Panthon®

SECTRA

Sectra Communications – ensuring security with flexibility

Sectra has more than 30 years of experience in developing secure communications. We know what is required to meet the toughest demands. Sectra's effective solutions ensure secure communications, also when operations require maximum flexibility and mobility.

Our customers include European defense ministries, government authorities, and other critical functions of society. Safeguarding sensitive information requires trust and expertise.

Our close cooperation with leading European security agencies is clear evidence that Sectra's solutions are considered the most secure on the market. Our expertise in encryption technology is well known and Sectra is one of the world's foremost specialists in the design and development of secure communication systems.

We offer solutions approved at national levels and within the EU and NATO. Four security levels – Top Secret, Secret, Confidential and Restricted – define the handling of sensitive information and any potential damage that might occur should an unauthorized party gain access.

Sectra Communications currently employs nearly 60 professional specialists in Sweden and in the Netherlands. The company's head office is located in Linköping, Sweden and the technology has sprung from leading researchers at Linköping University.

Don’t let anyone outsmart your smartphone

The advent of advanced smartphones enables us to work flexibly in a mobile environment. Unfortunately, we now face new threats that pose major security challenges for organizations.

Without encryption, communications may be subject to an array of attacks. The encryption used by operators is in many cases outdated or not even enabled, and the Internet provides ample information on how to crack standard algorithms.

Smartphones connect to the local base station with the best signal strength, a transmission can be directed to fraudulent base stations. Easily accessible and inexpensive equipment – and free software – allow hackers to set up these false base stations. Through similar deception, phone calls can be intercepted and recorded, and text messages read and even manipulated.

Leaving a smartphone unattended for just a couple of minutes leaves sufficient time for someone to install malicious applications or access stored information. A lost or stolen smartphone means that contact information and privileged business data is suddenly in the hands of others.

Most computers and networks are equipped with firewalls and antivirus software. But a smartphone is also susceptible to phishing or other malicious codes with hidden programming that records sensitive information and forwards data.
A compromised smartphone could be used as a tool for Trojan-based eavesdropping or the transfer of sensitive information from an internal network.

Smartphones are increasingly becoming targets for identity thieves. A hacker can easily gain access to a target identity and thereby gain access to sensitive information. Even worse, the contact network might be mapped.

Infringements are virtually undetectable and the victim is usually unaware of the attack until the damage is done.

Being aware of the risks associated with unencrypted communication is a first step. To install appropriate security solutions for the handling of sensitive or classified information is the next. With a security solution from Sectra, users can feel safe knowing that they only reach those with whom they intend to communicate.

Sectra Panthon
– user friendly security for smartphones

User-friendly security is Sectra's top priority. With Sectra Panthon, users can safely answer calls or exchange text messages, with assurances that only intended parties are privy to the information.

Sectra Panthon is a hardware-based security solution, in the form of a MicroSD card, which is installed in a smartphone. The MicroSD card is loaded with keys for a specific user and user group, then permanently locked and inserted into the smartphone. Once activated, calls can be set up to other Sectra Panthon users through a secure and centrally managed phonebook using VoIP (voice over IP) technology.

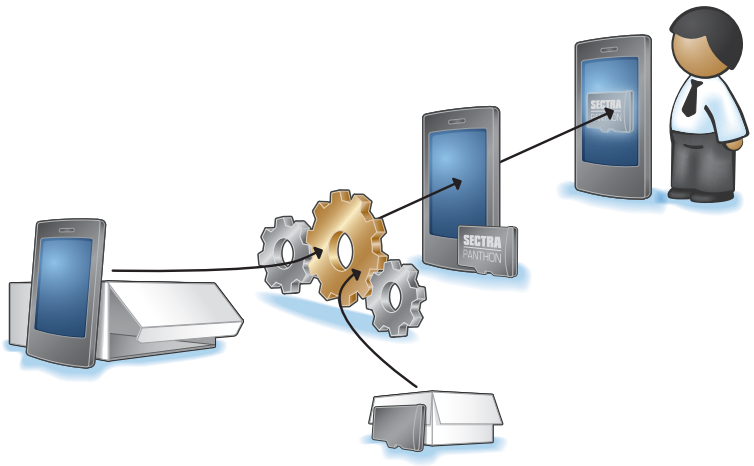
The Phone Integrity solution included in Sectra Panthon not only reduces the attack surface for malicious applications, the authorization procedures will also prevent usage if the phone is stolen or misplaced.

Panthon allows users to make secure calls and send text messages up to the Restricted security level. It works seamlessly on modern smartphones and users can enjoy all of the services they depend on – regular phone calls, contact information, e-mail, photos, web browsing and social networks.

The end-to-end encryption ensures protection from identity theft and eavesdropping. All attempts to tap into a transmission between two Panthon phones are futile since the culprit will only encounter random noise.

Sectra Panthon is available for a wide selection of Android phones and tablets. It is also presently being developed for compatibility with Sectra Tiger and the NATO Secure Communications Interoperability Protocol, SCIP. This standard enables safe communications with users of other vendors' security solutions.

Secure deployment process

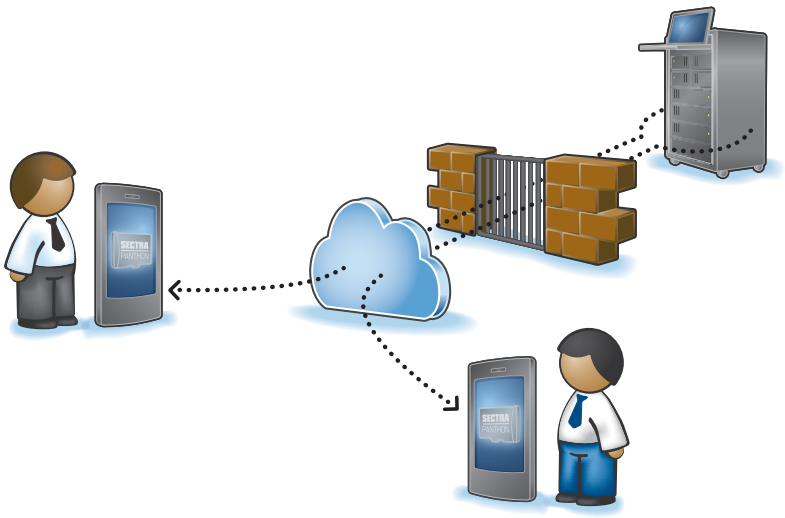


The smartphone is originally unmodified and “off the shelf”. Sectra erases the phone content in order to guarantee a new uncontaminated installation. The phone is equipped with the Phone Integrity solution, which strengthens the mobile phone platform and reduces vulnerability to malicious applications.

Finally, the application is installed on the phone and the MicroSD card is inserted to provide the hardware-based cryptographic functions.

The personal certificate for a specific user is created and loaded in a personalization process. All keys and certificates are permanently loaded on the card. The Sectra Panthon security solution is then ready for customer delivery.

End-to-end encryption



Panthon uses mobile voice over IP (VoIP) technology. The calls are routed via the secure communications gateway. All Panthon users and mobile phone units in a user group are connected to, and registered at, this server.

Panthon verifies that the user certificates are valid and that the two users belong to the same domain. When the secure call is established, the encryption is end-to-end and performed exclusively on the two mobile phones.

Technical specification

Security level/classification	Pending approval for security level Restricted by: - NLNCSA (Dutch National Agency for Communication Security) - EU - NATO
Security and encryption	End-to-end encryption of voice and SMS with 256bit AES Hardware based secure storage of keys and certificates True random number generation Hardware accelerated crypto on smart card Hardware accelerated Elliptic Curve Cryptography (ECC) and AES co-processor PIN code for user access Certificate-based user authentication Certificate revocation list (CRL) support, updated over the air. Secure voice uses with ECMQV protocol and ECDSA signature scheme. Text messages encrypted using pre-shared keys. Encrypted storage of settings, call history, text messages.
Functions	Secure end-to-end voice (VoIP) with real-time, full-duplex operation. Very fast secure voice call setup and low audio latency Secure end-to-end text messages (SMS) Centrally managed secure phone book Software updates over-the-air Phone integrity function which monitors the system for anomalies Whitelisting of Android applications Pending support for SCIP (Secure Communications Interoperability Protocol) Can be used as a normal smartphone for regular phone calls. Automatic start of the Panthon application Group setting to allow different phonebooks for different users
Interface	Touch screen graphical user interface designed by usability experts Multi-language user interface Secure phone book with name, number, photo and comments Clear sound provided by advanced audio processing with noise filtering and acoustic echo cancellation. Selection of special ring tones for secure voice and SMS Text message UI as a conversation view (chat) Printed users guide and built-in user instructions
Connectivity	Works on 2G, 2.5G and 3G mobile networks and WiFi Optimized for mobile VoIP and international calling with VoIP tunneling technology Automatically enabled optimized 2G-mode for low bandwidth conditions
Platform and devices	Selected Android phones from major manufacturers, such as Samsung Galaxy S2, Sony Arc S, Sony Xperia Active.
Accessories	2 x Additional 1000mA fast charger included (car and wall plug)

Keep communicating. For a more secure world.

Sectra Communications

Teknikringen 20
583 30 Linköping
Sweden
+46 (0)13 23 52 00
Fax: +46 (0)13 21 21 85
communications@sectra.com

Strandbergsgatan 61
112 51 Stockholm
Sweden
+46 (0)13 23 52 00
Fax: +46 (0)13 21 21 85
communications@sectra.com

Prinsessegracht 3
2514 AN The Hague
The Netherlands
Phone: +31 (0)70 302 30 00
Fax: +31 (0)70 302 30 09
communications@sectra.nl

communications.sectra.com