



LOCKED DOWN. FREED UP.

BORDERGUARD POCKET PC CLIENT

BORDERGUARD® SECURE MOBILITY SOLUTIONS — FACILITATING HOW ORGANIZATIONS MOVE AND WORK

The BorderGuard Pocket PC VPN Client is an integral part of the BorderGuard secure communications platform. This important software client protects the privacy of communications, prevents hackers from altering data, and blocks would-be intruders from penetrating the network or the mobile devices used to access it.

Strongest available authentication

Ensure that only authorized users can access network resources. The Blue Ridge Networks™ BorderGuard Pocket PC VPN Client relies upon mandatory, mutual, public key authentication to keep resources safe and people productive. The public key processes are invisible to end-users — no learning curve, no user burden. Contrary to SSL VPN solutions, and password-only VPNs, the Blue Ridge Networks BorderGuard Pocket PC Client is immune to man-in-the-middle attacks.

There is no need for users to memorize long, random alphanumeric passwords to mitigate risk from dictionary attacks because user passwords never leave the Pocket PC. The password unlocks a digital certificate within the handheld. Only the digital certificate passes through the air waves never exposing the password to the possibility of being intercepted.

Secure communications via any wireless network

The Pocket PC Client operates in managed Wi-Fi and any other Wi-Fi network that users encounter. To support the way organizations actually operate, it also supports EV-DO, 1xRTT, Wi-Max, satellite communications, and any other wide area wireless network. The Pocket PC Client employs the strongest cryptographic mechanisms available on handhelds to securely traverse any untrusted network.

Blue Ridge Networks VPN technology has been deployed for a decade without a security breach. There is no need to rely on the latest embedded wireless network security technology (e.g. WPA-2 or 802.1X). The protections that Blue Ridge Networks developed 10 years ago for VPNs work just as strongly in wireless environments. People can communicate using Pocket PCs with complete peace of mind.

- **Mandatory, mutual public key authentication**
- **Tunnel-Lock® deters wireless intrusions**
- **Layer 2 secure tunneling**
- **Immune to man-in-the-middle / back-door attacks**
- **PKI authentication invisible to users**
- **Secures Wi-Fi , EV-DO, 1xRTT, Wi-Max, etc.**
- **Application session persistence**



The Blue Ridge Networks BorderGuard Pocket PC Client enables secure mobility over a range of devices and applications.

BORDERGUARD POCKET PC CLIENT

Handle wireless roaming with ease

When a user passes out of range of one network, into a dead zone, and then into another wireless network, the Pocket PC Client automatically re-establishes secure connectivity. The nature of its layer two tunneling means that the handheld device would continue to be known by the same logical IP address to your intranet infrastructure and server applications, despite changes to the handheld's local network IP address from roaming.

Compatible with all Pocket PC network-enabled applications

Use any web browser and any application — don't limit access to HTML/SSL applications. Any application, even legacy and proprietary applications, will operate smoothly through the Pocket PC Client's high security tunnel. Voice over IP and other time-sensitive applications benefit from Blue Ridge Networks VPN technology that minimizes connectivity disruptions, latency, and jitter.

Tunnel-Lock deters wireless network intrusions

Many security vulnerabilities that cannot be exploited through the Internet can be exploited

via Wi-Fi. Tunnel-Lock, a Blue Ridge Networks developed solution, blocks all data traffic outside of the VPN tunnel. Hackers cannot leverage a vulnerability in the operating system or an application on the Pocket PC because Tunnel-Lock blocks the intrusion before it can reach the vulnerability. Therefore, hackers can neither penetrate handheld devices nor use them as back-doors to your network.

Tunnel-Lock allows users to leverage any wireless access medium but to only logically connect to their home network. Requiring all inbound and outbound data to pass through the organization's perimeter security systems adds the protections of the enterprise firewall, intrusion prevention system, anti-virus, anti-spyware, and other systems.

Hardware Requirements

- 128 MB memory
- 600 KB available FLASH storage

Cryptographic Algorithms and Keys

- Encryption: AES 128, AES 192, AES 256
- SHA-1 Data integrity check
- LZS Compression
- RSA and Diffie-Hellman 1024 bit keys

The diagram below illustrates how Tunnel-Lock, developed by Blue Ridge Networks, locks down devices to only the enterprise network with which they are intended to communicate. Remote devices cannot open direct connections to the Internet nor can they communicate with unsecured guest networks. Tunnel-Lock also extends the protections and policies to all mobile devices enforced by the enterprise firewall — regardless of where those devices roam.

