



**Sophisticated Security Architecture
designed by Crypto AG**



Security Architecture from Crypto AG – elegant and effective

You have to protect your vital and sensitive information from unauthorised access. Since 1952, Crypto AG has been ensuring that you can do just that, with the most modern means of cryptography available. This objective still permeates the entire company philosophy today. At the heart of our security philosophy is our Security Architecture, which is unique in kind and has been further developed over decades.

The design of this architecture allows Crypto AG to provide a secret proprietary algorithm that can be specified for each customer to assure the perfect degree of cryptographic security and optimum support for the customer's security policy. In turn, the Security Architecture gives you the influence you need to be fully independent in respect of your encryption solution. You can determine all areas that are covered by cryptography and verify how the algorithm works.

The original secret proprietary algorithm of Crypto AG is the foundation of the Security Architecture. Its design embodies cryptography at its best and lays the groundwork for solutions that deliver unique security quality.

Several interdependent main functions of the architecture are linked to the algorithm. Together, they form an extremely resistant and stable cryptographic nucleus. This functionality is supported by hardware-based encryption in a separate security module isolated from the IT network (ICT network). The security and key management system is efficient and easy to operate, ensuring full use of the flexibility of the architecture in everyday encryption. This system works seamlessly with your own network management. In sum, the Security Architecture from Crypto AG provides you with the high availability you require of your encryption solution.



The core functions of the algorithm make you independent

You get your own algorithm based on the basic secret proprietary algorithm from Crypto AG. With this independent starting point, no one has knowledge of your algorithm. The algorithm is designed so you can determine core functions yourself. This feature makes you completely independent of Crypto AG and gives you full control over your own security. On completing the next step yourself, namely doing the specific profiling, you take full possession of the algorithm. This function meets your needs for autonomy and separation. You now have an algorithm which is absolutely unique worldwide. Neither Crypto AG nor anyone else knows about it or has access to it. You are the only one with knowledge of and control over your security.

The algorithm is based on a symmetrical encryption process in which the

same keys are used for encryption and decryption. Most importantly, the (digital) key has to meet the quality of true randomness. This is assured by a separate random number generator that is hardware-based and of highest quality. This basis, in combination with the key length of at least 128 bits and the complexity of your secret encryption algorithm, means all attacks on your system will fail.

Resistant cryptographic protocols allow you to define keys at multiple hierarchical levels (multi-hierarchical key grouping). That makes your security management highly flexible. In your everyday practical use of the units from Crypto AG, you can support your security policy efficiently, for example, by defining cryptographic communication groups at different hierarchical levels and with mutual overlapping,

depending on the application scenario involved. Cooperation and separation can be adapted at any time to changes in organisational structure. The number of participants is unlimited.

The algorithm description from Crypto AG assures transparency in evaluation to give you, as a customer and owner of your own algorithm, absolute certainty about its structure and mode of operations. Together with the unique Acceptance Cipher Check (ACC), you can have an efficient tool at your disposal, if you wish, that allows you to check the correct implementation and operation of your algorithm independently any time and anywhere. This verification of the cryptographic operations creates understanding of and trust in the solutions from Crypto AG.

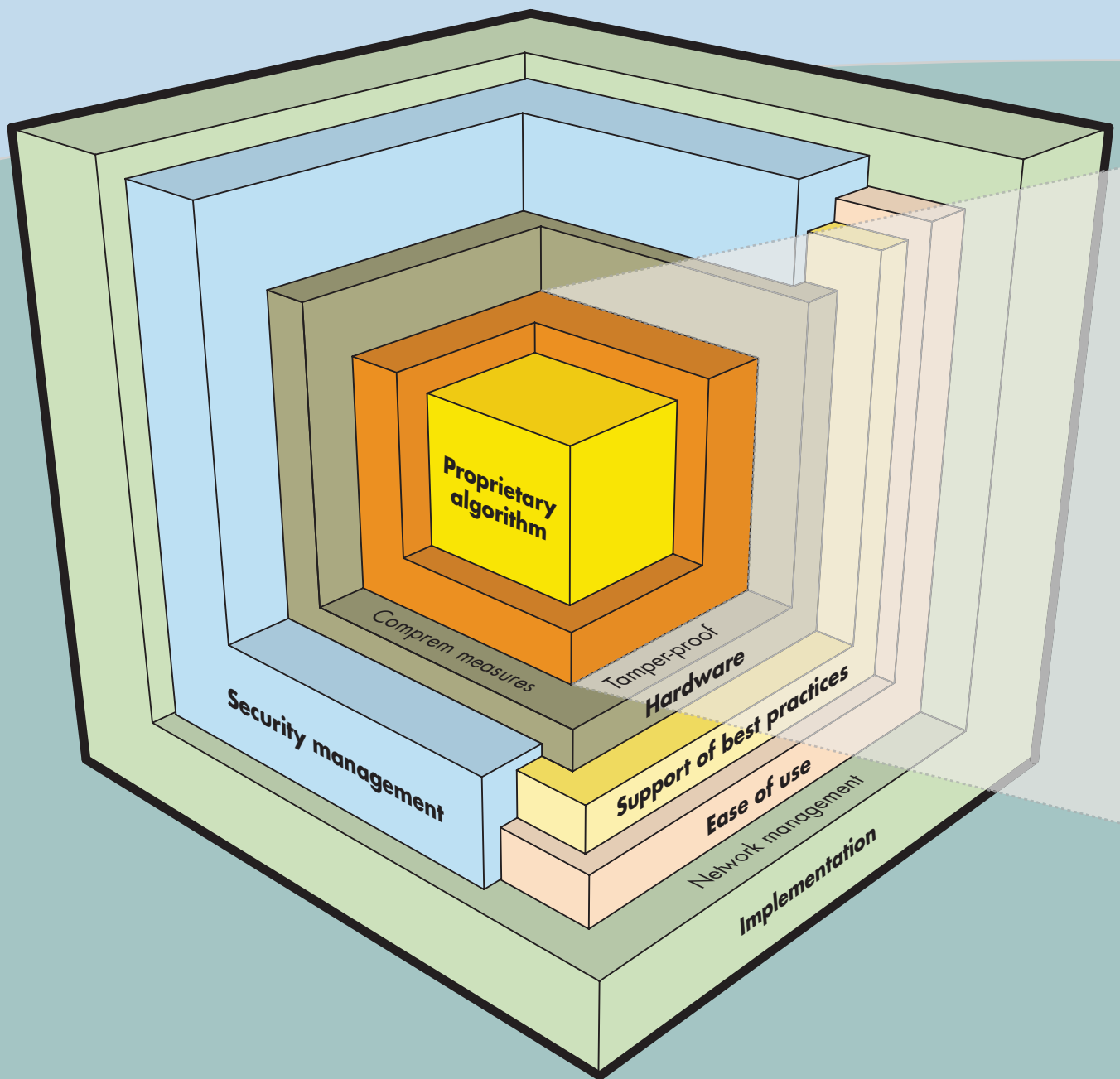


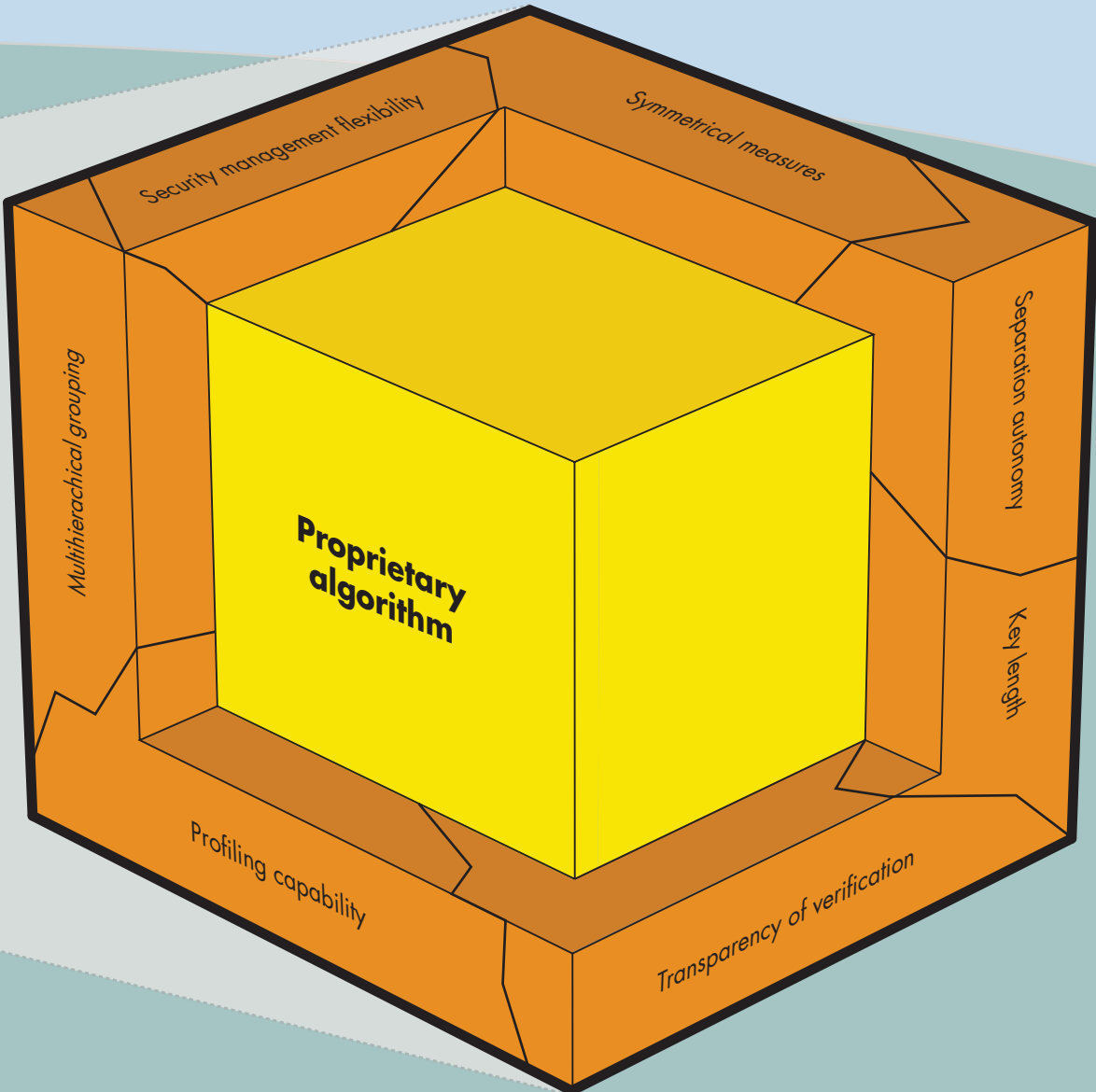
Hardware completes the security package

The core functions of the algorithm are supported by the design of the processors in the encryption units of Crypto AG. This includes the design of the security module, where the functions relevant to cryptology are run, and the design of the unit housing. Your security parameters (master keys) are stored in encrypted form in the security module of your encryption unit. All encryption processes are run in a manner protected from influences and dangers coming from the communication networks. The module is tamper-proof as part of the hardware design, so your logical security elements are completely protected from being accessed without authorisation.

The encryption unit design is based on a consistent separation of encrypted and non-encrypted data flows (red/black separation). At the same time, from the very outset of your unit's development, strict standards of design and material selection ensure effective countermeasures (measures against compromising emanations, which are inherent in all electronic equipment). The units are thoroughly tested in the laboratory of Crypto AG for resistance to irradiation and prevention of radiation.

Your information is surrounded by different layers of Security Architecture







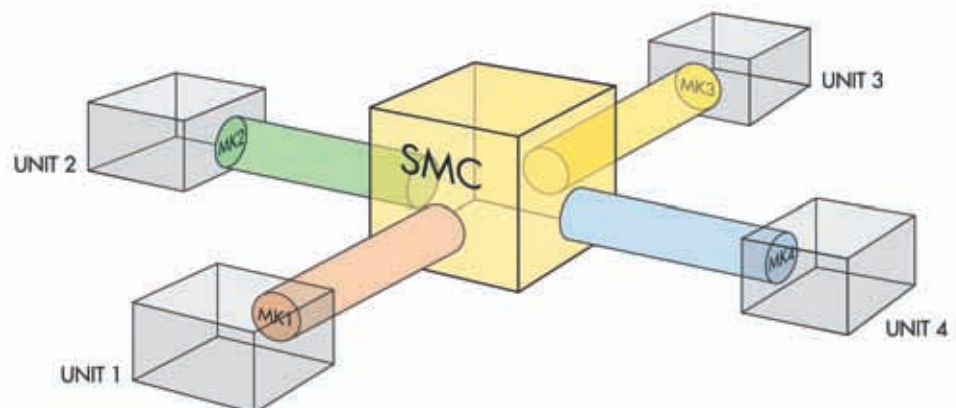
Security management: centralised, efficient and convenient

A convenient and customisable management of security functions is a decisive factor for end-to-end security and substantially increases the system efficiency of your network. With the computer-based Security Management Centre (SMC) from Crypto AG and its mature Security Architecture, you can carry out all management tasks quickly and conveniently right from your screen. That allows you, among other things, to distribute keys online and off-line in an encrypted process, to set up cryptological groups, to manage authorised relationships among network participants and groups of par-

ticipants and to include or exclude units in or from your security arrangements. Even encryption units that have been lost or stolen pose no problem to you. Keys can be changed automatically and at the date you wish. Thanks to the ingenious key system used in your units, the uninterrupted operation of your communication infrastructure is guaranteed even during key changes. This, in turn, assures the high availability of your encryption solution.

Your data is comprehensively protected on the SMC thanks to the encrypted storage of security parameters (local security), the encrypted

exchange of keys and the separation of the SMC from the public network by the Message Scheduler. With the Security Management Centre from Crypto AG and the Security Architecture, you manage your network security at the same security level as the encryption units from Crypto AG protect your communication.





The hardware security module

Encryption units from Crypto AG implement encryption in a separate security module, thus protecting your information against any risk of being accessed from the outside. Thanks to the tamper-proof hardware, the encryption process itself is protected from unauthorized access and manipulation. In addition, the module separates the encryption process completely from the ICT environment in which it is operating. That means effective protection against viruses and network attacks. This separation accelerates the pace of encryption.

The moment the hardware is broken into all security parameters are automatically deleted. Hardware-based encryption as offered by Crypto AG is therefore your best guarantee of maximum security.

Network performance is not impaired at all because encryption is done in the separate security module. Consequently you do not waste any time in your communications.



Support of best practices

Crypto AG has designed its Security Architecture to support recognised practices for strengthening your security and to be integrated seamlessly in your security policy. This applies particularly to the periodic change of keys. You can carry out this change easily and automatically in an encrypted and scheduled process thanks to the key hierarchy and the security management concept of Crypto AG. Under this approach, encryption units from Crypto AG use keys just once and only for a short time. Algorithm management (profiling) is separated from key management in line with the principle

of secrecy splitting. In keeping with this same principle, the aim of the Security Architecture is to keep management of the unit and encrypted communication cryptographically separate. Separation is important for controlling access to the security parameters. Different roles (e.g. security manager, network manager, operator) are granted different access rights.



Crypto AG – To Remain Sovereign

Crypto AG is your expert 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 been concentrating on developing, manufacturing and implementing custom security solutions for over 50 years.

Our range comprises the latest technology and comprehensive services. After-sales service and product training that guarantee autonomous operation and high availability are assured over the system's entire lifetime, whatever the user environment.

You too can rely on the expertise and capability of Crypto AG.

Customers from over 130 countries are already doing just that.

www.crypto.ch

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
Regional Office Middle East
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
No. 2 Jalan SS7/11 Kelana Jaya
47301 Petaling Jaya
Malaysia
Tel. +60 3 7872 2150
Fax +60 3 7872 2140

Muscat

Crypto AG
Regional Office
Seeb PC 111
Sultanate of Oman
Tel. +968 2449 4966
Fax +968 2449 8929

A member of
The Crypto Group