Operational Requirements

The requirements to properly operate PrivateGSM are very important due to the huge amount of mobile devices hardware/software availability and to the highly variable characteristics of mobile networks.

In order to operate it properly several operating requirements must be satisfied.

1.1 Mobile devices

- Device (manufacturer. Model) must be present in list of supported device, eg: iPhone 4, Blackberry Bold 9900
- Device OS version must updated to latest OS version certified, eg: IOS 5.1.1, BB 7.1 bundle 648
- Battery level higher than 10%. Some devices power off radio or switch to power-save statuses when batter is under critical level

1.2 Network

Network behavior and quality is crucial to provide a good quality service. Some requirements are mandatory to operate the solution, other requirements affects the service quality, ranging from “not very good” to “impossible to a secure call”.

1.2.1 Mandatory

All these requirements are mandatory to operate the solution. Even one single requirement not satisfied makes impossible to run the solution.

- **INPUT** (from the device to the server):
  - HTTPS: TCP/443
  - SIP over TLS: TCP/5061
  - RTP
    - UDP/X-Y. Width of port range is configurable on server and depends on number of concurrent calls to be managed. 4 ports are used per each concurrent calls. Range set by default to 16000-17000, which grants 250 concurrent calls.
    - UDP/1919: echo service to test test client network
- **OUTPUT** (from the server to the outside network):
  - HTTPS: TCP/443: this is used to let your PrivateServer check the licence status for any of your customers. Plus the SMS feature for the automatic activation uses this protocol/port. You can restrain the connection to just one outside server: rendezvous.privatewave.com.
- **Blackberry transport**:
  - DirectTCP transport must be enabled and available for blackberry SIMs. APN data (name, username, password) from mobile operator are required.
  - BES The users may experience high delay in call setup if RIM network is overloaded



There is no support for Proxy Server (being HTTP or SOCKS), so PrivateGSM when operated within an Intranet must be able to communicate directly with the PrivateServer

1.2.1.1 Mobile Subscriptions

Mobile Devices must be equipped with a “data” plan that allow full internet communications without IP/TCP/UDP filters to the server and without protocol filters (Es: VoIP filters, like Vodafone carrier does).

The SIM card must be enabled to do full traffic without restriction (Es: WAP or WEB only subscription are not usable).

In presence of protocol specific filters it’s required to enable VoIP data option. Whenever this option it’s not available and VoIP is blocked (Es: UAE), the protocol obfuscation of PrivateGSM typically let it bypass but without guarantee on transport quality.

1.2.1.2 Radio Interference

All the mobile devices must be equipped with a 2G/3G and/or WiFi connection that’s not subject to high radio interference.

In presence of Radio Interference (due to high load of network, to other equipment using same frequency or to distance/obstacles between mobile devices and radio concentrator) the voice quality would not be good due to high number of packet loss.

On critical network conditions it’s possible to finely tune PrivateGSM to operate like in a tactical environment, with reduced performance but higher reliability.

1.2.1.3 Firewall TCP timeout

PrivateGSM must keep an always on connection to the PrivateServer with SIP/TLS over a TCP channel. It exchange keep-alive packet once every 10/20 minutes depending on the mobile platform.

The Firewall managing the connection of the server and of the client must allow TCP idle connection of at least 21 minutes.

The typical timeout is 30-60 minutes, but in some environment this default value is lowered for security/performance reasons.

1.2.2 Required to provide adequate quality

Whenever these requirements are satisfied, the users will perceive good quality and will have nice feedback.

1.2.2.1 Quality of Service

(QoS) requirements affects the perceived audio quality during secure calls. When the following requirements are met audio will be clear, not distorted, continuous, without gaps and with almost not perceivable delay:

- minimum symmetric bandwidth 40kb/s
- packet loss under 1%
- latency under 200 ms
- jitter under 300ms
- SIP roundtrip under 1000 ms: this affects the Call Setup Time (CST), which is about 4 times the SIP roundtrip. Higher roundtrip times produce effect ranging from bad user-experience to impossibility to dial and receive call

1.2.2.2 Stability of network connection

It is important to have high Call Success Ratio (CSR).

Unstable network connection can lead to inability to dial/receive calls, abruptly broken calls while speaking and impossibility to dial long calls.

To provide good quality, is required to have a **stability window** on both side of the call, caller and called. The stability window must cover the call duration and also the preceding 10 minutes:

- no switch between 3G and/or 2G and/or WiFi
- no IP address changes
- no network errors that break TCP socket (Es: TCP socket timeout by statefull firewall)

Pre-call stability window is particularly critical with iPhone devices, which, currently, do not have a true multitasking OS and can adapt to network change typically within 10 minutes window period.

1.3 Server

We suggest to keep the following concept:

- A minimum of 2 CPU core for each PrivateServer. We suggest these models:
    - Intel(R) Core(TM) i7 CPU 950 @ 3.07GHz
    - AMD Athlon(tm) 64 X2 Dual Core Processor 6000+

but the product is known to run smoothly on slower ones.

- A minimum of 2GB of RAM for each PrivateServer (Consider quickly scaling up to 4GB of RAM)
- A minimum of 50GB of storage for each PrivateServer (consider raising up to 100GB in case of high number of users of a specific server)
- A minimum of one 100/1000 Mb/s NIC (or more NICs to setup the Network Segregation)
- Almost one public IP Address, NATted to the server's NIC or directly assigned to it
- One public hostname (with correct DNS resolution)
- One SSL Certificate (accordingly with the hostname)

1.2.3 Required to enable the update feature on the PrivateServer

The following configuration is needed to enable the update feature on the PrivateServer:

- **OUTPUT** (from the server to the outside network):
    - HTTP: TCP/80: The server acts like an http client in order to fetch update informations, download proper packages and install them.