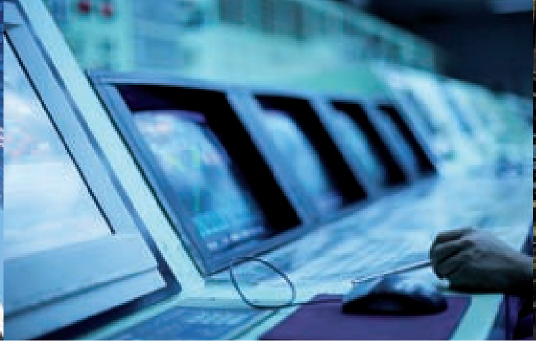
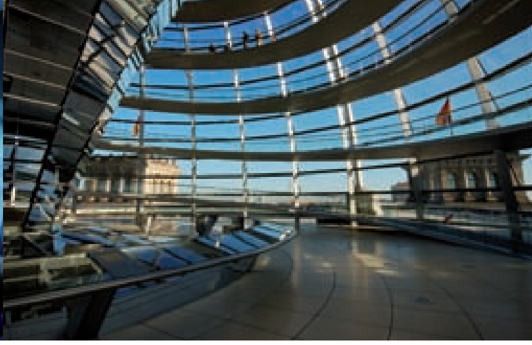
HAGELIN-CRYPTOS
CRYPTO AG

IP VPN Encryption: secure networks in today's virtual world

IT SECURITY SOLUTIONS

Only secure networks guarantee sovereignty

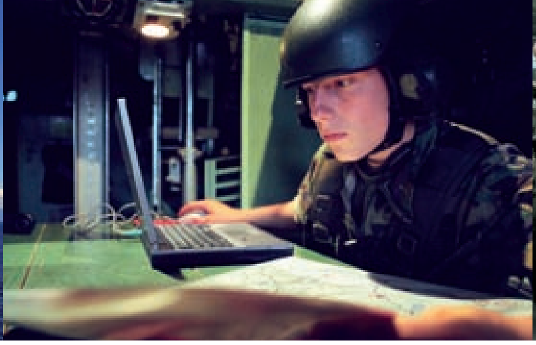
Nowadays, government and administrative agencies are interconnected. Without a standard infrastructure, collaboration and results-oriented policy management would be unconceivable within modern states. Government ministers, diplomats and political decision-makers are all integrated in a single communication group and can exchange digitalised information easily, securely and quickly.

There is still room for improvement, however. The tendency in future governments will be to have fewer people process ever-more complex topics in even greater quality than today. The key will be modern ICT architectural concepts that consistently take account of the organisational structures, work methods, processes and information and communication technologies involved.

These concepts will give rise to governmental communication structures that are divided into a central core network (core) and peripheral areas (edge). The network as a whole could consist of thousands of virtual connections (channels). Specific tasks are performed at a location where they can be done most efficiently, namely at a central place by subject specialists. The input and output of information could be quite decentralised, though, and occur wherever there is a need for information, e.g. at municipal level, in field offices or even at automated recording stations.

Networking in defence organisations

Defence organisations have been working for years on networked-enabled operations for armies, navies and air forces as part of a general transformation of the armed forces. Modern, high-performance core networks provide generals and strategists with a common operational picture. Information superiority is achieved when the relevant information is available at the right time and the right place. That means data streams have to be transmitted over thousands of kilometres in milliseconds. It is crucial that data congestion or run-time delays be avoided, especially in critical situations. The electronic infrastructure must be able to handle peak data volumes – no easy task given the constantly growing demand for bandwidth. Core networks are the backbone of a state. Their failure can endanger sovereignty.



The "everything over IP" strategy

The current trend toward worldwide networking will continue in the future, largely thanks to the Internet Protocol (IP). IP allows a convergence of voice, data and video on one, single standard-ised protocol, providing users with enormous potential for building simple and cost-effective ICT structures. Governments, administrations and industry can adopt an "everything over IP" strategy to create end-to-end networks with thousands of channels of different bandwidth while saving costs, as well as logistical and staff resources. The typical IP risks, however, must always be kept in mind and must be eliminated reliably.

Beware of real risks in a virtual world!

Despite their many advantages, public IP networks, such as the Internet and telecom provider networks, entail all the security risks of modern IP technology. Those risks include tapping attacks, viruses, Trojan horses and a number of other (lesser known) dangers. It is absolutely essential to maintain confidentiality, integrity and authenticity in the transmission of political strategies, military commands, personal data, and results from investigations by intelligence services or during financial transactions.

Comprehensive cryptographic protection is the only reliable, all-encompassing solution for ensuring the security of your information from all forms of attacks.

What is an IP VPN?

"Data highways" with Gigabit bandwidths enable the transport of huge volumes of data between different locations such as government ministries. Network connections for this task are established in so-called Virtual Private Networks (VPN). IP VPN puts voice, data or video payloads in Internet Protocol (IP) packets and builds a virtual and exclusive channel (tunnel) between two or more participants in public or private networks. Locations that may be several thousand kilometres apart exchange data with each other in real time, as in a local area network (LAN). The size of the network, however, is irrelevant to end users.

Multiple applications on the edge of the network

IP VPN technology is also useful in places where elaborate specialised technology was once required. For instance, IP-based video surveillance systems can be connected like computers to the existing IP network at remote locations in a star configuration. The virtual surveillance network can be expanded at will and managed together with other applications. Video data can even be transmitted to headquarters via wireless connections. The possibilities with IP are limitless in this regard.

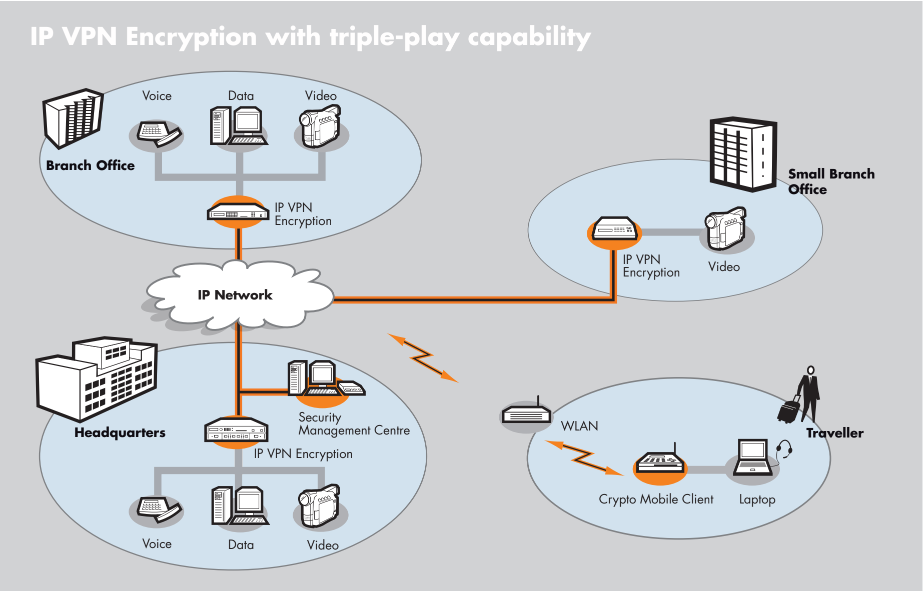
But the same rule applies to applications on the edge of the network as elsewhere: all channels (tunnels) have to operate with suitable protection. Wireless connections in particular are easy to tap and require a maximum degree of cryptographic protection.

IP VPN Encryption units from Crypto AG are available with different levels of encryption performance to cover all operating modes and user scenarios.

Access your data as securely on the road as you do in your own office

Our modern work methods mean we want to have data and information available to us everywhere, even on the road or at remote sites. With portable computers, it is quite easy to take your workplace right along with you. And updating data is no problem either, thanks to global networking. There is access to the Internet or other IP networks almost everywhere you go. But beware of creating security gaps! For example, always take your personal compact Crypto Mobile Client HC-7835 along with you. It protects data exchanged by IP VPN, e-mail, VoIP or in video conferences.

Crypto Mobile Client HC-7835: always take it with you!



IP VPN Encryption with triple-play capability

Secure IP connections operating at Gigabit speed

Core networks (backbones) are the lifeblood of extensively networked organisations. They make data available at practically any location. As the number of end users increases, so too does the bandwidth required in the core network.

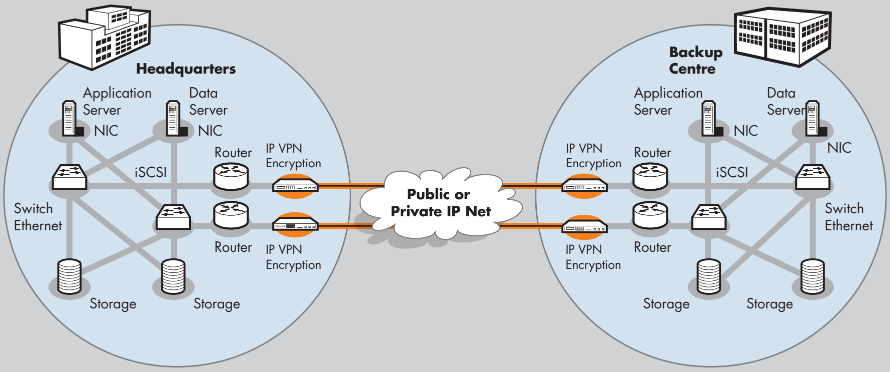
If a number of field sites are also connected, there may be several thousand channels converging at central servers. High-performance backbones must be able to handle the enormous volume of traffic generated. Technologically, this is not really a problem, but security must never be sacrificed for the sake of performance!

Gigabit IP VPN Encryption units from Crypto AG reliably eliminate this risk. Of course, other requirements for backbones must also be kept in mind, e.g. redundancy, load distribution, and fail-safe features.

IP VPN also protects SAN data

The universality of the IP protocol and the bandwidths available in WAN infrastructures today mean that high-capacity Storage Area Networks (SAN) solutions can also be implemented with this technology. The biggest advantage of an IP SAN is that it requires no change of protocol on transport links between the data centres and storage centres. It is, however, of no consequence to the end user which technical transport basis the network provider utilises. Finally, IP-based security and network management can be incorporated directly into the security operations concept of the ICT infrastructure without interface problems.

SAN scenario with IP VPN Encryption



IP VPN Encryption HC-7845: reliable protection with 1 Gigabit data throughput!

Your individualised and secure IP VPN solution – with products and services from Crypto AG

Government authorities around the globe have already benefited from IP VPN Encryption solutions that Crypto AG designed specifically for their user scenarios. The encryption solution that is implemented for you simplifies your operations, maintenance and staff training – thus enormously reducing outlays and logistical costs.

The IP VPN family from Crypto AG

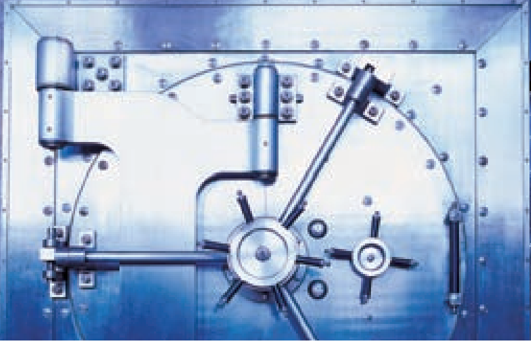
The Crypto AG portfolio offers you a choice of units for each user scenario with enormous flexibility in terms of configuration. All IP VPN units have triple-play capabilities (voice, data, video) and are mutually compatible.

- The **Small Office Version** is a desktop encryption unit for connecting a small office securely to the backbone
- The **Enterprise** and **Branch Office Versions** are high-performance encryption units for direct integration into the ICT rack and offer encryption outputs of up to 100 Mbit/s
- The **Crypto Mobile Client** is a small encryption unit for protecting mobile communications and for gaining remote access to central data at headquarters. Data can also be stored in encrypted form in the Crypto Mobile Client
- The **Gigabit Version** is the new flagship of Crypto AG! It accommodates a data throughput of 1 Gbit/s in the computing centre and encrypts each tunnel with individual keys. It ensures secure delay-free IP VPN tunnels for handling confidential government business round the clock
- **MultiCom Encryption** system: This military unit is designed to withstand maximum mechanical stress for use in the field or on the high seas and is tremendously versatile in meeting operational requirements.

Services from Crypto AG

To implement information security in complex ICT structures, security experts need fundamental knowledge and experience in the relevant technologies. We make available to you all the services you need to meet your specific requirements. We lay the technical and operational groundwork for your high-security solution based on recognised standards.

You can rely on Crypto AG every step of the way, from planning and implementation to training and system handover. And afterwards, for lifecycle management for as long as you wish.



The unique security architecture from Crypto AG

Maximum information security is based not on individual elements but on the entirety of a comprehensive security architecture. The most important elements of the security architecture from Crypto AG are:

- The secret and customer-specific algorithm whose major functions you can define and control yourself as the user
- Hardware-based encryption in its own separate security module that is separate from the ICT network to ensure protection against attacks
- The symmetric encryption process that is immune from cryptographic attacks
- The secure generation of keys with a hardware-based generator of random numbers
- The flexible algorithmic structure that allows you to form individual cryptographic groups with protected relationships
- Efficient security and network management that prevents errors and affords optimum support for your security policy.

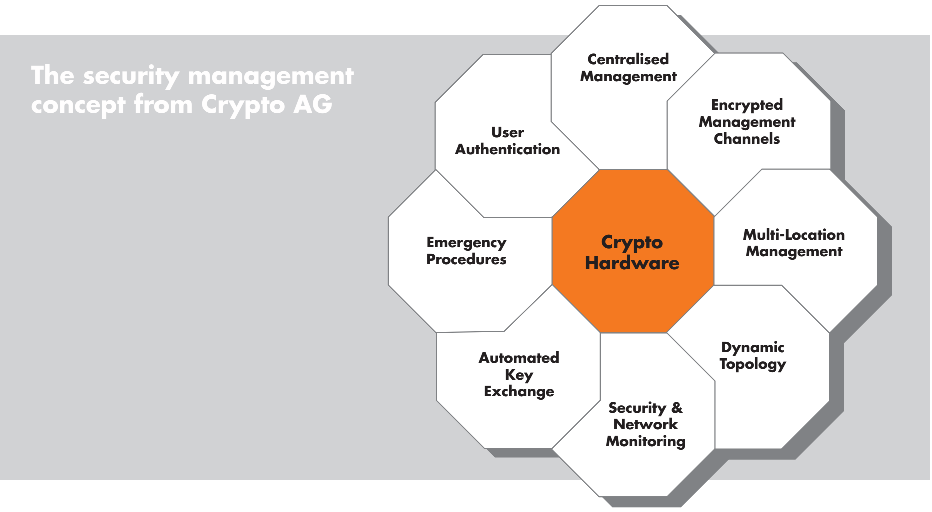
Security management

The security management system for an encryption solution determines how easily, reliably and risk-free you can support and implement your security policy in actual practice. Simplicity is a pivotal criterion for success and trust.

The security of the management system is guaranteed by a number of highly advanced elements:

- Hardware-based cryptographic processes and a centralised operational structure with multi-location capabilities
- Exclusive encrypted management channels, automatic key changes and dynamic topology change (cryptographic groups) while the system is in operation
- Monitoring and logging functions for security parameters and network settings
- Powerful user authentication system and emergency procedures adaptable to different scenarios.

With the computerised Security Management Centre SMC-1100 IP, you can utilise these functions with great efficiency, either online or offline.



The security management concept from Crypto AG

Crypto AG – To Remain Sovereign

Crypto AG is your ideal partner for the efficient and secure handling of information. As a legally and economically independent Swiss company, we are not subject to any export restrictions.

We have developed, manufactured and implemented customised security solutions for over 55 years. The package we offer features the latest technology solutions and comprehensive services. Throughout the entire lifetime of your system, we provide you with support services to guarantee autonomous operation and high availability whatever the user environment.

You too can rely on the expertise and capabilities of Crypto AG – just like our customers in over 130 countries.

Crypto AG, Headquarters

Crypto AG
P.O. Box 460
CH-6301 Zug
Switzerland
Tel. +41 41 749 77 22
Fax +41 41 741 22 72
crypto@crypto.ch
www.crypto.ch

Crypto AG, Regional Offices

Abidjan
Crypto AG
01 B.P. 5852
Abidjan 01
Ivory Coast
Tel. +225 22 41 17 71
Fax +225 22 41 17 73

Abu Dhabi
Crypto AG – Abu Dhabi
P.O. Box 41076
Abu Dhabi
United Arab Emirates
Tel. +971 2 64 22 228
Fax +971 2 64 22 118

Buenos Aires
Crypto AG
Maipu 1256 PB "A"
1006 Buenos Aires
Argentina
Tel. +54 11 4312 1812
Fax +54 11 4312 1812

Kuala Lumpur
Crypto AG
Regional Office Pacific Asia
Level 9B Wisma E&C
2, Lorong Dungun Kiri
Damansara Heights
50490 Kuala Lumpur
Malaysia
Tel. +60 3 2080 2150
Fax +60 3 2080 2140

Muscat
Crypto AG
Regional Office
P.O. Box 2911
Seeb PC 111
Sultanate of Oman
Tel. +968 2449 4966
Fax +968 2449 8929

A member of
The Crypto Group