HAGELIN-CRYPTOS
CRYPTO AG

Voice Encryption System

Security Applications

Voice is our most important means of communication. That is why the telephone is also the most successful communication equipment worldwide. Its speaker recognition is the basis for a personal conversation, often including confidential matters. What started with the switchboard operator listening to calls has developed into sophisticated monitoring stations and legal interception. No doubts that everywhere telephone calls are constantly being monitored.
The new Voice Encryption System from Crypto AG offers secure voice communication using latest VoIP technology. It protects voice calls end-to-end between mobile and fixed telephones against eavesdropping and monitoring from third parties.

Telephone communication is still the key for efficient operation of an organisation. Improved mobile data services have led to a new generation of mobile phones. However, with the technological advances in telephony on one hand, legal interception and governmental eavesdropping systems on the other hand, have improved as well. Today, anyone's mobile phone conversations can be tapped worldwide. Confidential conversations are unknowingly recorded by foreign intelligence services. For normal users that may just be a violation of their privacy, for governmental organisations it constitutes a violation of national secrecy and classification rules and can have severe consequences.

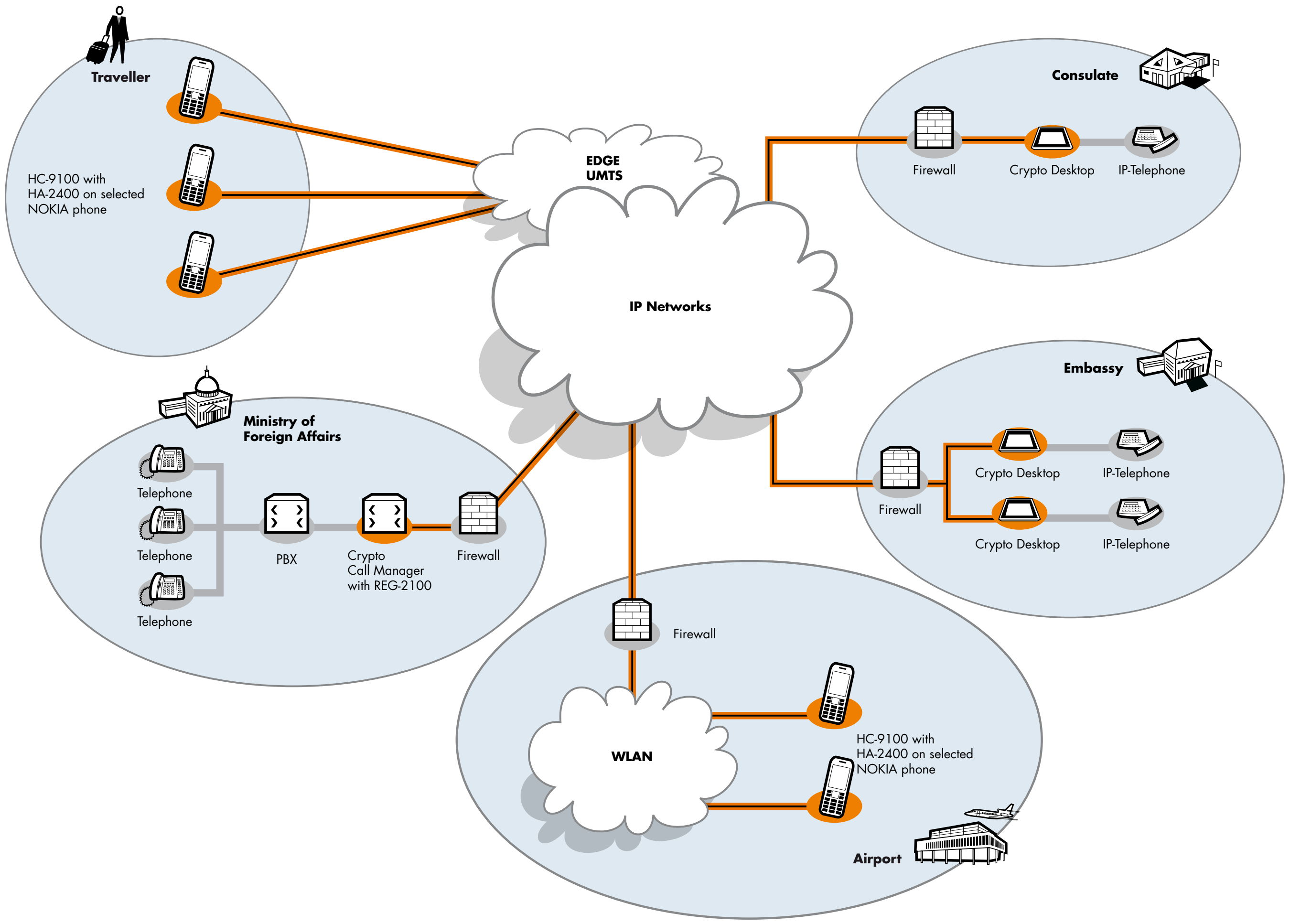
With the Voice Encryption System, Crypto AG has developed a high security solution which protects the confidentiality of your conversations while maintaining your mobility and flexibility.
The system is entirely based on Voice over IP (VoIP).

At the core of the system there is the Crypto Call Manager, which handles the call setup and relaying of the call. The mobile phones (Nokia E-Series with HC-9100 and the Security Application HA-2400) automatically register via a packet data service (EDGE / UMTS or WLAN) and can then be reached by other callers. Desktop VoIP telephones which are connected to a Crypto Desktop HC-9300 with the Security Application HA-2500, register via the fixed IP network.

The Voice Encryption System is an integral solution for highest security of your voice communication.

Key Features

- Highest level of security with hardware based encryption
- Maximum control of the algorithm by the customer thanks to the Crypto Algorithm Architecture
- End-to-end secure calls between mobile phones and fixed telephones
- Red enclave functionality to secure calls in protected office areas
- Superb voice quality and unnoticeable call setup times
- State of the art VoIP technology based on SIP standard
- Hardware encryption platforms for the office and selected Nokia smartphones
- For absolute secrecy: Crypto Call Manager supports encrypted call establishment
- The Crypto Call Manager simultaneously supports WLAN and mobile networks for cost efficiency and redundancy



Network topology/ System description

Similar to the telephone exchange in the legacy telephone system, every VoIP network requires a central infrastructure element, the call manager. To ensure absolute secrecy Crypto AG has developed its own Crypto Call Manager. It not only hides the entire network structure and call establishement but also relayes end-to-end encrypted calls between individual users.
The Crypto Call Manager offers also a unique functionality called Red Enclave Gateway. This functionality offers in a protected area (i.e. DMZ) the possibility to pass a call to a plain VoIP user inside the red enclave.
The system supports stationary office VoIP phones as well as mobile phones accessing the secure voice network through UMTS, EDGE or even WLAN. The VoIP-phone is connected to a Crypto Desktop HC-9300 which does the encryption. In the mobile phones the encryption is performed by a revolutionary hardware in the micro-SD card, the Crypto Mobile HC-9100.
With these system components, all combinations of secured communications end-to-end and end-to-gateway are possible. The unique concept of the Crypto Voice System makes it fully scalable and allows to start as a small system and develop it into a global system.

Crypto Call Manager HA-2100

In the traditional telephone network (PSTN) the telephone operator has been providing the central infrastructure in combination with the possibility of a local PABX. In the IP World, the same situation exists, however the major difference is that the organisation that provides the data lines is not operating the service of a telephone exchange. The shortage of IP addresses has led to concepts such as NAT, NAPT and dynamic IP address usage with the clients receiving an IP address through DHCP (Dynamic Host Configuration Protocol). This technology requires that everybody who wants to run VoIP networks has to establish its own switching-infrastructure, a functionality efficiently and geniously mastered by the Crypto Call Manager.

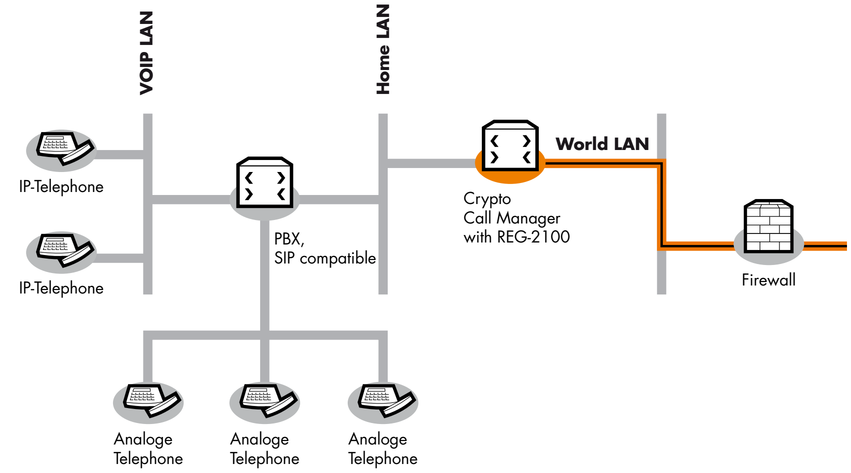
The Crypto Call Manager lists all member units of the network. After registration of the units the Crypto Call Manager is responsible for the call establishment between the "caller" and the "called". This exchange of information is of course encrypted. This unique function hides the network structure and call history from third parties. Once the two parties are connected, they try to send the encrypted voice data directly between each other.

In reality, mobile networks are designed to only allow mobile originated traffic between the mobile and station with a fixed IP address. Modern firewalls or even operator policies do not allow direct IP traffic between mobile phones. To bypass this unwanted network behaviour, the Crypto Call manager provides another vital and unique functionality: It is relaying encrypted voice data – without being able to decipher the traffic.

The Crypto Call Manager HA-2100 is a Security Application running on the HC-9300 platform. Using the same platform for the Crypto Call Manager HA-2100 and Voice Encryption Office HA-2500, as well as other office applications has an other significant advantage:
It facilitates logistics and spare unit management – as there is no need to foresee additional spare hardware.

Red Enclave Voice Gateway REG-2100 (Option to Crypto Call Manager)

In most cases voice communication within the organisation contains sensitive information. Although this is often acceptable to be in clear as long as it is inside the building, once outside it must be secured. For this typical scenario we highly recommend using a Crypto Call Manager with the Red Enclave Voice Gateway option. This application ensures that all outgoing calls from the connected VoIP telephones are encrypted at all times. Important persons equipped with their own encryption unit, will still be able to place end-to-end encrypted call as required – another high security feature.

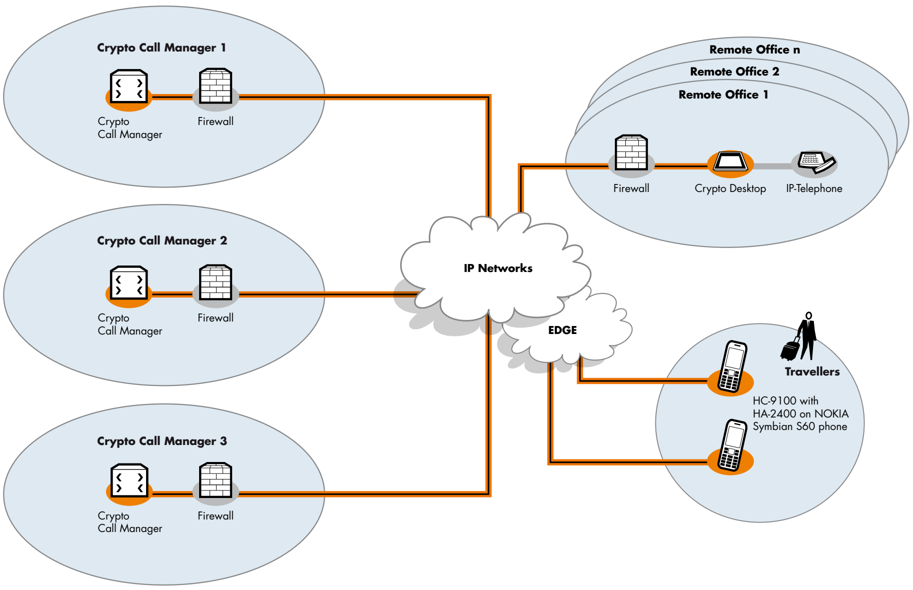


Crypto Call Manager – Redundancy and Load Balancing

The Crypto Call Manager is the core of the system and its availability must be ensured. In order to avoid any single point of failure, bottlenecks or even to avoid complete system failures, the Crypto Call Manager has a unique built-in redundancy and load balancing. This functionality allows scenarios with "Multiple Call Manager Support" in all client Voice Encryption Applications (HA-2400 and HA-2500) – Another major high security feature.

For small networks, using only one Crypto Call Manager is possible but it could lead to a single point of failure. In addition to that the public IP interface usually has some speed limitations as well. This could be a bottleneck if the system grows or in situations with heavy load.

It is therefore better to provide redundancy to eliminate the above shortcomings. At the same time this redundancy automatically also provides load balancing or in case of global distribution even optimises routing delays and even cost.



Voice Encryption Mobile HA-2400

The mobile solution of this system uses a high-end Nokia mobile phone with the Security Application HA-2400. The encryption is done in the smallest high security encryption unit available on the market, the Crypto Mobile HC-9100.
For the network, encrypted voice communication is technically a data communication. As a consequence it requires a data communication through a wireless network. The prerequisite is the availability of an EDGE or UMTS cellular mobile network or WLAN.
The hardware encryption HC-9100 combined with the advantages of VoIP technology provides you with the absolute unique advantages of highest security with unequalled superb voice quality and unnoticeable call setup time – worldwide unique security features.

Voice Encryption Office HA-2500

The stationary solution for Voice Encryption requires the Security Application HA-2500 running on a Crypto Desktop HC-9300. That gives the advantage that you can still use your existing SIP-VoIP phone or a SIP phone of your choice. The concept of the Voice Encryption System protects your long term investment for security independently from the rather short lived products like telephones. The HC-9300 provides high security hardware based encryption and also handles user authentication and login whenever appropriate.

On top of that, the HC-9300 Encryption platform is capable to provide many other office related security applications at the same time such as Fax Encryption or File Encryption – other major high security functions.

Technical Data Crypto Call Manager HA-2100

Prerequisites

- Requires Crypto Desktop HC-9300

Performance

- Up to 500 telephones (mobile or fixed) can be registered at the same time
- Up to 10 simultaneous calls per Crypto Call Manager can be relayed (no encryption / decryption)

Protocols

- SIP PLAIN, SIP Encapsulated for plain call establishment
- SIP Encrypted for secure call establishment provides fully confidential call history and network structure
- Crypto Proprietary protocol for encrypted voice traffic

Redundancy and Load Balancing

- Load balancing and redundancy functionality with multiple Crypto Call managers

Management

- The Crypto Call Manager is responsible for online distribution of the phone book and call manager list

Technical Data Red Enclave Voice Gateway REG-2100

Prerequisites

- Requires Crypto Call Manager HA-2100 with Crypto Desktop HC-9300
- Requires plain VoIP SIP PBX (RFC 3261)

Performance

- Up to 5 simultaneous calls can be encrypted / decrypted when using the red enclave option
- Up to 20 Red Enclave users are supported
- 50, 100 or more Red Enclave users on request

Technical Data Voice Encryption Mobile HA-2400

Prerequisites

- Requires Crypto Mobile HC-9100
- Requires compatible Nokia Phone

Connection management

- Multiple Crypto Call Managers can be installed and referenced in one unit
- "Keep alive" modes: Off, home network only and all networks

Voice quality

- Superb voice quality, supported voice coders:
  - AMR 4.8 - 12.2 kbps, ILBC, G729
- Call establishing time < 3-5 sec

Technical Data Voice Encryption Office HA-2500

Prerequisites

- Requires Crypto Desktop HC-9300
- Requires compatible SIP Phone

Connection management

- Connection a single Crypto Call Manager within it's own network
- Automatic registration with "keep alive"

Voice quality

- Superb voice quality, supported voice coders (depends on connected SIP phone):
  - AMR 4.8 - 12.2 kbps, ILBC, G729
- Call establishing time < 3-5 sec

Cryptography & Security

Algorithm

- Customer specific cipher algorithm HCA-820
- Customer managed profiling of algorithm with variety > 10^{506}
- Built-in high quality true random generator

Keys

- Key length 128 bit or 256 bit
  - Master Communication Keys
  - Communication Keys
- Tamper-proof key storage in encryption platform
- Key Change
  - Master Communication Keys according to their Key Activation Time
- Communication Keys are randomly generated for each session

Encryption Platforms

Crypto Mobile HC-9100

The Security Application HA-2400 for mobile phones requires the Crypto Mobile HC-9100 microSD Card as encryption platform in combination with a compatible NOKIA mobile phone.

Crypto Desktop HC-9300

The Security Applications for the office require the Crypto Desktop HC-9300. For Voice Encryption HA-2500 a suitable SIP capable VoIP phone needs to be connected to the HC-9300 Crypto Desktop.

Third Party Hardware

Nokia Mobile Phone

Not included in Crypto AG's Voice Encryption Mobile Security Application is the mobile phone. Crypto AG verifies the correct function of its application with state of the art high-end Nokia smart phones. Crypto will provied a list of supported mobile phones. This list will be periodicaly updated with latest models.

Standard VoIP Telephone

Not included in Crypto AG's products are the telephones connected to a HC-9300 with the HA-2500 Voice Encryption Application Office. These VoIP telephones must be compatible with the Session Initiation Protocol (SIP). Crypto AG provides a list of tested and recommended phones.