On-Ramp Total Reach Network Security Specification

On-Ramp Wireless Confidential and Proprietary. Restricted Distribution. This document is not to be used, disclosed, or distributed to anyone without express written consent from On-Ramp Wireless. The recipient of this document shall respect the security of this document and maintain the confidentiality of the information it contains. The master copy of this document is stored in electronic format, therefore any hard or soft copy used for distribution purposes must be considered as uncontrolled. Reference should be made to On-Ramp Wireless to obtain the latest revision.

On-Ramp Wireless Incorporated
10920 Via Frontera, Suite 200
San Diego, CA 92127
U.S.A.

Copyright © 2013 On-Ramp Wireless Incorporated.
All Rights Reserved.

The information disclosed in this document is proprietary to On-Ramp Wireless Inc., and is not to be used or disclosed to unauthorized persons without the written consent of On-Ramp Wireless. The recipient of this document shall respect the security of this document and maintain the confidentiality of the information it contains. The master copy of this document is stored in electronic format, therefore any hard or soft copy used for distribution purposes must be considered as uncontrolled. Reference should be made to On-Ramp Wireless to obtain the latest version. By accepting this material the recipient agrees that this material and the information contained therein is to be held in confidence and in trust and will not be used, copied, reproduced in whole or in part, nor its contents revealed in any manner to others without the express written permission of On-Ramp Wireless Incorporated.

On-Ramp Wireless Incorporated reserves the right to make changes to the product(s) or information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an “as is” basis.

This document contains On-Ramp Wireless proprietary information and must be shredded when discarded.

This documentation and the software described in it are copyrighted with all rights reserved. This documentation and the software may not be copied, except as otherwise provided in your software license or as expressly permitted in writing by On-Ramp Wireless, Incorporated.

Any sample code herein is provided for your convenience and has not been tested or designed to work on any particular system configuration. It is provided “AS IS” and your use of this sample code, whether as provided or with any modification, is at your own risk. On-Ramp Wireless undertakes no liability or responsibility with respect to the sample code, and disclaims all warranties, express and implied, including without limitation warranties on merchantability, fitness for a specified purpose, and infringement. On-Ramp Wireless reserves all rights in the sample code, and permits use of this sample code only for educational and reference purposes.

This technology and technical data may be subject to U.S. and international export, re-export or transfer (“export”) laws. Diversion contrary to U.S. and international law is strictly prohibited.

Random Phase Multiple Access™ is a trademark of On-Ramp Wireless Incorporated.

Other product and brand names may be trademarks or registered trademarks of their respective owners.

On-Ramp Total Reach Network Security Specification

014-0043-00 Rev. C

April 2, 2013

Contents

Figures

Tables

Revision History

Revision	Release Date	Change Description
A	September 10, 2012	Initial release
B	September 27, 2012	Updated to address open PRD security requirements.
C	April 2, 2013	Updated product names and figure.

1 Overview

The critical nature of utility, oilfield, industrial, and tracking automation requires strong security for communications between automation sensor devices and the back office systems processing the automation information. The On-Ramp Total Reach™ (OTR) Network delivers third-party verified security strength from end point to back-office interfaces. This specification describes the challenges securing communications for these types of automation solutions, and then addresses how the OTR technology meets these challenges.

2 The Challenge Securing the “Internet of Things”

2.1 What is the “Internet of Things?”

As the Internet changed the world of communications drastically, M2M (machine to machine) communications or the “Internet of things” was positioned to change the world even more dramatically. At its most basic definition, the “Internet of things” refers to uniquely identifiable objects (things) and their virtual representations in an Internet-like structure. It is clear that this structure alone will not deliver the potential for the “Internet of things” to change the world.

We believe that cost-effective, secure communications is the missing piece of the puzzle. A continued challenge is providing cost-effective and secure communications to the “things” that are often quite numerous, geographically dispersed, and in some cases, dependent on battery power. Being able to economically receive and send data to the millions of devices in an efficient fashion will make possible services that improve the quality of human life, reduce resource waste, and add incremental value to all devices by more intelligently using the collective network information. Examples of such services include:

- Improving use of utility and oilfield resources by measuring and reliably communicating critical values such as temperature, current, voltage, etc.
- Making human life better by measuring and reliably communicating critical values such as blood pressure, blood sugar levels, heart rate, etc.
- Enhancing human and asset safety with intelligent tracking applications.

Securely automating communications between the sensors that measure and generate data (i.e., the things) and the various users of the sensor data (i.e., the Internet portals) is critical to delivering on the anticipated potential of the “Internet of things.”

Of course, providing the communication links to the hundreds of millions of devices seems like an easy problem to solve: All we need to do is to enable these devices to use existing communications technologies. Low-tech solutions such as mesh, narrowband private networks, etc., have been deployed to fill the current need. And, of course, existing cellular networks have also been used to enable these communications. These radio retrofit solutions have had limited success because the fundamental issue of cost remains unaddressed, and many devices are left under-served. All these attempts reemphasize a need for a better solution that makes sense economically.

Unfortunately, the solution is not simple, and the following challenges are examples of why existing technologies such as cellular or wireless mesh networks have difficulty providing secure, reliable, and cost-effective communications:

- The devices in the majority of cases are widely dispersed, and often times concentrated in areas far from population centers.
- Devices are commonly located in very difficult radio environments (e.g., in basements, below ground, in shielded environments) where connectivity is typically nonexistent.
- These devices don’t resemble typical Internet end points; instead, the majority of these devices suffer from constrained power supply, processing capability, memory, etc.

- Some technologies rely on dedicated spectrum which adds significant cost to the communication network.
- Adding these simple devices to existing public networks designed for very different challenges (e.g., cellular networks driven by smart phone requirements) rarely yields an effective price point for the lower end usage of the network.
- The potential device population is orders of magnitude larger than the Internet or cellular population (i.e., humans and PCs).

So does this mean that the cellular or mesh networks are useless when it comes to providing connectivity to these devices? Not necessarily. Cellular networks, as an example, can still be used economically to provide a communication link for those devices that are not power constrained, have requirements related to high bandwidth and/or low latency, and are in the coverage of existing cellular base stations. Unfortunately a vast majority of the devices—by some estimates up to 90% of them—do not fall into these categories. The quest now is to get these devices securely and economically connected.

2.2 The OTR Communications Solution

On-Ramp Wireless has worked on providing such a solution to address the communication problem for the billions of constrained devices supporting diverse applications. There are two aspects of the OTR Solution that enable secure connectivity among these devices at price points that are orders of magnitude lower than other technology options:

- **Total Reach:** The devices that cellular and mesh have left behind are geographically disperse, underground, etc. Cellular providers, as an example, either cannot reach these devices or do not see the economic benefit of reaching them. Additionally, the ability to reach into places where power is unavailable is a key consideration. The Total Reach requirement is achieved by virtue of a single base station covering very large geographic territories, which is possible using the OTR technology developed by On-Ramp Wireless.
- **Total Connect:** Total Reach is not the full answer: Just because a particular device can connect does not mean that ALL devices can connect to the network infrastructure. It is critical that the technology make it possible for a tremendous number of devices to connect using as few base stations as possible. Only by doing so can we minimize the per end point network price. With the OTR solution, Total Connect is achieved in the globally available free spectrum known as the Industrial Scientific and Medical (ISM) band at 2.4 GHz. The vast majority of unconnected devices can all be supported on a single, very cost-effective OTR network.

But all this work being done by On-Ramp Wireless to reach and connect the 'Internet of things' will come to naught if we do not also focus on the security of the network. This is especially so in the current world of cyber threats. It is also important to note that security is closely associated with cost, and, therefore, it is vital that we balance the risks and costs associated with network security. One can build a Fort Knox, but the cost, inflexibility and lack of performance of the resulting solution would not be practical for wide area, diverse device communications.

For a given On-Ramp Wireless OTR network solution, the end-to-end application (e.g., pressure sensing, electric AMI) is comprised of sensing devices (e.g., pressure sensor, electric meter), the

OTR communications network, and the operator interfaces that provide information analysis and visualization. On-Ramp Wireless has attempted to address the end-to-end solution security challenge by dividing it up. The division is based on the commonly accepted concept of layering. The application sensing device and operator interfaces are layered on the core communication system. We have provided several security features as part of the core communication system, features that would be required by all applications that leverage the communication system. In some cases, an application may also drive requirements for additional security measures (e.g., revenue assurance, integration with other secure data feed), and those additional and unique features are built into the application sensing device and/or operator interface driving the requirement.

An example of application-level security might be addressing a temperature sensor that is lulled into reporting false temperature readings by altering its surrounding environment. There is nothing to prevent such an attack, but such an attack can be detected and false readings should be ignored. Since the data sent by the sensor is a valid packet, it would not be detected at the OTR network layer. It would be up to the temperature sensing application to detect the false reading and take action to recover.

The intent of this document is to focus only on the security attributes of the OTR communications network. We regularly consult with sensor manufacturers who integrate sensor devices with OTR components and operators who deploy OTR solutions to ensure that the non-OTR application components complement the security strength of the OTR communications system.

2.3 OTR Network Overview

Building on the foundation of OTR technology, On-Ramp Wireless has built a metro scale, end-to-end wireless solution, including:

- OTR Nodes—wireless modules used for simple and standardized integration with the end point devices.
- OTR Access Points (APs)—OTR network components that are mounted on mountain tops, pole tops, towers, rooftops, and other elevated sites, and provide the only field-installed network infrastructure. The AP uses GPS/UTC timing for its operation.
- OTR Network Gateway Controller—manages AP connections in a network, the handover between APs, and the data path to back-end applications.
- Security Key Management Server (KMS) —responsible for providing authentication and authorization services.
- On-Ramp Total View (OTV)—application that provides endpoint data management and seamless integration into back-office systems through a suite of standard interfaces.
- OTR Element Management System (EMS)—application that is responsible for configuration and management of OTR network components.
- OTR Database Services—responsible for managing storage of the end point application data.

Figure 1 illustrates the On-Ramp Wireless end-to-end system architecture along with examples of some third-party applications that can be integrated with the OTR network solution. As

mentioned earlier, the APs use GPS/UTC time for their operation while the Gateway and other components use NTP time. As described in the following sections, the OTR network wireless link is protected by On-Ramp Wireless' proprietary security design, and the communications between back office applications is protected by industry standard IP security protocols.

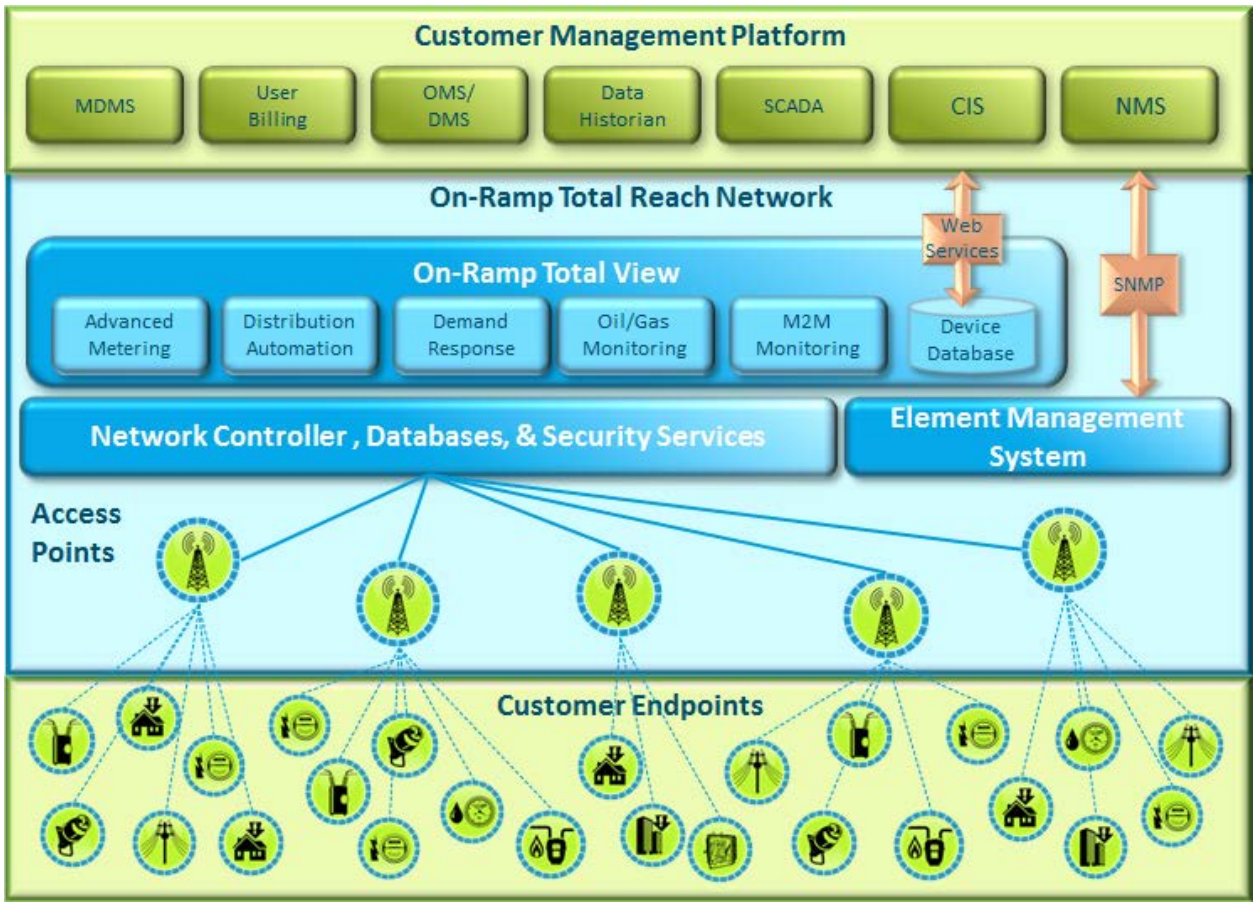

Figure 1. On-Ramp Total Reach Network and Components

3 OTR Network Security Principles

Ensuring the security of such a distributed system is not easy. Our approach to ensure the security of the core communication system shown earlier is based on the following principles:

- Security by design
- Design based on a defense in depth strategy
- Design tailored for constrained devices and network longevity
- Design based on established security practices
- Design complemented by established IT practices

We next explain these principles briefly.

3.1 Security by Design

The design of the security mechanisms for the OTR network was done during the design of the entire network, not bolted on once the system design was completed. This ensures that security is an integral part of the OTR solution.

In addition, during the software implementation of the various OTR network components, we followed industry best practices for building secure software. This includes conducting regular code reviews, leveraging static code analysis tools, and using various software tools during testing to verify the hardness of the implemented solution from a security perspective. Further, as part of the design of On-Ramp Wireless products, any test functionality and JTAG access is removed from production units and builds. On-Ramp Wireless recommends the same procedure for all partner developed products. We have also implemented development recommendations from various standard bodies such as NIST (SP 800-64) to ensure that information security is integrated into the software development life cycle.

3.2 Defense in Depth Strategy

A defense in depth security approach is to defend a system against any particular attack using several varying methods. As such, a comprehensive approach to information security in an OTR network depends on three types of mechanisms:

- Prevention mechanisms to prevent unauthorized access to the system. These include mechanisms focused on access control, integrity protection, confidentiality and availability.
- Detection mechanisms to detect attempts to break into the system. Any attempts to maliciously influence the system are thereby detected and result in alarms being sent to various human operators for follow-on action.
- Recovery mechanisms to ensure the system continues to operate as desired and degrades gracefully in the event of an attack.

In the context of the OTR network security framework, prevention mechanisms aimed at preventing unauthorized access to the network operate in tandem with detection mechanisms

that send out alarms when attempts to break into the system are detected. In addition the system does not shut down right after attempts to break in are detected, but rather isolates the offending system component, continues to operate, and degrades gracefully. For example, an attempt by a jammer to launch a denial of service attack on the system is detected and alarms are generated which give sufficient detail on the location of the jammer. In addition, the APs continue to operate at a degraded level based on the type of jamming.

3.3 Designed for Constrained Devices and Network Longevity

As indicated earlier, a vast majority of the sensor devices that can operate optimally on an OTR network are what could be characterized as constrained devices. These are devices that have one or more constraints associated with processing, memory or power. Further, such devices are expected to last for several years (10+) in the field. The OTR network security mechanisms have been designed for such constrained, long-life devices.

In the context of the OTR network solution, untrusted end devices always communicate directly with a trusted Access Point and not with each other directly. This is similar to a cell phone network where the cell phones do not communicate directly with each other but via secure communications with the base stations. This allows for the OTR end point security mechanisms to be based on symmetric key cryptography with hardware acceleration. The use of ensuing small key sizes results in efficient use of wireless bandwidth, plus symmetric key operations are much more amenable for constrained end devices.

It should also be noted that, contrary to popular perception, symmetric key mechanisms are not weaker compared to asymmetric key mechanisms. Table 1, taken from NIST Special Publication 800-57[1], shows the equivalence of the two types of mechanisms. This table also refers to the following forms of asymmetric cryptography:

- FFC (Finite Field Cryptography)
- IFC (Integer Factorization Cryptography)
- ECC (Elliptic Curve Cryptography)

The mechanisms used by ULP network are based on the usage of hardware accelerated AES-128, AES-256, and 3TDEA algorithms which have a security lifetime through 2030, as shown in Table 1 on the following page.

The backend network components (e.g., AP, Gateway, etc.), where such constraints on processing, memory and power do not apply, can make use of standard protocols such as SSL and IPsec; these, in turn, make use of asymmetric key mechanisms.

[1] NIST SP800-57, Recommendation for Key Management – Part 1: General (Revised), Table 4, page 66, http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf.

Table 1. NIST Symmetric Key Mechanism Comparisons

Algorithm security lifetimes	Symmetric key algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA 3TDEA AES-128 AES-192 AES-256	Min.: L = 1024; N =160	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256

3.4 Designed Based on Established Security Standards

Industry best practices for network security have been incorporated in the design and implementation of OTR networks. These practices include recommendations by various widely respected organizations such as the NIST security attributes required by a secure communications network (Ref. NISTIR 7628). We have also incorporated security practices followed by the cellular networks, since these networks are the most similar to the star topology architecture and security requirements of the networks deployed by On-Ramp Wireless. The OTR network security design also meets FIPS 140-2 Level 1 for communications devices, and follows guidelines prescribed in NISTIR-7628. The security design also addresses constraints faced on a factory floor, and provides for secure end point manufacturing capability in a manner that can scale to millions of end devices.

It should also be noted that fully integrated solutions that incorporate the OTR network will have additional challenges related to regulations, compliance, etc. For example, the utility industry has NERC CIP compliance (NERC CIP 002-009) required for the end-to-end deployed solution. We have designed the network to make it easier to demonstrate such compliance.

3.5 Designed Based on Established IT Security Practices

Complementing the OTR network security mechanisms, On-Ramp Wireless-hosted solutions use standard IT security practices such as properly configured firewalls, disabling of unused ports, different security tiers where the components live, access control to the components, cryptographic key management, password management, user management for access to the

components of the backend network, and system account management to name a few. All user actions are logged and audited to detect any abnormal activity. The OTR network logging and audit framework follows standard and efficient logging practices such as user identifies, activity dates and descriptions. This feature captures a log item each time devices are added or removed, or when an OTR system configuration parameter is set or changed. In addition, all OTR system or user-generated events are also time stamped using GPS time synchronization in the network and NTPv3 time synchronization throughout the back office. When an operator implements a private OTR network, recommendations are made for similar rigorous network security practices.

3.6 Verified by Third Parties

The robust OTR network security scheme passed rigorous third-party security assessments and has been deployed on the electricity grid of a metropolitan city, Tier 1 utility company with extremely stringent security standards.

The OTR network solution components are all certified by the US Bureau of Industry Standards (BIS) prior to export outside of the United States.

4 OTR Network Security Attributes

In this section we provide more details of the security mechanisms implemented in the core communication system. We start by explaining the prevention mechanisms in the system, and then follow with additional attention on the detection and recovery mechanisms.

4.1 OTR Network Prevention Mechanisms

OTR network provides the following prevention mechanisms to satisfy the demands of online OTR network operations:

- **Mutual entity authentication** ensures that valid sensors (devices employed for measuring some physical quantity such as electricity usage, voltage, temperature, etc.) will join only valid networks and the converse: valid networks will only recognize valid sensors. Similar to provisioning a cell phone for use on a given network, OTR devices are securely provisioned for a specific network by assigning unique keys during the manufacturing cycle. These unique sensor keys are then added to the network key management server. Mutual authentication is then done using these keys in an AES-based algorithm. Data from an unauthenticated node is dropped in the network without being delivered to the application. In addition, any two components (such as AP, Gateway, and EMS, etc.) on the backend network communicate over SSL links. Thus the standard mutual authentication mechanisms of SSL are leveraged to ensure that unauthorized network devices do not get access to the network components.
- **Message authentication** ensures that modification or replay of messages by elements in the path between source and destination is detected and modified data dropped. This is based on the usage of CMAC-AES mechanisms for messages sent over the OTR network wireless link. SSL based mechanisms are used for messages that do not go over the ULP wireless link and that terminate at one of the backend network components. Data that fails authentication verification at the Gateway is dropped in the network without being delivered to the application.
- **Message confidentiality** ensures that elements in the path between source and destination cannot decrypt any data and the privacy of end point data is protected. This is based on the usage of TDES-192 bit mechanisms for messages sent over the OTR network wireless link. SSL based mechanisms are used for messages that do not go over the OTR network wireless link and that terminate at one of the backend network components.
- **Limited anonymity** ensures that the identity of the end device sending data is not known. This aspect of OTR network security ensures that all end devices scramble their permanent identities when communicating over the OTR network wireless link. This does not apply to communication over the links constituting the backend network where we leverage IP communication.
- **Authentic firmware upgrade** ensures that only authentic firmware images will be used to upgrade the end points. This prevents a hacker from sending a malicious firmware binary to the end devices. To ensure efficiency in terms of delivering the firmware image, we broadcast the image over the network. Every end point uses end point specific keys to

authenticate the image and gain authorization to switch to the new image. This ensures both efficiency and security. As a result, typical OTR endpoint firmware upgrades proceed much faster and can complete in a matter of days as opposed to weeks or months with competing technologies. Upgrading the backend network components leverages the fact that these components are connected via secure SSL links, and that the images delivered to these back end network components are digitally signed. Software roll-back is supported for network component software updates in that the Access Point can be rolled back one version. There is no roll-back support associated with a node firmware update.

In addition to prevention mechanisms based on cryptography, the OTR network physical layer is based on DSSS (direct-sequence spread spectrum) which provides a natural prevention and recovery mechanism. This is similar to the use of CDMA in a cellular network.

4.2 Detection and Recovery Mechanisms

Prevention mechanisms by themselves are not sufficient. The system should also have detection and recovery mechanisms in place to detect and recover from attempts to break into the system. This is indeed the case with the On-Ramp Wireless Total Reach system. Several mechanisms aimed at detecting malicious behavior have been implemented and result in alarms to notify human operators. For example any attempt by a malicious node at gaining access to the system or passing off fake messages or replaying messages results in an alarm. This alarm also provides information about the location where the malicious behavior is occurring. The recovery attempts will ensure that such attempts are unsuccessful and do not impact the performance of the rest of the system.

Another example is related to jamming. Attempts at jamming the Access Point to cause a denial of service attack also results in alarms with information related to the Access Points affected by the jammer. The Access Point itself continues to operate, though with degraded capacity, until the jamming becomes so severe as to prevent any operation. Several such mechanisms focused especially on detecting denial of service attacks are implemented across the OTR network.

5 Frequently Asked Questions

This section provides answers to frequently asked questions (FAQs) about OTR network security.

Q: How do you configure the end nodes with the cryptographic keys?

A: The OTR Nodes are provisioned with the key material when these are integrated with the sensor devices. This key material is then securely transferred to the network-specific KMS by encrypting this using the public key of the KMS. The KMS stores these keys securely and releases the session keys to the Gateway when the node joins the network and is actively involved in sending or receiving messages.

Q: Do you allow for keys on end points to change periodically?

A: The node specific keys used in the solution can change depending on the policies of the network provider. The network provider can specify the number of days after which the keys have to change and the KMS and node will then update their keys without requiring any key exchange over-the-air.

Q: How do you provide for efficient and secure firmware upgrade?

A: Firmware is broadcast to the end points and secured using the broadcast keys, and each end point is then given the permission to switch over using the end point-specific keys. A patent-pending approach is used to perform this in a scalable manner.

Q: What is the risk to the overall network if a given end point was compromised?

A: The risk to the overall network of a compromised end point is minimal and contained to just that end point. The key material from the compromised end point would not impact the security of messages sent (received) by any other non-compromised end point in the system.

Q: How has OTR network security been verified?

A: On-Ramp Wireless has contracted with an independent security auditing firm who conducted a detailed design analysis of the OTR network solution. On-Ramp Wireless and the security auditing firm worked on plans to remediate any findings in the audit, and these plans have been implemented in the current commercial solution. In addition, our network operators conduct security audits once the OTR network solution has been integrated with their broader operations, and On-Ramp Wireless has consistently passed design and penetration testing of both customer-hosted and On-Ramp Wireless-hosted implementations.

6 Conclusion

On-Ramp Wireless continues to deploy wireless communications networks to enable our customers to monitor and control critical infrastructure assets. The security of these communications is paramount to the longevity and value of these networks, and On-Ramp Wireless will continue staying ahead of threats with robust and reliable security mechanisms and practices. While a document can only describe the security features of an OTR network so far, the real proof of security comes from the network operation itself. These features are not just bulleted items on an engineer's design list. They are fully functional and intentionally designed mechanisms that are delivering the highest level of security for a range of applications deployed on OTR networks.

Appendix A Abbreviations and Terms

Abbreviation/Term	Definition
3DES	Triple Data Encryption Standard
3TDEA	Triple Data Encryption Algorithm
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
AP	Access Point. The OTR network component geographically deployed over a territory.
CMAC	Cipher-based Message Authentication Code
DSSS	Direct-Sequence Spread Spectrum
ECC	Elliptic Curve Cryptography
EMS	Element Management System. The network component that provides a concise view of the OTR network for controls and alarms.
FFC	Finite Field Cryptography
IFC	Integer Factorization Cryptography
IP	Internet Protocol
IPsec	Internet Protocol Security
IPv6	Internet Protocol version 6. Protocol used to direct Internet traffic. This protocol provides an addressing scheme that specifies source and destination addresses for transferring data packets between hosts.
ISM	Industrial, Scientific, Medical
KMS	Key Management Server
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report
Node	The generic term used interchangeably with an end point On-Ramp Wireless device.
OTA	Over-the-Air
OTR	On-Ramp Total Reach™. The On-Ramp Wireless proprietary wireless communication technology.
OTV	On-Ramp Total View™. The network component used to manage and monitor all end devices. It is also used to pass data from the OTR network to associated upstream databases.
RSA	Rivest, Shamir, Adleman encryption algorithm.
SSL	Secure Socket Layer