



## Consulting Services 13-1: ICT Security Architecture & Concepts



**Information security and the protection of valuable data require a clear-cut architecture and well-defined interfaces. A comprehensive ICT security architecture is the key to minimising information security risks. If optimised, harmonised and standardised across the entire organisation, the architecture holds great promise of helping you to achieve a high level of information security while keeping costs firmly in hand.**

**With the “ICT Security Architecture & Concepts Package” you receive a technical architecture tailored to your organisation’s needs and situation. Important parts of the package are a zone plan for the different security levels in the network and plans for implementing the defined security requirements.**

The ICT security architecture determines the overriding parameters and approaches so that information security can be implemented uniformly and consistently. It provides a foundation for the design, construction and expansion of areas where information security must be considered and does so independently of any given products or manufacturers. The focus is not on systems for processing and saving data, it is on information as an asset worth protecting. This approach to information security defines the parameters that are applicable to all systems and components for saving, processing or transmitting electronic data and is the only way to create a thoroughly consistent and constant degree of information security.

Information security begins with defining the protection required for information within an organisation. Then, possible scenarios are determined along with the risks

resulting from them. Next comes the decision on whether to reduce risks and if so by what means. This is the point at which the “ICT Security Architecture & Concepts Package” enters the scene. Crypto AG creates this architecture based on best practices and then tailors it to your needs.

The ICT Security Architecture & Concepts Package from Crypto AG offers a standardised approach for defining technical requirements that ensure confidentiality, integrity and authenticity as well as availability and traceability. These requirements can be used later in invitations to tender so that all submitted tenders take a uniform approach to information security.

Information security is not a product or a state, it is an ongoing process.

### Key Benefits

- ICT security cost reduction thanks to optimisation, harmonisation and standardisation
- Broad-based and recognised best practice approaches adapted to your needs
- Product and manufacturer-independent technical ICT architecture to meet tough security demands in the network
- Concepts for secure Internet access
- Technical architecture and concepts for a high level of communication security in all common transmission channels
- Strict separation of communication and security components
- Defined security level can be maintained and traced

## Description of service

Crypto AG delivers the expertise and experience for creating an ultra-secure technical architecture to your specification utilising standardised modules. With your information security needs in mind, Crypto AG adapts best practice approaches to your environment and requirements:

- Definition of security zones
- Network security concept
- End-point security concept
- Architecture for secure operation (SOC) and separation from NOC

## Deliverables

The ICT Security Architecture & Concepts Package delivers the following technical concepts:

- The number of zones
- Zone definitions
- Definition and minimum requirements for zone transitions
- Perimeter architecture
- Minimum requirements for client PCs
- Minimum requirements for data storage
- Minimum requirements to be met by the organisation operating the security components

## Details

**Kick-off meeting:** At the kick-off meeting, the procedures are explained to you and the scope of activities and the deadlines are agreed. Your applicable security policy is the determining factor. It indicates the protection your information requires with regard to confidentiality, integrity, authenticity, availability and traceability.

**Zoning:** One key element is the determination of different security zones. Each zone has a different security level. They range from “public”, where data passes over public territory, all the way to “high security”, where the confidential data are saved. A maximum of five zones are defined, and minimal requirements are set for transitions from one zone to the next.

**Network and perimeter:** Network security involves providing appropriate protection to transmitted data to prevent unauthorised access and any manipulation of data by outsiders. Data must be adequately protected, especially in the public zone. Network security refers not only to technical precautions but also to organisational ones.

The perimeter is the transition from an untrustworthy, insecure world such as the Internet to a secure zone.

**End-point security:** End-point security is the overriding concept for security aspects in a client (PC, notebook) or server (storage, file server, database). The end-point is either the interface with the user, where it is determined who accesses the data, or the place where data are saved. All relevant aspects for the end-point are documented and minimum technological and organisational requirements are set.

**SOC architecture:** Finally, a determination is made of which minimum requirements should apply to the operation of the infrastructure. They cover technical measures such as access for administration and component monitoring, a uniform time system, and a central log file memory. Furthermore, they include organisational aspects, such as continuous monitoring of the defined security level. Minimum requirements for roles and responsibilities are also defined in this concept paper.

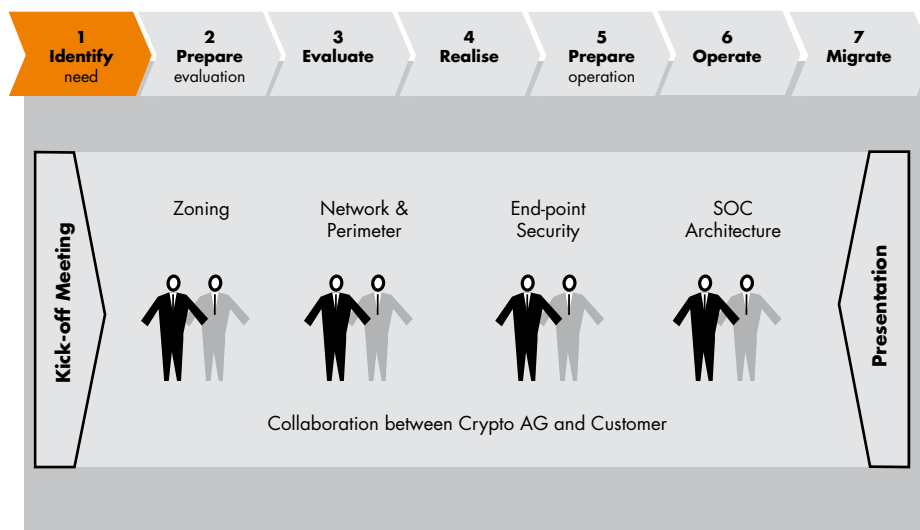
## Glossary

**SOC:** Security Operation Centre

**NOC:** Network Operation Centre

**ICT:** Information and Communication Technology

## Interaction with Crypto AG



## Related services

- 12-1 ICT Security Assessment
- 51-1 ICT Security Process Framework