T2 Transparent Technologies
Beyond AMR™

T2 Virtual Network
Security Overview

February 2013

System specifications are subject to change

— CONFIDENTIAL —

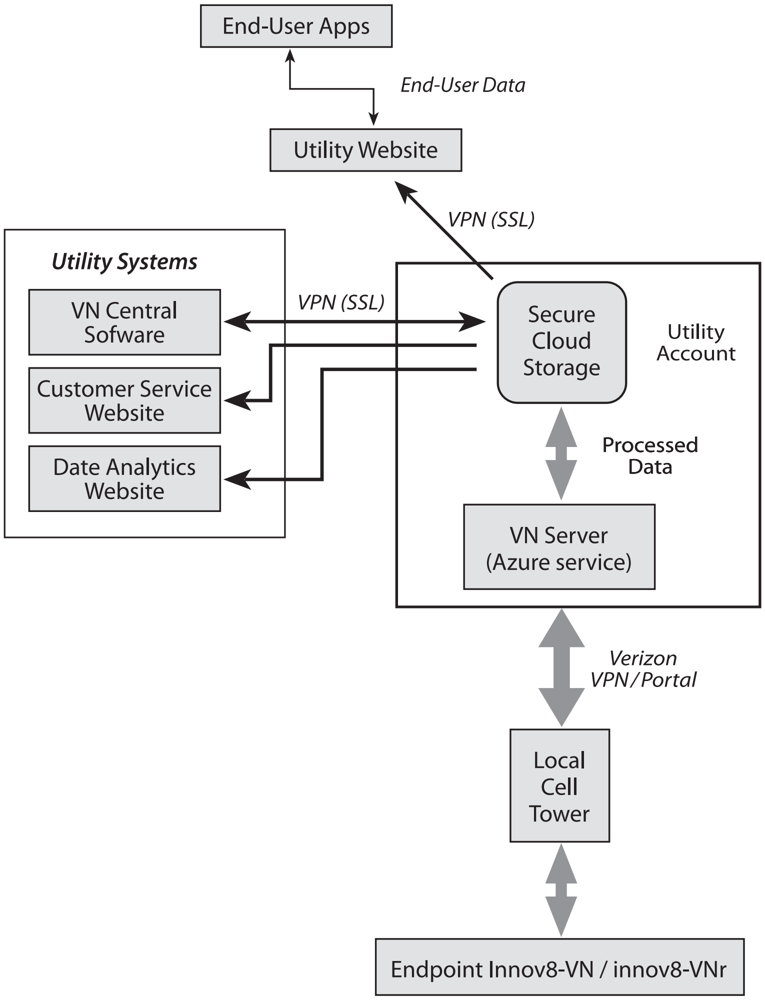
T2 VIRTUAL NETWORK
Security Overview for the VN System

Summary

The utility industry has been undergoing significant changes in recent years with the introduction of smart meters. In the electric utility world, the smart grid has accelerated the development of advanced metering infrastructure, meter data management software and more. However, along with the features and benefits come potential security concerns. These advanced systems and the volumes of "personally identifiable data" that they collect could be inadvertently exposed, or hacked, by malicious or meddlesome individuals. Thus, utility professionals are looking for assurances that AMI system manufacturers have designed their systems with appropriate security at all levels.

Transparent Technologies (T2) has designed the VN System for Water AMI with extensive security features throughout the system. Along with the intentional design security features, the system requires some security "best practices" from the utility. These features and best practices are described below.

The following diagram shows the main components of the system:



Endpoints

The innov8-VN and innov8-VNr endpoints are physically accessible by the utility's end-consumers of water. The endpoints are also the source of the consumption data and by identification number are linked to the end-consumer account and address. Thus, the endpoints require significant security emphasis.

The innov8-VN and the innov8-VNr are completed sealed units. The plastic housing is sealed with permanent UV-cured glue which makes disassembly and access to the microcontroller/firmware very difficult.

The endpoints have a combined bootloader and operational firmware file. This makes the scenario of having a hacked unit reloaded with new firmware very unlikely. The only method for new firmware uploads is via the endpoint's communication's ports via a proprietary protocol.

Each endpoint has a unique ID which must be authenticated on the network. No personally-identifiable data (i.e. address, name or account number) is set in the endpoint and all network information for the Verizon Wireless network interface is completely hidden from the user.

The innov8-VN and innov8-VNr use a pseudo-random transmission timing which minimizes the possibility of packet interception very difficult.

Another key to the security on the endpoints is best practice by the utility. The utility should carefully control access to the field computers used for endpoint installation/configuration and also implement user authentication (login/password) protocols for all personnel.

Verizon Wireless Network

The VN system utilizes the Verizon Wireless 2G network. The 2G network is a 1xRTT CDMA2000 network, which is extremely secure from eavesdropping, interception or deciphering.

CDMA stands for "code division multiple access" and it was originally a secure military transmission method. CDMA uses direct sequence spread spectrum (DSSS) which spreads the transmission across a broad frequency range. It utilizes specific spreading sequences and pseudo-random codes for the forward link (i.e. the path from the base station to the endpoint) and on the reverse link (i.e. the path from the endpoint to the base station). These spreading techniques are used to form unique code channels for individual users in both directions of the communication channel. Because the signals of all calls in a coverage area are spread over the entire bandwidth, it creates a noise-like appearance to other endpoints or mobiles devices in the network as a form of disguise, making the signal of any one call difficult to distinguish and decode.

References:	Qualcomm – CDMA2000 1xRTT Security Overview
	Verizon Wireless – CDMA Network Security

Virtual Private Network (VPN)

Verizon Wireless' network and the Microsoft network / data center are connected securely via a virtual private network (VPN). The VPN provides a dedicated security tunnel for all VN system data traffic between the Verizon network and the VN Server (located on a Microsoft Data center on the Microsoft network). The access points to both ends of the VPN are physically secure and tunneling and 128-bit encryption is used to prevent unauthorized access, interception or tampering.

References:	Terramark system brochure

Microsoft Network, Data Centers

Microsoft created the Microsoft Global Foundation Services to provide infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) businesses. The GFS infrastructure is in essence a broad network of ultra-secure data centers which employ security frameworks based on the ISO 27000 family of standards.   The Microsoft data centers provide the Azure platform which is the engine for the VN Server. The link below will provide extensive information on GFS.

References: http://www.globalfoundationservices.com

Microsoft Azure™

Microsoft Azure™ is a powerful and flexible Platform-as-a-Service (PaaS) tool which the VN Server and storage is built upon. As a platform hosting application, Azure™employs a wide range of security features including identity and access management tools and SSL authentication.   These tools are integrated into the overall VN Systems components such as the VN Central software and end-consumer access software.

Reference: Windows Azure™ Security Overview

Utility Network and Software Applications

Microsoft Azure™ is a powerful and flexible Platform-as-a-Service (PaaS) tool which the VN Server and storage is built upon. The utility software is particularly sensitive to security due to its access to end-consumer's personally-identifiable data (name, address, consumption history). The utility software solutions (VN Central, VN Customer Service, VN Data Analytics) all require an SSL connection to access the data in the Azure™ tables. Furthermore, each utility will have a unique ID and random pass code. The ID and passcode will be used for authentication for each connection.

The ability to modify data within the Azure™ tables is not possible within the VN Central, VN Customer Service or VN Data Analytics web applications. Data modification can only be accomplished with coordination with T2 system administrators.

Each endpoint installed in the system will have a corresponding entry in the Azure™ account list. Any invalid ID or transmission will be ignored by the VN Server and not be populated in the tables. Rogue transmissions are logged in a diagnostic file for potential troubleshooting.

The VN Server stores diagnostic information such as orphan transmissions, duplicate IDs, etc. to be used for troubleshooting. Missed transmissions can be identified with email notices. The Azure™ tables also store the firmware version for each endpoint which can be reviewed for unexpected deviations.

The VN Central software has reports which can assist in troubleshooting or researching potential security issues such as zero usage, high usage and missed transmissions. Utility personnel can also analyze the consumption history of any account to review abnormal changes in usage.

Another key to the security on the utility software is best practice by the utility. The utility should carefully control access to the office computers used for data access and also implement user authentication (login/password) protocols for all personnel.

End-consumer Data Access Software

The end-consumer data access software is a web application which must be accessed through the utility's website. This will allows the utility to setup an authentication routine (i.e. account name/password) to ensure secure data access.

The end-consumer data access software is a web application which requires a SSL connection to access the data in the Azure™ tables. The web access will also utilize the utility's unique ID and random pass code.