End-to-Site Security

End-To-Site security model encrypts audio stream on each end of the call and on PBX. PBX acts as encrypted media exchanger and encryption key dealer. So each end connects securely with common PrivateServer , using VPN style security model.

Main advantages of End-To-Site security model are:

- interoperability with existing phone networks for crypto-to-clear and clear-to-crypto setup
- advanced telephony features, such as 3-way calling and conference room

Verifying call security

Call is automatically secured during call setup so it does not require any human intervention. As soon as call is established you can immediately start to talk with securely your peer. The overall security verification system is based on TLS digital certificate verification. PrivateWave automatically verifies digital certificate of SIP/TLS server and (if it's authenticated) then the connection will be automatically secured.

figure 1. BlackBerry

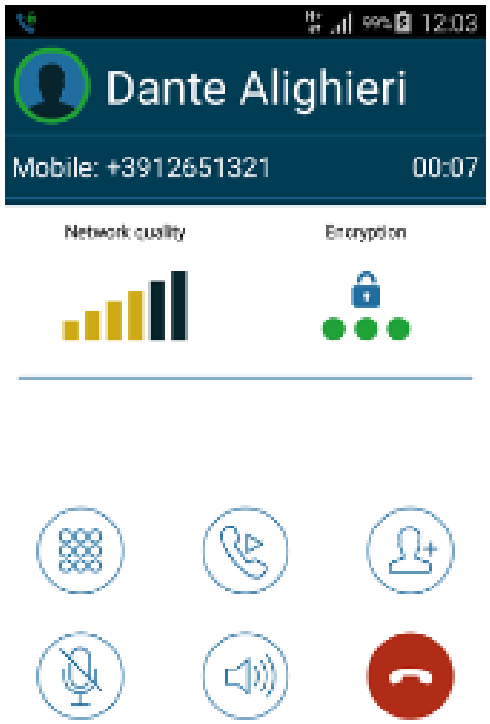

figure 2. Android

figure 3. i

This security model is exactly the same as HTTPS with internet browser, given the fact that on PrivateServer there is a valid digital certificate the call can be considered secure. By default, PrivateWave will not accept invalid SSL certificates, such as:

- Expired certificates: be sure that the system date of your device is properly set
- Self-signed certificates
- Common name mismatch

If the SSL certificate is a wrong or invalid (ex: one of the above mentioned reasons) or in the case of a man in the middle attack attempt, the user will see the following warning on the phone display:

SSL error message
You are attempting to open a secure connection, but the server's certificate is not trusted. Please contact your system administrator

On BlackBerry phone the message may be different, because it is a warning message of the operating system. It may also change in every operating system release.

Custom Certificate Authority

Since security is based on TLS digital certificates, it is mandatory that server certificates are signed by a known and trusted certificate authority. If your certificates is signed by a new CA (not present in phone CA list at ship time) or your private CA, you can import the CA's certificate and trust it. This feature is available only for OEM version of PrivateWave .

Being securely called

End-to-End Security