## Contents

### Introduction ................................................. 3

### Wireless Standards ....................................... 4
- LTE (4G) Access Networks ............................... 4
- Dynamic Mobile IP Update ............................. 5
- Digital Voice Services .................................. 5
  - HD Voice (Voice over LTE or VoLTE) ............... 5
  - WiFi Calling (Voice over WiFi or VoWiFi) ......... 5

### Network Services ......................................... 6
- User Authentication and Authorization ............. 6
- Intrusion Prevention ................................. 6
- Roaming ............................................. 6

### Enterprise Services ...................................... 7
- Private Network ....................................... 7
- Connectivity Management Tools ...................... 8
  - Machine to Machine (M2M) Management Center .... 8
  - ThingSpace Manage Customer Portal ............ 8
- Unified Web Services (UWS) .......................... 8
- ThingSpace Develop Portal .......................... 8
- Secure Access Control to Connectivity Management Tools 8

### Device Management .................................... 9
- Enterprise Mobility Management ....................... 9
- Mobile Iron ........................................ 9
- Verizon Mobile Device Management .................. 9

### Application Security .................................... 10
- Voice Cypher ....................................... 10
- IoT Security Credentialing ............................ 11
- OSI Model view of Security features - IOTSC ....... 11

### Device Security .......................................... 12
- Device Access Password & Device Storage Encrypted 12
- Verizon Support & Protection ....................... 12
- Device Security Features ............................ 12

### Policy & Governance .................................... 13
- Vulnerability Management ............................ 13
- Risk Management .................................... 14
- Security Monitoring & Response ..................... 14

### Physical Security ....................................... 15
- Partitioned Access Control Systems .................. 15
- Intrusion Detection & Alarm .......................... 15
- Systems Surveillance – 24x7 ......................... 15

### Legacy Technologies .................................... 16
- 1xRTT Access Networks ............................... 16
- EV-DO (3G Data) Access Networks .................. 16

### Summary ................................................ 17

### Glossary of Terms ....................................... 18
Introduction

As wireless networks become increasingly more prevalent, new possibilities and challenges continue to emerge. Addressing security needs becomes paramount to delivering solutions that meet today's demand for mobility. Verizon Wireless has been at the forefront of offering secure wireless solutions that reduce the security risk to personal and corporate information.

The Verizon Wireless mobile data network has many of the same components found in a typical corporate network, and managing these components requires innovative proprietary and commercially available methods for securing our network and protecting our customers. Verizon Wireless has instituted a multi-pronged strategy to security which encompasses our internal engineering teams, external software development partners, and 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 reputed bodies. Internally developed applications and infrastructure are measured by these standards prior to deployment.

Additionally, all externally developed applications are subject to pre-launch security audits conducted by trusted independent security experts, to verify that the applications have a limited attack surface and do not undermine Verizon Wireless' security posture. Furthermore, the security controls – both technical and procedural – for all commercial products are evaluated by third-party experts prior to their acceptance and introduction into the Verizon Wireless network.

In addition to the aforementioned tactical security projects, we also undertake several strategic initiatives such as proactively gathering intelligence, developing security standards for our OEM providers to abide by, and working closely with fraud detection teams to limit the exposure in the event of a security incident.

This white paper focuses on how Verizon Wireless addresses all aspects of security to enable mobile users to enjoy secure access.

For an in-depth look at overall and industry specific security best practices see Verizon's Data Breach Investigations Report.
Many elements in the Verizon Wireless network 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 Wireless operates 4G LTE (Long Term Evolution) as its primary wireless network, and CDMA (Code Division Multiple Access) as its legacy network (see Legacy Technologies section for details on CDMA). Both 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.

**LTE (4G) Access Networks**

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 IP (Internet Protocol) based infrastructure. With LTE, Verizon Wireless continues to meet both business and consumer demands for a higher bandwidth, low latency service that will work broadly in the United States and globally, since many carriers around the world have chosen LTE as their long term direction as well. We discuss below the key security enhancements in LTE Access.

**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, and is shared with Verizon Wireless only, via a secure connection, keeping the data from being co-opted. 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 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 the network credentials. Mutual authentication protects against attacks from rogue base stations, and hence, defeats any kind of man-in-the-middle attack. The 4G SIM card contains the necessary authentication algorithms and certificates, which aids in the secure accessing of the network. The primary algorithm for accessing the LTE network services is the 3GPP defined algorithm, MILENAGE. During initial attachment to the network, 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 doubles the key strength and in so doing requires a greater "level of effort" in attacking the algorithm. The security keys in the LTE network are derived from a Key Derivation Function (KDF). Each key has a different input but 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 Wireless LTE network. The key for UP traffic is retained for the period that the UE is in a valid connected session and the keys are deleted on transition to idle mode or on handover to another LTE cell site. Also, 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 Wireless LTE network supports 128-bit AES and SNOW3G algorithms for integrity protection.

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

<table>
<thead>
<tr>
<th>Secure storage</th>
<th>Device with credentials and secret data for secure access of the network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual authentication</td>
<td>In LTE, both the device and the network authenticate each other.</td>
</tr>
<tr>
<td>Root key length</td>
<td>Key length better secures user plane and signalling information.</td>
</tr>
<tr>
<td>Security context</td>
<td>Keys to encrypt signalling and subscriber data created for each session</td>
</tr>
<tr>
<td>Integrity protection</td>
<td>Additional algorithm to check the integrity of data translated.</td>
</tr>
<tr>
<td>Encryption</td>
<td>Signalling and subscriber data encryption</td>
</tr>
</tbody>
</table>

Dynamic Mobile IP Update

The CDMA2000 mobile IP standard was designed to incorporate cryptographic keys for Mobile IP (MIP) security. However, the standard did not provide an efficient means to distribute MIP keys to mobile stations. To address this, Verizon Wireless developed the Dynamic Mobile IP Update (DMU) standard which allows manufacturers to embed public RSA (an algorithm for public-key cryptography) encryption keys into mobile stations to enable secure distribution of mobile IP keys. The DMU standard enables stronger cryptographic keys – 128-bit authentication – and provides stronger authentication of MIP registration messages. DMU is used to provision simple IP and mobile IP credentials, where it is used to enforce key lifetimes and establish security policies on the keys such as key length, etc. Security and protection continue even as the subscriber moves through the service area. Overall, the DMU standard adds another layer of device authentication.

Digital Voice Services

Digital voice services are based on the SIP/RTP protocols. The signaling protocol (SIP – Session Initiation Protocol) is routed from the mobile device to the signaling servers in the Verizon core network. The media traffic is peer to peer.

HD Voice (Voice over LTE or VoLTE)

The mobile device uses the 4G LTE network to connect to voice services. This occurs after the mobile has authenticated to the network, and therefore utilizes the inherent 4G LTE security features. The signaling registration or SIP registration uses the credentials in the UICC to perform mutual authentication between the mobile and the signaling server. Once registration is complete, the mobile is able to make and receive voice calls. Media traffic for any voice call is mobile to mobile (peer to peer aka P2P). IP traffic for voice signaling and media is prioritized on the network and over the RAN.

WiFi Calling (Voice over WiFi or VoWiFi)

This service allows Verizon customers to connect to HD Voice services while outside of 4G coverage. This service uses mutual authentication, based on the UICC credentials, to establish an IPSec connection between the mobile and the edge of the Verizon network.

Voice and video calls are encrypted using IPsec – industry standard encryption and transport mechanism to provide secure IP communications. Both voice and video traffic are encapsulated inside the IPSec Tunnel. WiFi calls are carried within IPSec tunnels. The key protocols to support the IPSec tunnel are IKEv2 (Internet Key Exchange Version 2, RFC 5996), ESP (IP Encapsulating Security Payload, RFC 4303), and UDP Encapsulation of IPsec ESP Packets (RFC 3948). The enterprise WiFi network/ISP must ensure they do not block these protocols and the corresponding ports used by these protocols. After establishment of the IPSec connection, the mobile will perform SIP registration just like the standard HD Voice service. Only SIP signaling/registration, as well as media traffic, flows over the IPSec connection to the Verizon network.
Network Services

The Verizon Wireless mobile data network uses authentication protocols to establish a user's identity before network access is granted. Verizon Wireless follows many of the established security and access procedures implemented by corporate IT organizations. This section will cover those topics, plus roaming.

User Authentication and Authorization

With the 1xRTT & EV-DO data networks, once a subscriber is authenticated on the Verizon Wireless access network, he or she is authenticated for IP services using CHAP with the Packet Data Serving Node (PDSN), during PPP establishment between the mobile station and the PDSN. Authenticating subscribers at the packet data level provides differentiated services to Internet users and mobile subscribers. The subscriber profile in the AAA defines which services the subscriber is authorized to access.

In the 4G LTE network, both network and subscriber authentication/authorization is based on the SIM card credentials and is performed during the access authentication process.

Intrusion Prevention

The Verizon Wireless network also incorporates mobile network protection mechanisms that monitor and protect against anomalous and detrimental behavior. These tools include firewalls, Intrusion Detection, IP data controls and rules, correlation & analysis and malware detection/prevention.

Firewalls are a key factor in maintaining the overall security of the mobile data network. As part of Verizon Wireless best practices security plan, firewalls are used to partition the network into easily controllable security domains. Verizon Wireless also has firewalls on the direct circuit to enterprise networks and has choke routers to protect its Internet interface.

Roaming

Verizon Wireless allows its subscribers to roam on other networks operated by carriers with whom Verizon Wireless has roaming agreements, while maintaining security. This is achieved by employing the same authentication mechanisms across users – whether home users or roamers. For roaming authentication, Verizon Wireless securely stores the authentication credentials on its network and doesn't share them with any other network operator. This helps to prevent operator fraud. In addition, authentication occurs between Verizon Wireless and the mobile station, with the roaming network as a pass-through for authentication information.
Enterprise Services

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

Private Network

Verizon Wireless Private Network (Private Network) is a comprehensive solution that joins wireless devices to the 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 Private Network, 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 Private Network, 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 radio access network, 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.

Verizon Wireless offers a variety of IP addressing options that provide differing levels of accessibility, protection, and manageability. The private network supports enterprise-owned private IP address assignment to the devices, which essentially makes the 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 IT administrators to define which users get Internet access. 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:

- 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.
- 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, and 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.
- Each Private Network is assigned to a unique set of ingress and egress IP resources in our Packet Gateway (PGW- Enterprise Universal Gateways). Each mobile device provisioned for the Customer Private Network 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.
- Each Private network is assigned to a unique egress routing domain at the provisioned PGW; this is done by assigning a unique Virtual Routing and Forwarding (VRF) or VLAN.
- 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 Private Network gateway and the customer premises equipment (CPE), which allows access only into the company's IP network with their hosted applications.
- Private Network is isolated from the Public Internet.
- Private Network, by virtue of its design, 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.
- Supports Internet Protocol Security (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.
- The Dynamic Mobile Network Routing (DMNR) option on the private network 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 enterprise 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.
Connection Management Tools

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

Machine to Machine (M2M) Management Center

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

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.

Unified Web Services (UWS)

Verizon Wireless offers Unified Web Services as 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 SSL (with 128 bit or higher encryption) with white-listing of the customer’s application server IP address.

Secure Access Control to Connectivity Management Tools

The connectivity management tools 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 RESR web services API technology. Customers use these APIs to integrate connectivity management tools 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.

See Private Network White paper for more information about Verizon Private Network
Device Management

Device Management takes security beyond the initial setup. Enterprises can send new applications via Over The Air (OTA) to the mobile station to keep it current with Enterprise IT policies. As a mobile station is subscribed to new services, or as Enterprise IT policy changes, Device Management allows mobile stations to be brought up to date. If a mobile station has been compromised, an Enterprise IT administrator can lock the mobile station by sending a message to it. The Enterprise IT administrator can also erase the contents of the mobile station, rendering it useless until it is re-provisioned. Mobile stations can also be backed up and restored via OTA.

For an in-depth look at overall and industry specific security best practices see Verizon’s Data Breach Investigations Report

Enterprise Mobility Management

For enterprises that are looking for a partner that manages the device and its data security, Verizon offers a broad suite of products for device management, application management, firmware and software management, and device diagnostics. Verizon teams with MobileIron and other Enterprise Mobility Management (EMM) providers to deliver traditional EMM capabilities. Verizon Mobile Device Management (MDM) is a suite of products that enhances an enterprises traditional EMM service. Verizon can provide these products due to its unique knowledge of our network and customer devices.

MobileIron

Verizon offers MobileIron as an add-on solution. MobileIron is an Enterprise Mobility Management (EMM) solution that allows IT to manage and secure devices, apps and content on multi-OS environments (Android, Apple and Blackberry smartphones) as well as utilize cloud services. EMM solutions allow companies to leverage mobile technology as a tool of business transformation by empowering end users to be more productive where and when they need to be, on virtually any device, while enabling IT to meet security requirements. EMM is made up of three components, Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Content Management (MCM). With MobileIron customers can:

- Selectively wipe work data.
- Separate between work and personal apps.
- Allow single sign-on & secure access.
- Secure email.

Verizon Mobile Device Management

To help maintain security and continuity of your business, Verizon MDM enables enterprise firmware over-the-air (FOTA) management and device diagnostic services. Using FOTA management, an enterprise can postpone and assess customer/corporate applications on new device firmware updates to their devices prior to large-scale deployment, which can improve overall security and efficiency. With Verizon’s robust device diagnostics tool, an enterprise can download and monitor diagnostic data from mobile devices, including network signal strength.
Application Security

Many of our enterprise customers choose to utilize their own encryption applications to encrypt voice/data end-to-end. Secure Sockets Layer (SSL) and Transport Layer Security (TLS) are standards-based protocols that allow 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 an additional layer(s) of security to help thwart cyber-attacks.

Application protection enhances security even if the call or data crosses over multiple networks. Application protection consists of a number of security tactics working to protect your 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.

Voice Cypher

Verizon offers Voice Cypher as an add-on service. Voice Cypher is an encrypted Voice over Internet Protocol (VoIP) solution that provides end-to-end voice encryption between smartphones, even if the call crosses over multiple networks. Voice Cypher encryption provides inherent security, so calls are secure even if intercepted. This advanced security solution also provides encryption for critical text messages.

Voice Cypher also delivers:

- Advanced functionality and cost effective solution with ease of management.
- High-level assurance with National Institute of Standards and Technology (NIST)-certified voice security, using AES-256 encryption to counter cyber security threats.
- Software-based Voice over IP (VoIP) application that can operate on virtually any LTE, CDMA, GSM network or any network with Internet access.
- In cases when enterprise and government do not want to utilize a vendor hosted Management Portal, a Private Switch can be deployed behind the customer’s firewall.
- The Voice Cypher Gateway provides the capability to connect the secure Voice Cypher users to most Office-based PBX phone systems.
- Voice Cypher operates on supported Android, Apple, Windows Mobile and BlackBerry smartphones.
IoT Security Credentialing

IoT Security Credentialing (IOTSC) enhances security by Mutually Authenticating and Encrypting your services, devices, and applications. Verizon's IoT Security Credentialing 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 IOTSC provides the security services needed for establishing trust in online electronic transactions: confidentiality, integrity, identity authentication and non-repudiation. The establishment and operation of IOTSC certificate authority are governed by their respective Certificate Policies (CP) and Certificate Practice Statements (CPS).

• Helps enable identity management for data protection and integrity both “at rest” and “in transit”; Authentication, encryption, signing and time-stamping for mobile users, machine-to-machine, internal infrastructure and internal/external web-services

• Automated authentication: While humans can input things like user name and passwords, devices will not function at full efficiency without high levels of authentication speed; IOTSC facilitates secure connectivity to non-traditional computing devices (e.g. medical devices, HVAC systems, televisions, home appliances, smart meters, etc.)

• Defense in depth: Digital credentials (a.k.a. PKI) secure digital communications transparently and provide additional layers of protection for your network devices, servers and applications.

• Highly reliable and scalable: IOTSC is operated from Verizon data centers in the United States and around the world, and can produce tens of millions of digital credentials in a fast and cost-efficient manner based on customer’s needs.

OSI Model view of Security features - IOTSC

<table>
<thead>
<tr>
<th>OSI Model</th>
<th>Security Solution</th>
<th>Function</th>
<th>Customer Impact Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>IoT Security Credentialing</td>
<td>Application protection</td>
<td>• Helps customer address the authentication and encryption requirements of security standards.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Helps protect devices and applications using multiple networks (ex: Wi-Fi, LTE).</td>
<td>• Protects against lost/stolen SIM cards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mutual authentication</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Best practice designed to “break the attack chain” before systems are breached</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SIM protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Prevents SIM from being used on devices that are not part of the Private Network</td>
<td></td>
</tr>
<tr>
<td>Transport</td>
<td>VZW Private Network</td>
<td>• Segmentation of data and devices from the internet</td>
<td>• Helps reduce overages on remote devices, due to Internet attacks, using VZW's network.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• One-way network authentication</td>
<td>• Extends existing Private Networks to mobile devices.</td>
</tr>
<tr>
<td>Network</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Link</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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.

Device Access Password & Device Storage Encrypted

Verizon Wireless provides devices to its customers that are capable of password protection on the use of 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 Wireless. Verizon offers a complete suite of managed services in device configuration management.

Verizon Support & Protection

Verizon offers a security suite of applications for smartphones which is 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 risks applications present in transmitting personal information. Customers are also alerted if connected to an unsecure WiFi connection, or if spoofing is detected.

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

Device Security Features

The following features are available on most recent devices; however, verify specific feature set for each device.

Secure Boot: Helps prevents any OS modification or unauthorized OS software from being executed. During 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: Helps prevents interception and alteration of data being transmitted across the network, including via the radio access network using TLS and VPN.

Device rooting detection (Android only): Detects OS modification and reports to user through VSP app.

Anti-Theft (Kill Switch): Helps prevents device from being used by unauthorized user.
Policy & Governance

Policy and Governance is the cornerstone of any good security program, and Verizon Wireless has created enterprise-wide policies that conform to the ISO 17799 and NIST standards for the protection of customer and employee information. We have created standards for our operations that reflect these corporate policies and have instituted a program to maintain adherence to the corporate policies.

Vulnerability Management

Vulnerability management is a key aspect to protecting the Verizon Wireless network. We have implemented a four stage vulnerability management model, described in more detail below.

**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 company'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 the four stages outlined above, we regularly monitor various sources to identify trends for potential new vulnerabilities emerging in the hacker community. Tracking vulnerabilities is one measure of how well we are performing when it comes to security assessment, evaluation and resolution.

**Key Policies & Guidelines**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidential and Proprietary Data Policy</td>
<td>Network Firewall Guidelines</td>
<td>External / Extranet Supporting Practices</td>
</tr>
<tr>
<td>Disposition of Personal Computing Assets</td>
<td>Desktop &amp; Laptop Security</td>
<td></td>
</tr>
<tr>
<td>Database Standards</td>
<td>Encryption Key Management</td>
<td>Internal / Intranet Supporting Practices</td>
</tr>
<tr>
<td>Internet and Web Users</td>
<td>Externally Hosted Internet Applications</td>
<td></td>
</tr>
<tr>
<td>Secure Socket Layer (SSL) Certificates</td>
<td>Wireless LAN</td>
<td>Third Party VPN/Extranet</td>
</tr>
<tr>
<td>Violation Reporting</td>
<td>VPN Security</td>
<td></td>
</tr>
<tr>
<td>Electronic Mail/Instant Messaging Access &amp; Usage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wireless Device Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCI Logging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Support Center Data Privacy Practice</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2. Stages of Vulnerability Management**
Risk Management

Verizon Wireless conducts a pre-launch security risk assessment for all 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, which could be exploited. The penetration testing is conducted by both Verizon employees 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).

The information gleaned from the Security Risk Assessment is used to decide whether or not to move forward with a commercial launch of the product. In addition, we work with the product or platform vendor to make sure that all identified issues are either resolved prior to commercial launch or, at a minimum, that mitigation plans are in place prior to complete resolution.

Verizon Wireless also performs Network Data Leakage Protection (DLP) to analyze network traffic for unauthorized information transmissions, including email, IM, FTP, HTTP, and HTTPS (called data in motion).

Security Monitoring & Response

Verizon Wireless 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 (Denial of Service, SYN Floods, Ping Sweeps, BotNets, etc) 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 (CISPP, 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 reoccurrence 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 24x7 basis.

Verizon employs experienced security and privacy professionals with several professional certifications (i.e. CISSP, CISM, etc) 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 described in detail below.

- Separation of Duties: This is a practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the overall process.
- Dual Control: This is 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 (for example, the cryptographic key).
- Access Control: Mechanisms that limit availability of information or information processing resources only to authorized persons or applications.
Physical Security

Partitioned Access Control Systems
As per Verizon Wireless 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.

The 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. The 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.

Intrusion Detection & Alarm
The 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.

Systems Surveillance – 24x7
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. The local control point may not be manned 24x7 however the NOCs are fully manned and are monitoring these facilities. 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 24x7 to respond if necessary.
Legacy Technologies

1xRTT Access Networks
1xRTT works by using a unique pseudo-random noise (PN) sequence to encode each user's information. This sequence is then spread across the full channel bandwidth (1.25 MHz) before it is transmitted over the air. The signal resembles white noise when transmitted over the air, except that it can be filtered out only by the receiving radio, which is aware of the exact PN sequence used to encode the user's information. There are over 4.4 trillion different PN code combinations, making it extremely difficult to intercept a specific connection's PN sequence. 1xRTT technology supports the use of multiple cells (soft handoff) simultaneously (up to 6 cells) making it very difficult to “follow” the 1xRTT call.

1xRTT authenticates device identity and subscriber identity using three components: A-key (secret value), MIN, and ESN. For example, if someone tries to steal a mobile device and sell it, Verizon Wireless can track the subsequent usage of this mobile device, thus reducing the incentive to steal devices. To authenticate, the Mobile Switching Center (“MSC”) sends a random binary number (RANDSSD) to all of the mobile devices in its service area. Mobile devices use the CAVE algorithm, A-Key, ESN, and MIN to generate Secret Shared Data (SSD) and forward it to the MSC. The network authentication center generates SSD using the same set of authentication inputs. If the signature of the authentication center and the mobile station match, the MSC is informed of the successful authentication and both the ESN (device) and MIN/IMSI (subscriber) are authenticated. If they do not match, then access to the network is denied for that mobile station, and its user is denied network access.

EV-DO (3G Data) Access Networks
EV-DO is protected on the up link (from the mobile to the cell site) by the same long code mechanism used in 1xRTT. The EV-DO down link (from the cell site to the mobile) uses a method called time-multiplexing. This method ensures each user has full use of the airlink during the time slots dynamically scheduled for them. Each user’s packets are coded and repeated over multiple slots and transmitted over the air. The receiving mobile has the ability to acknowledge the first successful receipt of the data and uses an early termination mechanism to prevent any subsequent transmission of that packet. These attributes make it virtually impossible to identify the user or to correlate user packets.

During EV-DO session setup, the mobile requests an identifier – the Unicast Access Terminal Identifier (UATI) from the EV-DO access network. This identifier allows the EV-DO access network to uniquely identify a mobile within the EV-DO network. The mobile includes the UATI whenever it sends the access request. Access authentication between an EV-DO mobile station and Radio Network Controller (RNC) takes place when the mobile initiates the Point-to-Point Protocol (PPP) connection. Access authentication does not require any user interactions but uses Challenge Handshake Authentication Protocol (CHAP) and Message-Digest algorithm 5 (MD5).

It requires that the mobile supports the MD5 algorithm and saves the A12 Network Access Identifier (NAI) and authentication keys. The RNC obtains the subscriber-specific NAI, authentication keys (passwords), and International Mobile Subscriber Identifier (IMSI) from the Authentication, Authorization and Accounting (AAA) server via the A12 interface.
Summary

Verizon Wireless complies with industry, statutory and regulatory requirements regarding safeguards and controls of protected information. Verizon Wireless 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 and will meet our customer expectations, because we have instituted a multi-pronged strategy to security, and offer several additional security products.

**Wireless Standards & Services:** Verizon Wireless operates CDMA & LTE 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 Wireless has created enterprise-wide policies that conform to the ISO 17799 and NIST standards for the protection of customer and employee information.

**Vulnerability Management:** Verizon Wireless has implemented a four stage (Discovery, Assessment, Remediation and Validation) vulnerability management model to guard against vulnerabilities.

**Risk Management:** Verizon Wireless 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 Wireless 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 reoccurrence of that event. The NSIRT team is on-call on a 24x7 basis.

**Physical Security:** Verizon Wireless has implemented a partitioned access control systems by which access is granted based on individual needs. The Network centers and cell sites are designed and equipped with intrusion detection and alarm systems and 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.

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.

2G (third generation) – Third-generation cell-phone technology appeared in the 2000s and forms the foundation of our current cell-phone capabilities. 2G technology offers even faster Internet access, plus enables worldwide roaming capabilities.

3G (third generation) – The introduction of 2G technology has enabled a high-speed data service that gives users high-speed data rates, lower latency over current 2G systems, and the facilitation of arrangements between countries allowing for international phone calls.

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.

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.


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.

DMN R (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.

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 are 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 5-12 Mbps downlink and 2-5 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.


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.

SSH (Secure Socket 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.

Transport Layer Security (TLS) — 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 — The Universal Integrated Circuit Card (UICC) is 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 WiFi) — A digital voice service that allows users to access Verizon voice services over a WiFi connection while not in 4G LTE coverage.
Contact Information

For more information about Verizon Wireless, speak with a Verizon Wireless sales representative, visit verizonwireless.com, or call 1.800.VZW.4BIZ.

Legal Disclaimer
This document and the information contained herein (collectively, the “Information”) is provided by Verizon Wireless, on behalf of itself and its affiliates for informational purposes only. Verizon Wireless is providing the Information because Verizon Wireless believes the Information may be useful. The Information is provided solely on the basis that each business will be responsible for making its own assessments of the Information and businesses are advised to verify all representations, statements, and information before using or relying upon any of the Information. Although Verizon Wireless has exercised reasonable care in providing the Information, Verizon Wireless does not warrant the accuracy of the Information and is not responsible for any damages arising from the use of or reliance upon the Information. Verizon Wireless in no way represents, and no reliance should be placed on any belief, that Verizon Wireless is providing the Information in accordance with any standard or service (routine, customary or otherwise) related to the consulting, services, hardware, software, or other industries.