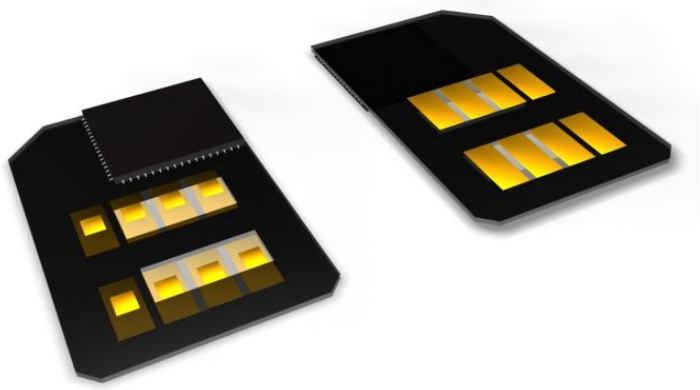
TURBO SIM
Security Edition

Turbo SIM – Security Edition is a device with a set of pre-installed applications targeted at SMS encryption and privacy protection. Inserted in the SIM Lock together with the operator SIM card, the device can be used in any GSM SIM Toolkit enabled mobile phone, i.e. almost every mobile phone produced since 1998.



Turbo SIM - Security Edition has been developed to be used by financial institutions, security organizations, businesses and every other area that uses SMS for critical communications with a need for protection against eavesdropping and message spoofing (sender faking). Furthermore, it can be used for general mobile phone protection and as a secure store of private information.

Being independent of the mobile phone used makes it ideal for deployment in the heterogeneous environments of governments, large organizations or any establishment with a high mobile phone turn over rate.

After inserting the **Turbo SIM – Security Edition**, a new menu item called **Secure** appears on the mobile phone – containing the following applications:

- **Encrypted SMS** – SMS communications are protected against eavesdropping and message spoofing by the employment of the strong Twofish[1] symmetric cypher. To simplify the usage of Encrypted SMS, secret keys can be assigned to individual phone numbers. It is possible to have dozens of keys for communication in large enterprises – including secret keys that can be hidden against a user (users then do not know the keys and cannot view them).

- **Killing SMS** – it is possible to define a special “Killing SMS” that blocks or resets the mobile phone in the event that it is lost or stolen. This makes it impossible to make calls, or otherwise manipulate the phone, when used together with the SIM card PIN and phone locking.

- **Attention SMS** – messages sent using this application appear directly on the recipient's mobile phone display. No more wasting precious seconds going into the SMS inbox – the message are instantly displayed on the screen.

- **Secrets** – an application for the secure storage of private information, e.g. passwords, bank accounts, credit card numbers, etc. A very handy way of keeping that critical data conveniently in your phone, yet safe from possible discovery.

The user interface is localized to **English**, **French**, **German** and **Czech** languages.

Notes on security mechanisms used

1. **Turbo SIM – Security Edition** uses **128 bit symmetric cipher Twofish**, http://www.schneier.com/twofish.html

2. Messages and secrets are encrypted in **CBC** mode, i.e. the same text encrypted several times will look different every time.

3. It uses a **unique random number generator** that combines pseudo random generation techniques with **physical behaviour of the mobile network**.

4. For **protection against application manipulation**, the device is **locked** and it is impossible to upload or remove applications without first deleting the pre-installed applications.

5. For **protection against invasive attacks**, all keys and data are stored **encrypted** in memory, with the main unlock keys not being stored at all. In the case of an invasive attack no data is accessible in plain text. All messages stored on the SIM card are also encrypted for added security.