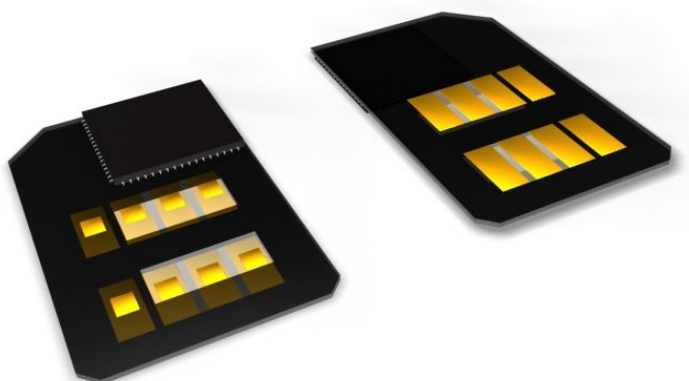


Turbo SIM – Security Edition je zařízení a soubor aplikací zaměřených na šifrování SMS komunikace a ochranu soukromých informací. Zařízení, které se vkládá do SIM konektoru současně se SIM kartou operátora, je určeno pro GSM mobilní telefony vybavené technologií SIM Toolkit a lze ho použít v prakticky každém telefonu uvedeném na trh po roce 1998.



Zařízení **Turbo SIM - Security Edition** je určeno pro finanční instituce, bezpečnostní organizace, firmy a ostatní subjekty, které využívají SMS komunikaci a mají potřebu ochrany před odposlechem a před podvrženými falešnými zprávami. Dále je vhodné pro zajištění telefonu při ztrátě a pro bezpečné uložení důvěrných informací.

Nezávislost na použitém mobilní telefonu umožňuje použití v heterogenním prostředí velkých organizací a státní správy.



Vložení **Turbo SIM – Security Edition** se v menu telefonu objeví nová položka **Secure** obsahující tyto aplikace:

- **Šifrované SMS** – ochrana před odposlechem a falešnými zprávami (SMS spoofingem). Zprávy jsou šifrovány silnou symetrickou šifrou Twofish, pro jednoduchost použití lze klíče svázat s telefonními čísly. Je možné mít desítky klíčů pro komunikaci v rámci větších organizací, tajné klíče lze skrýt před uživatelem (uživatel pak nezná a nemá k přednastavené klíčům přístup).

- **Blokovací SMS** – možnost definovat speciální blokovací SMS, která způsobí zablokování, případně reset telefonu. Tím lze v případě ztráty či odcizení telefonu zabránit neoprávněným osobám volat a jinak manipulovat s telefonem (spolu s nastavením PIN SIM karty a zamčení telefonu).
- **Výstražné SMS** posílané na displej mobilního telefonu. Pro zdůraznění sdělení lze poslat zprávu, která se příjemci zobrazí přímo na displej telefonu.
- **Tajemství** – aplikace pro bezpečné uložení důvěrných informací, např. hesel, bankovních účtů apod.

Uživatelské rozhraní je lokalizováno do **češtiny, angličtiny, francouzštiny a němčiny**..

Použité bezpečnostní techniky

- **Turbo SIM – Security Edition** používá **128 bitovou symetrickou šifru Twofish**, viz. <http://www.schneier.com/twofish.html>
- Zprávy i tajemství jsou šifrovány v **CBC** módu, tj. stejný text má pokaždé jinou zašifrovanou podobu.
- Je použit **unikátní generátor náhodných čísel**, který kombinuje techniky generování **pseudonáhodných čísel s fyzikálním chováním mobilní sítě**.
- Pro **ochranu před podvržením a manipulací** s aplikacemi je zařízení **zamčeno**, nelze nahrávat ani mazat jednotlivé aplikace bez smazání všech stávajících aplikací.
- Pro **ochranu před invazivním útokem** jsou všechny klíče a data uloženy v paměti v zašifrované podobě, hlavní odemykací hesla aplikací nejsou uložena vůbec. V případě invazivního útoku nejsou data volně přístupná. Zprávy jsou uloženy na SIM kartě v šifrované podobě.