ShoreTel
Brilliantly simple™

WHITE PAPER

SECURITY IN MOBILITY SOLUTIONS

Table of Contents

1. Executive overview

With increasing proliferation of mobile devices in the enterprise, extending Unified Communications (UC) capabilities to today's highly sophisticated smartphones is key to a holistic UC approach. Mobile UC can not only increase user productivity, but also drive down telecom costs.

However, I.T. managers need to ensure that the Mobile UC solution they deploy has built-in security. One of the key aspects for any mobility solution is that it provide secure connections for all voice communications. This means secured communications wherever you are and whatever network you are on - both internal and external Voice over W-Fi, Voice over cellular data (3G/4G) and regular cellular calls.

2. Key components of a mobile UC infrastructure

Security and policy enforcement should be accomplished through the collaboration of the mobility server, the mobile device client, and the enterprise Wi-Fi and network authentication infrastructure. Each of these key components of a mobile UC infrastructure plays a key role in securing enterprise communications.

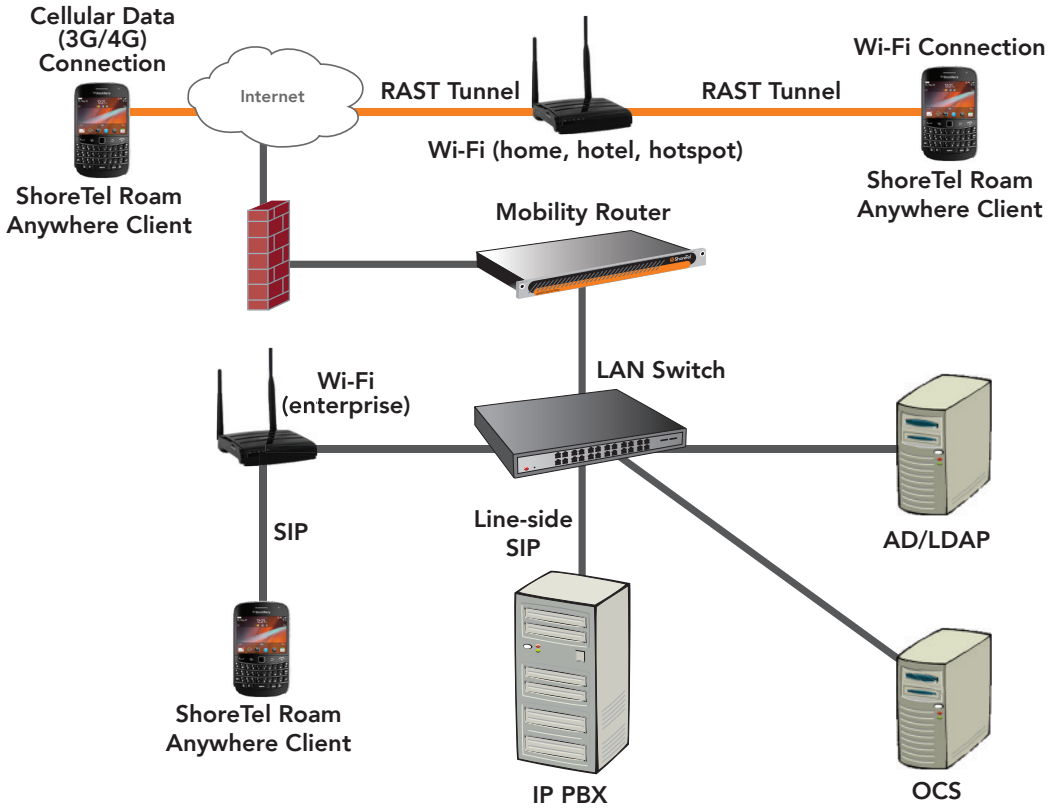

Figure 1.1

Mobility Server

The Mobility Server is the heart of the mobile UC infrastructure. It routes voice and Unified Communications (UC) between the client on the mobile device and enterprise PBX, UC systems, Active Directory and LDAP. This is the central point for driving secure protocols and authentication.

Mobility Client

The Mobile Client is the voice application on smartphones/tablets that gives users access to UC features and capabilities. It has to not only enforce the security policies defined on the server, but also maintain ease of use.

Wi-Fi infrastructure:

Although a mobile UC solution does not control the Wi-Fi infrastructure, authentication standards and protocols such as 802.1X, WPA2 Enterprise, and WPA2 Personal can ensure secure communications over Wi-Fi.

3. Securing mobile UC

Robust security for Mobile UC can be achieved by ensuring all communications between the mobile device and the mobility server are secured. This can be achieved by user and device authentication, and securing communications outside the firewall.

Securing communications with robust authentication and encryption authorization credentials can ensure that all communication between the client and the server is authenticated and encrypted where necessary. User credentials and device information provided by the client to the server during the initial user setup or registration process can be used to validate all future transmissions between the server and the client. This is easily done with digital certification.

Ensure that the mobility server is able to act as a Certificate Authority (CA) in order to generate, manage and plumb the digital certificates on the client.

If it becomes necessary to de-authorize a particular client, credentials should be easily removable from the mobility server by removing, deleting or deactivating the user account.

While communications over enterprise WLAN can be secured with standard protocols, additional measures are required when a mobile device is connecting from home or a hotspot. Some mobile UC solutions require the user to manually launch a VPN client when connected from outside the enterprise firewall. While this addresses the basic security need, the need for a user to take this step makes the solution a less user-friendly.

A solution that can automatically detect when the device is outside the firewall, and automatically secure the session is ideal.

4. Secure communications with ShoreTel Mobility delivers secure mobile UC

ShoreTel Mobility is an award-winning mobile UC solution that enables businesses of all sizes to integrate leading smartphones and tablets (Android, Apple iOS, BlackBerry OS and Symbian S60) with existing enterprise communication applications and infrastructure (Cisco, Avaya, ShoreTel, Nortel and Microsoft) securely, simply and cost-effectively. The solution includes two components – the Mobility Router and the RoamAnywhere Client. The Mobility Router integrates with enterprise PBX/UC systems and extends deskphone and UC capabilities to mobile devices via the RoamAnywhere Client.

ShoreTel Mobility delivers security and policy enforcement through the collaboration of the ShoreTel Mobility Router, the ShoreTel RoamAnywhere Client, and the enterprise Wi- Fi and network authentication infrastructure.

ShoreTel RoamAnywhere Client:

- Enforces the security policies defined on the Mobility Router.
- Utilizes ShoreTel RoamAnywhere Secure Tunnel that supports TCP and UDP transport layer. Based on the TLS protocol.

ShoreTel Mobility Router:

- Securely routes voice and UC between the client and enterprise PBX and UC systems.
- Utilizes application layer SSL session to secure communications for users “outside the firewall”.
- Utilizes WPA2 Personal and WPA2 Enterprise for internal users.
- Acts as a Certificate Authority (CA) to generate, manage and plumb X.509 certificates on the RoamAnywhere Client.
- Communicates with PBX, UC systems, Active Directory and LDAP.

5. Device and user authentication initiated during provisioning

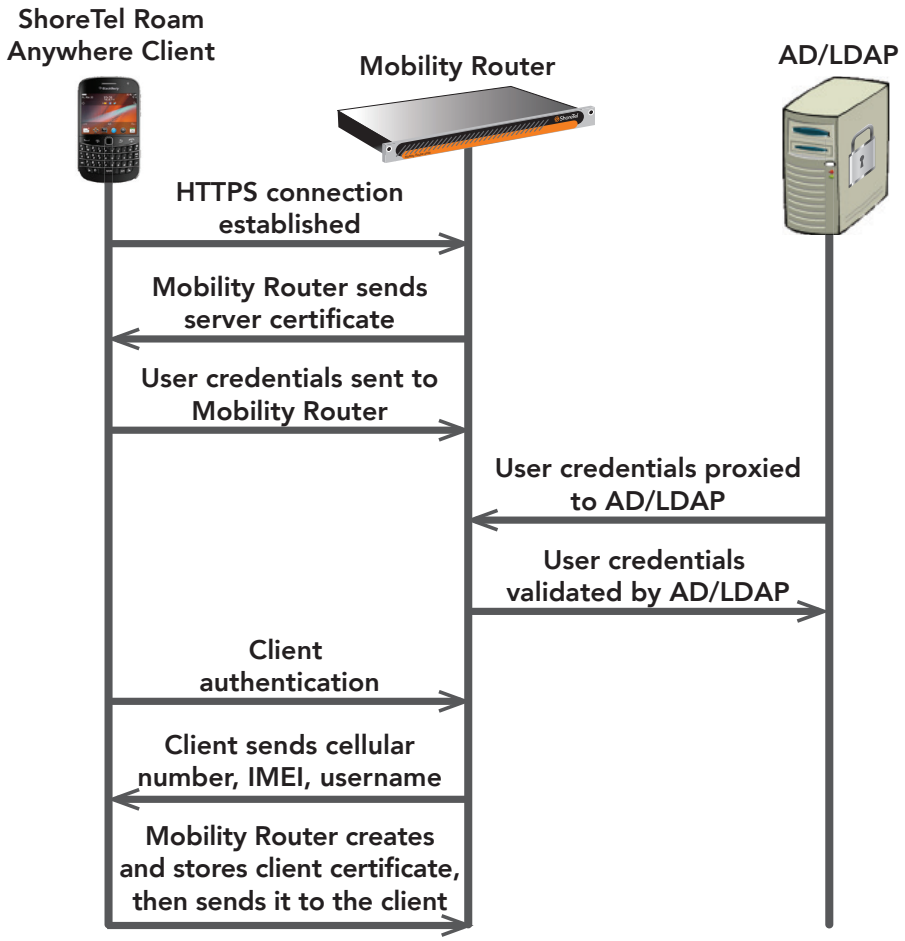

Figure 1.2

The client provides credentials to validate that it is authorized to utilize the ShoreTel Mobility solution during initial provisioning. All future communication between the client and Mobility Router that requires authentication will use the client certificate for authentication.

6. Secure remote technology

Secure Remote Technology performs the following functions:

- Secures calls and sessions over the various networks (Wi-Fi, cellular data, or cellular).
- Allows the RoamAnywhere client to connect to the Mobility Router using a TLS/DTLS tunnel which is initiated automatically.
- Uses standard SSL/TLS-DTLS handshake protocol to establish an application level SSL/ TLS tunnel and to negotiate secure attributes for the session.
- The Mobility Router utilizes TCP-based TLS for control traffic while utilizing UDPbased DTLS for VoIP/ RTP traffic. This ensures the highest voice quality when network congestion or loss is encountered.
- The server and client use the standard options during the handshake. Cipher suite and key size are configurable, but the typical/default configuration is AES-256.

7. Summary

Mobile UC solutions can leverage multiple technologies to secure enterprise communications.

World Headquarters
960 Stewart Drive
Sunnyvale, CA 94085
USA
shoretel.com

+1 (800) 425-9385 Toll Free
+1 (408) 331-3300 Tel
+1 (408) 331-3333 Fax

EMEA
Inspired
Easthampstead Road
Bracknell, RG12 1YQ
+44 (0) 1344 208800 Tel

APAC
8 Temasek Boulevard#41-03
Suntec Tower 3
Singapore 038988
+65 6517 0800 Tel