

Sectra Panthon®



SECTRA

Paving the way for secure communication

Sectra creates approved effective security solutions that allow secure communication even when you and your business demand the highest degree of flexibility and mobility.

Our clients include European government authorities, defense departments and other critical functions of society. Taking care of a country's most sensitive information requires trust and expertise. Choosing Sectra's secure communication solutions guarantees high quality. Our close cooperation with leading European security agencies serves as a guarantee that our solutions are the most secure on the market.

Sectra has developed and marketed security solutions since the company's inception in 1978. As an international supplier we have built up a solid core of expertise in the area of encryption technology. Currently we qualify as one of the world's foremost specialists in the design and development of secure

communication systems. We know what is required to meet the tough demands of today and tomorrow.

Security solutions approved at national levels as well as within the EU and NATO

Top Secret, Secret, Confidential and Restricted. These four security levels define the treatment of sensitive information and any potential damage should an unauthorized party gain access. Sectra's solutions are approved at the Secret or Restricted security levels and trusted by government authorities, defense departments and other critical functions of society in 17 European countries, in the EU and NATO.



Don't let anyone outsmart your smartphone

User friendly security is our top priority. Sectra Panthon is a security solution designed for flexible and mobile users. You need not hesitate to pick up the phone or send the necessary data, but can feel safe in the knowledge that you only reach those with whom you intend to communicate.

The advent of advanced smartphones enables people to work in a highly flexible and mobile way. Unfortunately, these developments have also resulted in new attack methods and created major security challenges for organizations. A smartphone is an important source of information. It contains contact information, e-mail addresses, text messages, picture messages and photos. It also stores details about your phone calls, your location, the items you search for on the Internet and your passwords for various social networks, such as Facebook and Twitter.

These are some of the most common threats

Without an encryption solution your communications may be subject to an array of attacks. These are undetectable and most likely you will never know until the damage is done. But it doesn't end there. Everyone in your contact network may also be mapped. Or even worse, a

compromised smartphone could be used as a tool for Trojan based eavesdropping or transfer of sensitive information from your company's internal network.

Local eavesdropping

Your smartphone connects to a local base station with the best signal strength. Easily accessible and inexpensive equipment and technology makes it simple for hackers to set up counterfeit base stations. Your phone calls can be intercepted and recorded and your text messages manipulated.

Network eavesdropping

The encryption used by operators is in many cases outdated and the Internet provides ample information on how to crack standard algorithms. Any calls made from your smartphone may also be transmitted unencrypted through your operator's network. This allows anyone, with or without authorized access to eavesdrop on your conversations and read your text messages.

Lost or stolen smartphone

Leaving your smartphone unattended for just a couple of minutes is enough time for someone to install malicious applications, malware or even an eavesdropping microphone. If your smartphone is lost or stolen all the contact information and

privileged business data you have stored is suddenly in the hands of others.

Trojans and other malware

Most computers and networks are equipped with firewalls and antivirus software. But your smartphone is also susceptible to phishing or other malicious code. A Trojan is a program that appears to contain normal and desired functions. In fact, this type of malware contains hidden programming that records sensitive information and then forwards the data to an attacker.

Spoofing

Smartphones are increasingly becoming targets for identity thieves. A hacker can easily forge your identity and gain access to sensitive information. Never trust that the person on the other end of the line is who they claim to be. A text message you have received may in fact come from someone else posing as a contact in your address book.

“A couple of minutes is enough time for someone to install malicious applications, malware or even an eavesdropping microphone”

End-to-end encryption puts an end to eavesdropping

Sectra Panthon is a hardware based security solution, in the form of a smartcard, which is installed in the smartphone. Using end-to-end encryption efficiently protects you and your crucial business information.

User friendly security for smartphones
Sectra Panthon's security solution comes in the form of a smartcard that is installed in each smartphone. This is greatly appreciated by anyone requiring security approved devices that also want all the

advantages and convenience of a modern smartphone. The user basically performs an encrypted call the same way as a regular phone call. Users can seamlessly surf the Internet, check share prices or weather maps, update Twitter and Facebook pages and take high-quality photos.

End-to-end encryption

Sectra Panthon is based on end-to-end encryption that protects you from identity theft, malware and

eavesdropping. It renders all text traffic unreadable and anyone attempting to tap into your smartphone calls hears nothing but random noise.

Phone Integrity™ strengthens the platform

All Sectra Panthon smartphones are equipped with our own Phone Integrity™ solution. This strengthens your smartphone platform and reduces the attack surface for malicious applications. Should your smartphone be lost or stolen,



authentication routines prevent it from being used by unauthorized parties.

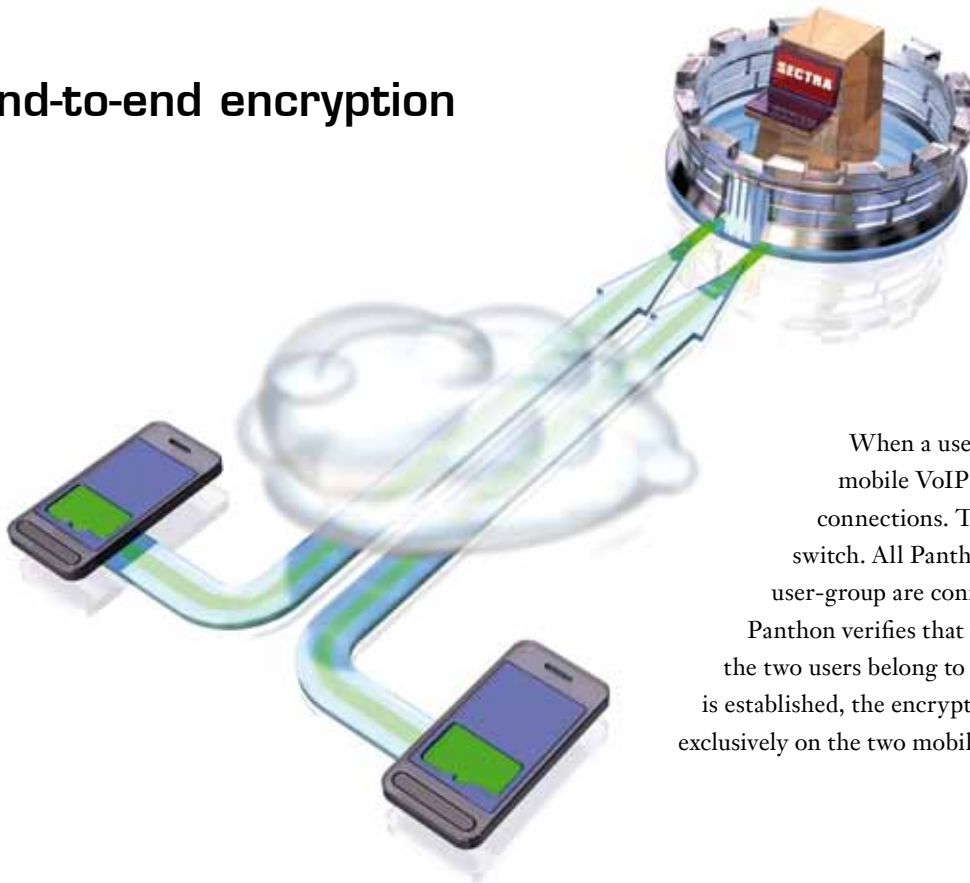
Future proof secure communication

Sectra Panthon are now being introduced on a wider selection of Android smartphones and tablets. Compatibility with Sectra Tiger and the NATO Secure Communications Interoperability Protocol (SCIP) is also on the roadmap. This standard enables secure communication with other vendor's telephony products essentially everywhere.

“Sectra Panthon's security solution comes in the form of a smartcard.”



End-to-end encryption

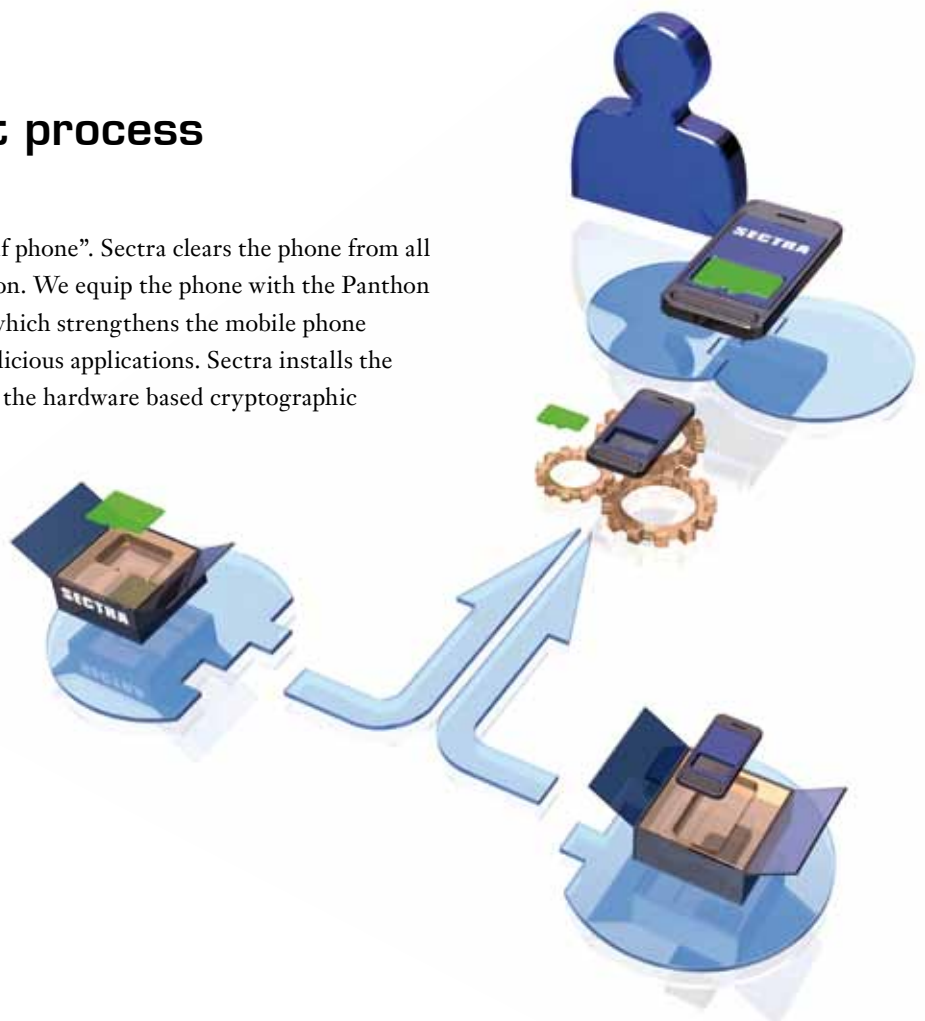


When a user makes a secure call, the Panthon mobile VoIP technology uses Internet IP packet connections. The call is routed via the Sectra VoIP switch. All Panthon users and mobile phone units in a user-group are connected to and registered at the server. Panthon verifies that the user certificates are valid and that the two users belong to the same group. When the secure call is established, the encryption is end-to-end and performed exclusively on the two mobile phones.

A secure deployment process

The smartphone is an unmodified “off the shelf phone”. Sectra clears the phone from all content in order to make a new clean installation. We equip the phone with the Panthon application and a Phone Integrity™ solution, which strengthens the mobile phone platform and reduces the attack surface for malicious applications. Sectra installs the Panthon microSD-card software that provides the hardware based cryptographic functions.

The phone and the microSD-card are then combined in a personalisation process. Keys and certificates for the specific user are generated and permanently loaded on the card. Now, the Sectra Panthon security solution is ready to be delivered to the customer.



Sectra Panthon® facts

Security level & functions

Voice crypto at security level Restricted approved by:

- NLNCSA (Dutch National Agency for Communication Security)
- EU
- NATO

SMS at security level Restricted available during 2011

User interface

Designed by usability experts to provide an easy to use application

Graphical user interface with address book and call logs

Crystal clear sound provided by advanced audio processing with noise filtering and acoustic echo cancellation

Multi-language user interface

Quick guide and built-in user instructions

Real-time, full-duplex operation

Optimized for mobile VoIP and international calling with VoIP tunneling technology

Security & encryption

End-to-end encryption with 256bit AES

Hardware accelerated crypto supported by Infineon™ SLE88 family smart card crypto controller at common Criteria EAL5+ security level

Pending support for SCIP (Secure Communications Interoperability Protocol)

Hardware accelerated Elliptic Curve Cryptography (ECC) and AES co-processor

True random number generation

PIN code for user access

Certificate-based user authentication

Certificate revocation (CRL) support, updated over the air

Hardware based secure storage of keys and certificates

Optimized for fast key exchange, short call set-up time and low latency

Session key generation with ECMQV protocol

ECDSA signature scheme

Connectivity

Works on 2G, 2.5G and 3G

Automatically enabled optimized 2G-mode for low bandwidth conditions

WiFi (Custom configurations of customer network might be needed)

Platform

Supported operating systems: Microsoft Windows Mobile 6.5™ and Android 2.3 or higher

Supported devices: HTC HD2™ and selected Android phones from major manufacturers

SECTRA

Sectra Communications AB

Teknikringen 20
SE-583 30 Linköping
Sweden
Phone: +46 13 23 52 00
Fax: +46 13 21 21 85
info.security@sectra.com
www.sectra.com/security

Sectra Communications BV

Prinsessegracht 3
2514 AN Den Haag
Netherlands
Phone: 070 302 30 00
Fax: 070 302 30 09
info.security@sectra.nl
www.sectra.nl/beveiliging

Sectra Communications AB

Motnica 7
1236 Trzin
Slovenia
Phone +386 59 936 387