What's new

Here are descriptions of the more relevant changes in EVSS 14.3

PrivateWave changes

Message persistency, protected PIN

In previous version of PrivateGSM, message are transient and their content disappear 15 minutes reading.

If you enable PIN protection, your messages are stored in encrypted form inside your device. PIN protection adds a protection layer to your privacy and opens new ways of use for PrivateWave . You can now set your 4 digits PIN so that accessing PrivateWave application would need your authorization. As always we worked on improving performances and robustness of PrivateWave .

This additional security measure does not compromise usability: PIN is not required to answer incoming call.

PIN under duress

You can configure an additional PIN for critical situations. Every time you unlock PrivateWave using your duress code, call and message history are immediately deleted, and nobody can access to them. Unlocking your your primary PIN does not affect call and message history.

UI improvement

UI has been re-designed to clearly separate call and messaging features, in a more intuitive way.

PrivateServer changes

TLS support

Due to recent "Poodle" vulnerability (CVE-2014-3566), we definitely dropped support for SSLv3 protocol on incoming connections. This completely fixes the problem even for clients which support it and are vulnerable to downgrade attack.

SSL support is removed on a code basis, so there is no way to enable it.

On SIP/TLS outgoing connections it could be enabled to provide support for legacy PBX integration.

TLS support covers TLS1.0, TLS1.1 and TLS1.2, including forward secrecy with DHE and ECDHE cipher suites. Keep in mind that Blackberry OS5/7 and Android 2.x do not support ECDHE, but only DHE.