Ruckus
Simply Better Wireless.

feature sheet

FEATURES/BENEFITS

- Leverages Ruckus' patented Dynamic Pre-Shared Key™ (DPSK) technology along with Zero IT Activation™
- Simple provisioning of client encryption on an open network
- "No-touch" for administrators or end users to authenticate or pre-register users
- Excellent solution for high density public venues such as stadiums, conference centers, or hotspot locations
- Secure key times out with preset limits ensuring optimal network uptime for encrypted client connections
- Unique encyption key for each device
- Highly simplified, highly secure
- No expensive AAA or RADIUS servers needed
- "IT Lite" - simple to deploy and maintain

Security Option	Benefits	Drawbacks
Open network	• Simple to use and deploy	• Completely insecure • Some client configure still required
Pre-Shared Key	• Straightforward implementation • Link layer encryption	• Easily compromised • Same key for all wireless clients • Client configuration required
802.1X	• Robust and comprehensive framework • Strong encryption and authentication	• Costly authentication server • Requires 802.1X supplicant on every end device • Highly complex • Time-consuming to implement
Dynamic PSK	• Easy to use • Strong encryption without 802.1X • No admin intervention • Works with existing authentication without EAP	• Manual configuration required for handheld devices (e.g., phones, PDA) • Requires manual configuration or end user password managment
SecureHotspot	• Highly secure • Extremely simple to deploy, manage, and use • Integrates with hotspot portal	• Initial set-up requires web server

SecureHotspot

AUTO SECURE UNPROTECTED HOTSPOTS WITHOUT CLIENT OR IT CONFIGURATION

Ruckus' innovative approach using Dynamic Pre-Shared Key™ (DPSK) technology along with Zero IT Activation™ seamlessly encrypts client connections

Ruckus Secure Hotspot is a unique approach to Wi-Fi security that lets end users choose to securely connect to hotspots effortlessly. One of the many free optional features available with the ZoneFlex system, SecureHotspot is only available from Ruckus.

Typically, Web-based hotspots are not encrypted or protected in any way without a tedious and cumbersome registration process at a minimum, and encryption is only available with additional complicated layer 3 technologies such as VPNs. The lack of security in these types of environments, such as with high density outdoor venues, discourages the purpose for enabling wireless connectivity in the first place; direct or indirect revenue generation or for end user to access sensitive information.

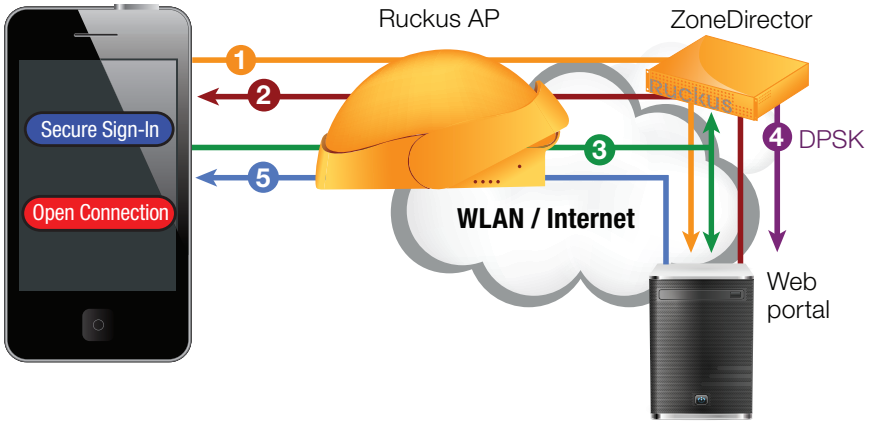
Without secure connectivity, hotspot users are less inclined to do what they normally do on their devices as they are well aware of the vulnerability to attacks or confidentiality breaches in an open network. This is especially true since open hotspots are particularly vulnerable to security breaches.

Ruckus' approach to securing clients connecting to open hotspots leverages Ruckus' existing patented technology to generate unique 63-character encryption keys for each user device on an open network without the need to authenticate or pre-register users. These encryption keys are then downloaded and installed within each client device automatically.

For hotspot providers and their users who want the highest level of Wi-Fi security with the least amount of effort, Ruckus Secure Hotspot is the ideal solution

SecureHotspot

SECURE UNPROTECTED HOTSPOTS WITHOUT CLIENT OR IT CONFIGURATION



1. Client associates to AP; ZoneDirector doesn't recognize anonymous device, sends client to Web portal
2. Web portal redirects to Branded Portal page, requesting user for secure sign-in or open connection
3. Sign-in request sent from client to Web portal, which requests zero IT config DPSK from ZoneDirector
4. ZoneDirector send DPSK to Web portal
5. Web portal forwards DPSK to client and auto-provisions; WLAN session traffic now encrypted

Open networks are fast becoming marginalized as end users are now more skeptical of transmitting any sensitive information over such networks than ever before. Additionally, even typical open networks require some client configuration. Security is the only way to ensure your users will use their devices to the full potential available to monetize hotspot networks.

Because most current secure solutions, such as 802.1x authentication, pre-shared keys, etc, require tedious pre-configuration from the hotspot administrator and / or complex registration on behalf of the end-user, these solutions are impractical for the typical ephemeral hotspot user and hotspot administrator rendering them completely useless.

SECURE HOTSPOTS IN ACTION

Ruckus' SecureHotspot solution leverages Ruckus' existing patented Dynamic Pre-Shared Key™ (DPSK) technology along with Zero IT Activation™ to provide a robust, simple to use solution that will enable end users to securely and comfortably connect to their sensitive applications.

With SecureHotspot, all of the 'authentication' is done in the background ubitiquously. After the client associates to a Ruckus hotspot AP with SecureHotspot enabled, the ZoneDirector takes over and sends the client device to the web portal. The end user then receives a request to log in either securely or in the open network.

After signing in securely, a unique pre-shared key with a limited life is sent to the device and the encrypted handshake is then completed from the ZoneDirector, web portal, and the client device thus completing an encrypted session. The only thing the end user sees is the option to connect securely or not. There is no need on the part of the hotspot administrator to pre-configure any users, however, administrators can log details on users and usage within the hotspot.

Breaking the relationship paradigm between higher levels of security and higher complexity in implementing stronger security, Ruckus can now deliver a unique solution that is highly secure, easy to deploy, and simple for the end user to manage.

Ruckus®
Simply Better Wireless.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx

www.ruckuswireless.com