globally applicable third-generation (3G) mobile phone system specification within the scope of the ITU's IMT-2000 project. In practice, 3GPP2 is the standardization group for CDMA2000, the set of 3G standards based on earlier 2G CDMA technology.

4G (fourth generation)
The next generation of wireless technology beyond 3G. Offers increased voice, video, and multimedia capabilities, a higher network capacity, improved spectral efficiency, high-speed data rates, and lower latency over current 3G benchmarks.

5G

An evolution and improvement over 4G cellular technology secured by design, resulting in the incorporation of the features such as user equipment authentication and authorization, end-to-end encryption, privacy enhancing features, and zero trust architecture, among others. 5G also provides flexibility around service deployment, due to its use of a number of technology solutions used in the cloud, and with virtualization at its core. This means 5G can support mobile edge computing, enabling cost-efficient ways of tackling latency issues, among other things. 5G also provides ubiquitous access, road-map flexibility and support for WAN and LAN technology.

AAA (Authentication, Authorization, and Accounting)
A network server used for access control Authentication identifies the user Authorization implements policies that determine which resources and services a valid user may access. Accounting keeps track of time and data resources used for billing and analysis.

AES (Advanced Encryption Standard)
A National Institute of Standards and Technology specification for the encryption of electronic data It employs a symmetric encryption algorithm and the Rijndael block cipher in order to protect user data It is comprised of three block ciphers, AES-128, AES-192, and AES-256 Each AES cipher has a 128-bit block size with key sizes of 128, 192, and 256 bits respectively. The AES ciphers have been analyzed extensively and are now used worldwide.

CAVE (Cellular Authentication and Voice Encryption) algorithm
A cryptographic hash function used in CDMA mobile systems for authentication, data protection, anonymity, and key derivation.

CDMA (Code Division Multiple Access)
A method for sending multiple voice and/or data signals simultaneously across the radio spectrum.

CDMA 2000
The brand name for telecommunications Interim Standard-2000 (IS-2000) that supports 3G CDMA-based cellular networks.

CHAP (Challenge-Handshake Authentication Protocol)
The protocol used to authenticate remote users to an internet access provider.

Ciphering
An algorithm for performing encryption or decryption. It is a series of well-defined steps that can be followed as a procedure, usually depending on a piece of auxiliary information, called a key The encrypting procedure is varied depending on the key, which changes the detailed operation of the algorithm A key must be selected before using a cipher to encrypt a message Without knowledge of the key, it should be very difficult if not nearly impossible to decrypt the message.

DMNR (Dynamic Mobile Network Routing)
A network-based mobile technology capable of providing dynamic routing and support for mobile or stationary routers in primary wireless access or automatic wireless back-up configurations using Mobile IPv4 based NEMO (Network Mobility) protocol, regardless of the application being used.

DMU (Dynamic Mobile IP Update)
A procedure used to distribute and update mobile IP cryptographic keys in CDMA, 1xRTT, and 1xEV-DO networks.

ESN (Electronic Serial Number)
The unique identification number found in mobile stations. Called International Mobile Equipment Identity (IMEI) or Mobile Equipment Identifier (MEID) for later devices.

EV-DO (Evolution-Data Optimized)
Also expressed as "1xEV-DO," the network used to provide wireless data service with average downlink speeds of 600 Kbps to 1. 4 Mbps and uplink speed of 300 to 500 Kbps.

HTTP (Hypertext Transfer Protocol)
The method used to convey information on the World Wide Web.

HTTPS (Hypertext Transfer Protocol Secure)
A combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encrypted communication and secure identification of a network Web server HTTPS connections are often used for payment transactions on the World Wide Web and for sensitive transactions in corporate information systems (source: Wikipedia).

IDS (intrusion detection system)
A software system that detects attacks on the network.

IETF (Internet Engineering Task Force)
The governing body responsible for establishing standards for the internet.

IMSI (International Mobile Subscriber Identifier)
A unique 15-digit number assigned to a mobile station issued at the time-of-service subscription containing subscriber identification information which is distinct from the subscriber's phone number.

IP (Internet Protocol)
The network layer protocol in the TCP/IP communications protocol suite (the "IP" in TCP/IP) Also references IP address, the four-element number with three decimal points that is the numeric identification of every node in a TCP/IP network.

ITU (International Telecommunications Union)
An international governing body that develops standards recommendations for telecommunications, consumer electronics, broadcasting, and multimedia communications The ITU's main responsibilities governing the mobile telecommunications industry is standardization, radio spectrum allocation, and the facilitation of arrangements between countries allowing for international phone calls.

KDF (Key Derivation Function)
Derives one or more secret keys from a secret value such as a master key and/or other known information such as a password or passphrase using a pseudo-random function. They are often used in conjunction with non-secret parameters to derive one or more keys from a common secret value (which is sometimes also referred to as "key diversification"). Such use may prevent an attacker who obtains a derived key from learning useful information about either the input secret value or any of the other derived keys. A KDF may also be used to ensure that derived keys have other desirable properties, such as avoiding "weak keys" in some specific encryption systems.

LCM (long code mask)
A 42-bit binary number that creates the unique identity for a long-code generator whose output is used in the CDMA coding and spreading process.

LTE (Long Term Evolution)
A 4G technology proposed and developed by 3GPP to improve the UMTS wireless standard LTE offers average data speeds of 9 -56 Mbps downlink and 2 - 13 Mbps uplink.

MD5
A widely used cryptographic hash function with a 128-bit hash value MD5 is an internet standard (RFC 1321) that is deployed in a wide variety of security applications.

MIN (Mobile Identifier Number)
The unique 10-digit number used to identify a mobile phone.

Mobile IP (MIP)
In MIP, the packet data session is not dropped each time the user changes location The session continues as long as mobility is still connected to the home agent.

MPLS (Multiprotocol Label Switching)
A datagram transport service designed to emulate circuit-switched network characteristics over a packet-switched network It can be used to carry many different types of traffic, such as IP packets, ATM frames, and Ethernet frames.

MSC (mobile switching center)
A core-network switching structure that bridges the mobile telephone access network with another telephone network such as the public switched telephone network (PSTN).

NAI (Network Access Identifier)
The user identification submitted by the mobile station during network access authentication.

OTA (over the air)
The process by which mobile stations are updated with new software or monitored for security.

PDSN (Packet Data Serving Node)
A PDSN establishes, maintains, and terminates a PPP session to a mobile station.

PIN (Personal Identification Number)
An optional 4- to 8-digit security code used to lock a SIM card in order to prevent unauthorized usage or access If the PIN is entered incorrectly too many times consecutively, then an end user will need the PUK to unlock the SIM card (see PUK definition).

PN (Pseudo-Random Noise) sequence
A set of bits intended to simulate the statistical randomness of noise A PN sequence is generated by a deterministic process and will repeat; therefore, it is “pseudo”-random.

PPP (Point-to-Point Protocol)
A common method to establish a direct connection between two points PPP is link layer-agnostic and is commonly used to establish a connection between a networked device and the internet.

PUK (PIN Unblocking Key)
A PUK is required to unlock a SIM in the event that an incorrect PIN is entered too many times consecutively The PUK code is typically provided by the service operator upon proper verification. If the wrong PUK code is entered too many times consecutively, the SIM will become permanently blocked and a new SIM card would be required.

RAN
Radio Access Network.

RANDSSD (Random Variable Shared Secret Data)
A 56-bit random number generated by the mobile station’s home station.

RNC (radio network controller)
A network element that controls and manages a group of connected base station controllers.

SIM (Subscriber Identity Module)
SIM is the term commonly used to identify the UICC, an integrated circuit in the form of a smart card which can be moved from device to device, required for Verizon Wireless 4G devices It is also a module used in GSM that may be added to the UICC It provides a means to authenticate the user, but it may also store other subscriber related information or applications such as text messages and phone book contacts.

SIP (Simple IP)
Simple IP is an IP address that is valid within a PDSN coverage area A mobile station must obtain a new IP address (and lose existing connections) when it moves from one PDSN coverage area to another coverage area A mobile station must obtain a new IP address (and lose existing connections) when it moves from one PDSN coverage area to another.

SNOW3G
A stream-cipher algorithm available in UMTS and LTE for the 3GPP encryption algorithms UEA2 and UIA2.

SSD (Shared Secret Data)
SSD is used to respond to authentication challenges SSD is a 128-bit number derived from the A-Key and random numbers.

SSL (Secure Sockets Layer)
Cryptographic protocols that provide security over the internet.

TIA (Telecommunications Industry Association)
A nonprofit trade association serving the telecommunications and information technology industries.

TMSI (Temporary Mobile Subscriber Identity)
Used instead of IMSI before authentication, to protect subscriber identification.

TLS (Transport Layer Security)
A cryptographic protocol to encrypt the segments of network connections at the Application Layer to ensure secure end-to-end transit at the Transport Layer.

UATI (Unicast Access Terminal Identifier)
An over-the-air signaling identifier that associates a mobile terminal with the access network’s radio resources used during the connection and call setup procedure.

UICC Universal Integrated Circuit Card)
The smart card used in mobile terminals in GSM and UMTS networks The UICC ensures the integrity and security of all kinds of personal data.

VoLTE (Voice over LTE)
A digital voice service that runs over the Verizon 4G network.

VoWiFi (Voice over Wi-Fi)
A digital voice service that allows users to access Verizon voice services over a Wi-Fi connection while not in 4G LTE coverage.

verizon business