THE MANY DIMENSIONS OF DISCRETION

OFFICE SECURITY AND SECURE DIPLOMATIC MESSAGING

Government organisations traditionally cultivate a strong culture of secrecy. Global information risks and technological change force them to optimise their security policies constantly. It is therefore crucial for them to have a security solution that covers all the work processes for the handling of highly sensitive information on a daily basis. Crypto AG has two security solutions customised to meet these needs: the Crypto Desktop HC-9300 platform with individually selectable security applications and CAG MAIL, a secure messaging system.

by Beat Püntener, Product Manager

It is as fast and easy to copy a huge amount of information onto a USB stick as it is difficult or virtually impossible to monitor what subsequently happens to that information. There is an enormous difference between the present-day situation and the days when most documents and archives were still kept in paper format. Unfortunately, an information security project often mutates into a doomsday scenario, given the immense quantities of information and data generated, processed, stored and communicated today. Leaks can lead to a veritable disaster, but this does not mean organisations are simply at the mercy of these risks. What they need most is a well-conceived security policy as a foundation on which to build the necessary security structures and processes.

Confidential information at risk during all stages of the process

Confidential information is confidential, even during its inception, and must be treated accordingly when being recorded and subsequently processed. In other words, its classification must be determined from the very outset, along with authorisation for accessing it. Depending on the degree of protection involved, this step can mean preventing processes such as printing, copying, sending or reclassifying. Organisational and technical steps are taken to ensure the enforcement of these requirements and are defined in a security policy. The technical actions consist largely of using encryption units that can consistently enforce the technically feasible aspects of the security policy with cryptographic processes and other security functions. It is important to bear in mind the following areas:

Information processing

Only authorised persons should be allowed access to plain text or further processing. Where such access exists, an organisation must eliminate two weaknesses: first, the risk of the information becoming visible to outsiders because of unintended emissions, be they electrical, acoustical or optical; second, the risk of information being removed from the secure environment or copied without permission. An organisation can take technical measures to prevent removal or copying, or at least make it very difficult. One of these measures is to record complete logs showing who did what, when, and with which information.

Information transmission

While being transmitted, information often passes through unprotected areas (e. g. WAN), where it is open to all conceivable types of attacks. Excellent encryption is the only way to eliminate unequivocally the information risk (information leak) at this stage (transitional phase, transmission phase). The reliable transmission of information is also part of availability in the broader sense of the term. For instance, crisis-proof transmission systems that automatically resort to other media when communication channels fail are far superior to simple systems in this context.

Information storage

The storage of information is just as fraught with risks. This fact is driven home by the recurring reports of hacker attacks against government computers and websites. These situations endanger both the confidentiality and the availability of information. To eliminate these risks totally, an organisation needs a high-security storage solution that ensures confidentiality while preventing or at least detecting data loss or data tampering.

With appropriate security solutions deployed, a well-designed security system of this type prevents information from "becoming endangered" in the first place. There is also a need for organisational security actions that take effect when information leaves the internally protected area as part of the organisation's mandated activity, for example, to support negotiations.

Core criteria for a long-term security policy

In drawing up a security policy, an organisation or company must start with a comprehensive analysis of security in all areas and conclude with a set of regulations and protective mechanisms which are defensive in character in that they are based on the need-to-know principle. That means only individuals who need sensitive information for their work should be given access to such information. A security policy has to go much further, though. For example, it must state:

- which information is sensitive
- who has access to it
- how access is handled
- how information is designated and classified
- where and how information is deposited or saved (e.g. locally only)
- how information is communicated (protective mechanisms, addressees)

The security policy specifies how to implement technical and operational security zones with varying security requirements in actual practice. This arrangement includes user clearance (rights), user roles and user duties. Any security technology being set up must ideally meet these conditions.

> *An organisation can only comply with its security policy if that policy can be successfully implemented by means of organisational measures and technical security solutions.*

Security architecture in the office required for top security

In a modern working environment, all applications and technologies are interconnected. For this reason, an organisation can only achieve the degree of security it desires with a complete end-to-end security chain perfectly suited to the technology used. That is exactly why Crypto's security architecture contains not only encryption but also other features such as consistent access protection with classification and user-specific clearance, COMPREM, tamper-resistant design and encrypted storage of all information.

Office solutions: Crypto Desktop HC-9300 for office applications

The Crypto Desktop HC-9300 and its available security applications meet the need for high security in office setting. This solution is based on our new platform idea: HC-9300. This modern desktop encryption unit has security applications such as fax, voice or file encryption implemented on it and guarantees users security and efficiency as well as availability and a safe investment.

Complete system for secure messaging in diplomacy

CAG MAIL is a secure diplomatic messaging system geared to the special needs of a diplomatic organisation. The tasks of processing and communicating messages between exposed points such as embassies and a government ministry are handled comprehensively and consistently with a focus on maximum security. The advantage of this approach is that the diplomatic organisation can retain its well-attuned method of operation.

Any given organisation has its own specific processes and work methods. That is why you need to sit down with our experts and determine the ideal solution for your needs.

The secure Crypto Diplomatic Messaging System consists of two components: the Crypto Workstation and the Crypto Message Server.

The COMPREM workstation includes a printer and scanner as well as a messaging application and standard office tools. Workstation and server are connected to each other via LAN and IP/VPN.

Crypto provides individual mailboxes, document classification and identity-based user access with user clearance – in other words, all the protective mechanisms needed for a comprehensive security system.

Once recorded in the system, a message can no longer be reclassified. With this feature, an organisation can consistently implement a major policy provision and prevent documents from being declassified and made public. Message tracking keeps the sender of a message constantly informed about its status. The sender finds out exactly when the recipient receives the message and has read it. With all these precautions, messages attain a binding and official character. An organisation can reconstruct its flow of information seamlessly, even months afterwards.

The Crypto Message Server can communicate automatically over multiple media and gains more user trust as a result. If one communication channel such as the IP network fails, an organisation can have its exchange of messages re-routed automatically via satellites, phone line or radio. Redundancy plays a part in the selection of a communication channel but so, too, does prioritisation. With message prioritisation, you can be sure that important messages are given the appropriate priority treatment. You can determine the transmission strategy individually for each of the three priority settings. That means you decide the respective weight assigned to transmission duration and cost.

Special feature

CAG MAIL is a fully self-contained system. Messages cannot be removed from the system electronically. This special feature eliminates the risk of data theft. The operator benefits from the advantages of the new technologies without the disadvantages normally associated with them.

The bottom line

Three factors determine the success of a secure messaging solution.

1. The system must operate according to individual work processes geared to the customers and their security policies, and not vice versa.
2. Steps must be taken to ensure that the secure messaging system can be systematically integrated into an existing communication infrastructure.
3. Simple security management prevents mistakes in daily operations.