

TopSec Mobile

Sprachverschlüsselung für Mobiltelefone



TopSec Mobile

Auf einen Blick

Das TopSec Mobile ist ein Sprachverschlüsselungsgerät, das über eine Bluetooth® Funkschnittstelle mit handelsüblichen Mobiltelefonen verbunden werden kann und so eine vertrauliche, weltweit verfügbare, abhörsichere Kommunikation ermöglicht. Durch die Realisierung der Verschlüsselung in einer eigenen Hardware ist eine Manipulation – anders als bei ungesicherten GSM-Telefonen – ausgeschlossen.

Das TopSec Mobile wird über Bluetooth® an ein Kommunikationsendgerät angeschlossen. Als Kommunikationsendgeräte werden hauptsächlich Mobiltelefone verwendet. Von einem TopSec Mobile aus kann über Mobiltelefone mit Bluetooth® eine verschlüsselte Kommunikation mit einem interoperablen Partnerschlüsselgerät erfolgen. Der Dienst Sprachverschlüsselung steht somit für die meisten Mobiltelefonmodelle unterschiedlichster Hersteller zur Verfügung.

Zur Verschlüsselung werden die bei der TopSec-Produktfamilie bewährten Algorithmen und Verfahren eingesetzt. Das TopSec Mobile ist das sicherste heute zur Verfügung stehende Sprachverschlüsselungsgerät für Mobilfunkkommunikation. Es zeichnet sich durch ein elegantes Design, hervorragende Sprachqualität und eine denkbar einfache Bedienung aus.

Das TopSec Mobile ist

- „Plug and Play“
zusammen mit den meisten handelsüblichen Mobiltelefonen
- Interoperabel
zu anderen TopSec-Produkten in analogen und digitalen Netzen sowie in Mobilfunk- und TETRA-Netzen
- Sicher
zukunftsichere Verschlüsselungs- und Sicherheitsverfahren



TopSec Mobile

Wesentliche Merkmale und Vorteile

Universell einsetzbar

- Bluetooth® Funkschnittstelle zur Anbindung an ein Kommunikationsendgerät
- TopSec Mobile funktioniert mit den meisten modernen Mobiltelefonen
- Weitgehende Unabhängigkeit von Mobilfunkfrequenzen
- Verwendung auch mit Modems und Satellitentelefonen mit Bluetooth® Funkschnittstelle

▷ [Seite 4](#)

Manipulationssicher

- Komfortfunktionen des Mobiltelefons uneingeschränkt nutzbar
- Sicherheit des TopSec Mobile ist unabhängig vom Mobiltelefon
- Nicht identifizierbar durch den Mobilfunkbetreiber

▷ [Seite 5](#)

TopSec-Kryptoverfahren

- Verfahren für höchstmögliche Sicherheit
- Schlüsseleinigung mit elliptischen Kurven, 384 bit
- Vortäuschen einer Kryptoverbindung und Man-in-the-Middle-Angriffe wirksam verhindern
- Zertifikatsbasierte Authentifizierung
- Sprachverschlüsselung mit AES, 256-bit-Schlüssel

▷ [Seite 6](#)

Ladbare Kryptoverfahren

- Lesegerät für Sicherheitskarten
- Unterstützung der BOS-Digital-Sicherheitskarte

▷ [Seite 7](#)

Interoperabel

- Interoperabilität mit:
 - TopSec Mobile in Kombination mit einem Mobiltelefon
 - Krypto-Mobiltelefon TopSec GSM
 - Verschlüsselungsgerät für digitale Anschlüsse TopSec 703+
 - Verschlüsselungsgerät für analoge Anschlüsse TopSec 711
 - Gateway für Sprachverschlüsselung TopSec 830
- Zukunftssicherheit

▷ [Seite 8](#)

Universell einsetzbar

Bluetooth® Funkschnittstelle zur Anbindung an ein Kommunikationsendgerät

Das Sprachverschlüsselungsgerät TopSec Mobile verfügt über eine Bluetooth® Funkschnittstelle zur Anbindung an ein Kommunikationsendgerät.

Als Kommunikationsendgeräte werden zusammen mit dem TopSec Mobile vor allem Bluetooth® Mobiltelefone verwendet. Bluetooth® ist ein gut spezifizierter Standard und bietet eine stabile Kommunikationsschnittstelle zwischen dem TopSec Mobile und dem Mobiltelefon. Das TopSec Mobile ist sowohl hinsichtlich der Anbindung an Kommunikationsendgeräte als auch bezüglich der Netzanbindung ein universell einsetzbares Sprachverschlüsselungsgerät.

TopSec Mobile funktioniert mit den meisten modernen Mobiltelefonen

Das TopSec Mobile funktioniert zusammen mit den unterschiedlichsten Mobiltelefonen der unterschiedlichsten Hersteller. Die Voraussetzungen dafür sind: Das Mobiltelefon unterstützt den nicht-transparenten GSM-Datenmodus CSD (Circuit Switched Data) und verfügt über eine Bluetooth® Funkschnittstelle ab Version 1.2 mit dem Profil DUN (Dial-up Networking) für eine Kryptokommunikation. Dies ist bei den meisten modernen Mobiltelefonen der Fall. Der Anwender ist somit relativ frei bei der Wahl seines Mobiltelefons. Er kann sein bevorzugtes Mobiltelefon nutzen und gleichzeitig auf Wunsch sicher kommunizieren.

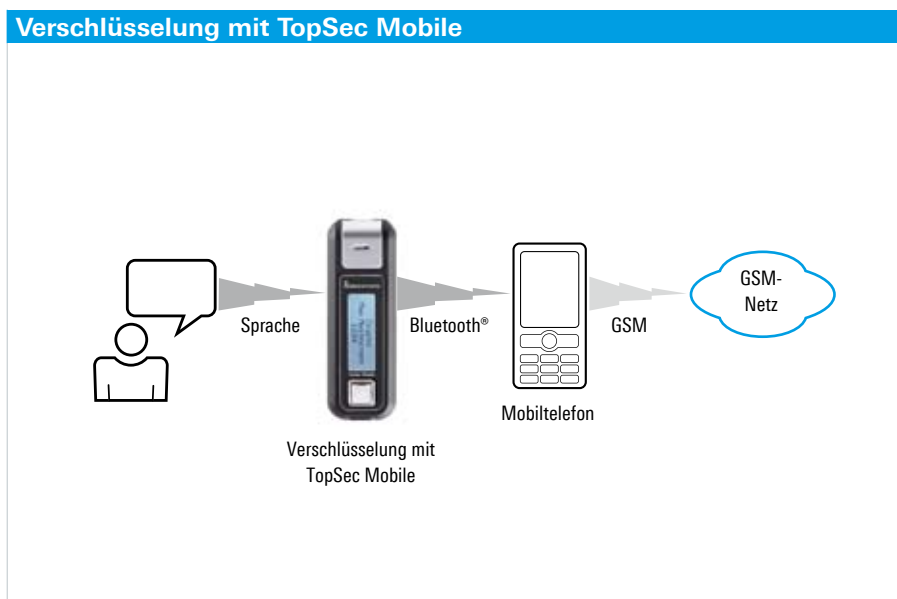
Weitgehende Unabhängigkeit von Mobilfunkfrequenzen

Ein weiterer Vorteil der Anbindung des TopSec Mobile über Bluetooth® ist die weitgehende Unabhängigkeit von Mobilfunkfrequenzen. Mit dem Bluetooth® Mobiltelefon und dem davon genutzten Mobilfunknetz stehen die vom Anwender gewünschten Mobilfunkfrequenzen und Netzanbieter zur Verfügung.

Für eine Kryptoverbindung benötigt das TopSec Mobile eine Datenverbindung (nicht-transparent) mit einer Datenrate von 9,6 kbps. Als Kommunikationsprotokoll wird entweder V.110 oder V.32 verwendet, abhängig von den Möglichkeiten des Partner-Schlüsselgerätes. Diese Anforderungen werden von den meisten Bluetooth® Mobiltelefonen und von den meisten Mobilfunknetzen unterstützt.

Verwendung auch mit Modems und Satellitentelefonen mit Bluetooth® Funkschnittstelle

Das TopSec Mobile kann über die Bluetooth® Funkschnittstelle mit einem Analog- oder ISDN-Modem oder einem Satellitentelefon verbunden werden. Damit kann das TopSec Mobile auch an Festnetzanschlüssen eingesetzt werden oder eine weltweit verfügbare sichere Kommunikation über Satellit herstellen. Für eine Kryptoverbindung benötigt das TopSec Mobile eine Datenverbindung (nicht-transparent) mit einer Datenrate von 9,6 kbps.



Manipulations- sicher

Komfortfunktionen des Mobiltelefons uneingeschränkt nutzbar

Mobiltelefone stellen dem Anwender eine Vielzahl von Funktionen zur Verfügung. Oft können nachträglich Applikationen über das öffentliche Netz geladen werden. Von den Providern werden ohne explizite Anforderung des Mobiltelefonnutzers ebenfalls Informationen auf das Mobiltelefon gesandt, die dieses nach den Wünschen des Providers konfigurieren. Diese Möglichkeiten sind erforderlich, um die Mobilität so groß und flexibel wie möglich zu gestalten, um immer aktuellste Informationen bereit zu haben oder um jederzeit Zugriff auf Termine zu haben. Die Akzeptanz von Mobiltelefonen ist sehr stark von solchen Komfortfunktionen abhängig.

Sicherheit des TopSec Mobile ist unabhängig vom Mobiltelefon

Die Komfortfunktionen bergen die Gefahr, dass sie von Angreifern unerlaubt genutzt werden können, um an vertrauliche Informationen zu gelangen. Die Manipulationsmöglichkeiten von Mobiltelefonen sind äußerst vielfältig.

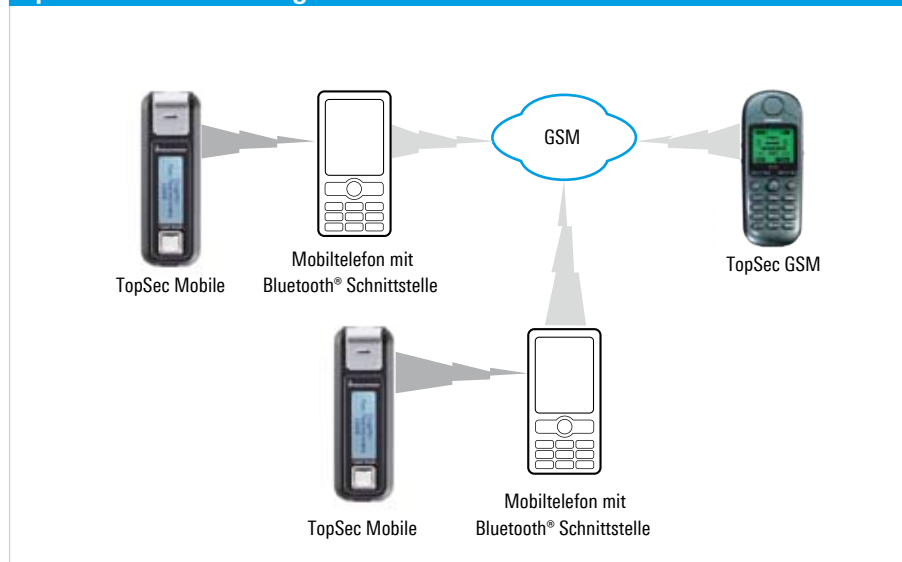
Das TopSec Mobile benötigt weder Informationen eines Providers, noch können zusätzliche Applikationen geladen oder ausgeführt werden. Das TopSec Mobile ist ein Spezialgerät, welches eine vertrauliche Sprachkommunikation ermöglicht. Deshalb sind Bedienelemente, Audiokomponenten – Mikrofon und Lautsprecher – und alle Kryptofunktionen im TopSec Mobile integriert. Die Sicherheit des TopSec Mobile ist unabhängig vom Mobiltelefon. Das TopSec Mobile bietet die bestmögliche Manipulationssicherheit.

Nicht identifizierbar durch den Mobilfunkbetreiber

Mobiltelefone können über die IMEI (International Mobile Equipment Identity) identifiziert werden. Wenn sich ein Mobiltelefon an ein Mobilfunknetz anmeldet, wird auch die IMEI übertragen. Diese gibt Auskunft über Hersteller und Gerätetyp. Der Betreiber eines Mobilfunknetzes ist somit auch in der Lage, bestimmten Mobiltelefonen den Betrieb ganz oder teilweise zu verweigern.

Das TopSec Mobile selbst ist kein Mobiltelefon, sondern wird über die Bluetooth® Funkschnittstelle an ein solches angeschlossen und kann mit verschiedenen Mobiltelefonen verwendet werden. Eine Identifizierung des TopSec Mobile ist nicht möglich; die Verwendung kann somit nicht durch die Betreiber von Mobilfunknetzen verhindert werden.

Sprachverschlüsselung im Mobilfunknetz



Das TopSec Mobile kann zusammen mit den meisten Bluetooth® fähigen Mobiltelefonen eingesetzt werden; als Gegenstelle im Mobilfunknetz kann entweder ein Mobiltelefon zusammen mit einem TopSec Mobile oder ein TopSec GSM verwendet werden.

TopSec-Kryptoverfahren

Verfahren für höchstmögliche Sicherheit

Im TopSec Mobile basiert die Verschlüsselung auf einem Hybridverfahren, um höchste Sicherheit zu erreichen. Die Voraussetzung dafür wurde geschaffen, indem die Partner-Kryptogeräte über die gleichen mathematischen Parameter verfügen und die gleichen Algorithmen verwenden.

Schlüsseinigung mit elliptischen Kurven, 384 bit

Durch Verwendung des Diffie-Hellman-Schlüsseinigungsverfahrens ist ohne administrative Eingriffe eine verschlüsselte Kommunikation zwischen zwei Partner-Kryptogeräten möglich. Im TopSec-Sprachgebrauch wird dies als „offenes System“ bezeichnet, weil die Möglichkeit einer sicheren Kryptoverbindung mit jedem beliebigen TopSec-Kryptogerät gegeben ist. Der in den beiden Partner-Kryptogeräten errechnete Sitzungsschlüssel K wird von den symmetrischen Algorithmen verwendet, um die digitalisierte und komprimierte Sprache zu verschlüsseln beziehungsweise zu entschlüsseln.

Vortäuschen einer Kryptoverbindung und Man-in-the-Middle-Angriffe wirksam verhindern

Der Anwender des TopSec Mobile will sicher sein, dass weder eine Kryptoverbindung vorgetäuscht wird noch ein sogenannter Man-in-the-Middle-Angriff erfolgt, bei dem sich ein unbefugter Dritter als Kommunikationspartner ausgibt. Zu diesem Zweck wird im offenen System ein individueller vierstelliger Sicherheits-Code berechnet. Er wird auf dem Display der Gesprächspartner dargestellt und ist ausschließlich in den beiden Geräten verfügbar. Bei einer sicheren Verbindung sind die Sicherheits-Codes identisch.

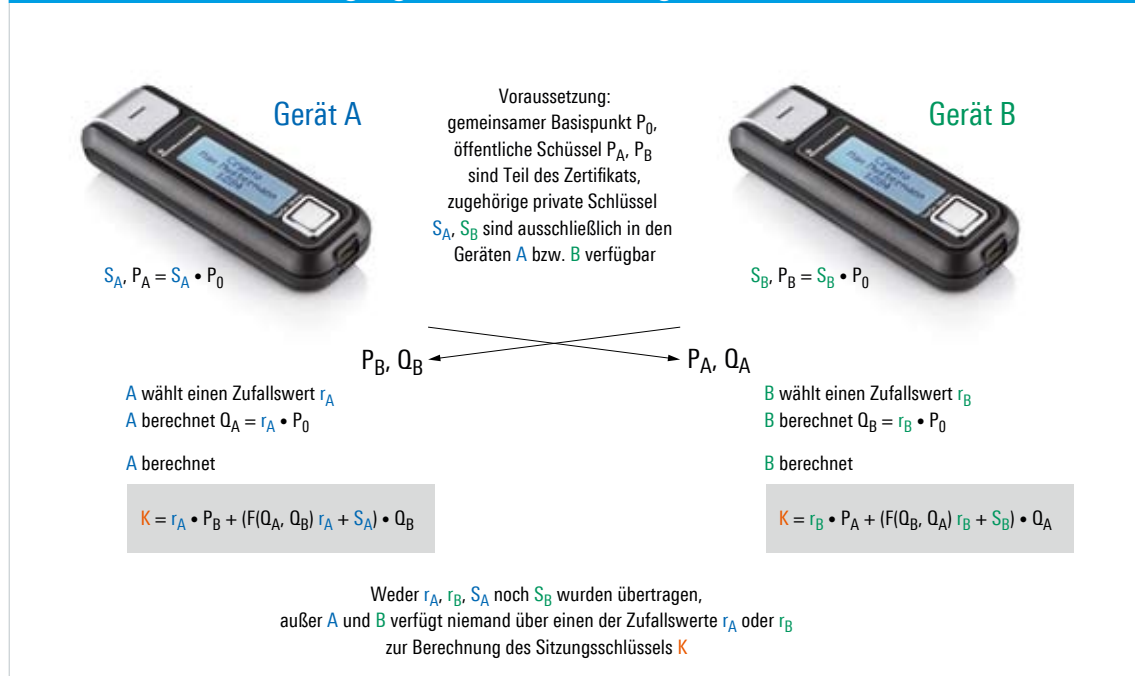
Zertifikatsbasierte Authentifizierung

Eine weitere mögliche Maßnahme zur Vermeidung von Man-in-the-Middle-Angriffen ist die Bildung von geschlossenen Benutzergruppen. Dazu wird der TopSec Administrator benötigt, eine Kombination aus einem Trust Center und einer zentralen Verwaltung von Betriebsparametern. TopSec-Geräte erhalten im Rahmen einer Initialisierung ein Zertifikat und generieren ein Public-Key-Schlüsselpaar zur Authentisierung. Bei geschlossenen Systemen authentisieren sich die TopSec-Kryptogeräte automatisch. Nur wenn die Authentisierung erfolgreich ist, wird eine Kryptoverbindung etabliert (siehe Grafik). Die Vertraulichkeit der Gespräche entspricht somit höchsten Sicherheitsanforderungen.

Sprachverschlüsselung mit AES, 256-bit-Schlüssel

Das TopSec Mobile vereinbart mit dem Partner-Kryptogerät bei jedem Verbindungsaufbau automatisch einen neuen, 256 bit langen Schlüssel. Dabei wird nach dem Zufallsprinzip einer aus 10^{76} möglichen Schlüsseln gewählt und nach Beendigung der Kommunikation sofort gelöscht.

Kombinierte Schlüsseinigung und Authentisierung



Ladbare Kryptoverfahren

Lesegerät für Sicherheitskarten

Das TopSec Mobile ermöglicht neben der Benutzung der fest im Gerät implementierten TopSec-Verschlüsselungsverfahren auch die Verwendung weiterer Kryptoverfahren zur Sprachverschlüsselung. Über das Benutzermenü des TopSec Mobile können die Kryptoverfahren über das integrierte Kartenlesegerät aktiviert und deaktiviert werden. Bei jedem Rufaufbau entscheidet der Nutzer des TopSec Mobile, sofern die Sicherheitskarte im Lesegerät steckt, mit welchem Algorithmus der Gesprächspartner angerufen werden soll. Die Sicherheitskarte wird vom TopSec Mobile über Befehle angesprochen, welche dem vom BSI entwickelten SNS-Standard (Sichere Netzübergreifende Sprachkommunikation) entsprechen.

Unterstützung der BOS-Digital-Sicherheitskarte

Für die Verschlüsselung stehen über das Kartenlesegerät die Algorithmen der BOS-Digital-Sicherheitskarte zur Verfügung. Die Kryptografie dieser Karte beinhaltet eine zertifikatsbasierte Authentifizierung nach Diffie-Hellman mit elliptischen Kurven zur Schlüsseinigung und die Sprachverschlüsselung mit AES.

Für die zertifikatsbasierte Authentisierung wird von einem Trust Center im Rahmen der Initialisierung das Zertifikat zusammen mit dem öffentlichen Schlüssel (zur Prüfung von Zertifikaten) und einem Public-Key-Schlüsselpaar (zur eigentlichen Authentisierung) auf der BOS-Digital-Sicherheitskarte abgelegt. Zur Authentisierung wird das Zertifikat des Partner-Kryptogerätes geprüft. Für die Schlüsseinigung wird das Diffie-Hellman-Schlüsseinigungsverfahren mit elliptischen Kurven zur Berechnung des für jedes Gespräch individuellen Sitzungsschlüssels verwendet. Im Verschlüsselungsmodus vereinbart das TopSec Mobile mit dem Partner-Kryptogerät bei jedem Verbindungsaufbau automatisch einen neuen symmetrischen AES-Schlüssel, nach Beendigung der Kommunikation wird dieser sofort gelöscht.



Interoperabel

Interoperabilität

Das TopSec Mobile verwendet die bei der TopSec-Produktfamilie bewährten kryptologischen Verfahren. Damit ist die Voraussetzung für eine Interoperabilität innerhalb der TopSec-Produktfamilie gegeben. Die Sprachverschlüsselung in Mobilfunknetzen ist dabei das Haupteinsatzgebiet des TopSec Mobile. Der Gesprächspartner kann ebenfalls über Mobilfunk, aber auch über ein analoges oder digitales Festnetz erreichbar sein. In jedem Fall ist eine sichere Sprachverschlüsselung möglich.

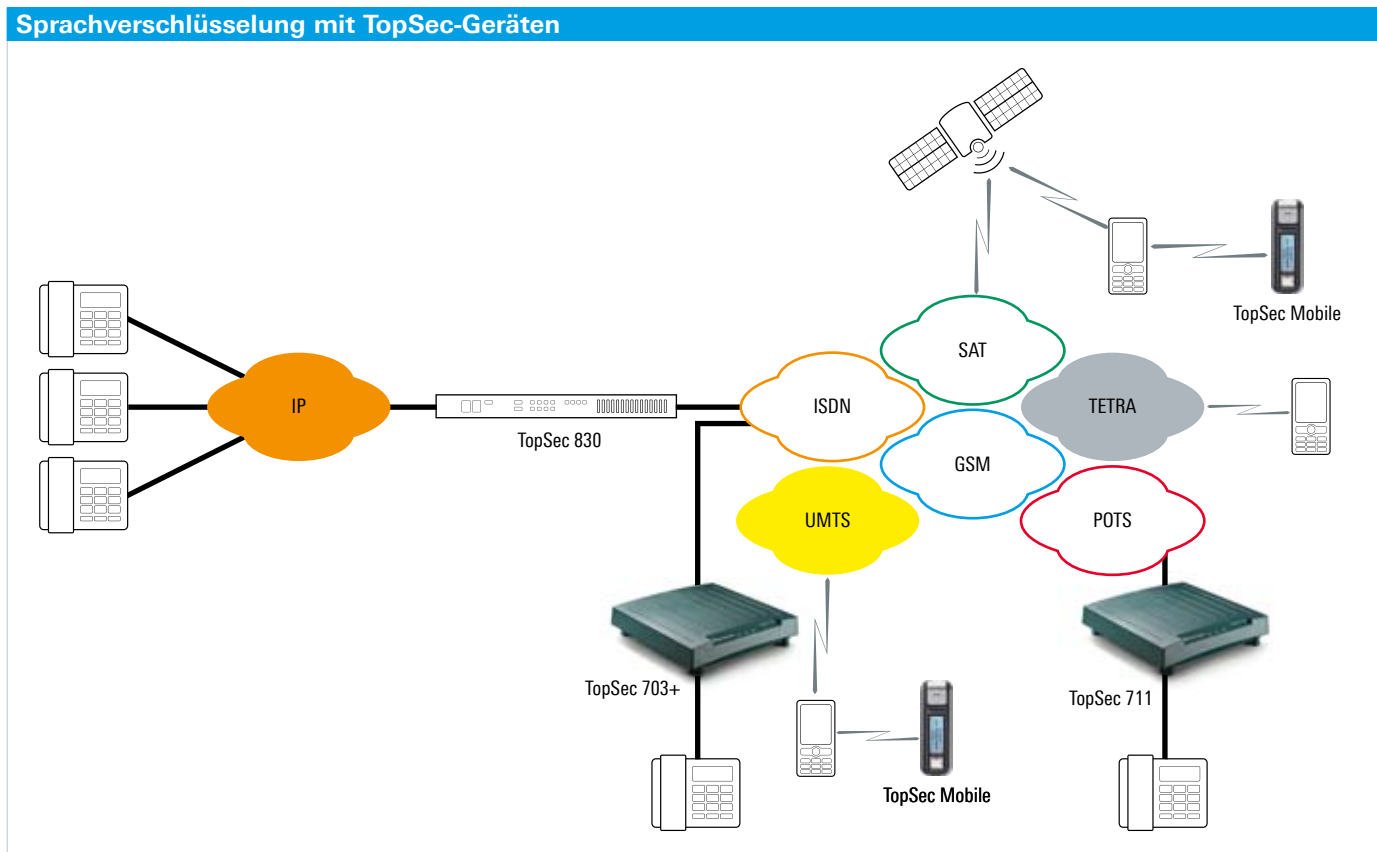
Das TopSec Mobile komprimiert die Sprache so weit, dass sie mit einer Datenrate von 9,6 kbps übertragen werden kann. Zu einem Gesprächspartner, der ebenfalls über Mobilfunk erreichbar ist, kann sowohl das V.110- als auch das V.32-Protokoll verwendet werden. Damit ist eine Interoperabilität zu einem anderen TopSec Mobile oder zum Krypto-Mobiltelefon TopSec GSM gegeben.

Um eine verschlüsselte Sprachverbindung über das Gateway TopSec 830 zu einem VoIP- oder ISDN-Telefon oder über das ISDN-Kryptogerät TopSec 703+ aufzubauen, wird das Protokoll V.110 gewählt. Ist der Gesprächspartner für eine verschlüsselte Sprachkommunikation im analogen Netz über ein TopSec 711 erreichbar, wird das V.32-Protokoll gewählt.

Nach der Auswahl des für das jeweilige Netz geeigneten Protokolls – V.110 oder V.32 – ist das Sprachverschlüsselungsgerät TopSec Mobile interoperabel mit dem TopSec GSM, dem TopSec 703+, dem TopSec 711 und dem TopSec 830.

Zukunftssicherheit

Das TopSec Mobile basiert auf einer performanten Hardware mit großem Speicherbereich. Die Firmware des TopSec Mobile kann über ein sicheres Verfahren am TopSec Administrator aktualisiert werden. Damit ist sichergestellt, dass mit TopSec Mobile auch neue Herausforderungen gemeistert werden können.



Design und Funktionselemente

Design

Die Anwender des TopSec Mobile kommen aus allen Bereichen, in denen vertraulich kommuniziert wird. Sie gehören zur Führungsriege von Wirtschaft und Politik, sind mit Sicherheitsaufgaben betraut oder in den Bereichen Vertrieb, Finanzen, Technik und Wissenschaft tätig.

Passend zu diesem Anwenderkreis ist das TopSec Mobile einerseits repräsentativ, andererseits aber unauffällig. Das Design ist hochwertig, elegant und zeitlos.

Getragen wird das TopSec Mobile in der Hemd- oder Jackentasche; dort wird es mit einem breiten Clip befestigt. Alternativ dazu kann auch ein Umhängeband am TopSec Mobile befestigt werden.

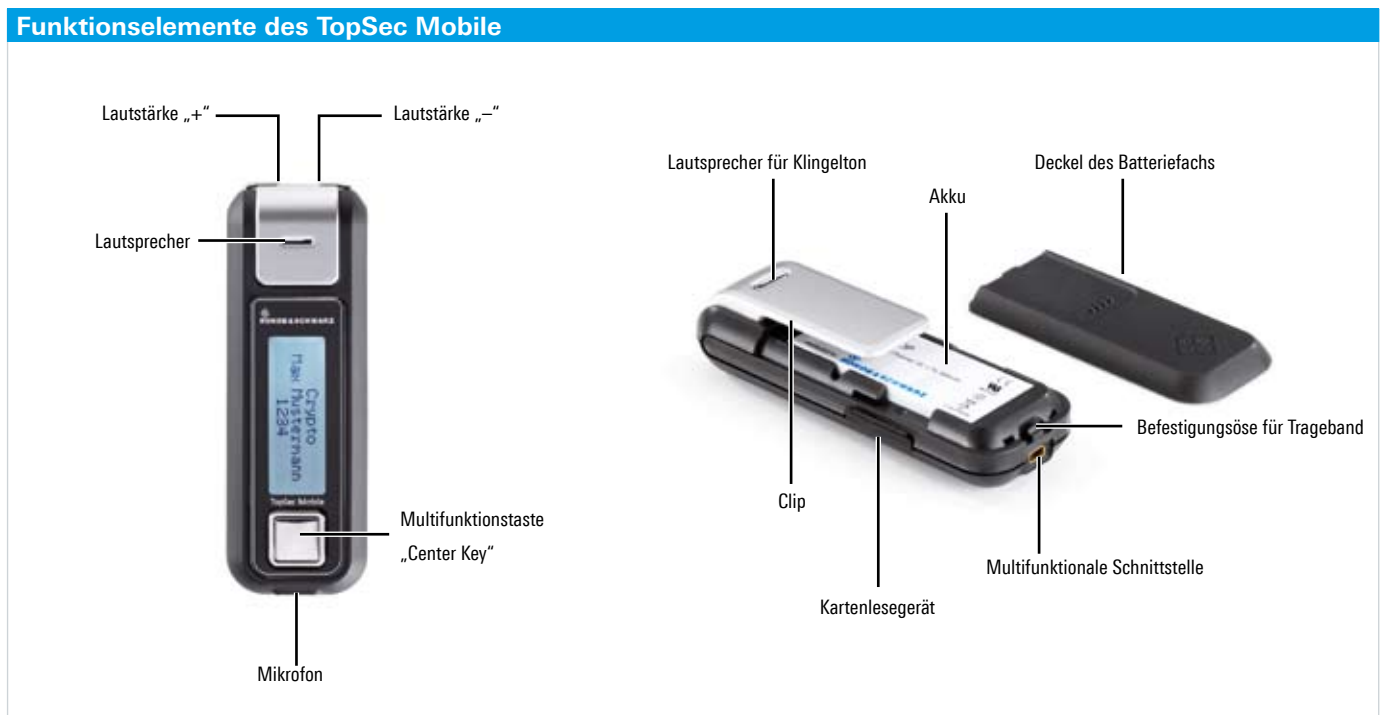
Funktionselemente

Das TopSec Mobile ist ein Sprachverschlüsselungsgerät mit integrierten Audiokomponenten. Die Grafik zeigt die verschiedenen Funktionselemente des TopSec Mobile.

Zum Sprechen verfügt das TopSec Mobile über ein integriertes Mikrofon. Zur Alarmierung und zum Hören dienen zwei Lautsprecher. Der im Clip auf der Rückseite des TopSec Mobile integrierte Lautsprecher wird zur Signalisierung bei ankommenden Rufen verwendet. Der auf der Vorderseite im Clip integrierte Lautsprecher wird während des Gesprächs benutzt und liefert eine hervorragende Sprachqualität.

Die Bedienung erfolgt über einen Fünf-Wege-Taster, bestehend aus einem zentralen Taster, dem sogenannten Center Key, sowie aus einem Ring, der in vier Richtungen betätigt werden kann. Als Anzeigeelement wird ein dreizeiliges Display verwendet. Damit sowohl Links-, als auch Rechtshänder mit dem Gerät gut zurecht kommen können, kann die Darstellung auf dem Display um 180° gedreht werden. Zusätzlich verfügt das TopSec Mobile über zwei Taster, mit denen die Lautstärke geändert werden kann. Auf der Unterseite ist zum Laden des Akkus und zum Verbinden mit einem PC eine multifunktionale Schnittstelle integriert.

Für die ladbaren Kryptoverfahren steht an der Seite des TopSec Mobile ein Kartenlesegerät zur Verfügung.



Betrieb

Inbetriebnahme

Bevor das TopSec Mobile eingesetzt werden kann, muss es mit einem Mobilfunktelefon gekoppelt werden. Zum Pairen wird am TopSec Mobile der Bluetooth® Suchmodus gestartet. Sobald das gewünschte Mobiltelefon ausgewählt wurde, wird am TopSec Mobile eine achtstellige Zufallszahl, die PIN, angezeigt. Diese PIN muss am Mobiltelefon eingegeben werden. Anschließend wird die Bluetooth® Verbindung zwischen dem Mobiltelefon und dem TopSec Mobile hergestellt. Das TopSec Mobile ist jetzt für die Sprachverschlüsselung bereit.

Aufbau einer verschlüsselten Verbindung

Soll ein Kryptoruf aufgebaut werden, dann wird aus dem im TopSec Mobile integrierten Telefonbuch der gewünschte Teilnehmer gewählt. Das TopSec Mobile sendet die Telefonnummer über die Bluetooth® Funkverbindung an das Mobiltelefon. Das Mobiltelefon baut dann eine Datenverbindung zu dem Partnergerät auf. Als Protokoll wird entweder V.110 oder V.32 verwendet.

Annehmen einer verschlüsselten Verbindung

Sobald die eingehende Datenverbindung vom gerufenen Gesprächspartner durch Drücken des Center Key angenommen wird, starten die beiden Kryptogeräte mit der Kryptosynchronisation. Nach erfolgreicher Kryptosynchronisation erscheint auf dem Display ein vierstelliger Sicherheitscode, mit dem die sichere Verbindung verifiziert wird. Die beiden Gesprächspartner können jetzt ein vertrauliches Gespräch führen.

Software zum Editieren des Telefonbuchs im TopSec Mobile

Das Telefonbuch im TopSec Mobile kann jederzeit über die Bedienelemente editiert werden. Mit der mitgelieferten Software TopSec Mobile Phonebook Editor für einen PC ist das Editieren noch benutzerfreundlicher. Das Telefonbuch wird über das mitgelieferte USB-Kabel vom TopSec Mobile an einen PC übertragen, dort editiert und dann wieder vom PC zurück zum TopSec Mobile übertragen.

Betrieb des TopSec Mobile mit einem Headset

In der Regel wird das TopSec Mobile wie ein Mobiltelefon benutzt, der Anwender spricht in das integrierte Mikrofon und hört den Gesprächspartner über den integrierten Lautsprecher. Alternativ dazu kann ein Headset verwendet werden.

Für die Anbindung des Headset wird die multifunktionale Schnittstelle des TopSec Mobile verwendet. Dazu wird ein Headset-Adapter an die Schnittstelle des TopSec Mobile angesteckt. Der Headset-Adapter verfügt über ein Bedienelement zum Annehmen von Gesprächen, über ein Mikrofon und über eine 2,5-mm-Klinkenbuchse. An diese 2,5-mm-Klinkenbuchse wird das Headset angesteckt.

Stromversorgung

Die Stromversorgung des TopSec Mobile erfolgt über einen Akku. Zum Laden des Akkus wird das USB-Kabel verwendet. Dieses Kabel ist Teil des Lieferumfangs. Der Akku kann auf zwei verschiedene Arten geladen werden: entweder durch Anschließen des TopSec Mobile an eine USB-Schnittstelle – zum Beispiel die eines Laptops – oder mit dem mitgelieferten Steckernetzteil.



Technische Daten

Technische Daten	
Bluetooth® Standard	Version 2.0
Betriebszeit	bis zu 100 h
Sprechzeit	bis zu 4 h
Datenrate	9,6 kbps
Übertragungsprotokoll	V.32, V.110
Abmessungen	99 mm × 34 mm × 22 mm
Gewicht	58 g

Bestellangaben

Bezeichnung	Typ	Bestellnummer
Sprachverschlüsselungsgerät	TopSec Mobile	5411.0002
Mitgeliefertes Zubehör: TopSec Mobile Phonebook Editor		

Service Ihres Vertrauens

- | Weltweit
- | Lokal und persönlich
- | Flexibel und maßgeschneidert
- | Kompromisslose Qualität
- | Langfristige Sicherheit

Rohde & Schwarz

Der Elektronikkonzern Rohde&Schwarz ist ein führender Lösungsanbieter in den Arbeitsgebieten Messtechnik, Rundfunk, Funküberwachung und -ortung sowie sichere Kommunikation. Vor mehr als 75 Jahren gegründet ist das selbstständige Unternehmen mit seinen Dienstleistungen und einem engmaschigen Servicenetz in über 70 Ländern der Welt präsent. Der Firmensitz ist in Deutschland (München).

Der Umwelt verpflichtet

- | Energie-effiziente Produkte
- | Kontinuierliche Weiterentwicklung nachhaltiger Umweltkonzepte
- | ISO 14001-zertifiziertes Umweltmanagementsystem

Certified Quality System
ISO 9001

Rohde & Schwarz SIT GmbH

Am Studio 3 | D-12489 Berlin
+49 30 65884-223 | Fax +49 30 65884-184
E-Mail: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

www.rohde-schwarz.com

Kontakt

- | Europa, Afrika, Mittlerer Osten
+49 89 4129 137 74
customersupport@rohde-schwarz.com
- | Nordamerika
1 888 TEST RSA (1 888 837 87 72)
customer.support@rsa.rohde-schwarz.com
- | Lateinamerika
+1 410 910 79 88
customersupport.la@rohde-schwarz.com
- | Asien/Pazifik
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com