



Secure voice and data communication on every wavelength. Crypto AG.

RADIO SECURITY SOLUTIONS

Modern radio communication: Secure, reliable and user-friendly



Radio communication is a reliable and very easy to master communication mode over any distance. Thanks to technical advances, potential new uses for it are opening up all the time.

High transmission standard	Modern radio systems offer high transmission standards – thanks to a higher data rate,
	parallel channels and easy-to-generate, high transmitting power. Today, they can be used
Many automated functions	without any problems because the transmitter, receiver and the antennas are normally
	integrated into a complete, computer-controlled system. This means that many functions
No specialist knowledge	such as frequency selection, connection and antenna management are automated. As a
necessary	result, the user needs no special knowledge and can concentrate on his actual tasks.
HF-radio always functions	And the hard and fast rule that radio communication will continue to function even when,
	for operational or political reasons, everything else has failed, has not changed to this day!
Operation in quite large	Radio communication today normally takes place in quite large network configurations,
networks.	whether for military purposes (e.g. as a part of C4ISTAR systems), or for communications
	between Foreign Ministries and embassies, which can be made secure at moderate
	expense with a backup radio system.





Operative linkage with other networks – e.g. HF-voice communication with telephone networks or data communication with IP applications – is no longer a problem. One advantage of it being "freely" available is that stationary and mobile/portable equipment (ships, vehicles, aircraft) can be deployed in any chosen combination.

A deciding factor in this renewed interest in radio communication is that, in addition to voice communication, it also supports data communication and messaging. Thanks to protocols/forms that can be standardised, data (command information, sensory analysis, battle reports, etc.) can flow into databases and be assembled and analysed into situation reports from there.

Radio is an open communication mode – which is why it can easily be misused. It is therefore vital to protect the information/data against interception and misuse, both in civilian and military applications. The only really secure solution to prevent unauthorised access is to encrypt the information that has to be transmitted.

Crypto AG has tried-and-tested solutions available for virtually all radio applications, but we also design and manufacture individual systems for use in complex user scenarios. While a project is being implemented, we support the customer with services at each project phase. To guarantee availability and operational autonomy, we prepare individual maintenance plans and guarantee the necessary services. We have an in-house training centre to train the staff.

No problems with mixing stationary, mobile and portable applications

Voice, data and messaging

Security through encryption

Tried and tested solutions

Individual maintenance plans

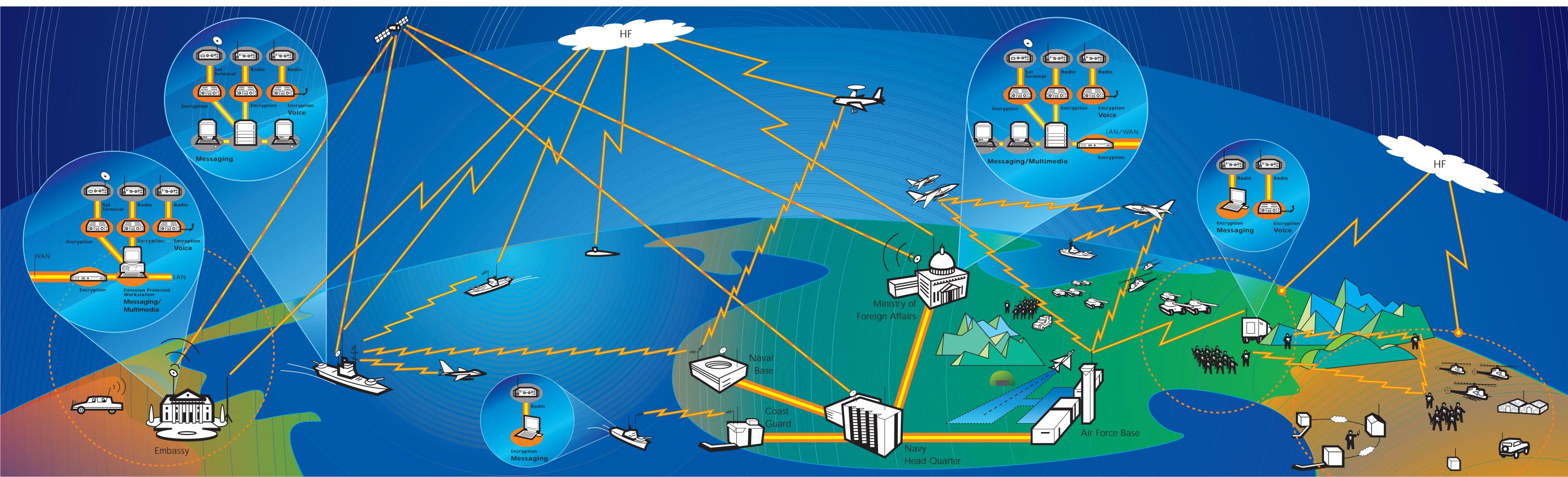
HF-Radio communication: Tried and tested, powerful and secure – thanks to encryption from Crypto AG

Foreign ministries/Embassy radio communications:

HF-communication always functions, even in times of crisis! It enables worldwide main and backup connections for radio telephony or messaging (also as a supplement to document transmission by fax). Simple operation, including by staff with little training, and comfortable key management ensure the highest level of security and permanent availability.

Navy/Communication on the high seas:

Here, HF continues to be essential, because of the great distances involved. The complex communications technology with on-board LAN systems must be absolutely reliable on the high seas. Technical reliability and operational autonomy are of vital importance. The large data volume is managed with messaging and control systems. HF traffic takes place in multi-channel operations and is supplemented with tactical VHF/UHF



and SAT connections. Only through homogenous encryption will the interoperability of all channels be guaranteed. Protection against direction-finding and special operating modes are important tools in Electronic Warfare.

Strategic HF-links:

HF has an integrative function as the main and backup connection between government departments, headquarters and bases. The large data volumes that can now be transmitted are used for messaging and multimedia-applications (e.g. battlefield reports). Across-the-board networking and intercommunication mean that homogenous, scalable encryption becomes a must.

Tactical links:

Being highly mobile and coordinating several commandos typically involves the combined use of voice and data communication via HF, but also via VHF and UHF. Air transport and mobile units rely on HF because it is now possible to install the infrastructure (mobile devices with high transmission power, incl. antennas) almost anywhere. Voice communication means short response times are possible, and increas-

ingly, the command structure is supported by secure messaging which is simple and thus suitable for use at the front. At the tactical level, all aspects of Electronic Warfare are relevant – especially protection against direction-finding and resistance to interference. Information security must be guaranteed at the same standard as in strategic communication.

Front communication:

Where mobility and reliability under the harshest conditions are essential, both communication (radio telephony and messaging), as well as their protection against interception must be designed for simple operation, compact size as well as mechanical/electrical stability. Encryption in this environment relies on easy to use key management and requires an Emergency Clear function.



Voice encryption - reliable, and with a guaranteed future

	Voice communication via radio waves continues to be an essential communication mode. For example, for military command structures, frontline troops, police organisations or foreign ministries (embassy radio telephony). Simple point-to-point connections are just as possible as large networks with numerous fixed and mobile stations (vehicles, ships, aircraft).
	What all these applications have in common is that the sensitive information that is exchanged needs the greatest possible protection against unauthorised access.
Hardware encryption with user-controlled algorithms	Here, too, security systems from Crypto AG are the right solution. Because the highest degree of security can only be created through hardware encryption with secret, user-controlled algorithms. Irrespective of the particular deployment scenarios.
Robust voice encryption	For many years, this concept has been implemented in the internationally tried and tested voice encryption unit HC-265, with a reliable, robust encryption mode. Units of this type will continue to be used in many networks in the future, because they are cryptographically, electrically and mechanically extremely robust and offer the highest operational reliability.







Radio Encryption V/D HC-2650

Radio Encryption V/D Voice/Data

The successor Radio Encryption Voice/Data HC-2650 unit has, as a new feature, three modes which can be used to meet very different requirements and priorities such as channel quality, deployment scenario and backward compatibility in the most effective way. Added to this is the facility for data encryption. The unit works with virtually all standard radios of both new and slightly older designs (HF, VHF, UHF), allowing homogenous encryption in mixed network structures. Thanks to builtin interfaces, remote control of the operation is possible.

Can be connected to all radios

The multi-mode design allows the user to expand his existing network in stages with new applications (without interrupting operations), and the parallel operation of voice and data encryption. At the same time, it is the perfect platform for future applications (e.g. mobile messaging with hand-held computer) and for upgrades or updates. The system as a whole is geared to a long life and thus to optimum investment protection.

Seamless expansion of the networks

Of the greatest importance in daily operations is the excellent voice quality and voice recognition. Even where the quality of the transmission channel is poor, there is no difference in the security of the connection, compared to plain text operation!

Outstanding transmission quality

The very compact dimensions, and the extremely tough, even smaller light metal case are designed for use in harsh conditions. The unit meets all major military standards with regard to operational and environmental conditions. This means that high reliability is guaranteed.

Meets all major military standards

The simple operation makes it suitable for use at the front, prevents operating errors and is designed to ensure a high degree of availability: Thanks to menu guidance (2-line display), one knob and two keys are sufficient. It offers three options for key input: Manually, via ruggedised Security Data Carrier and, thanks to the built-in browser-based user interface, through easy programming on a PC. Managing it can thus be adapted to every network configuration.

Simple operation High degree of availability



jléfűreruf456 985851 488/rtg(11123 23434±8\ fghdre ka fjadófkjieru erur456 98585 1489/111' 913483 4x£Xrrt176ec56115368 (x./%c3030 1696351533c32434 cfta fehdre ka fjadófkjieru erur456 98585 94885111 2011123 23434±8\ fghdre ka fjadófkjieru erur456 98585 9888514897111897111' gg11123 23434±8\ fghdre ka fjadófkjieru erur456 98585 rtl2eeeqw45432354545657(& /r433010 1489'1'1'

Unbeatable plug-and-play messaging system on a laptop basis

Digitisation of the battlefield	The across-the-board "digitisation of the battlefield" has been widely implemented as a defence philosophy in all military units. The reasons for this are messaging systems, which facilitate information processing and distribution and are invaluable in allowing the rapid and selective evaluation of command information.
Simple operation – without specialist knowledge	Normally, the use of messaging systems is associated with quite large networks with com- plicated structures. However, there are uses where flexibility, mobility and very simple oper- ation – without specialist knowledge – are an important consideration. Highly developed technology solves these requirements without compromising security.
Wide range of uses	In military deployment profiles, requirements such as mechanical and electrical robustness, compact dimensions and direct integration with existing radios are paramount on the list. Similar requirements can also be found in police organisations, Ministries of the Interior, Foreign Offices (travelling diplomats) and with internationally active NGOs.





Secure Field Communication Terminal HC-6830

Secure Field Communication Terminal

Crypto AG has developed the Secure Field Communication Terminal HC-6830 precisely for such deployment scenarios. Thanks to encryption, this unique, extremely user-friendly system based on laptops enables the error-free, secure messaging communication and protection of all data on the hard disk against any outside interception – including against viruses and spamming.

Error-free, secure

messaging communication

Its design is entirely geared to

practical requirements: All major

functions are already included as

standard features. This allows com-

missioning and integration in the

network in "plug and play" mode.

"Practical" can certainly mean

"under difficult climatic conditions"

as far as the HC-6830 is concerned, because it comes in an

extremely strong, water-tight light

metal case and meets all the major military operating standards. A modem for PSTN communication

is already integrated. With the

optional radio modem (ARQ and FEC functions), connection with virtually all types of radio (HF, VHF, UHF) is almost as easy as child's play. Additional communications technologies such as SAT, GSM, ISDN, LAN etc. are also possible, if the customer requires them. The possibilities for deployment are thus virtually unlimited.

Virtually unlimited deployment potential

Equally unique is the special applications software with the very user-friendly messaging system and file management. Any number of attachments (text, images, graphics, data) can be attached to each message. The fact that this system requires only very limited training – for the very user-friendly key management – is an important consideration for many users when making their decision.

Very user-friendly Little training required

As is the case for all products from Crypto AG, the Secure Field Com-



munication Terminal also provides the greatest cryptographic protection against electronic attacks on the communications and security data. The basis for this are a customer-controlled algorithm and encryption in a protected hardware security module. All data are only stored encrypted. Access to the system is only possible via an authentication process.

Radio Link Encryption Units for Messaging Systems and Data Links

Powerful data channel	It is now also possible to deploy radio communication in the HF-field as a powerful data chan-
	nel. Where they form part of large information and communication systems with decen-
Networking via messaging	tralised partial networks (LANS), for example in government ministries, naval bases or large
	ships, radio links (HF, but also VF, UHF and satellite links) serve as important main or back-
	up connections. The comprehensive networking based on messaging systems allows the
	transmission, storage and evaluation of sensory or logistic data, position and movement
	information as is required, for example, for situation reports and command decisions
	(C4ISTAR functions).
Two compatible	Because HF links are also part of the global network, protecting the information against
HF-data encryption units	unauthorised access is of the greatest importance. For this process, Crypto AG offers two
	compatible HF data encryption units. Both are compatible with the STANAG 5066 model.
	And both are built to be extremely sturdy. Thanks to highly robust synchronisation and large-
	ly automated operation "in the background", they guarantee high system availability. How-
	ever, they prove their worth in a range of different deployment scenarios.

rtTZeeeqw45432354545657(& /r433010 1489/1/1/







HF Data Encryption HC-7665



HF Data Encryption MC HC-7660

HF Data Encryption

This ultra-compact, robust singlechannel HF Data Encryption unit HC-7665 is predestined for tactical and mobile deployment scenarios. It is very easy to install in vehicles, ships or aircraft (stackable) and is compatible with virtually all radio systems (including older designs). It meets all major military standards.

Ultra-compact tactical unit

A high degree of availability means simple operation: Thanks to menu guidance (2-line display), one knob and two keys are sufficient. The security management is designed to be possible while mobile, and can be done either manually, with the Security Data Carrier or via the browser-based user interface. Appropriate interfaces exist for remote-controlled operations.

Simple operation means a high level of availability

The unit, which is extremely versatile, works in simplex, semi-duplex and full-duplex operating modes and encrypts data in asynchronous and synchronous mode. Cryptographically, it is fully in line with the TIS philosophy of Crypto AG, with user-controlled algorithm. As a tactical device, it has an emergency clear function.

Simplex-, semi-duplex and full-duplex operation

HF Data Encryption MC

Where large data volumes are generated for transmission – especially in strategic networks – the Multi-Channel HF Data Encryption unit HC-7660 is the best solution. It combines a controller unit and up to 5 independent encryption modules in a robust 19-inch case. Thanks to the integrated serial interface, it can be linked into communication systems of any size.

Up to 5 independent encryption modules

The multi-channel design allows the user to simplify the operating and control functions and the security management within integrated total systems: All important functions can be controlled centrally including, for example, the strategically important, fast choice of different channels. The available operating modes also offer flexibility: Simplex, semiduplex and full-duplex (synchronous and asynchronous mode).

Information security starts with the manufacturer's own security philosophy

Across-the-board in-house security philosophy	Developing and implementing systems for information security without any weak points demands not only technological and cryptographic expertise, but also an absolutely across- the-board internal security philosophy on the part of the manufacturing company. All inter- nal processes and structures must at all times be directly controllable, and all influence by outside third parties must be excluded.
No third-party influence possible	Only then can the customer have confidence that under no circumstances can knowledge and sensitive information about his projects and associated aspects fall into outside hands, or that third parties might be in a position to have any influence over his systems.
	Crypto AG's internal security philosophy is based on the following principles:
Secrecy policy	We have a rigorous in-house policy of confidentiality to safeguard knowledge about the cus- tomer's security projects and to protect our own expertise.
Independence	We maintain our complete independence as a company and consequently promise the cus- tomer that the encryption solution we supply cannot be influenced from outside, and is unique:
	Political independence: As a Swiss company, we are not subject to any
	export restrictions for strong encryption technology.
	Legal independence: As part of "The Crypto Group", Crypto AG is owned
	by a trust company and is thus removed from any outside influence.
	Economic independence: As a successful, strong company (more than 200 employees), we have been a stable, reliable partner for over 50 years.
	Technological-cryptographic independence: We maintain all the
	major skills and expertise in-house and exclusively for our customers and for ourselves.
	Own production plant: We make all security-relevant components in our
	own production plants – this keeps external influences at bay.
	Long-term security guarantee: Our extremely long-term readiness to
	deliver replacement parts, service, training and advice enables the customer
	to maintain and control security over the long term.

The multi-dimensional security concept "Total Information Security[®], TIS by Crypto AG"



Information security must eliminate all actually existing risks and all possible forms of attack. Including attacks on the security installations themselves. There must be several reliable protective measures for each type of threat. This requirement has led Crypto AG to develop its security philosophy of "Multiple lines of defence". It is implemented in the security concept of Total Information Security, TIS by Crypto AG:

Symmetric encryption processes: The mathematically secure solution – encrypted messages cannot be, and never will be, breakable.

Protected hardware encryption separated from the network: No unauthorised access to security data and processes is possible, each unit is cryptologically identifiable.

Secret, customer-controlled algorithm: No possibility of attack, even if the cipher key is lost.

Complete cryptographic transparency for the customer: The customer can verify the security completely at any time.

Long-term security concept (Technical design, logistics, training): Highest security guaranteed over the entire life cycle.

Key management with the same cryptographic design as communication: Balanced security as far as the exchange of keys.

Autonomous and independent company: No third-party influence possible during the development, production, sale or export.

Separate development and production processes: Protection of the Crypto AG products against manipulation.

Secrecy-Splitting: Protection against internal attacks and against loss of usable security knowledge.

Error-preventing operating designs (Encryption process invisible in the background and automated operator functions): Makes security-endangering operator errors impossible.

Total Information Security°, TIS by Crypto AG



Total Information Security[®] TIS by Crypto AG

Crypto AG - for total information security



Crypto AG is a legally and commercially independent Swiss company which, for more than 50 years, has focused on the development, production and implementation of systems geared to the highest standard of information security. Security technology from Crypto AG has a proven track record in all types of communications networks. For most user scenarios, we can draw on the experience gained from solutions we have already implemented: There are good reasons why governments, government departments, diplomatic services, police, border patrol and defence organisations in more than 130 countries choose Crypto AG as their trusted partner for security.







Leader in Total Information Security®

www.crypto.ch



Total Information Security® TIS by Crypto AG

Crypto AG, Head office

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

Crypto AG, Regional offices

Abidjan

Crypto AG 01 B.P. 5852 Abidjan 01 République de Côte d'Ivoire Phone +225/22 41 17 71 Fax +225/22 41 17 73

Abu Dhabi

Crypto AG Regional Office Middle East P.O. Box 41076 Abu Dhabi/UAE Phone +971 2/44 55 737 Fax +971 2/44 55 151

Buenos Aires

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

Kuala Lumpur

Crypto AG Regional Office Pacific Asia No. 2 Jalan SS7/11 Kelana Jaya 47301 Petaling Jaya/Malaysia Phone +60 3/7872 2150 Fax +60 3/7872 2140

Riyadh

Crypto AG Representative Office P.O. Box 59701 Riyadh 11535 Kingdom of Saudi Arabia Phone +966 1/454 1011 Fax +966 1/454 9030

Sultanate of Oman

Crypto AG Representative Office P.O. Box 2911 Postal Code 111 Seeb Sultanate of Oman Phone +968 504 966 Fax +968 504 929