Custom Certificate Authority

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.

Custom CA on Blackberry

Open Options -> Security Options -> Advanced Security Options -> Certificates
Select the CA root and trust it. PrivateGSM can now connect to your server.

Custom CA on iPhone

Connect your iPhone to USB and open using iTunes application.
Select your device -> "Apps" section -> scroll down and you will see a list of applications that have a shared folder.
Import a file named "cachain.pem" containing the whole certificate chain, from Certificate Authority Root down to server certificate, including intermediate CA, using PEM format (ASCII format, starting with line "----~~BEGIN CERTIFICATE~~----").

Custom CA on Nokia

Nokia devices accept certificate in DER format (binary format, non ASCII as PEM). Remember to use a DER format certificate, otherwise Nokia phones will not recognize it properly.
You can install a new CA root in three ways:

- Point your phone's browser to the CA root certificate URL
- Send the certificate via Bluetooth
- Copy your certificate to the SD and open with a file manager application

You will be prompted to trust the certificate. PrivateGSM can now connect to your server.

Restrict Certificate Authority

SSL certificates management is the key point in SECRET security level, so PrivateGSM takes all SSL aspects in great consideration. You can further restrict the constraints on SSL choosing one single CA root, which you trust particularly. This feature gives you some additional advantages:

- Use certificates signed by your private internal CA, not known and present on OTS devices
- Choose one single CA root that you trust, reducing the risks that an attacker uses a compromised, but still valid CA root, to carry on a MITM attack.

Restrict CA on iPhone

Import a custom CA (see 9.2.2"Custom CA on iPhone"). Open and edit Sip settings, and set to ON setting named "Enable custom CA root"

Restrict CA on Nokia

Import a custom CA (see 9.2.3 "Custom CA on Nokia"). Open **Settings -> Advanced Settings -> TLS Settings** and set to ON setting named "Enable custom CA root"