

SECFONE & SECBOX

Tap-proof Communication worldwide– Secure Protection against Organisational Data Leakage and Productpiracy

The Navayo Solution

Worldwide, voice and data communication is systematically scanned and screened for the purpose of industrial espionage using highly sophisticated technical equipment. Not only national security agencies and intelligence services extract information that seem relevant to their national industry. Companies receive such information without any need to attack competitors directly. Commercially available software based encryption technology (e.g. VPN, https) is by no means sufficient to stop such practice.

Therefore the independent and privately owned European company Navayo developed an innovative 3-level hardware-based High-security Internet Encryption for the exchange of sensible information – data and voice (VoIP).

SECFONE allows professionals and executives to exchange sensitive strategic information, solve problems, or discuss highly confidential strategies of technical or commercial nature with utmost secrecy. Navayo offers Android based Smartphones HTC Desire, Samsung Galaxy S and Tab.

SECBOX supplement existing security measures of the company with a vital facility not previously available: tap-proof secure voice and data communication between two or more participants from their laptops or VoIP phones – independent of the actual location. They make up a Private Cloud for organisations of all kind.

The Unprecedented 3-level Encryption

Navayo ist he inventor of the 3-level Highly Secure Crypto Concept. The functional concept was internationally patented by Navayo (Europe, Japan, USA) and is named Manageable Virtual Closed Network (MVCN®). MVCN works principally as follows:

1. Prior to their usage the crypto keys of all deployed security devices are signed with an identification code in a *system-initialisation* process and the public keys are stored on the autorisation server. The autorisation server (redundant server cluster) communicates with the mobile security devices via **RSA 2048 Bit** encryption.
Enables the recognition of manipulations of all kind.
2. All mobile security devices use a particular smart card hardware developed by a recognised German vendor which deploys an especially designed crypto-microprocessor that is certified according to highest international IT security standards. Each single smart card generates its own **RSA 1024 Bit** key pair and stores the private key on its crypto-microprocessor; it never leaves this storage. The public key is copied to the central autorisation server and registered during the *system-initialisation* of the smart card so that other devices may find and communicate with it.
Certified hardware based security prohibits remote access to private keys.
3. Prerequisite to TCP/IP based data exchange the roaming Internet addresses and access conditions (proxy, NAT, etc.) of the mobile security devices are constantly updated and managed by the zentral autorisation server. A calling device firstly receives the actual IP address of the called device and its public key after successful autorisation. As soon as both devices have successfully established a connection both smart cards generate a temporary symmetrical key using **Blowfish 448 Bit** Algorithm, which is very well suited for realtime data and voice (VoIP) encryption. Every 5 minutes both devices generate a new key and exchange the both keys via their public RSA 1024 Bit keys adding just another safety lock.
Patented 3-level encryption delivers utmost secrecy.

The Devices



Its high time - get in contact with us, now!

SECFONE & SECBOX

Tap-proof Communication worldwide– Secure Protection against Organisational Data Leakage and Productpiracy

Secfone and Secbox Technical Specifications Overview						
	Secbox Industrial	Secbox 5	Rabbit	Secbox 15	Secbox H	Secfone
Environment						
Embedded operating system	Security Enhanced Linux (Smart Card)					Security Enhanced Linux (Smart Card)
Operating platforms (PC,SP)	Platform-independent (Mac, Linux, Windows)					Security Enhanced Android (Government/Red) Android (Business/Orange; allows other Apps)
Hardware	Industrial grade compact hardware					HTC Desire, Samsung Galaxy S and Tab
Processor Speed	500 MHz	500 MHz	700MHz		Quadcore 2.1GHz	max. 1 GHz
Management						
Firmware upgradeable	yes					yes
Full remote management	yes					no
Biometric authentication	no	yes			no	Personal Pin
Management Tool	Internet Browser based					Secfone App
Networking						
Max. encrypted bandwidth	5 Mb/s	5 Mb/s	8 Mb/s	15 Mb/s	600 Mb/s	-
Used bandwidth	-	-	-	-	-	from 24Kb/s Speex10 to 8Kb/s Speex4
DHCP server/client	yes	yes	yes	yes	yes	yes
Supported protocols	HTTP, HTTPS, FTP, SFTP, SSH, Telnet, SNMP, FISH, SMB, NTP, RSYNC, SIP, POP3, IMAP, SMTP, IAX2, etc.					SMS, MMS, Email, Filetransfer
Connectivity						
Ethernet WAN/LAN	10/100Base-T	10/100Base-T	PCMCIA	100Base-T	1000Base-T	HSDPA/UMTS(3G), WiFi, EDGE
USB host/device	0/1	1/1	PCMCIA/USB	1/1	no	no
Serial Ports	2 (RS232 or RS422 or RS485)	no	no	no	no	no
HSDPA/UMTS modem support	yes	yes	provided by OS	yes	no	provided by OS
Wifi USB dongle support	no	no	provided by OS	no	no	no
Security						
Trusted Platform Module	yes					Smart Card - Hardware: CC EAL5+, BSI AIS 31, BSI DSZ CC0227; Software: CC EAL4+
Storage						
Built-in storage	no	no	no	no	no	no
USB attached storage	ftp accessible	ftp accessible	no	ftp accessible	no	no
Diagnostics						
LEDs	MVCN, Power	MVCN, CPU	no	no	no	no
LCD Display Monitoring	no	yes	no	yes	no	Secfone App
LCD (Pixel)	no	128 x 32	no	128 x 64	1024 x 768 VGA	480 x 800
Rack-Mount						
Rack Type	no				standard 19", 1U	no
Power						
Input	9-36V DC	USB or 5V DC	Express Card (5V)	USB	100-230V	USB
Power consumption	2.1 W	2.1 W	2.2 W	2.5 W	400 W	-
Uptime	-					UP to 6h 30 min TalkTime (3G)
Operating Conditions						
Ambient Temperature	25°C... +75°C	10°C... 40°C			(see vendor specifications)	
Humidity	10-90%, non-condensing					(see vendor specifications)
Dimension and Design						
Dimensions	107 x 60 x 99 mm	145 x 95 x 30 mm	110 x 34 x 10 mm	80 x 80 x 30 mm	1U rack-mountable chassis 42,7 x 426.2 x 914.4 mm (1.68" x 16.78" x 26")	119 x 60 x 11.9 mm (HTC Desire)
Weight	220 g	126 g	25 g	142 g	3.175 kg (7 lbs)	135g (HTC Desire)
Case	TS dinrail mountable metal	durable plastic	ExpressCard 34	durable plastic	metal cage	durable plastic
Warranty	2 years					2 years
Compliance						
CE	yes					yes
Made in EU	yes					yes
RoHS	yes					yes

Remark: Navayo's latest high-security product is a next generation Smart Meter which enables sabotage proof control of decentralised electrical power supply structures.

If you require utmost secrecy and IP based protection then we at Navayo are pleased to support you with our proven and established technologies. In individual projects we cater to your special requirements.



Its high time - get in contact with us, now!