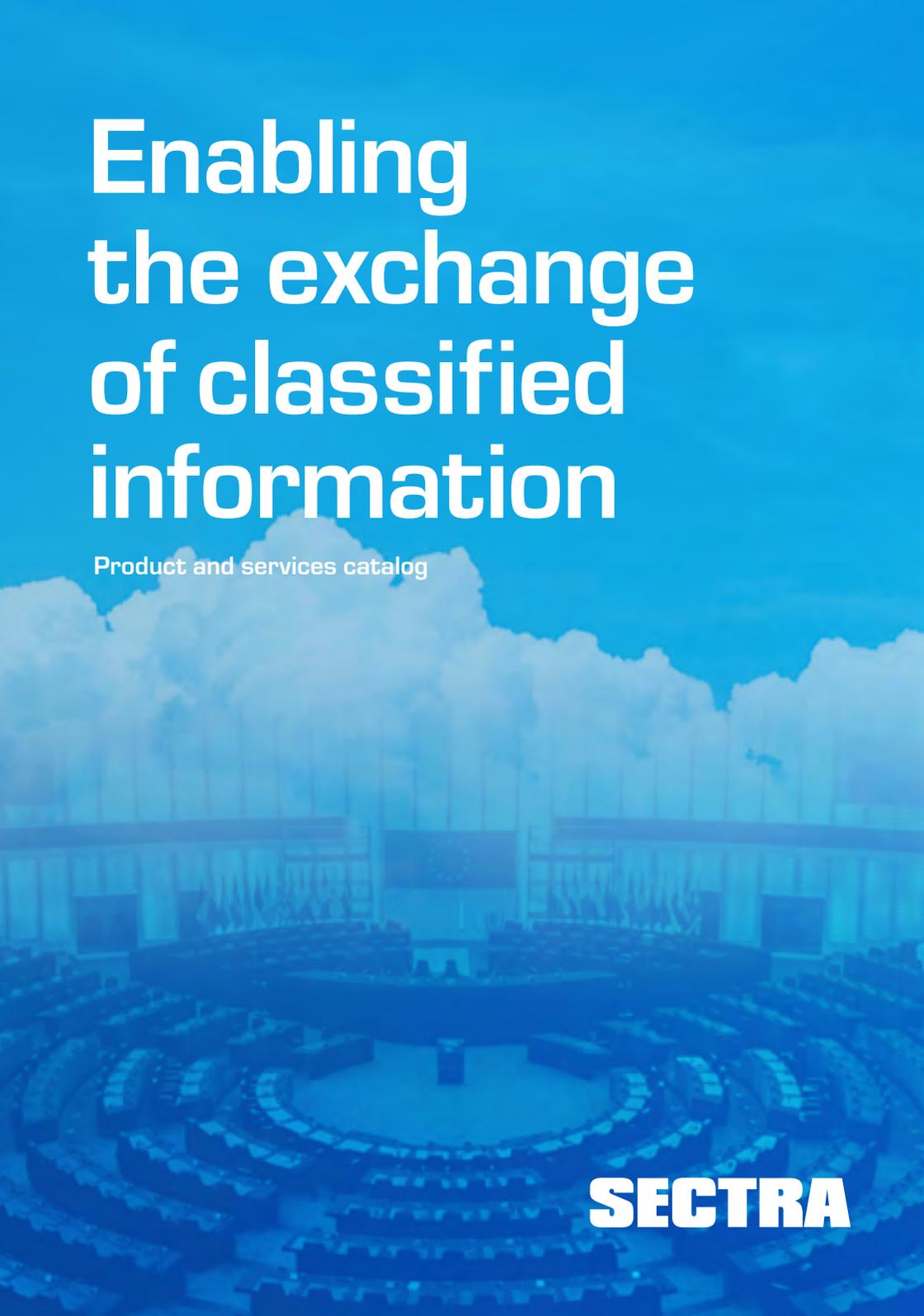


Enabling the exchange of classified information

Product and services catalog



SECTRA



For a stable and secure society

Setra is an expert and a leading provider in the field of cybersecurity, specialized in developing high assurance communication systems. Our offering includes systems for secure voice and data communications certified by the EU and NATO and at several national levels. We also provide security analysis and monitoring of critical IT/OT systems to protect critical infrastructure such as electricity and water supply—always contributing to a stable and secure society.

The world is changing

IT development and increased cybercrime as well as the unstable security situation in Europe are driving the need to reduce vulnerability in society's critical functions. People are no longer bound to their offices, and since remote working is here to stay, organizations need to improve their availability and flexibility. Even in society's most important functions, where secure information transfer is required, there is a need for mobility.

Governments, defense forces, the public sector and multilateral organizations such as the EU and NATO handle classified information on a daily basis—and it is vital for them to be able to communicate securely. Sectra contributes to a more secure and stable society by helping these organizations maintain their availability, securing their communication against eavesdropping and protecting their systems against unauthorized access.

“The people at Sectra are knowledgeable and experienced, and they seem to enjoy their work. That makes it easy to build a relationship of confidence. They are also interested in our feedback and input, which gives us the confidence that the products will evolve in a direction that is important for us. This is a key characteristic of a good relationship.”

– Senior representative from an EU organization, October 2022

A person with long dark hair is sitting at a desk, holding a black Sectra Tiger/S mobile phone. The phone's screen displays the time 10:16. The person is also holding a small black USB device. In the background, there is a laptop displaying a blue interface, a potted plant, and some office supplies. The scene is set in a modern office environment.

Sectra Tiger/S can be used for both secure phone calls and file transfers.

SECTRA TIGER/S

The most secure mobile phone in the world

Sectra Tiger/S is a secure mobile phone that is approved up to the classification level EU and NATO SECRET and has several national approvals. The hardware and software are developed by Sectra, and the solution supports encrypted speech, messaging and data transfer. Sectra Tiger/S utilizes IP networks, such as satellite, fixed and mobile networks, for all types of communication.

- Quantum computer resilient
- TEMPEST-verified design and active tamper response
- Over-the-air re-keying and phone book updates
- Based on NATO SCIP technology
- Anonymization with Sectra Network Protector

The system is delivered with high availability infrastructure, including a Key Generation Center (generates all the keys needed in the system), Security Management Center (over-the-air key distribution/deletion and phone book updates) and Communications Manager (enables call switching and network separation).

SECTRA TIGER/S

Voice use cases



1: STATIONARY VOICE COMMUNICATION UP TO SECRET

Secure information exchange with a fixed line

Together with Sectra Tiger/S, Sectra Tiger Connector makes it possible to connect to a fixed Ethernet network. This fixed line set-up enables users to make a call and exchange classified information in locations such as bunkers, shielded rooms or onboard a vessel.



2: MOBILE VOICE COMMUNICATION UP TO SECRET

Secure calls wherever you are

Sectra Tiger/S is designed to guarantee availability anywhere at any time, which makes it easy to use for voice communication in any location needed. The user can choose between different types of networks, making it easy to always communicate securely.

SECTRA TIGER/S

Use case for secure data transfer

Sectra Tiger/S is a highly secure solution for exchanging classified information. You can rely on it to handle and distribute state secrets with ease. With its user-friendly interface and advanced security features, Sectra Tiger/S ensures that end-users can manage their tasks efficiently while keeping their data safe. The secure file transfer process is straightforward—simply connect the phone to an approved computer and send the encrypted files with complete confidence. As a result, you obtain a secure, mobile, and user-friendly solution for handling highly classified information. To make this use case possible you need the following tools:

SECTRA TIGER USER TOOL

- Can be used to chat, transfer files and to dispatch messages
- A Microsoft Windows™ computer application designed to allow secure data transfer

SECTRA TIGER FILE SERVER

- Secure file sharing and storage between users
- Useful when users are not online at the same time
- Store files for personal use

“Sectra’s solution for file sharing offers the best possible combination—high security but still user-friendly.”

– Project manager at a European authority



SECURE MOBILE WORKPLACE UP TO SECRET

More than just a phone

With Sectra's Secure Mobile Workplace, you can exchange classified information up to and including the classification level SECRET while working remotely or in locations other than the head office. You need the following tools to set up a Secure Mobile Workplace with Sectra Tiger/S:

- Sectra Tiger/S phone: for secure voice communication and messaging
- TEMPEST computer and Sectra Tiger User Tool: for secure data transfer
- Sectra Tiger Connector: for fixed network connection
- Optional add on—Sectra Tiger File Server at central location: for file storage, both personal and shared space



SECURE MISSION PACK UP TO SECRET

Off-grid connectivity

The Sectra Secure Mission Pack is designed for battlegroups, mission-based personnel or embassy employees who need to communicate with their headquarters, other offices or units out in the field. It is well suited for harsh environments with poor network connectivity or no network at all. The solution consists of:

- Sectra Tiger/S phone: for secure voice communication and messaging
- TEMPEST computer and Sectra Tiger User Tool: for secure data transfer
- Sectra Tiger Connector: for stationary connection or connection to the satellite terminal
- Satellite terminal: to enable satellite connectivity for Tiger/S
- Turtle backpack
- Optional add on—Sectra Tiger File Server at central location: for file storage, both personal and shared space

SECTRA NETENCRYPTOR L2

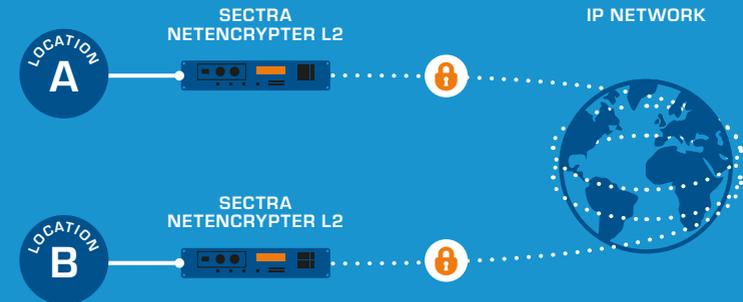
TOP SECRET Link Encryption



Our Sectra NetEncryptor L2 enables the rapid and secure transfer of large amounts of information over civilian and military networks. The security level is the highest—Top Secret—which means that it is evaluated to meet the highest security requirements and approved to protect communications within government and military organizations.

- Point-to-point network encryption on OSI level 2
- Encryption/decryption 10 Gbit/s full duplex
- Can be used over existing IP networks
- Height: 88.9mm (2U) Width: 482.6 mm (19") Depth: 347mm Weight: 10kg
- Peak power <90 W. Mean power ~40 W
- Can be administrated both locally and remotely

Secure data transfer over IP network.



Routing layer 2 frames over IP networks

Sectra NetEncryptor L2 is designed to use fiber cables to connect between two devices. In many cases, when extremely low latency and highly predictable jitter are not critical, it is possible to use external network equipment to route the encrypted Ethernet frames in IP packets. This enables data to be transferred securely over very long distances and takes advantage of the flexibility and redundancy of typical IP networks.

Connecting data centers

Data centers are used to store large quantities of data for organizations. For availability reasons, the data centers need to be redundant and geographically distributed, and all data stored needs to be synchronized between them. With low delay times, predictable throughput and high performance, Sectra NetEncryptor L2 is well suited for demanding real-time applications. Some customers use parallel pairs of Sectra NetEncryptors L2 to achieve higher bandwidth than 10 Gbit/s or to enable redundancy to keep data centers synchronized.

Protecting physically separated networks

When Sectra NetEncryptor L2 implements encryption at the Ethernet level (meaning on OSI Level2), the computers connected to these local networks perceive that they are connected over the same local network. A shared virtual local network is formed using the strongest encryption protection available.

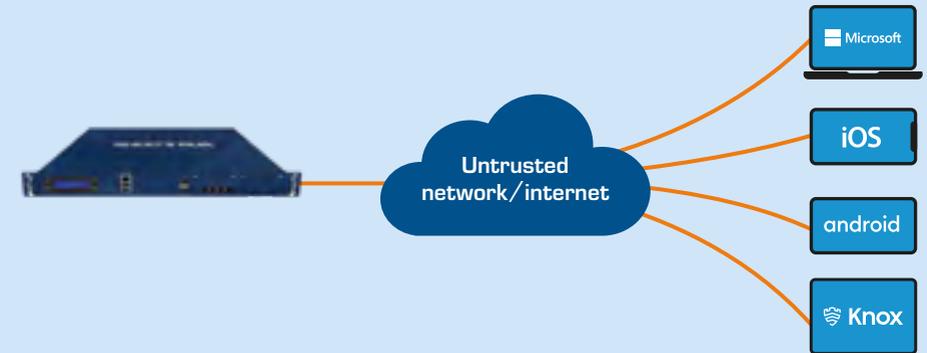
Sectra VPN technology

Sectra VPN technology is a platform VPN developed to secure information and communication—regardless of operating system or device. Sectra VPN adds a layer of security to private and public networks, allowing individuals and organizations to send and receive data safely over the Internet. The solution is delivered with continuous support and security updates.

ENCRYPTION

- Certificate-based authentication
- Elliptic Curve Diffie-Hellman Ephemeral, ECDHE
- Perfect forward secrecy through session keys
- AES-256 encryption

Sectra's VPN works with many different operating systems and ensures that your data is secure.



Sectra VPN Server

Sectra VPN Server protects against network intrusion and makes sure that clients can securely connect to the internal network. It is designed to integrate with existing IT infrastructure.

- Appliance—delivered as an appliance
- Industrial hardware platform for 24/7 operations
- All interfaces on the front
- Upgrades on the management network
- Centralized syslog
- External CRL server
- CE/FCC certification class A

Sectra Mobile VPN client

Sectra Mobile VPN is a platform VPN that can be installed on your portable devices (mobile phone, tablet or laptop). It enables network intrusion protection on your client and secure data exchange with the corporate network via the Sectra VPN Server.

- All traffic enters and leaves through the VPN (protects communications for all apps)
- Roaming seamlessly with session persistence (3G/4G/5G/Wi-Fi).
- Support for Android, iOS and MS Windows

SECTRA TIGER/R

A secure smartphone and tablet

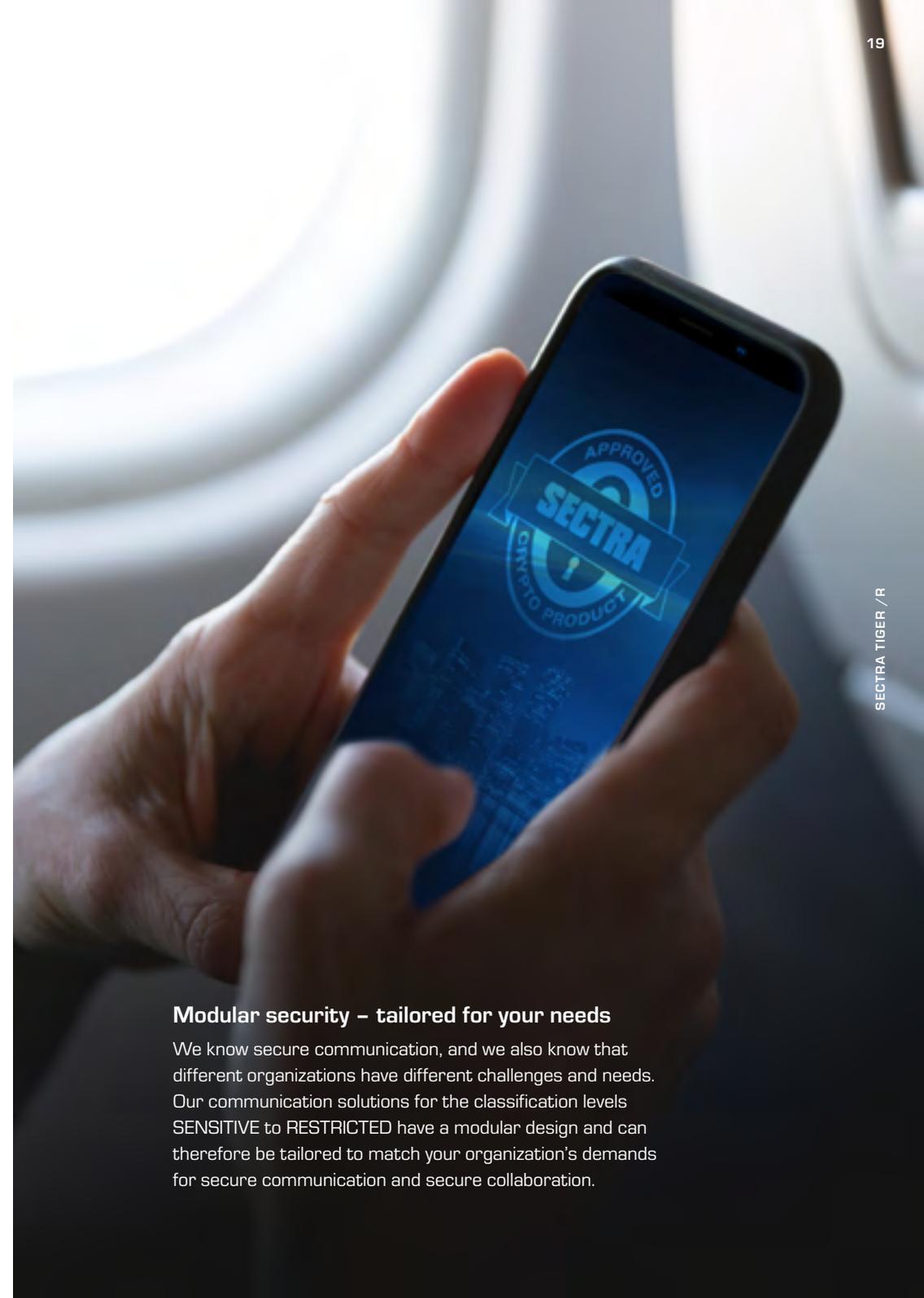
Sectra Tiger/R is a hardened crypto solution developed for a mobile environment, that protects information at the classification level RESTRICTED. With Sectra Tiger/R, users handling highly sensitive information can take advantage of the latest mobile technology.

The solution balances security, functionality and user experience and is available on both tablet and smartphone. It is based on Samsung Knox and is always equipped with Sectra Mobile VPN.

Our strategic partnership with Samsung

Sectra's secure smartphone and tablet solutions for the classification level RESTRICTED have been approved for over ten years. Built on the Samsung android smartphone or tablet, they provide a proven user interface. Sectra has had a strategic partnership with Samsung Electronics Co. Ltd since 2015.

- Modular design that enables scalable security
- Well-known algorithms and open standards
- Encrypted endpoints—devices act like a platform VPN
- Frequent security patches and OS upgrades
- Hardware agnostic



Modular security – tailored for your needs

We know secure communication, and we also know that different organizations have different challenges and needs. Our communication solutions for the classification levels SENSITIVE to RESTRICTED have a modular design and can therefore be tailored to match your organization's demands for secure communication and secure collaboration.

New operational capabilities will rely on secure communications

The increasing adoption of digital technologies will lead to a new level of operational capabilities and effectiveness among defense organizations. As defense organizations become more reliant on digital technologies, the need for secure and robust communication systems with high availability will be more important than ever.

With the growing use of sensors and the incorporation of low latency autonomous systems, we will see a major increase in the amount of data that needs to be communicated, stored, and processed. The reliability and confidentiality of this data will be crucial for an efficient operational organization. Also consider the increased importance of cooperating across borders. Secure communications will be critical for improved interoperability and autonomy—which in turn are vital when it comes to building relationships between different units, systems, and allies.

Sectra develops high assurance products to support defense organizations over several domains. Our products ensure effectiveness and support a holistic approach to secure communication.

Support during every step of your journey

As every organization has its own challenges and needs, we offer tailor-made solutions and different delivery options. You can either subscribe to the software and hardware and deploy it on-premises, or subscribe to the software and hardware as a service. No matter which option you choose, Sectra will be there to support you every step of the journey.

Delivery and deployment options

ON-PREMISES SOLUTION

All Tiger products can be delivered as an on-premises solution, where we deliver all necessary equipment, help with installation/deployment and train your personnel. The customer runs the system on its own.

AS A SERVICE

When software and hardware are subscribed for as a service, Sectra finances the equipment and manages the infrastructure for the customer. Customers are placed on the same infrastructure, but cryptologically separated, running either in Sweden or the Netherlands.



Systems that stand up to scrutiny

Sectra's customers handle classified information and thus need to protect information at various classification levels. Systems that handle this information must, according to national legislation, be reviewed and approved by an independent security authority. The same regulations apply to organizations such as the EU and NATO.

All of our solutions for secure communications stand up to this scrutiny. They are evaluated and approved by security authorities in several countries as well as by the EU and NATO, which means they meet the strict standards required for national security. During the certification process, the full chain from threat and risk analysis to implementation of security measures is scrutinized from both a holistic and a targeted perspective. This provides transparency—the basis for trust.

Scan the QR code to find out more information
about our secure communication solutions.



SECTRA

Knowledge and passion

Sectra Communications
communications@sectra.com • communications.sectra.com

This is a marketing material and may be changed at any time without prior notice.
Sectra will not be held liable for any errors or misconceptions herein.

DOC-ABOK-CNNJKV-1.0 © 2023 Sectra AB