

TopSec Mobile

Voice encryption for mobile phones

TopSec Mobile

At a glance

The TopSec Mobile connects to a communications terminal equipment by means of Bluetooth®. These terminals are predominately mobile phones. A TopSec Mobile allows encrypted communications with a suitable encryption device using almost any mobile phone with a Bluetooth® interface. This provides voice encryption services for the majority of the mobile phones from a variety of manufacturers.

The algorithms and methods used for encryption have been tried and tested with the TopSec product family.

The TopSec Mobile is the most secure voice encryption device for mobile communications on the market today. It features an elegant design, outstanding voice quality and is easy to use and operate.

The TopSec Mobile is

- ⇒ **plug-and-play** - compatible with most commercially available mobile phones
- ⇒ **interoperable** - with other TopSec products in analog and digital fixed networks, as well as in mobile radio networks
- ⇒ **secure** - through state-of-the-art encryption and security processes

TopSec Mobile

Benefits and key features

Versatile

- ⇒ Bluetooth® interface to connect to an end user communications terminal equipment
- ⇒ TopSec Mobile works with almost every modern mobile phone
- ⇒ Largely independent of mobile radio frequencies
- ⇒ Can also be used with modems with Bluetooth® interfaces

-page-2-

Manipulation-proof

- ⇒ Unrestricted use of the mobile phone's convenience features
- ⇒ TopSec Mobile security is independent of the mobile phone
- ⇒ Cannot be identified by the mobile network provider

-page-3-

Secure encryption algorithms

- ⇒ Hybrid approach for maximum security
 - Asymmetric method using 1024 bit encryption key length for key agreement
 - Symmetric encryption algorithm: 128 bit encryption key randomly selected from 10^{38} possible keys

-page-4-

User authentication

- ⇒ Pretended encrypted connections are impossible

- ⇒ Man-in-the-middle attacks are effectively prevented
- ⇒ Ability to create closed user groups

-page-5-

Interoperable

- ⇒ The following products are suitable as partner encryption devices:
 - the TopSec Mobile in combination with a mobile phone
 - the TopSec GSM crypto mobile phone
 - the TopSec 703+ - ISDN fixed network encryption device
 - the TopSec 711 - analog fixed network encryption device
- ⇒ Future-ready

-page-6-

Versatile

The TopSec Mobile voice encryption device utilizes a Bluetooth® interface to connect to communications terminal equipment.

The majority of the devices that are used with the TopSec Mobile are mobile phones with Bluetooth®.

Bluetooth® is a clearly defined standard that provides a stable communications interface between the TopSec Mobile and the mobile phone. The TopSec Mobile provides voice encryption versatility when connecting communications terminal equipment to the network.

TopSec Mobile works with almost every modern mobile phone

The TopSec Mobile is interoperable with diverse mobile phones from a variety of manufacturers. Prerequisite: The mobile phone must support the CSD (circuit switched data) nontransparent GSM data mode, and must have a Bluetooth® interface (version 1.2 or later) with a dial-up networking (DUN) profile for encrypted communications. Most modern mobile phones have this capability.

As a result, users have the freedom to select and use their preferred mobile phone and, at the same time, use their TopSec Mobile for secure communications when desired.

Largely independent of mobile radio frequencies

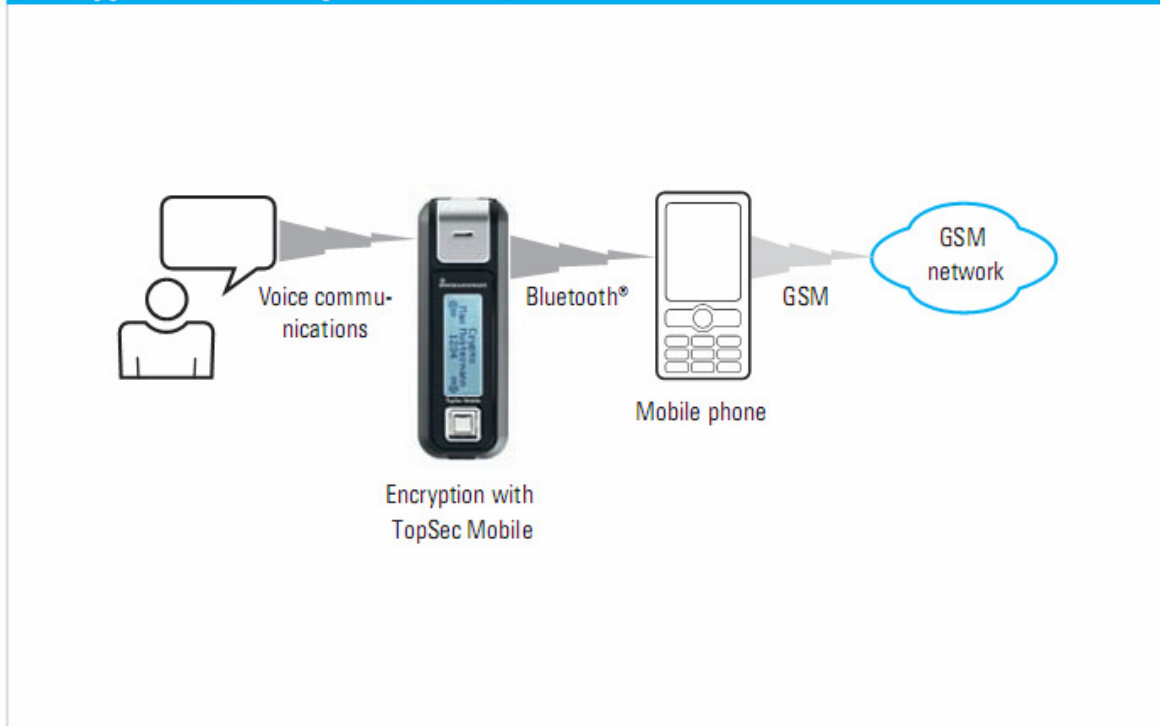
An additional advantage of using Bluetooth® connectivity is that the TopSec Mobile is largely independent of the mobile radio frequencies. With a Bluetooth® mobile phone and its associated mobile radio network, users can rely on having access to their desired frequencies and network providers.

The TopSec Mobile requires a non-transparent data connection at 9.6 kbps. Depending on the capability of the partner encryption device, either the V.110 or V.32 communications protocol is used. The necessary requirements are supported by most mobile phones with Bluetooth® and most mobile radio networks.

Can also be used with modems with Bluetooth® interfaces

Network access is not only possible through mobile phones with Bluetooth®, but also by using analog or ISDN modems with Bluetooth® interfaces. The TopSec Mobile can be operated within fixed telephone networks as well. The TopSec Mobile requires a non-transparent data connection at 9.6 kbps for encrypted connections.

Encryption with TopSec Mobile



Manipulation-proof

Unrestricted use of the mobile phone's convenience features

Mobile phones provide a wide selection of features. Applications can often be downloaded later from the public telephone network. Providers also send unsolicited information to the mobile phone. This information is then used to configure the phone according to the provider's preferences. All of these capabilities are necessary to make mobility as broad and flexible as possible to have the most current information on hand, or to ensure around the clock access to meeting and appointment schedules. Mobile phone acceptance depends heavily on such convenience features.

TopSec Mobile security is independent of the mobile phone

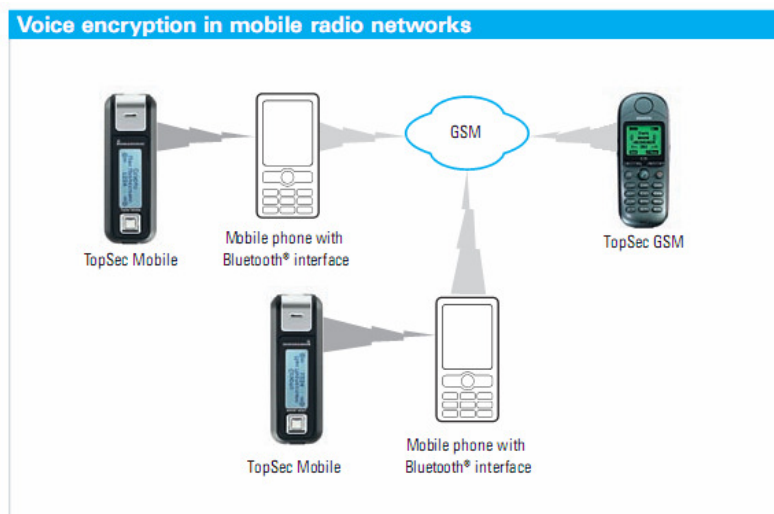
The elements of telephone convenience conceal the risk of unauthorized use by attackers to obtain confidential information. There are many ways to manipulate mobile phones.

However, the TopSec Mobile does not require information from a provider and additional applications cannot be downloaded or executed. The TopSec Mobile is a device that permits confidential voice communications using a mobile phone. The control features, the audio components such as microphone and speaker, and all encryption functions are integrated in the TopSec Mobile. The security of the TopSec Mobile is independent of the mobile phone. The TopSec Mobile offers best protection against manipulation.

Cannot be identified by the mobile network provider

Mobile phones can be identified by the international mobile equipment identity (IMEI). The IMEI is automatically transmitted whenever a mobile phone logs on to a network. The IMEI provides information about the manufacturer and equipment type. This allows network providers to deny full or partial service to specific mobile phones.

In contrast, the TopSec Mobile is not a mobile phone. It connects to, and operates with, a variety of mobile phones by means of a Bluetooth® interface. This makes it impossible for a mobile radio network provider to identify and thus deny service to the TopSec Mobile.



The TopSec Mobile is interoperable with most mobile phones with Bluetooth®; either a mobile phone in combination with a TopSec Mobile or a TopSec GSM phone can be used as partner equipment in the mobile radio network

Secure encryption algorithms

Hybrid approach for maximum security

The algorithms and methods used for encryption have been tried and tested with the TopSec product family. Encryption is based on a hybrid process for maximum security. This process combines a 1024 bit asymmetrical algorithm for key agreement and a symmetrical algorithm for encrypting confidential information.

Encryption concept

The encryption concept of the TopSec product family is designed for secure voice communications between two callers. The encryption devices can verify if both parties belong to the same closed user group. As a prerequisite for conducting an encrypted phone call, the partner encryption devices must have the same mathematical parameters and use identical algorithms. The TopSec encryption devices utilize the Diffie-Hellman key agreement protocol to generate individual session keys for each call (see figure). The Diffie-Hellman protocol is a public key method; both public and private parameters are used. Both parameters are preinstalled during the manufacturing process and delivered with the equipment.

The Diffie Hellman private parameters of the key agreement protocol (a, b, α, β, K) are used exclusively to generate session keys for each encrypted connection. Afterwards, the parameters are deleted. The Diffie-Hellman protocol permits encrypted communications between two encryption partner devices without the need for central administrative services. This is referred to as an open system since the possibility exists to establish a crypto connection between any two TopSec encryption devices. The session key calculated by the two partner encryption devices is used by the symmetric algorithms to encrypt or decrypt the digitized and compressed voice call.

128 bit encryption key randomly selected from 10^{38} possible keys

In encryption mode, the TopSec Mobile and the partner encryption device automatically agree on a new 128 bit key during each call setup. A key is randomly selected from a pool of 10^{38} possible keys and then deleted upon completion of the call.

User authentication

Pretended encrypted connections and man in the middle attacks are effectively prevented

TopSec Mobile users want to be absolutely certain that they have a secure, exclusive connection with their partner. All pretended encrypted connections, and man-in-the-middle attacks in which unauthorized third parties masquerade as the legitimate communications partner, must be avoided.

In theory, the Diffie-Hellman key agreement protocol is susceptible to a man-in-the-middle attack. The TopSec encryption concept includes measures to detect and stop man-in-the-middle attacks.

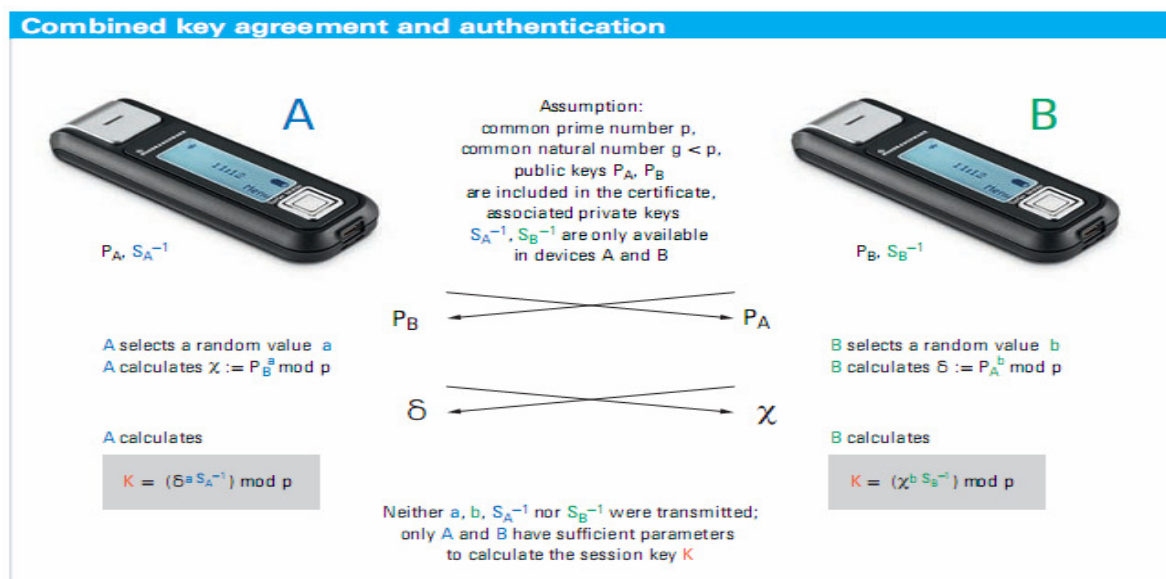
For this purpose, an individual four-digit security code is generated for each encrypted connection. The code is displayed on and is only available in the TopSec Mobile and the partner encryption device. A secure call can be conducted only when the security codes are identical.

Creating closed user groups

Another measure to stop man-in-the-middle attacks is to create closed user groups. This requires an entity referred to in most systems as a trust centre. In the TopSec system, the trust centre is called the TopSec Administrator. The TopSec Administrator combines the functions of a trust centre with the centralized administration of operational parameters. The trust centre function is required when creating closed user groups.

TopSec devices that belong to a closed system receive the certificate and the public key for verifying certificates during an initialization process. The initialization process also generates an additional public key pair that is used for authentication. The private authentication key remains in the TopSec device. The public authentication key is included in the certificate. Initialization occurs by means of a cable connected directly to the TopSec Administrator in a secure environment.

In closed systems, authentication between the TopSec encryption devices takes place automatically. The first step in authentication is the verification of the certificate of the partner encryption device. This is followed by a combined key agreement and authentication (see figure). An encrypted connection is only established upon successful authentication. This means confidential voice calls that comply with the highest levels of security can be carried out using TopSec encryption devices.



Interoperable

Interoperability

The TopSec Mobile uses algorithms and methods for encryption that have been tried and tested with the TopSec product family; the products of the TopSec family are interoperable. This ensures that new network and security protocols can be easily integrated into the TopSec Mobile. The communications partner can be reached over a mobile radio network, an analog or a digital fixed network. Secure voice encryption is possible in all the above scenarios.

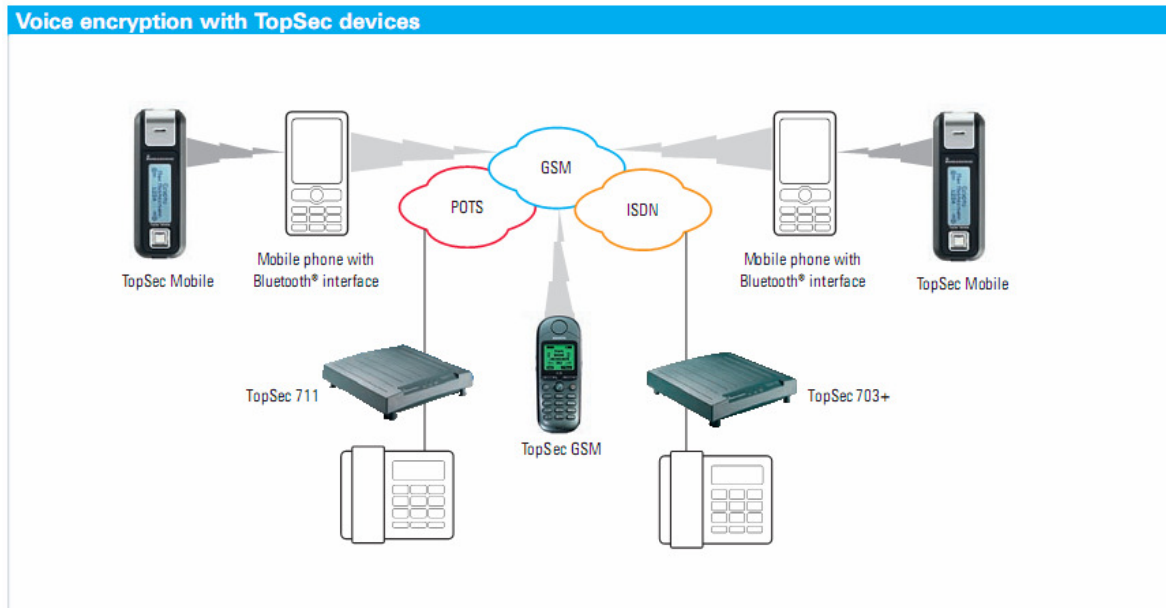
The TopSec Mobile compresses the voice call so that it can be transmitted at a data rate of 9.6 kbps. Both the V.110 and V.32 protocols can be used to place a secure call with a communications partner on a mobile phone. This ensures interoperability with a second TopSec Mobile or with a TopSec GSM crypto mobile phone.

If the communications partner is using a TopSec 703+ for encrypted voice calls over an ISDN connection, the V.110 protocol is selected. If the communications partner is using a TopSec 711 for encrypted voice calls over an analog connection, the V.32 protocol is used.

After the appropriate network protocol has been selected, i.e. V.110 or V.32, the TopSec Mobile voice encryption device is now interoperable with the TopSec GSM, TopSec 703+ and TopSec 711.

Future-ready

The TopSec Mobile is based on high-performance hardware with large storage capacity. The TopSec Mobile firmware can be securely updated with the TopSec Administrator. This ensures that new network and security protocols can be easily integrated into the TopSec Mobile.



TopSec Mobile

Design and functional elements

Design

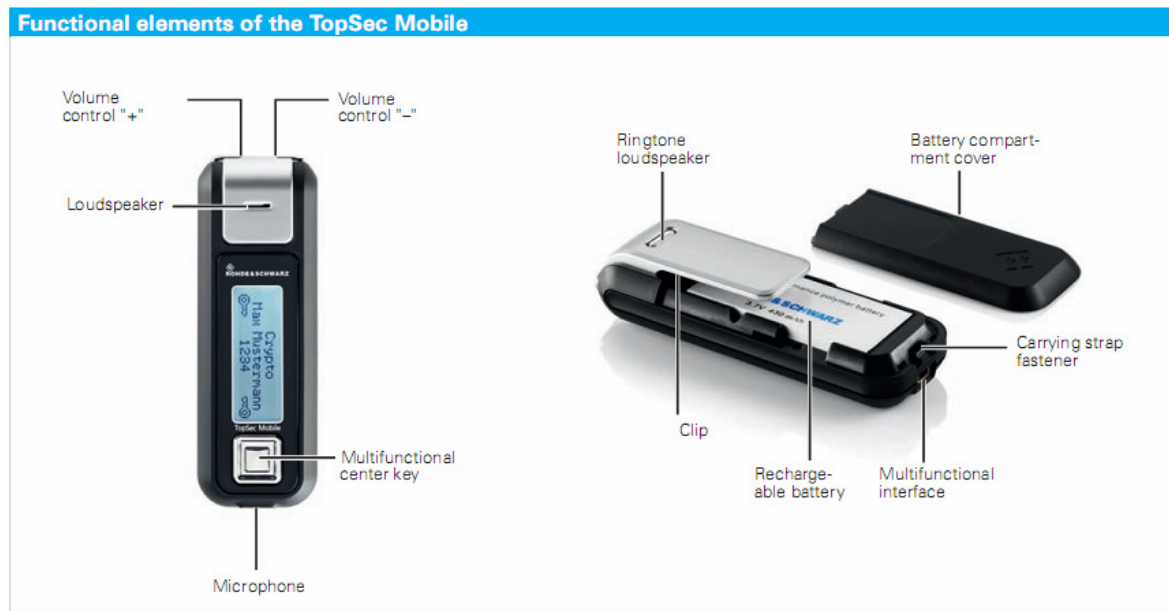
The TopSec Mobile is targeted at senior management levels in government and at business leaders in important industries and sensitive departments such as security, sales, finance, engineering and science. The elegant and timeless design of the TopSec Mobile is representative for this user group without attracting undue attention. The TopSec Mobile can be carried in a shirt, suit or coat pocket; a wide clip provides secure fastening. It can also be attached to a carrying strap.

Functional elements

The TopSec Mobile is a voice encryption device with integrated audio components. The figure depicts the various functional elements of the TopSec Mobile.

The TopSec Mobile has an integrated microphone for talking. Two loudspeakers are provided for signalling and listening to conversations. The loudspeaker integrated into the clip on the reverse side of the TopSec Mobile is used to signal incoming calls. The loudspeaker integrated into the front side of the clip is used during the phone call and delivers outstanding voice quality.

The TopSec Mobile functions are controlled using a multifunctional element that consists of a center key and a ring that can be activated in four directions. Information is shown on a three-line display. The display can be rotated by 180 degrees to accommodate both right and left-hand end users. The TopSec Mobile has two keys to control the loudspeaker volume. A multifunctional interface for the headset, the phonebook synchronization and the power supply is integrated on the bottom of the device.



TopSec Mobile Operation

Start-up

The TopSec Mobile must be "paired" with a mobile phone before it can be used. Pairing is started by activating the Bluetooth® search mode on the TopSec Mobile. As soon as the desired mobile phone is selected, the PIN a random eight-digit number – is displayed on the TopSec Mobile. This PIN must be entered in the mobile phone. A Bluetooth® connection between the mobile phone and the TopSec Mobile is then established. The TopSec Mobile is now ready for encrypted voice communications.

Establishing an encrypted connection

When an encrypted call is placed, the telephone number of the party to be called is selected from the integrated telephone directory. The TopSec Mobile sends the telephone number to the mobile phone over the Bluetooth® connection. The mobile phone then establishes a data connection to the communications partner device. Either the V.110 or V.32 protocol is used. Encryption synchronization is started as soon as the data connection is operational between the TopSec Mobile and the partner encryption device. During the key agreement phase, two key icons will move from the side of the display toward each other and return. The partner encryption device or a connected telephone will ring as soon as the encrypted connection is established. A four-digit security code to verify the secure connection is displayed as soon as the encrypted call is accepted. The call participants can now carry out a confidential phone call.

Accepting an encrypted call

During incoming calls, the TopSec Mobile generates a short beep tone, followed by the start of the encryption synchronization. Two key icons will move from the side of the display toward each other and return. After successfully completing synchronization, the TopSec Mobile rings. The user accepts the encrypted call by pressing the center key. A four-digit security code is displayed and used to authenticate the call participants, after which the confidential phone call can begin.

Software for editing the TopSec Mobile telephone directory

The TopSec Mobile telephone directory can be edited at any time by using the control elements. The telephone directory software for the PC, which is delivered with the TopSec Mobile, makes it easier to edit the telephone directory. The telephone directory is transferred from the TopSec Mobile to the PC over a USB cable (included in equipment supplied), where it can be edited and transferred back to the TopSec Mobile.

Using the TopSec Mobile with a headset

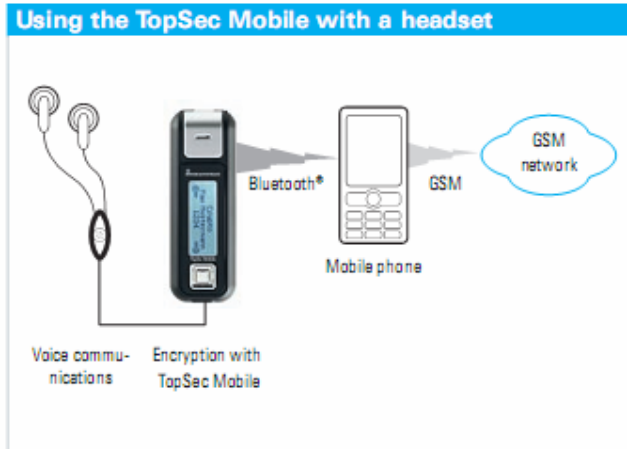
The TopSec Mobile is typically used like a mobile phone. The user speaks into the integrated microphone and listens to the integrated loudspeaker. Alternatively, a headset can also be used.

The TopSec Mobile multifunctional interface is used to connect the headset. A headset adapter is plugged into the TopSec Mobile interface. The headset adapter has a microphone, a 2.5 mm jack and a control element to accept incoming calls. The headset plugs into the 2.5 mm jack.

Power supply

A rechargeable battery supplies power to the TopSec Mobile. The battery is recharged using the USB cable supplied with the TopSec Mobile.

There are two ways to recharge the battery: connecting the TopSec Mobile to a USB port, such as on a laptop, or using the power supply unit that is supplied with the device.



Specifications

Specifications	
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 x 34 mm x 22 mm (3.9 in x 1.3 in x 0.9 in)
Weight	55 g (0.12 lb)

