



Technical Solutions

Secure Two-Way Paging

THIS ANALYSIS OF THE SECURE TWO-WAY PAGING SOLUTION HIGHLIGHTS THE FOLLOWING

- Introduction
- Technical description and conceptual drawings
- Appropriate uses
- Advantages and disadvantages
- Costs
- Spectrum requirements
- Management issues
- Security and standards issues
- Additional information

RECENT EVENTS AND ADVANCES IN PAGING DEVICES AND OVERALL PAGING TECHNOLOGY HAVE DRAWN ATTENTION TO PAGING AS AN ALTERNATIVE METHOD OF COMMUNICATIONS FOR THE PUBLIC SAFETY COMMUNITY

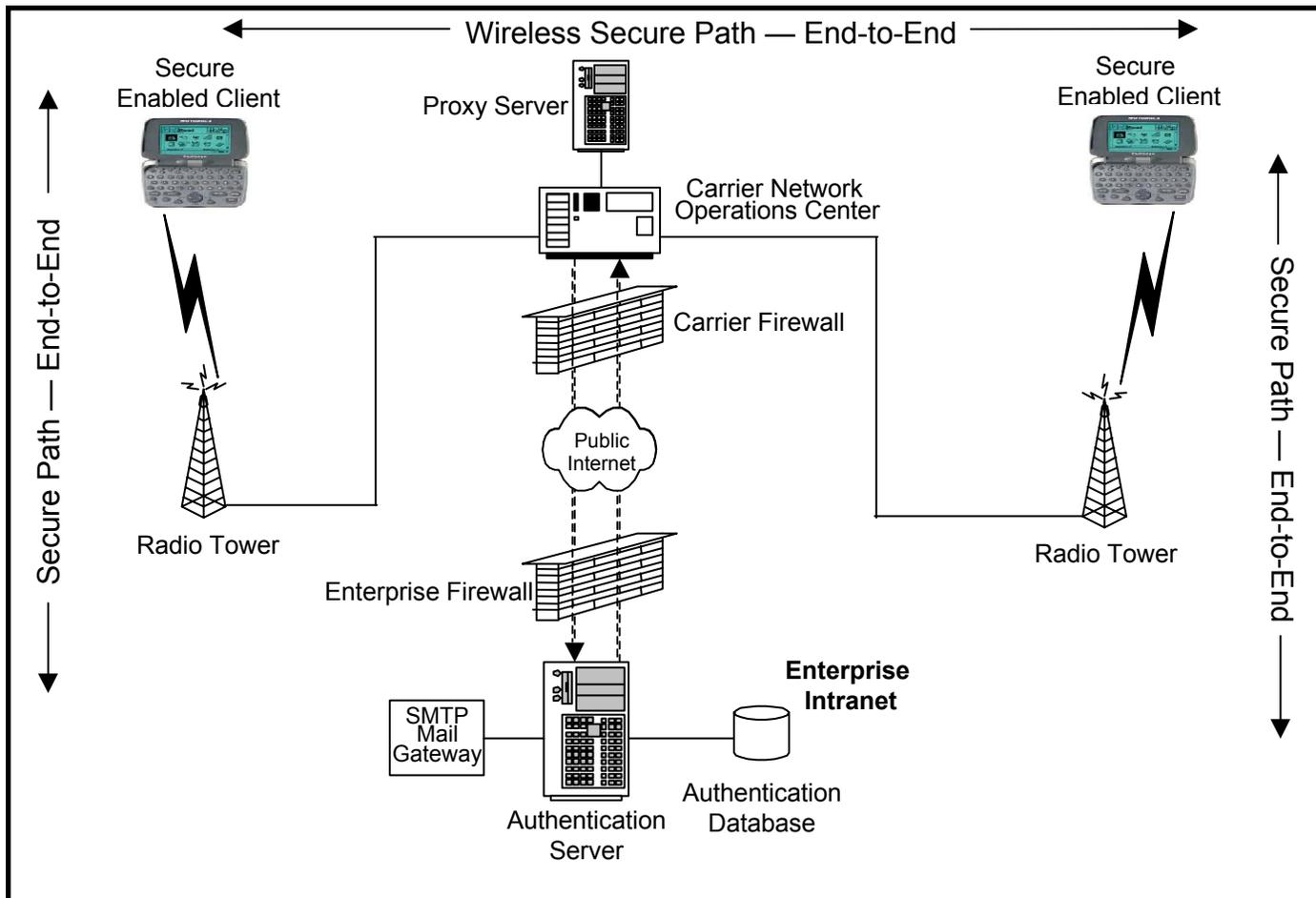
- Two-way paging is a mature communications medium with near-ubiquitous coverage in most major metropolitan areas, including most outlying suburbs
- Two-way paging has proven itself as a viable alternative to voice communications in crisis events
 - In the wake of the terrorist attacks of September 11, 2001, two-way pages successfully transmitted information between parties while other forms of communications suffered from massive traffic overload and system failures
- Advances in two-way paging devices, combined with new applications in virtual private network (VPN) software, have given rise to secure transmission capabilities within commercial two-way paging networks
 - Encryption is applied from end to end, at the user device level (rather than at the network level)

PUBLIC SAFETY AGENCIES CAN ACHIEVE INTEROPERABILITY BY IMPLEMENTING THE SECURE SOLUTION ON A TRADITIONAL TWO-WAY PAGING SYSTEM

- Secure two-way paging can be used between agencies operating on the same paging system that wish to interoperate with each other
- Agencies that use secure two-way paging for interoperability must have—
 - Subscriber units with the capability and memory to be loaded with and run third-party software applications (e.g., security-related)
 - A secure VPN environment
 - A proxy server located at the paging provider's network operations center (NOC). This proxy server is used to direct pages sent via the secure client to the VPN
 - An authentication server within the VPN environment to authenticate users
- Both secure and non-secure paging—
 - Allow users to transmit messages to other paging subscribers
 - Allow broadcast of pages in voice, numeric, or text format to an individual subscriber or simultaneously to a selected group of users
 - Use the most advanced text units to receive—
 - Short Message Service (SMS)
 - E-mail
 - Voice mail notification

Secure Two-Way Paging Solution...Conceptual Drawing...

THE DRAWING BELOW ILLUSTRATES THE CONCEPT OF TRANSMITTING AN ENCRYPTED MESSAGE FROM PAGER TO PAGER



SECURE TWO-WAY PAGING IS A VIABLE SOLUTION TO SUPPORT PUBLIC SAFETY AGENCIES' COMMUNICATIONS NEEDS

- Public Safety Wireless Network (PSWN) Program studies indicate that agencies use secure two-way paging to—
 - Send secure and non-secure pages across disparate service providers
 - Support applications, such as wireless data, to minimize the risks associated with accommodating uncertain capacity requirements in an existing land mobile radio (LMR) system
 - Minimize capital investment
 - Add to the subscriber functionality currently offered by their LMR system
 - Interoperate with each other when the agencies use different systems on either the same frequency band or different frequency bands
- Agencies must be willing to use services that are separate from their own private LMR systems

Secure Two-Way Paging Solution...Advantages...

THE SECURE TWO-WAY PAGING SOLUTION HAS MANY ADVANTAGES

- Two-way paging networks are available in most urban areas and major highways throughout the United States
- Equipment and service is inexpensive
- Group paging capabilities are available
- Only software is required to modify a commercial off-the-shelf two-way pager for secure capabilities
- Because paging technology uses a “store and forward” technique to send messages to users, users can be assured that they will receive their messages whenever their paging device is registered on the network

THE SECURE TWO-WAY PAGING SOLUTION ALSO HAS SEVERAL DISADVANTAGES

- Pagers must be powered on at all times to ensure that urgent, time-critical messages will be received
- Some subscriber units have character limitations when sending pages
 - Character count includes all characters in the address field(s), subject field, and message body
 - There are no known character limitations associated with receiving messages
- Coverage gaps result from geographic impediments, low demand, building interference, or a weakness in a carrier's signal

THE SECURE TWO-WAY PAGING SOLUTION PRESENTS SEVERAL COST CONSIDERATIONS

- Subscriber units are readily available and relatively inexpensive
- Paging service and VPN service are required for each pager
- Spare equipment (e.g., additional batteries) cost must also be considered
- Nationwide toll-free number plan is available
- Software licensing costs may be included in VPN service costs or other service-related fees
- The costs associated with servers that are installed in the service provider's NOC and within the VPN must be considered

Secure Two-Way Paging Solution...Spectrum Requirements...

THE SECURE TWO-WAY PAGING SOLUTION REQUIRES NO ADDITIONAL SPECTRUM

This solution uses previously licensed commercial spectrum resources

THE SECURE TWO-WAY PAGING SOLUTION REQUIRES MINIMAL TO MODERATE MANAGEMENT BY THE PUBLIC SAFETY AGENCIES INVOLVED

- Training is required to distinguish the difference between secure and non-secure pages (there are separate message management applications for these two types of messages)
- Usage policies must be established for the subscriber units
- Managers must—
 - Provision subscriber units with toll-free or local numbers
 - Maintain the VPN authentication database
 - Determine service availability in a given region
 - Determine coverage in a given region

THE SECURE TWO-WAY PAGING SOLUTION ACCOMMODATES COMMUNICATIONS SYSTEM SECURITY

- This solution uses RC-4 encryption, which is—
 - Not appropriate for the transmission of classified information
 - Roughly equivalent in strength to Triple-DES (digital encryption standard)
 - Decipherable by those entities with malicious intent using the proper technology
- Secure solutions have already been proven viable using all the major two-way paging standards

THE PSWN PROGRAM, IN CONJUNCTION WITH THE DEPARTMENT OF THE TREASURY, CONDUCTED A PILOT TEST OF THE SECURE TWO-WAY PAGING SOLUTION

- The purpose of the [Secure Two-way Paging Pilot Test](#) was to prove that secure paging is a viable enhancement to traditional LMR communications
- Testing occurred in two stages, a proof-of-concept test in the Washington, DC, metropolitan area and a robust operational test in Salt Lake City, Utah, in support of the 2002 Winter Olympic Games
- Findings from the pilot testing include—
 - Latency is not introduced when sending encrypted pages to and from the paging devices
 - Paging device operations are user friendly and do not require extensive training
 - Interoperability is supported through the secure two-way paging solution as tested (i.e., encrypted and non-encrypted pages were successfully sent/received across two disparate paging service providers' networks)
 - Secure two-way pagers can be acquired, provisioned, and deployed on a wide scale to support major events