

TOPSEC MOBILE

Гласово криптиране за мобилни телефони

Общ преглед

TopSec Mobile е мобилно устройство позволяващо криптирани комуникации със съответни криптиращи устройства, използвайки почти всеки мобилен телефон с Bluetooth® интерфейс. Това осигурява криптиране на гласовите услуги, за по-голямата част от мобилните телефони от различни производители.

Алгоритмите и методите, използвани за криптирането са изпробвани и тествани с продуктите на TopSec фамилията.

TopSec Mobile е съвместимо с повечето налични мобилни телефони, с други TopSec продукти в аналоговите и цифрови фиксирани мрежи, както и в мобилните радиомрежи.

Основни характеристики

Разностранност

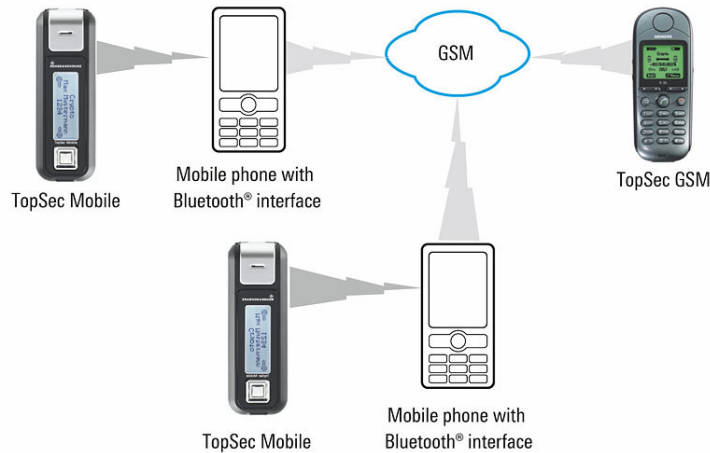
- ⇒ Bluetooth® интерфейс (версия 1.2 или по-късна), за връзка с крайни комуникационни терминални съоръжения;
- ⇒ Работи с почти всички съвременни мобилни телефони – условие – мобилният телефон:
 - трябва да поддържа CSD (circuit switched data) режим на непрозрачно предаване на GSM данни и
 - трябва да има Bluetooth® интерфейс с Dial-Up мрежов (DUN) профил за криптирани комуникации;
- ⇒ Независимост от мобилните радио честоти - в зависимост от възможностите на партньорското криптиращо устройство, TopSec Mobile използва V.110 или V.32 комуникационни протоколи.
- ⇒ Може да се използва и с модеми с аналогови или ISDN Bluetooth® интерфейси - за криптирани връзки TopSec Mobile изисква непрозрачна връзка за данни на 9,6 Kbps



Криптиране с TopSec Mobile

Устойчивост на манипулации

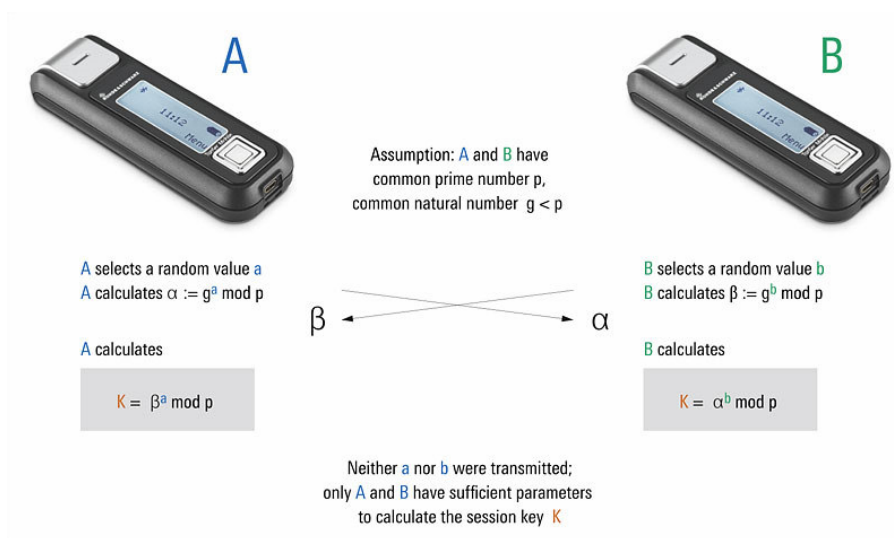
- ⇒ Неограничено ползване на удобните функции на мобилния телефон
- ⇒ Сигурност, независима от мобилния телефон
- ⇒ Не може да бъде идентифицирано чрез мрежата на мобилния оператор



Гласово криптиране в мобилните мрежи

Алгоритми за защитно криптиране

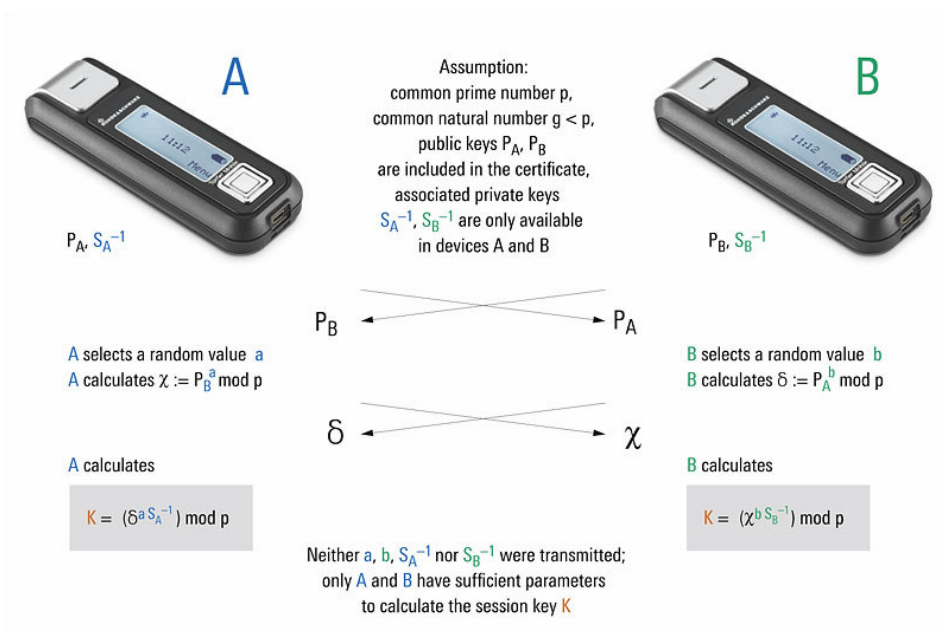
- ⇒ Хибриден подход за максимална сигурност
- ⇒ Асиметричен *Diffie-Hellman* алгоритъм използващ 1024 битов криптиращ ключ при „договаряне“
- ⇒ Симетричен криптиращ алгоритъм за криптиране на гласа (данните): 128 битови криптиращи ключове произволно избрани от 10^{38} възможни ключове



Договаряне на ключовете с *Diffie-Hellman* алгоритъм.

Удостоверяване на потребителя

- ⇒ Лъжливите криптирани връзки са невъзможни
- ⇒ Man-in-the-middle атаките са ефективно предотвратени
- ⇒ Възможност за създаване на затворени групи потребители

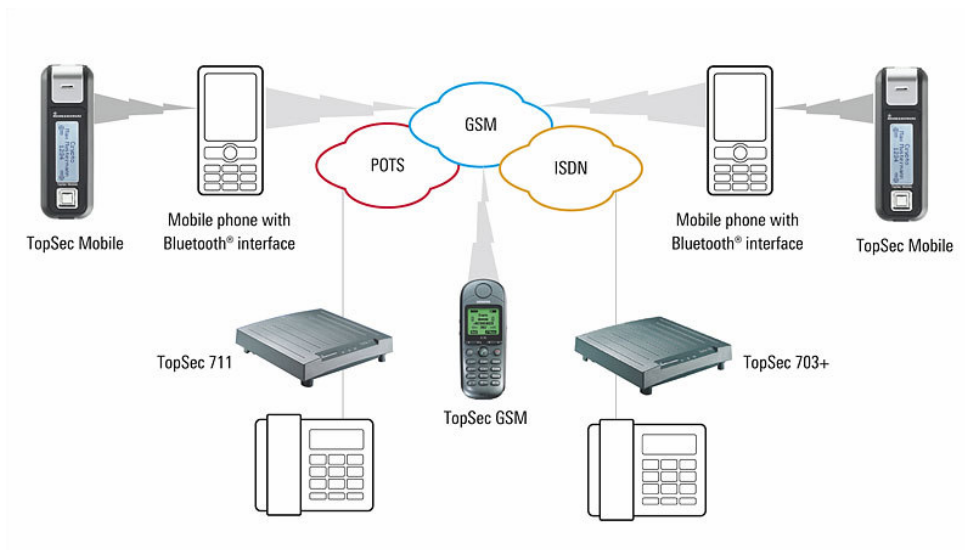


Комбинирано договаряне на ключовете и проверка за автентичност.

Взаимна свързаност

Подходящи партньорски криптиращи устройства:

- TopSec Mobile в комбинация с мобилен телефон
- TopSec GSM CRYPTO мобилен телефон
- TopSec 703+ - ISDN криптиращо устройство за фиксирана мрежа
- TopSec 711 - криптиращо устройство за фиксирана аналогова мрежа



Гласово криптиране с TopSec устройства

Технически данни

Bluetooth® standard	version 2.0
Standby time	up to 100 h
Talk time	up to 4 h
Data rate	9.6 kbps
Transfer protocol	V.32, V.110
Dimensions	99 mm × 34 mm × 22 mm (3.9 in × 1.3 in × 0.9 in)
Weight	55 g (0.12 lb)

Списък на мобилните телефони тествани и работещи с TopSec Mobile

Manufacturer	Model
Alcatel	OT-C701
BenQ/Siemens	S 55, S 68
LG Electronics	KU 990 Viewty
Motorola*	L6i, RAZR V3i, RAZR V8, Rock E6
Nokia	E 51, E 61i, E 62, E 65, N 70, N 71, N 72, N 73, N 78, N 82, N 92, N 90, N 95 2630, 3109, 3109c, 5220, 5500, 5610 Express Musik, 6151, 6230i, 6233, 6300, 6301, 6310, 6500 Classic, 6500 Slide, 6680, 7500, 7500 Prism, 8800 ARTE, 9500 Communicator
Sagem	My X6-2, Porsche Design P 9521
Samsung	SGH-D900, SGH-E900, SGH-E250, SGH-E250V, SGH-ZV30, SGH-Z500V
Sonim	XP1
Sony Ericsson	C 902, K 320i, K 530i, K 750, K 750i, D 750i, K 790, K 850i, K 800i, P 1i, P 910, W 910i, P 990i, S 500i, T 610i, T 650, W 660i, W 880, W 890i, W 960i, Z 660i
Roda Computer	BOB-M DA05

* Reduction in stand-by time of mobile phone and TopSec Mobile