

# CRYPTOMAGAZINE

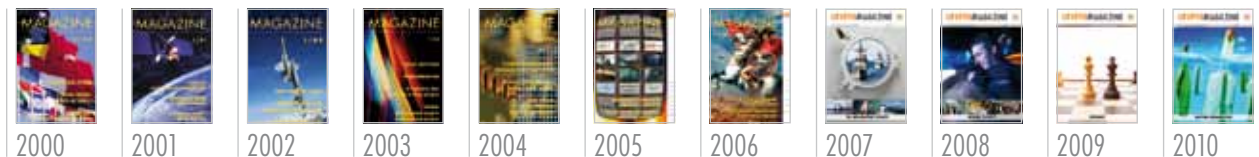
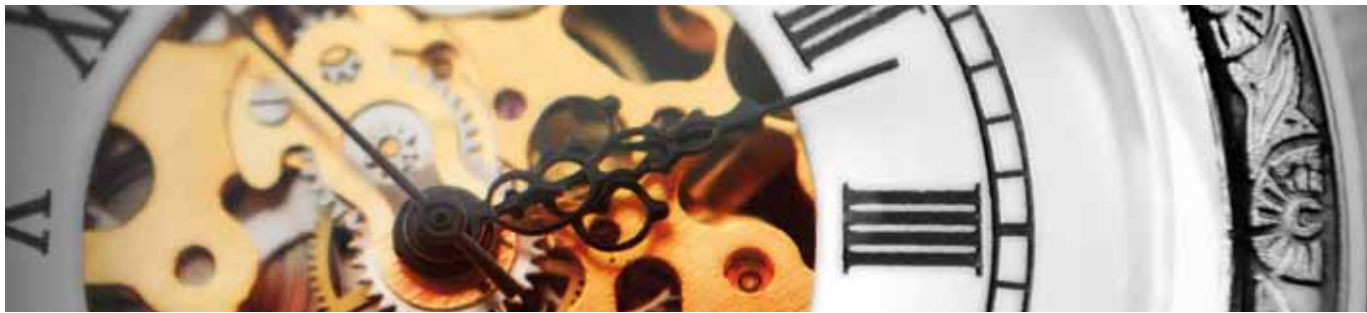


For the customers of Crypto AG, Switzerland

3 ■ 2010



thank you  
10TH ANNIVERSARY OF CRYPTOMAGAZINE



### Dear Reader

The first issue of our CryptoMagazine appeared ten years ago. This anniversary is a welcome opportunity to review not only the business of Crypto AG over the past decade but also the enormous changes that have occurred in important parts of information and communication technology. After all, these changes are ultimately driving us to develop and implement end-to-end security solutions in a globally networked world.

You cannot ascribe every change in living conditions in a globalised world to technology, but its influence on individual lifestyles is obvious. The world of 2010 is no longer the world of 2000. We live in the constant presence of information and many assets that were previously real are now virtual in nature. Most users of modern ICT resources benefit from the tremendous increase in capability their “interfaces” have undergone. Yet we are probably too little aware that the developments behind this progress are unprecedented in human history.

However, this decade of globalisation has not necessarily made the world more peaceful. It has also created new forms of conflict. You could call our age “the age of asymmetric threats”. The potential for danger is increasingly spreading to the structures and processes of civil society. Social structures and processes are under a constant threat from the kind of data misuse inevitably associated with this change, in both civilian and military settings. A company supplying security solutions in this environment logically has to work intensively to cope with main and side effects of this threat.

Safeguarding information security ultimately entails assuming responsibility. In doing so, the security provider cannot focus solely on the primary security solutions. Risks today are simply too cross-sectoral and interconnected. Among other tasks, the security

provider must bear in mind the interplay of different technologies and applications, advising the customer where necessary and pointing out specific practical risks. Of course, customers are free to define and apply their own individual security policy, but project discussions usually open the way to considering other problem areas.

The much-cited phenomenon of global networking is also transforming the technological base in entirely new dimensions. Given this high degree of complexity, a company handling information security needs broad expertise in network technology. New protocols and transport technologies create enormous possibilities but also require security solutions to be implemented with greater effort and care. New customer needs, such as the increasing need for mobile work with remote data access, have to be met within a dynamic, global topology without creating additional risks.

These changes have also shaped the content of previous issues of CryptoMagazine. The focus has shifted specifically to issues of communication technologies and the customer scenarios associated with them. We have therefore begun to concentrate on the way in which our customers work.

This anniversary issue of the magazine has therefore turned into something of a historical account of the technological and social developments over the past ten years. Of course, the magazine has undergone constant change as a medium, too. The content it covers today is broader. We also like moving beyond actual security issues into areas connected to security in interesting ways. Obvious changes have occurred graphically. The layout has become leaner, the colours more differentiating and the graphics simpler.

Readers regularly send us stimulating feedback, which has been an important source of motivation for us. That is also how we came upon the idea of publishing Russian and Arabic issues along with our original four language versions German, English, French and Spanish.

We invite you to send in your opinions on individual articles or the magazine as a whole. For instance, feel free to e-mail us at the following address: [redaktion@crypto.ch](mailto:redaktion@crypto.ch)



Giuliano Otth

President and Chief Executive Officer

4	New Customer Centre for Crypto AG <b>A real gain technologically, visually and functionally</b>	INHOUSE
7	Old and new types of ICT threats <b>“Evil stems not from technology but from those who misuse it”</b>	SECURITY AWARENESS
10	Interview with Felix Bollmann, Director of Swiss Solidarity <b>Fund-raising for flexible disaster relief</b>	INTERVIEW
12	Security Services & Solutions as a new business area <b>All services from a single source</b>	SOLUTIONS & SERVICES
14	Keeping confidential information confidential <b>Stationary and mobile voice encryption</b>	TECHNOLOGY
16	10 Gigabit Ethernet Encryption Multipoint <b>Ethernet Multipoint for growing data streams</b>	TECHNOLOGY
19	The quality management system generates trust <b>Crypto AG certified to ISO 9001 for 25 years</b>	INHOUSE
20	Stationary, mobile, portable, on the high seas ... <b>The right encryption platform for each environment</b>	FOCUS
22	P3I: Pre-Planned Product Improvement with the HC-2650 <b>Are modems the “better operators”?</b>	TECHNOLOGY

**IMPRINT**

Published three times a year **Print run** 6000 (German, English, French, Spanish, Russian, Arabic) **Publisher** Crypto AG, P.O. Box 460, 6301 Zug (Switzerland), [www.crypto.ch](http://www.crypto.ch) **Editor-in-chief** Casha Frigo Schmidiger, Crypto AG, Tel. +41 41 749 77 81, Fax +41 41 741 22 72, E-mail [casha.frigo@crypto.ch](mailto:casha.frigo@crypto.ch) **Design/Typesetting** illugraphic, Sonhalde 3, 6332 Hagendorn (Switzerland), [www.illugraphic.ch](http://www.illugraphic.ch) **Translation** Apostroph AG, Töpferstrasse 5, P.O. Box, 6000 Luzern 6 (Switzerland), [www.apostroph.ch](http://www.apostroph.ch) **Printing** Ennetsee AG, Bösch 35, 6331 Hünenberg (Switzerland) **Reproduction** Free of charge with the consent of the editorial office, courtesy copies requested. All rights reserved Crypto AG **Illustrations** Crypto AG: p. 4, 5, 6, 13, 14, 15, 18, 20, 21, 22, 23 · Glückskette: p. 11 · illugraphic: p. 24 · Imagepoint: p. 7, 16 · Shutterstock: cover, p. 2, 8, 9, 12, 17

NEW CUSTOMER CENTRE FOR CRYPTO AG

# A REAL GAIN TECHNOLOGICALLY, VISUALLY AND FUNCTIONALLY

The first impression is breathtaking. A spacious lounge extends over an area of 800 square metres and features a reception area and a variety of seating. The counter at the front of the reception area seems to “float”. The floor is a warm and shiny grey Swiss quartzite and the high glass windows reflect the water canal outside. The stylish modern lounge furniture is especially attractive on the boardwalk in the outside loggia. The building is surrounded by ginkgoes, the Chinese tree symbolising wisdom, fertility and resilience. The new Crypto AG Customer Centre represents the qualities for which the company stands: competence and high tech, style and modernism.

*By Casha Frigo Schmidiger, Publicist*



## The premises of Crypto AG from 1952 to the present

The beginnings of Crypto AG can be traced back to 15 May 1952. At that time, the Swedish cryptologist and industrialist Boris Hagelin could already look back on a successful career as an inventor and businessman. He moved to Switzerland in 1948 and also shifted parts of his company A.B. Cryptoteknik from Stockholm to Zug. The pool of highly qualified engineers and technicians in the area had appealed to him. Like Hewlett Packard, Crypto AG initially had all the charm of a garage business. Originally located in a small Swiss chalet on Weinbergstrasse in Zug, the company grew quickly and the chalet became increasingly cramped. In 1966 Crypto AG moved to its current site in the town of Steinhausen in the canton of Zug.

Crypto AG put up a new building on a green meadow and subsequently built several extensions to the facility. Thus, the main building was soon joined by additional buildings such as the training centre, the production centre (“Shedhalle”) and the cafeteria building. In the 1980s, the main wing underwent a comprehensive

makeover involving a restoration of the building envelope.

After the turn of the millennium the structures began hitting the limits of their capacity, both in accommodating employees and increasingly in offering a representative area for receiving guests. Crypto AG is a competent and modern provider of high-tech systems and products whose every activity revolves around its customers, and it wants to express that in the external image it projects. So, in 2005, it was decided to expand and renovate existing building facilities to create a customer centre worthy of a supplier of top technologies.

## Transparency and authenticity

According to CEO Giuliano Otth, transparency was a central goal in planning. The new building is designed to meet high representational standards visually and to express openness as well as a sense of style and class. The choice of material shows the company to be modern and cosmopolitan, yet strongly rooted locally. The floor and walls in the new customer centre are made of Vals quartzite, a high-grade natural Swiss stone



### The 2000-year history of cryptography

The museum was also re-housed. The first text encryption devices Boris Hagelin built in 1935 are neatly displayed in glass cases along with the army version of the world-famous Enigma machine used by the German “Wehrmacht”. The exhibition also provides an overview of encryption methods from Julius Caesar to Maria Stuart and beyond to ultra-modern encryption products of the present day. ■



synonymous with constancy and stability. With our choice of wood in the outdoor lounge, and in particular with the large water-covered areas around the new building, we pay tribute to our customers and guests, who come from the widest variety of cultures.

---

*The products and services of Crypto AG are seen to even greater advantage in the modern showroom.*

---

Whenever customers come to Crypto AG, the company presents its information security systems, products and services as a central aspect of the visit. The showrooms were previously housed in big self-contained rooms. Now Crypto AG can demonstrate all its solutions in an expansive and elegant space that is bright and cheerful with ample room for everything.

### Ginkgo biloba

The Ginkgo (*Ginkgo biloba*, also known as Maidenhair Tree) has its origins in East Asia, where it is cultivated for its seeds or as a temple tree. Dutch seafarers first brought it back from Japan to Europe, where it has been appreciated as an ornamental tree ever since 1730. It is considered a “living fossil” because it is the only existing representative of the Ginkgophytes, an otherwise extinct order of Spermatophytes or seed plants.

It is considered a miracle tree because of its unique botanical traits and unusual origin. China was medically in the forefront, having used this tree’s bark, leaves and fruits for medical treatments ever since the 11th century. In recent times, the European cosmetics industry has also starting incorporating various versions of Ginkgo extract as an ingredient in cosmetics and body care products.

The fascinating history of the Ginkgo and its brilliant prospects for the future (thanks to its resistance to pest infestation and its undemanding nature) have made the Ginkgo an important symbol for today’s world. It is regarded as a global tree of strength and hope. Many cultures honour the Ginkgo as a symbol of longevity, fertility, friendship, adaptability and invincibility. It is not rare for these huge trees to live for 1000 years or more.

A story from Hiroshima has done much to enhance the modern mythology of the Ginkgo. A temple tree went up in flames when the atomic bomb exploded in 1945. Yet, that same year, it began to revive and sprout leaves.

Source: Wikipedia, the free encyclopaedia





## INTERVIEW WITH CEO GIULIANO OTTH

### *What do you consider the highlight of the new building?*

The exterior now matches the interior and corresponds to the image of Crypto AG as a high-tech company. In terms of style, I like the way Swiss elements such as the Vals stone floor harmonise with international details alluding to our customers.

### *How will customers benefit from the new Customer Centre?*

The new facility has six fully air-conditioned conference rooms with the latest in presentation equipment, all operable from user-friendly control panels. That means we can respond more effectively to our customers and their needs, even during presentations. As a result, meetings have a completely different impact. Most of the rooms are equipped with a WLAN-based network for our guests and have TV outlets as well as outlets for laptops. During breaks, people can relax with a coffee in the reception area or the outdoor lounge. With the larger number of conference rooms, we can also receive and host several delegations at the same time. In addition, the Auditorium Maximum seats over 200 and is ideal for seminars and training sessions.

---

*“The new facility allows us to respond more fully to our customer’s needs, even during presentations.”*

---

The presentations of our products and services to our customers will be even more effective in the new showroom because we have enhanced equipment and far more space. We are proud of the systems and facilities we have created specifically for customers, such as the prayer room and areas where customers can withdraw.

### *How is security handled in the new facility physically, organisationally and logically?*

I would like to answer this question at some length. Only a business partner who is absolutely trustworthy can provide security. It is no coincidence that Crypto AG has become this partner for the most demanding customers around the world. For many of our customers, the deciding factor was and continues to be that we are an independent Swiss company. Our research, development and production facility in Zug with its 500 employees lays a solid foundation for business.

Our new Customer Centre itself now provides security, as you will see for yourself on your next visit to our company. Customers remain in a zone specially designed for them. No one can enter or leave this area without authorisation. Customers have everything they could possibly want here, information plus peace and quiet.

### *Where will Crypto AG create the additional offices you mentioned at the outset of the interview?*

New office facilities will be installed where the new building meets the old, in the former reception area. Staff from Production Management will work there. Currently they are temporarily housed in a container on our business premises. They are great sports about this, in the truest sense of the word. This transitional housing was first used for the UEFA EURO 2008 Football Tournament in Switzerland.

### *Glass dominates the overall appearance of the structure. What impact does this have on the energy situation?*

The windows are of special shatter-proof glass in three layers. Appropriate shades for privacy are naturally also included. One-third of the power needed for air-conditioning and heating the building is drawn from an earth-coupled heat exchanger fed from groundwater and two-thirds are covered by natural gas instead of oil.

### *When is the official opening of the buildings?*

The new facility will be opened at the end of 2010 and the additional premises in mid-2011. ■

## OLD AND NEW TYPES OF ICT THREATS

# “EVIL STEMS NOT FROM TECHNOLOGY BUT FROM THOSE WHO MISUSE IT”

By Rudolf Stirnimann, Customer Segment Manager

*Quote from Jacques Yves Cousteau (1910-1997),  
French naval officer and marine researcher.*

Alongside the Internet and real estate bubbles, Harry Potter, the iPhone and spectacular buildings like the Burj Khalifa in Dubai or the Bird's Nest in Beijing, the first decade of the 21st century has produced one thing in particular: a rapidly increasing global interconnection of data networks and a growing threat for data and information associated with that interconnection. Hand in hand with technological progress, interlopers have been launching increasingly effective attacks in order to access sensitive data belonging to others. Existing processes are constantly being further developed, automated and adapted to the latest technology. You once needed a whole team to tap a single phone line. Team members would have headphones on round the clock, monitoring the line and recording and writing down what was said in the calls. Today, with digitised switchboards, one computer can automatically handle all that for any number of lines for phone calls and fax transmissions.

Global networking continues to advance. ICT infrastructure is being extended into our homes and into the most remote corners of the world. Formerly separate networks are increasingly linked and virtually merging into one. Years ago, people were amazed that a microwave link could be used for transmitting phone, TV and data simultaneously. Today these services are delivered on a single line all the way into our homes or offices. As the networks merge, the distinctions between them blur and monitoring becomes more difficult. Weak points become more than mere local problems of sub-networks: they endanger the entire network.

### **Convergence: a blessing or a curse?**

The current trend towards the convergence of technologies means that Ethernet is winning out as a technology at Layer 2 (based on the OSI model) and IP (Internet Protocol) at Layer 3. Networking is ever more continuous from end-to-end while dangers can move and spread with increasing ease over and throughout the areas of the network. Any gains in consistency, efficiency and costs must be juxtaposed at a greater total risk with respect to information security.

The lurking dangers are as varied in nature as the networks are tightly intermeshed. Of course, entire computer systems can be paralysed by fire, flooding, earthquakes, lightning or a power failure.

The availability of information is naturally as important as its confidentiality, integrity and authenticity. When a big data network fails, all the services using that network also come to a grinding halt. For instance, an organisation may obtain its land line, mobile phone, fax and IP services from the same provider and that provider may route all these services over one and the same network. If so, the organisation has a typical “single point of failure”. That means: if the provider's network fails for any reason, the organisation has no functioning services – it has neither e-mail nor fax nor phone.





With the convergence of technologies, intruders can re-route even more data and analyse it with greater efficiency. Data collectors in the Internet are not confined to hackers, terrorists and criminals. They also include civil servants working on behalf of their government. Certain countries do not stop at merely collecting data. They try to gain control of as many computers and network infrastructures as possible to obtain the latest information on sensitive projects. They can evaluate this data for their own ends or, if need be, block certain projects as they please.

According to the Kiel Institute for the World Economy (IfW), Internet crime is the fastest-growing sector of international criminal activity. This finding is substantiated by current figures from the United States. Last year, Internet crime there caused losses of USD 560 million (EUR 440 million). The year before that, the figure was just USD 265 million (EUR 208 million).

### **Commercial off-the-shelf goods**

Another problem is the use of commercial off-the-shelf goods (COTS goods). Politicians are ordering many public institutions, including defence ministries, to cut costs. To comply, yet modernise at the same time, these institutions may cease purchasing expensive special solutions or military products and rely on less expensive COTS goods instead. With a simple set of communication hardware and software you have to be sure it can also be maintained using standard products and can communicate with other equipment. This fact can be exploited, as an incident in December 2009 shows. According to Computerworld, Afghan rebels used Sky-Grabber, a program costing USD 26, to intercept and record video signals from the American unmanned aircraft Predator with a notebook. This was only possible because standard formats were used for signal transmission and operators dispensed with signal encryption – either to economise or out of negligence.

### **Security policy and zone system as an effective countermeasure**

The bigger an organisation is, the more complex will be the design of its infrastructure and the more difficult that infrastructure will be to monitor and protect against potential attacks and manipulations.

The security policy of the organisation is the point of departure for each protective measure. Based on this policy, an organisation regularly reviews physical, organisational and logical aspects of security to detect any gaps, shortcomings or areas requiring improvement. Physical security controls access to an organisation, for instance using keys or biometric checkpoints. Organisational security is provided by the organisational structure and the targeted dispensing of information within an organisation (need-to-know principle). Logical security, for its part, is put in place with cryptography.

One recognised way of increasing security is to create multiple lines of defence, to put multiple barriers or protective mechanisms in place one behind the other. This method is highly effective, especially if it covers all three areas mentioned above. For instance, people can access certain data only from a specific room, access to which is monitored. Furthermore, people need a password and a specific piece of hardware (e.g. an encryption unit) to read the data.

Not all information is equally deserving of protection, so that not all of it requires these protective measures. This is why many organisations classify documents. The resulting zone system provides for different sectors with protective measures of varying stringency within an entity, based on the confidentiality of the information. The zone system is applied at the physical and logical level but also pertains to organisational security.

A bank is a good example. Diamonds and currency reserves are kept in a safe behind several security doors. The only way the safe can be opened is if the director and the head cashier open it jointly. The controls are less strict in the main hall of the bank. There, anyone can walk in as long as they are properly dressed and do not hold the doorman's eyes too long. Cashiers do not check anyone's identity until they want to withdraw cash. Then they also check whether the person is even authorised to withdraw money.

People also use this zone system in ICT infrastructure. There, too, a distinction is made between public, restricted and internal areas. Your provider's website is certainly public. You need no password to enter it. And you do not have to identify yourself with your e-mail address and password until you want to download e-mails. Most people are not even aware of this happening because their e-mail program takes care of everything for them.

### **People also need protection**

Information security pertains not only to digital data and the underlying information. Behind that information are objective assets and, not least, people who deserve protection. Information security is fundamental to the security of a government or society. Our efforts to demand and promote security must therefore be as relentless as those for achieving road safety. As in road safety, we must continually monitor and improve information security; as technology continues to advance and evolve, so do the threats to information security and its methods. ■



INTERVIEW WITH FELIX BOLLMANN, DIRECTOR OF SWISS SOLIDARITY

# FUND-RAISING FOR FLEXIBLE DISASTER RELIEF

**Swiss Solidarity is a humanitarian platform sponsored by the Swiss Broadcasting Corporation (marketed as SRG SSR idée suisse) with the aim of displaying solidarity and collecting donations. The organisation conducts highly successful national collection campaigns in response to major disasters such as the earthquake in Haiti or the worst flooding in a century in Pakistan. It is highly respected throughout Switzerland.**

*By Casha Frigo Schmidiger, Publicist*

*What does it entail to conduct these campaigns? What must you do to get a campaign up and running?*

With each disaster, no matter how extensive, we investigate how Swiss Solidarity might be able to help. If there is a possibility for us to help in the affected regions, we automatically take action. The possible scope of relief, access to images in the area, emotions stirred up by the disaster etc. are the factors that determine how we conduct the campaign. For instance, it is difficult to conduct a campaign after an event in countries like China or the United States because their authorities refuse to cooperate with Swiss NGOs. A decision is made in a matter of hours, followed by a corresponding media release. Newspaper ads and commercials in which we urge people to demonstrate their solidarity require a lead time of at least 24 hours. Organising one fundraising day takes four to five working days. During that period, we set up switchboards, mobilise 600 telephone operators and coordinate the activities of partners such as SRG SSR idée suisse, Swisscom or the Swiss Post Office.

*What additional tasks does your organisation perform?*

Swiss Solidarity manages the collected cash donations, analyses the projects submitted by the 31 Swiss relief organisations with which we cooperate as partners, and decides which projects to support. After a decision has been made, the foundation assists and supervises these projects and evaluates the relief provided. We apply our findings to improve our system of cooperation with our partner organisations and our own standards and processes. In project financing, we follow a budget plan and gear ourselves to the results already achieved.

*How significant is Swiss Solidarity in the global concert of cooperation among relief organisations? Many tasks had to be performed to help Pakistan cope with its catastrophic floods, for instance. How are the tasks divided among the individual organisations in cases like this?*

Swiss Solidarity does not provide direct assistance.

Instead, we define an intervention strategy with appropriate key parameters for the relief effort. In the case of Pakistan, such aid is provided by organisations with years of experience in this country. We do not work with new organisations. Swiss Solidarity respects and honours the build-up of special skills in the corresponding organisations with a certification-based acceptance system for the organisations with which we collaborate.

---

*Swiss Solidarity does not provide direct assistance. This relief is provided by organisations with years of experience in the given country.*

---

*In the event of a natural disaster, how do you ensure that the local relief organisations receive the knowledge and advance information they need?*

We use a diversity of information sources and close contacts with our approved partners, the local, international and Swiss media and specialised media (e.g. Reuters, Reliefweb etc.). Swiss Solidarity staff and/or specialists with whom we collaborate are on site at important times as a project unfolds. To broaden our perspective, we also request international consultants to draw up expert opinions.

*Natural disasters always take on “unbelievable dimensions”. One need only think of Haiti, Russia or Pakistan. Does this fact have ramifications for the work of Swiss Solidarity?*

In the first decade of the millennium, we staged a number of record fund-raising campaigns. Two were for disasters in Switzerland (exceptional precipitation in Valais [Gondo], Ticino and the neighbouring regions in 2000: CHF 74 million; storms and floods in Central Switzerland, the Bernese Highlands and the Grisons in 2005: CHF 50 million). The collection after the tsunami in 2004 generated record donations of CHF 227 million. The collection taken five years later after the earthquake in Haiti also brought in a record CHF 65 million. The work has not changed but it extends over longer

and longer periods because reconstruction, a special strength of Swiss aid, usually takes several years (five to six years).

*What significance is attributed to secure information transmission in regions with an ecological or humanitarian crisis? We are referring here to the flow of information, the authenticity of the information and the non-availability of the information to third parties.*

Swiss Solidarity has a communication policy based essentially on candour and transparency at every level. This approach is fundamental to our trustworthiness for donors and relief recipients alike, as well as for the aid agencies at the disaster site. It follows that we make no provisions for special encryption or a secrecy system. That does not apply to the names of people making contributions and donations. We never divulge those names to outsiders nor do we use them commercially. We never ask a donor to make further donations of any kind. In addition, our partner enterprises take special precautions for financial transactions, particularly credit cards.

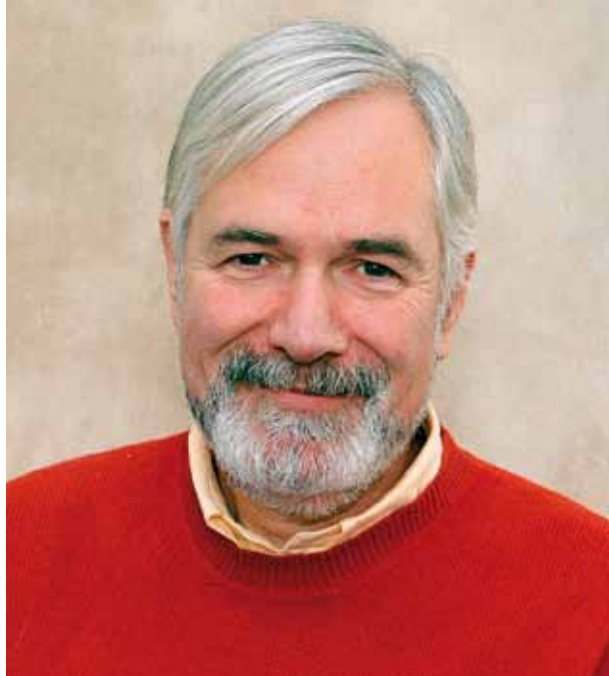
*Does Swiss Solidarity protect transmitted data?*

No, as I said before we do not consider that necessary.

*What ramifications does it have if data in a crisis area gets into the wrong hands?*

Besides personal data and each personal contact, our transparency regarding contacts between Switzerland and the relief sites means fewer questions and fewer dangers than any attempt at encryption.

*Thank you very much for your comments,  
Mr Bollmann!*



### CHAÎNE DU BONHEUR, GLÜCKSKETTE, CATENA DELLA SOLIDARIETÀ, SWISS SOLIDARITY

- Humanitarian platform for solidarity and collections in Switzerland
- Launched in 1946 when Radio Suisse Romande à Lausanne called for donations
- Has been a separate foundation since 1983
- Collaborates with SRG SSR idée suisse
- Headquarters in Geneva, offices in Bern and Lugano
- 19 staff members
- Donations collected since 1983: CHF 1.1 billion (USD 1 billion)
- Current portfolio: 220 projects, 43 countries, 31 supported organisations
- Disaster relief and support of humanitarian aid projects, child relief projects and social aid for individuals

[www.bonheur.ch](http://www.bonheur.ch)

[www.glueckskette.ch](http://www.glueckskette.ch)

[www.swiss-solidarity.org](http://www.swiss-solidarity.org)



## SECURITY SERVICES & SOLUTIONS AS A NEW BUSINESS AREA

# ALL SERVICES FROM A SINGLE SOURCE

**Civilian and military authorities worldwide use encryption technologies from Crypto AG to protect communication between individuals and organisations. Data volumes are growing, as is the complexity of the surrounding infrastructure. Users have to conduct comprehensive assessments to ensure smooth performance. However, classical security systems often reach their limits in cases demanding top security with no compromises.**

*By Casha Frigo Schmidiger, Publicist*

This is exactly where Services & Solutions, a business area at Crypto AG, steps into the picture. A high-calibre team of security experts can help our customers to plan, create and implement complete systems and solutions complying with the most stringent security standards. These experts intentionally expand classical implementation methods by adding methods and solutions which they specially develop to achieve the highest possible security within the overall system. The range on offer extends from various consulting services to suggestions for specific solutions. The rising demand for services and complete security solutions has motivated Crypto AG to group these items into a single business area called Security Services & Solutions under a new management. The advantage for our customers is that we can concentrate on their needs and provide them with our services even more quickly and flexibly.

After all, management is so much more complex, networked and demanding than it was ten years ago. Managers have to take decisions under time pressure and quickly issue orders that are understandable and clear-cut. At the same time, people are less tolerant when it comes to accepting management mistakes. In short, managers today have to perform like professional athletes. Even that is not enough. Managers face growing threats from the ICT environment. Digital technology brings immense advantages but, at the same time, dangers of equal enormity. Those attacking digital infrastructure are often one step ahead of those defending it. Information security consequently becomes a key task.

### **Information security as an ongoing process**

Managers need to concentrate on their core responsibilities and also communicate quickly and securely with their superiors and employees. For them to do so, a company must be able to depend fully on its security partner. Crypto AG is a global leader in information security with years of experience in the field. The company has a superb range of security technology, encryption systems, information security services and complete information security solutions. With this line-up, Crypto AG ensures that customers at civilian

and military authorities can concentrate on their established areas of activity, secure in the knowledge that their flow of information is protected.

The implementation of information security has long involved much more than just installing hardware. It covers an **array of services** extending from status-quo analysis and tamper-proof implementation of high security to lifecycle management and the empowerment of customers to operate installed solutions safely and autonomously in the long run. Information security is implemented as a logical project process that integrates all security services throughout the project.

### **From analysis to after-sales support and training**

The object of Security Services & Solutions, the new business area at Crypto AG, is to support the security manager in achieving an ideal interplay of people, systems and processes. Crypto AG's familiar and relentless call for top security is applied consistently throughout. This new business area, in turn, is based on five main pillars: **Consulting Services, Implementation Services, Education Services, Operational Support Services and Lifecycle Management Services.** It is important to note in this context that classical approaches to the implementation and operation of security solutions often reach their limits in cases demanding absolute



top security. Crypto AG can address these issues with its self-developed approaches and then discuss appropriate solutions with its customers. With security experts from **Crypto Consulting Services**, customers can bring expert knowledge into their company. Crypto AG's security experts will also check whether the organisational processes and their technical and operational implementation unintentionally allow data theft or unauthorised access to data and whether the processes are professionally planned. With **Crypto Implementation Services** customers can ensure that their security system is implemented in heterogeneous environments applying maximum security standards in line with their objectives. The Crypto Academy bears the "Premium Class" mark of quality from the International Training Centre Institute. The Academy takes a holistic approach to training as summed up in **Crypto Education Services**. With these services, customers can counter the mounting threat in an informed and proactive way while also making effective use of Crypto AG products. "A system is secure if used seamlessly from end to end." That is the motto of **Crypto Operational Support Services**. These services give all-round support for all installed products and solutions. **Lifecycle Management Services** constitute an important part of this sub-area. There, Crypto AG experts suggest recommendations and approaches for extending the life of systems wherever possible.

#### **Successful implementation as illustrated by an e-government solution with a three-zone security system**

We would like to share a success story that illustrates the success of Crypto Services. The government of a relatively small country commissioned Crypto AG to develop an e-government security solution. The key ministries and parliamentary services were to be protected in a joint ICT infrastructure using a secure Intranet. In addition, there were to be three information classification levels: "top secret", "secret" and "confidential", each with separate encryption solutions. The requirements were tough. Crypto AG was contracted to develop a full-coverage security architecture for the ICT infrastructure of the government. As a turnkey provider, Crypto AG was responsible for planning, creating, and implementing a security solution and for transferring the necessary expertise to the customer. Another objective involved protecting the legacy Ethernet backbone between the organisations with a maximum security encryption solution and defining various security and information classification levels and security zones. In the process, Crypto AG implemented 1-10 Gigabit Ethernet encryption units at all external links. End-to-end encryption for top secret applications was based on IP VPN encryption. All security management functions were grouped together in a centralised security operation centre (SOC). The contract also entailed

#### **UWE KISSMANN, SENIOR VICE PRESIDENT SECURITY SERVICES & SOLUTIONS**

Uwe Kissmann is head of Security Services & Solutions. He has more than 15 years of experience in the fields of information security engineering, consulting, and sales and marketing. Having worked for a number of years as a security executive in a multinational setting, he is keenly aware of the theoretical and operational challenges specific to this task. Just before joining Crypto AG, he managed the security services, consulting and implementation business of a major international IT enterprise. Uwe Kissmann is also a lecturer on information security at various Swiss universities.



implementing e-business and e-citizens functions, so Crypto AG assumed responsibility for training these external technology suppliers, too. Drawing on its comprehensive range of expertise in consulting and implementation, Crypto AG provided the government of this small nation with a fully functional e-government system. The government ministries can now engage in protected data exchange with each other and citizens can communicate risk-free with the authorities.

With our services, we furnish our customers with the expertise they need to concentrate on their core responsibilities. And we also give them the option of placing all other confidential issues in our trustworthy hands. ■

KEEPING CONFIDENTIAL INFORMATION CONFIDENTIAL

# STATIONARY AND MOBILE VOICE ENCRYPTION

**Spoken language is our most important means of communication. The written word lacks directness and emotions. That is why most of us still prefer phoning in many cases, despite the availability of e-mail and text messaging.**

*By Rudolf Stirnimann, Customer Segment Manager*

In professional life, people still make phone calls when they need an immediate answer or want to clarify a matter in dialogue with someone else. If you place an order over the phone you can verify at the same time whether the other person has understood everything correctly.

However, a phone call is also relatively easy to tap. It does not really matter whether you are calling over the traditional analogue telephone network PSTN (Public Switched Telephone Network) or digitally with VoIP (Voice over Internet Protocol). In either case, tapping the call is child's play. All it takes is a minimum of expertise and the right computer program. Modern tapping systems start and stop fully automatically and have whatever memory capacity desired. Recordings of calls can be forwarded over the network to any computer.

Phoning is direct communication and a call can quickly turn to confidential subjects. That is why it must be a top priority to protect against unauthorised eavesdropping.

## **Crypto AG protects Voice over IP ...**

IP telephony is fast gaining ground on traditional analogue telephony. The inexpensive rates for IP telephony have long been attracting more than just young people and computer freaks. Data networks have expanded worldwide, triggering an associated increase in performance capacity. IP telephony has seen huge improvements in voice quality and reliability ever since and is increasingly winning acceptance. It is even available for mobile phones.

We want to protect confidential calls. With the new Voice System HA-2000 from Crypto AG, you can phone within the IP network confidentially (and inexpensively). The system is fully based on VoIP and SIP (Session Initiation Protocol) and has a central switching and connection unit called the Crypto Call Manager. Standard commercial SIP phones serve as the terminals. They are hooked up to the office platform Crypto Desktop HC-9300 where the security application Voice Encryption Office HA-2500 runs.

## **... and mobile telephony**

Making calls on mobile phones is a matter of course for everyone these days.

Voice Encryption Mobile HA-2400 is the security application that enables you to conduct highly confidential calls on your mobile phone in top sound quality, absolutely tap-proof. As is customary with Crypto AG, the encryption takes place in physically protected (tamper-proof) hardware specially designed for the purpose. It takes the form of a microSD card and contains everything needed for encryption, including a secure data memory with a capacity of about 1 GB. Nokia sets incorporating the Symbian S60 operating system are compatible mobile phones for this application. Calls are transmitted over EDGE, UMTS or, as the better priced option, WLAN networks. With these technologies, people can register with the Crypto Call Manager, which then establishes the connection.

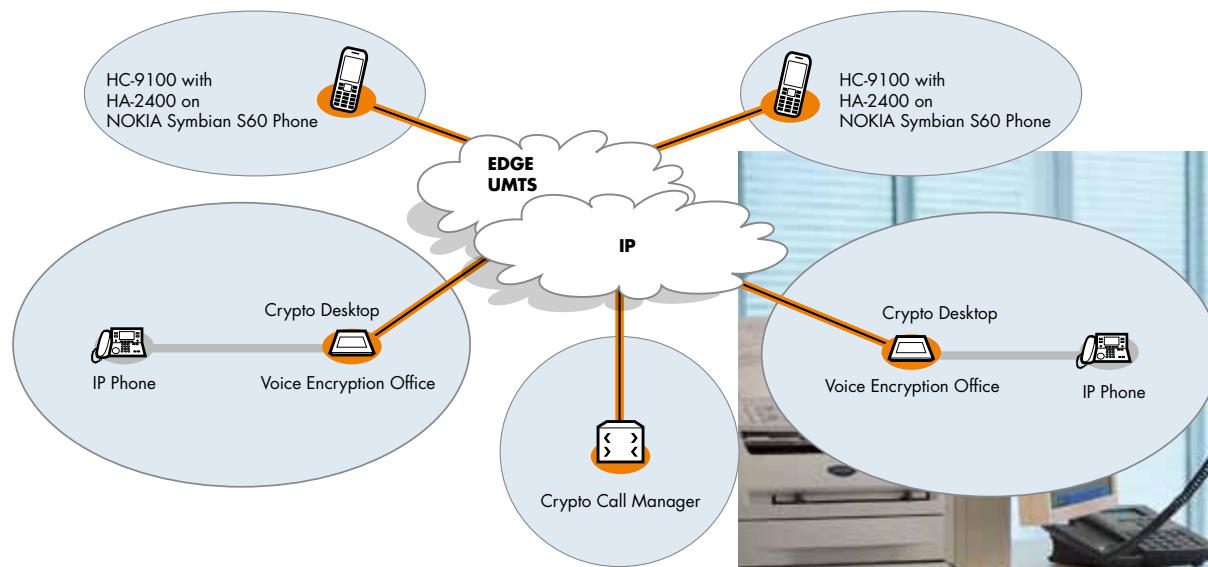
## **The main IP switchboard: the Crypto Call Manager**

In the traditional PSTN telephone network, switching was automated with mechanical systems. Today, this



The office platform Crypto Desktop HC-9300 is suitable for voice, fax, file encryption and data transmission (e-mail).

process is electronic and digital. The IP world also needs an infrastructure to establish connections. However, IP network providers furnish no services for switching calls. If you want to operate a VoIP network in this environment, you need an infrastructure to manage the current IP addresses of subscribers and, where necessary, to establish a connection between the party calling and the party being called. As soon as the



connection is established, only encrypted VoIP packets are sent back and forth. Like a conventional main switchboard, the Crypto Call Manager not only establishes the connection but also forwards the encrypted VoIP packets as long as the call lasts. A single Crypto Call Manager can concurrently connect and maintain up to ten calls. The Crypto Call Manager HA-2100 is a security application also running on the Crypto Desktop HC-9300.

#### **Voice encryption in the VIP Office**

Absolute top security is needed in a single office abroad or in the office of a VIP. In these cases, the encryption unit must be in the same room as the phone. The Crypto Desktop HC-9300 with Voice Encryption Office HA-2500 serves as the encryption unit in this case. A standard commercial SIP phone can be used as the terminal on the non-encrypted end. In other words, customers can select a phone of their choice.

As a result, long-term investments in security (HC-9300 and HA-2500) are no longer linked to the rather short-term investments in the actual phone, a lifestyle product. The HC-9300 contains the hardware for encryption and for the phone directory and address book in a protected memory area. Where required, it authenticates users during log-in, based on passwords.

The Voice Encryption System utilises established IP telephony. If you combine this system with the Crypto Desktop HC-9300 as a multifunctional encryption and communication platform, you are making a long-term investment in the security and future of your organisation. ■

### **ENCRYPTION PLATFORMS FOR VOICE**

#### **Crypto Desktop HC-9300**

This encryption platform is suitable for voice, fax, file encryption and data transmission (e-mail) and has interfaces with phone, fax and Ethernet for PC and SIP phone.

#### **Crypto Mobile HC-9100**

This encryption platform is suitable for mobile telephony.

### **SECURITY APPLICATIONS FOR VOICE**

#### **Voice System HA-2000**

With the new Voice System HA-2000 from Crypto AG, you can phone within the IP network confidentially (and inexpensively).

#### **Voice Encryption Mobile HA-2400**

Voice Encryption Mobile HA-2400 is a security application that enables you to conduct highly confidential calls on a Nokia mobile phone in top sound quality in an absolutely tap-proof manner. As is customary with Crypto AG, encryption is done in hardware specially designed for the purpose.

#### **Voice Encryption Office HA-2500**

Voice Encryption Office HA-2500 is the security application for a stationary office phone. It runs in the Crypto Desktop 9300, where encryption also takes place.

#### **Crypto Call Manager HA-2100**

The Crypto Call Manager HA-2100 is a security application also running in the Crypto Desktop HC-9300.

# ETHERNET MULTIPOINT FOR GROWING DATA STREAMS

**Observations of the network market clearly reveal that bandwidths keep doubling every six months<sup>1</sup>. Ethernet has won out as transport technology because of its special performance traits. Once designed for networking local computers, Ethernet today has proved highly effective for interconnecting sites on a regional, national and international scale. To address the trend towards constantly bigger data throughput, Crypto AG continually improves its encryption performance and expands its Multipoint capability. The reality today for an encryption solution is data throughput of 10 gigabits per second with Multipoint character.**

*By Urs Kürzi, Customer Segment Manager, and Willy Landolt, Product Manager*

In search of efficient ways to network various sites, you soon need a fully meshed hub-and-spoke<sup>2</sup> topology. In fact, this need already arises when you connect your headquarters (HQ) to a second site (branch office) with an external backup data centre (see diagram). This topology is an advance on the star-shaped networking used earlier when direct communication from branch to branch was not yet possible. In the Multipoint scenario, users at several branches access data storage at the data centre. The data centre, in turn, is capable of supplying the data redundantly to headquarters. What was once implementable with a conventional (point-to-point) link technology comprising six encryption units can today be created elegantly with an Ethernet Encryption Multipoint solution involving three Multipoint units (and additional redundant units).

Ethernet Encryption Multipoint also has the advantage of scaling. Speeds of 10 gigabits per second at headquarters can be distributed among several branches with one gigabit per second and/or 100 megabits per second apiece. None of the locations ever use their full bandwidth at the same time, so the capacity can be employed ideally in a Wide Area Network (WAN). If monitoring detects a trend towards peak overloads, a widening of bandwidth can be considered in good time.

Field offices can also be connected in the process with a transmission capacity of 100 megabits per second. These transmission capacities can be increased later on if data flows increase. Networks based on Ethernet Encryption Multipoint are an intelligent way to network branches and data centres while complying with maximum cryptographic standards.

## Easy commissioning

With Ethernet Multipoint, several hundred locations can be interconnected to form an intermeshed network. A configuration of this type poses entirely new commissioning challenges compared with point-

to-point networks. In a specially developed installation mode, you can conveniently configure and test all settings between headquarters and the branches and go live on schedule.

## All-purpose transportation network

Ethernet service providers offer standardised connection services, scalability, reliability, quality of service (QoS) and service and service-level management<sup>3</sup>. With this great flexibility, service providers achieve ideal cost efficiency in distance transport networks. The Metro Ethernet Forum has set several standardised types of services for providing carrier Ethernet: E-Line (a virtual point-to-point connection), E-Tree (a point-to-Multipoint connection) and E-LAN (a virtual connection in a Multipoint-to-Multipoint configuration). Voice, video and data are transmitted using these types of services. The widest variety of demands related to transport behaviour can be depicted in this manner. The customer obtains an all-purpose transportation network with maximum performance at an optimum price. This network is based on a robust technology and can be expanded at any time, i.e. it is scalable.

## Ethernet Encryption: compelling advantages

The Ethernet service satisfies transport functions at Layer 2 according to the OSI model. It can come in the guise of E-LAN, E-Line or E-Tree. These principles are ideal for transmitting all multimedia applications. Encryption on Layer 2 generates no overheads and involves absolutely minimal time delays. Ethernet Encryption delivers excellent performance with throughput 100% encrypted at a rate of 10 Gbps and negligible latency time. Ethernet Encryption is recommended for use even in time-critical applications in defence and storage networks, either as Ethernet or Fibre Channel over Ethernet transport.

Security is essential, even at 10 gigabits per second. The enormous transmission capacity of 10 gigabits per



ultra-sensitive and the routes it follows must be under control. That is why the Security Management and Monitoring System from Crypto AG supports encryption solutions in Ethernet Multipoint topologies in offline (management) and online mode.

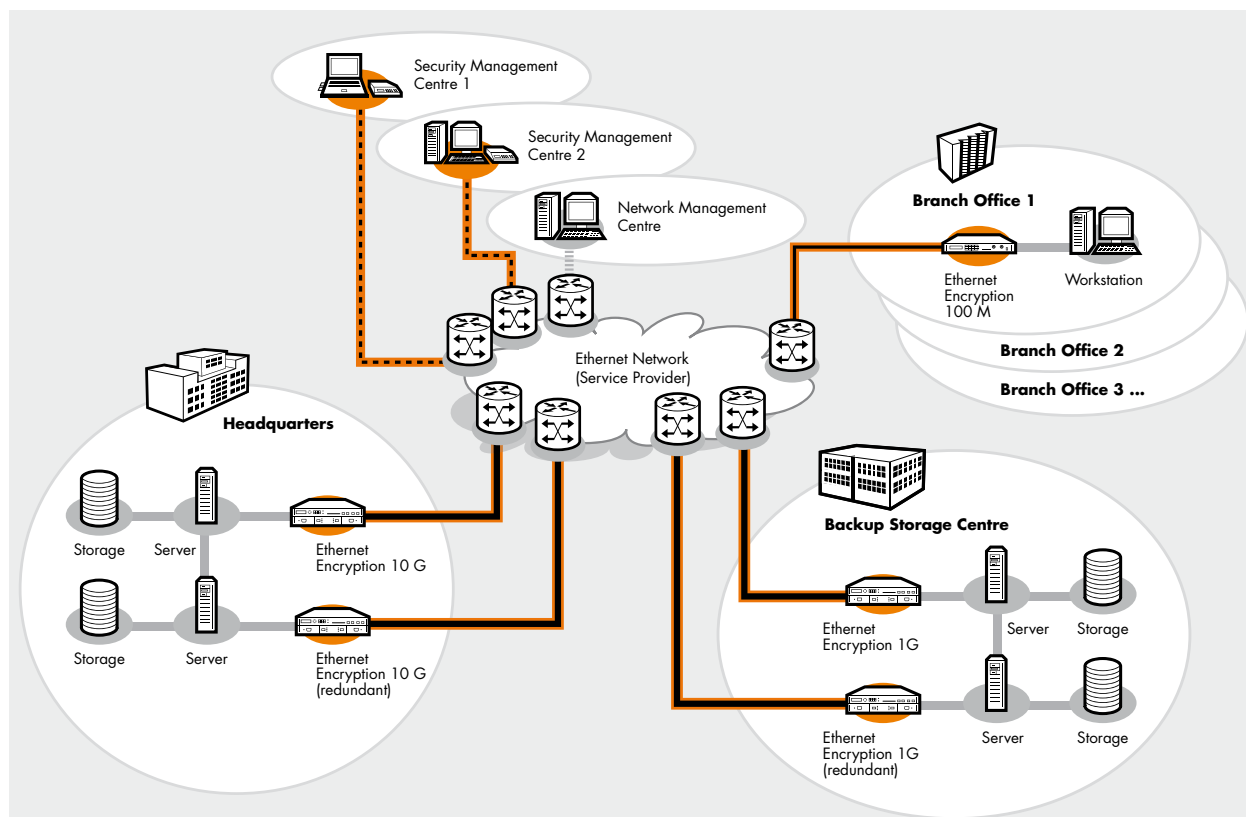
For larger networks, Crypto AG recommends the convenient online mode and can set up both an in-band and an out-of-band process. Users can then consider which process best suits their own individual needs and/or the available infrastructure. The object is to enable security managers to do the commissioning as easily as possible and to control the encryption units in the network with maximum efficiency. In performing these tasks, they can rely on two proven technical work tools: SMC-1100 Broadband and the Remote Access Device RAD-1100. Most operations are supported by user-friendly graphical user interfaces. Effective wizards and design mechanisms help to prevent mistakes. In the background, there are many additional protective mechanisms, including user authentication, for instance.

second is perceived security at best. Even at this data throughput of 10 gigabits per second, no single byte can “hide in the crowd”. No matter how fast a data packet is sent, it still has a destination and source address and specifically defined structures (frames). There is only one way to counter modern attack techniques: seamless, high security encryption of all information being transported.

### Convenient security management and monitoring

Security management takes on great significance in an organisation or company operating with large networks and/or globally distributed sites. In these scenarios, the data transported is almost always

Crypto AG has paid careful attention to the roll-out process. The encryption units are extremely simple to implement because they are pre-configured. They contain the security parameters for the specific customer, all protected from access by others. You simply loop these units into the network and activate them in plain mode. With equal ease, users can monitor and administer each connection from this point forward while



Ethernet Multipoint scenario: reduction of necessary encryption units, support of all topologies specified by Metro Ethernet Forum.



the network is operating and, if need be, switch off the connection. Users can set specific points in time for key changes to be performed automatically and without the presence of personnel. Periodic key changes are considered part of best practices.

The monitoring approach allows the system to check the load on individually encrypted connections between sites. If a trend towards peak loads materialises, users can take any necessary action in good time without endangering availability. With the Multipoint technology, users can perform management functions of this kind of their own volition even in provider networks.

---

*Security is essential, even at 10 gigabits per second.*

---

If sites are widely spread out geographically, several of them can be set up for security management. The individual locations work with a single common database that is accessible exclusively and with absolute security via encrypted connections. This approach prevents collisions or misunderstandings, and the data is consistent at all times. Users can maintain simple and efficient management round the clock with this approach by setting up management sites in multiple time zones.

These and other advantages of Ethernet technology help persuade users to opt for this secure and convenient network philosophy to handle growing data streams on their backbones. All things considered, the Crypto AG approach is also good value for money. ■

**Source:**

<sup>1</sup> Gilder's Law: George Gilder is the author of the well-known Gilder Technology Report and various other publications on telecommunications and microprocessor engineering. He derived his law about the growth of bandwidth or transport capacity from empirical studies. This law says that the bandwidth for communication grows about three times as fast as processor and computing capacity (see Moore's Law). Gilder expands this law by concluding that communication capacity doubles every six months.

<sup>2</sup> In a hub-and-spoke configuration, no one branch can communicate directly with another. Communication has to be routed from one branch to another via headquarters.

<sup>3</sup> Crypto AG Magazine 2/2009, page 13, 14, Ethernet Encryption for next generation networks



THE QUALITY MANAGEMENT SYSTEM GENERATES TRUST

# CRYPTO AG CERTIFIED TO ISO 9001 FOR 25 YEARS

**Crypto AG was among the first companies in Switzerland to obtain certification under the ISO 9001 standard. The company's objective was to lay a foundation of trust for customer relations. Over the past 25 years, we have continually refined the quality management system above and beyond the ISO specifications to satisfy the different requirements of our customer groups.**

*By Rudolf Meier, Publicist*

Crypto AG celebrates a special anniversary this year. The company was certified to the ISO requirements for the first time in 1985, making it a pioneer in quality management. As part of this year's conformance audit, Crypto AG CEO Giuliano Otth received a special certificate for the company's 25-year commitment to quality management from Erwin Peter, representative of the Swiss Association for Quality and Management Systems (SQS).

---

*In June 2010, Crypto AG received a certificate for maintaining its SQS certification for 25 years.*

---

ISO certificates are the most widely recognised credentials for quality management systems. These certificates are issued by authorised certification agencies only and their validity is generally limited in time. Companies must pass regular extensive assessments to renew their certificates. This process shows our business partners and customers that we take quality seriously and that we continue to effectively improve our quality management system. When awarding contracts, customers often only consider suppliers with the appropriate credentials.

Over the past 25 years, Crypto AG has subjected itself to the periodic certifications every time and regularly integrated the new findings from practical management into its daily business activities. With this policy, the company ensures that the services, values and behaviours requested and confirmed are actually guaranteed for the long term and that it will promptly conform to subsequent further developments in the standard. ■

## INTERNATIONAL ORGANIZATION FOR STANDARDIZATION ISO

ISO is the International Organization for Standardization and was established in 1947. It is recognised in all important industrialised countries and has over 150 of these countries as members. Independent certification organisations are entrusted with conducting certification processes in the member states. Over the years, ISO has created several standards for specific sectors.

Basically, the ISO quality standards state which requirements a company's quality management system must meet. ISO has defined eight fundamental principles of quality management:

1. Customer orientation
2. Management that assumes responsibility for quality
3. Employee involvement
4. Process-based approach
5. System-oriented management approach
6. Continuous improvement
7. Objective approach to decision-making
8. Mutually beneficial supplier relations

Source: ISO International Organization for Standardization  
[www.iso.org](http://www.iso.org)

There are extensive guidelines such as ISO 9004 to help with the practical implementation of the principles. Further standards relevant to Crypto AG include ISO 27 000 (IT security) and ISO 20 000 (service management) or ISO 31 000 (risk management).



STATIONARY, MOBILE, PORTABLE, ON THE HIGH SEAS...

# THE RIGHT ENCRYPTION PLATFORM FOR EACH ENVIRONMENT

**Thanks to global networking and wireless communication, people can work flexibly, no matter where they are and with nearly all common applications. Despite all this flexibility and efficiency, however, information protection continues to be a top priority. This goal can continue to be achieved in the future if encryption is applied as homogeneously as possible across all applications. The platform approach from Crypto AG gives users a foundation that will retain its effectiveness in the future.**

*By Urs Kürzi, Customer Segment Manager*



Modern business communication is inconceivable without mobile and fixed network phoning, e-mail or video conferences. At the same time, the volume of data being communicated keeps growing at a rapid pace. A big factor in that growth is that mobile employees can access data in government and business networks from almost anywhere in the world. Global computer networks form the backbone for this activity, connecting thousands of employees at different locations over high-performance data lines and enabling them to work together directly in real time. Everyday applications are technically converging as a result, with the two key catchwords being “IP convergence” and “Ethernet”. Naturally, this trend also has ramifications for information security. Regardless of how and where people work, information security is not automatic. Certain elements and processes have to be heeded first and solutions have to be designed for specific customers so that confidentiality, authenticity and integrity are assured under all circumstances. The goal in the medium term is therefore to put homogeneous security architecture in place in all work scenarios and across all the different applications if possible. New integrated approaches are emerging for this purpose. Users find them more advantageous than

having to run a separate encryption solution for each communication medium.

## **The formula is: Crypto AG platform plus security application**

Crypto AG implemented these requirements for modern encryption solutions in a platform approach. That means a certain Crypto AG platform was designed for a specific use and can be fitted with one or more security applications as needed. So hardware platforms are in use for mobile work, for stationary office communication (desktop) or even for more robust action, such as use in vehicles. Each hardware platform can encrypt voice, data, text messaging, or video applications, depending on its configuration. In other words, Crypto AG takes a multifunctional and flexible approach that is not only tempting in theory but highly effective in actual practice. Changes are occurring against the following backdrop:

## **Away from the expensive procurement philosophy**

Increased requirements due to budgets and cost pressures have compelled most government administrations to rethink the issue. Previously, classical use scenarios allowed certain encryption equipment to be planned in advance. Extensive stock-keeping was needed to maintain system reliability (logistically). With this perspective and mode of organisation for the supply chain, governments and organisations were able to develop and purchase encryption solutions to meet their specific needs. These approaches gave rise, among other things, to expensive small series and the complicated stock-keeping of replacement units (individually for each medium of communication) which threatened to become outmoded with time. Now, anyone who can quickly implement the most modern technology from shortened development cycles will have less expensive and more flexible security solutions in the future. The platform approach from Crypto AG is a reliable way of doing so.



### Mobile Platform

- Security Application:
- IP VPN (VoIP)
  - File
  - Storage
  - Thin Client



### Desktop Platform

- Security Application:
- Fax
  - Voice
  - File



### Ruggedised Platform

- Security Application:
- Radio Voice
  - Radio Data
  - MIL Messaging
  - IP VPN



## Multifunctional MultiCom

The platform approach is the pivotal idea nowadays and dramatically simplifies logistics. For instance, the Multi-Com Radio Encryption solution HC-2650 was originally designed for encrypted radio communication (HF, UHF, VHF). Now armies are using it for secure IP VPN communication. The 200-hardware platform opens the way to a degree of flexibility that greatly simplifies logistics in defence organisations. Operators can transform a radio encryption unit into an IP encryption unit at the press of a button or vice versa, of course. A platform offers many logistical advantages. Repairs, stock-keeping of spare parts and training can all be managed far more simply than with conventional equipment. Another advantage of a modular approach is that security applications can be procured successively.

With the P3I approach (Pre-Planned Product Improvement), expected technological innovations are anticipated and planned for implementation in existing systems practically throughout the service life of the system. Users can rely on always having state-of-the-art work equipment.

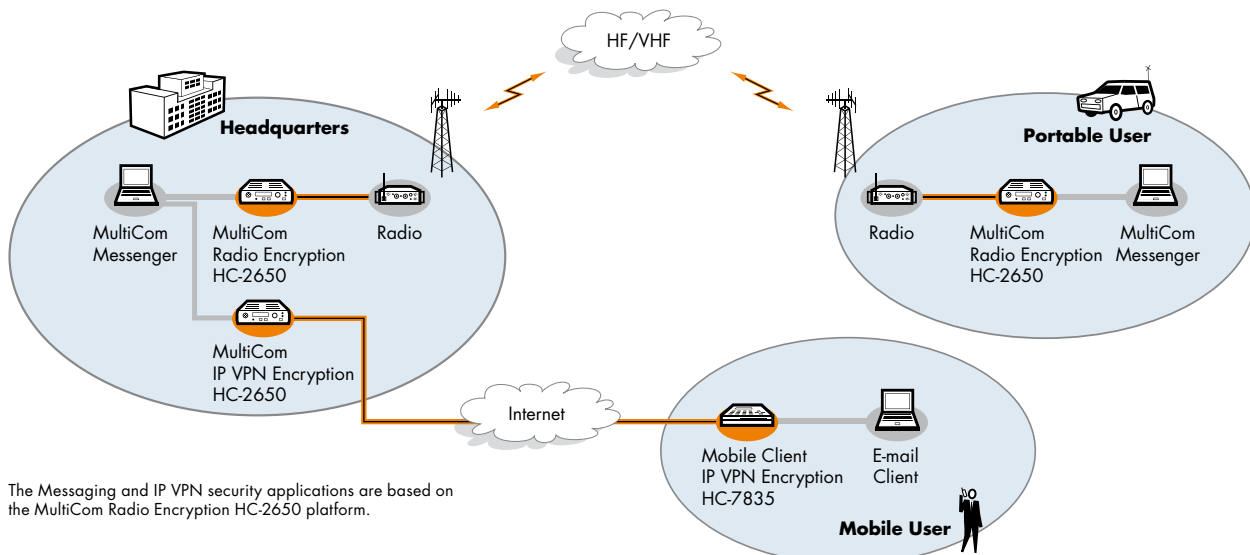
## Another example: secure office communication

There is hardly any need for phone, fax or PC users to be interested in the underlying technology. They simply want these capabilities to be readily available. The new all-purpose Office Platform Crypto AG Desktop HC-9300 addresses this situation. It protects data and information from all configured applications in the given work

setting. HC-9300 is available today with the fax encryption security application and there are plans for it to be an upcoming voice solution. In future, it will offer absolutely reliable end-to-end protection with a secure e-mail application. Incidentally, this platform also makes a handsome addition to any desktop.

## Platforms minimise training effort and sources of error

A first-rate encryption solution naturally has to include highly trained expert staff. As we all know, the best security solution is only as good as the individuals who install, configure, use and maintain it. Users quickly recognise that Crypto AG has paid great attention to this factor. Once they know the general operating approach for a solution they can usually run another security application on the same platform intuitively. These synergy effects simplify system operation and make the platforms and their applications more acceptable and trustworthy to users. Easy-to-understand wizards and menu prompting help users to avoid errors and make work easy. ■



The Messaging and IP VPN security applications are based on the MultiCom Radio Encryption HC-2650 platform.

# ARE MODEMS THE “BETTER OPERATORS”?

**Along with units used exclusively for encryption, Crypto AG also develops supplementary products that work together with digital encryption. Digital signal processing has a special role to play in this field. As part of its P3I approach, Crypto AG will soon make a new modem available for MultiCom Radio Encryption HC2650. This will achieve substantially more efficient data communication over radio channels – for example in civilian and military messaging.**

*By Tim Harms, Product Manager Radio Security*

HF radio channels can perform much better today than they did a few years ago, thanks to digital technology. Contrary to what many radio experts expected, we have been able to keep pushing the envelope on the limits of “usable” physics. It is not only a matter of what is theoretically feasible but also of what can be implemented and works reliably in daily practice.

Crypto AG has always dealt with modem technology since in modern encryption technology the voice signal has to be digitised anyway. Voice coding is one field that stands out – it is crucial to determining what voice information and voice quality can be transmitted. As a result, periodic innovations in voice coding and associated modems inevitably took place.

---

*Performance in HF radio channels is much better today than it was a few years ago – the envelope on the limits of applied physics has been further extended.*

---

## **Planned innovation also protects investments**

In the HC-2650 encryption platform, Crypto AG made provisions from the outset for continuing to push the physical potential of radio channels for data transmission. This foresight is in keeping with the P3I principle at Crypto AG (Pre-Planned Product Improvement). Applying this principle, Crypto AG comes up with innovations that constantly incorporate and integrate findings from different fields of knowledge without having to use additional hardware units. Another advantage: investments retain their value in the future.

Crypto AG is now developing a modem in-house that conforms to MIL-STD-188-110B and transmits data over radio at a whole new level of performance. It is a software innovation and eliminates the need for a separate hardware modem outside the radio or encryption system. This modem delivers an increased maximum



data transmission rate on HF and VHF/UHF of up to 9600 bps and shortens transmission times in the process. This trait can be existentially important for messaging systems in particular.

## **Automated operator functions**

Modem technology would be much more trivial if radio channels were physically and qualitatively stable, like optical signals in fibre optics, for example. Transmission quality in HF channels fluctuates strongly, depending on physical and atmospheric conditions. For example, operation of a high-performance modem with constant parameters in a noisy channel would be quite frequently brought to a complete halt.

This problem can be solved by adding a more robust modem mode with constant adjustments of modem parameters. Until now, the operator has usually been the one to enter changes in modem parameters, usually manually, and had to be present for as long as the

modem was operating. This was especially true in the case of channel changes or establishing new connections to other stations.

This is where the new data rate adaptation feature and the MIL-STD-188-110B modem come into play. Together, they analyse channel quality autonomously and optimise the relevant parameters automatically with no outside influence, e.g. transmission rate or operating mode. Even under the worst of propagation conditions, data communication is possible. Thanks to the Automatic Repeat ReQuest Protocol (ARQ), data transmission is even error-free.

---

*The data rate adaptation will of course also be integrated in the MultiCom Messenger, Crypto AG's own messaging solution. That further boosts the performance of this product as it ensures optimum transmission.*

---

product that can be integrated into the system. It is installed in the robust waterproof housing of the HC-2650 – most modems available on the market are



MultiCom Radio Encryption HC-2650 now also with integrated modem conforming to MIL-STD-188-110B

Under the best of conditions, data can be sent at a maximum rate of 9600 bps, which is a very high speed for HF. If VHF and/or UHF frequencies are also available in the same system, the user can benefit from this larger bandwidth with no additional effort or expense.

#### **Integration simplifies other functions**

The modem conforming to MIL-STD-188-110B has further operational advantages as a pure software

not ruggedised. The weight is the same, as is the space needed. Power is supplied from within and on top of this, no extra cabling is required, so such sources of error are also eliminated.

Basic configuration is taken care of by the convenient browser interface of the HC-2650 or manually right on the front panel. The HC-2650 can be readily interfaced with radios of all major makes – there are corresponding test protocols for over one hundred types. The ultimate reason this innovation has such an appealing price is that it can be fully integrated into a hardware unit that customers require anyway.



## TRADE FAIRS

### **IDEX Abu Dhabi**

20 to 24 February 2011

## PRESS REVIEW

### **Criminal hackers cause damage in the nine-digit dollar range**

Cyber crime is on the rise, whether in the form of fraud or industrial espionage. In most cases, criminal hackers are the ones behind this crime. According to the Kiel Institute for the World Economy (IfW), Internet crime is the fastest growing sector of international criminal activity.

This finding is substantiated by current figures from the United States. Last year Internet crime there caused losses amounting to USD 560 million (EUR 440 million). One year earlier the figure was less than half this amount at USD 265 million (EUR 208 million).

The US telecom group Verizon estimates that industrial espionage is behind 35 per cent of the viruses and Trojans being disseminated. Institutions are being created to deal with this problem in the United States and increasingly also in Europe.

Possible solutions from experts are already materialising in the web forum of the Global Economic Symposium in the working group on cyber crime, cyber security and the future of the Internet. One suggestion is to make sure potential criminal hackers are identified at an early stage in their careers. It is important to find ways to use their capabilities and involve them in constructive, web-based activities instead of locking them away for being hackers.

Experts discussed solutions to this and other hacker problems at the third Global Economic Symposium co-organised by the Kiel Institute for the World Economy (IfW) in Istanbul in September. Experts from science, security authorities and computer companies demanded stepped-up international collaboration, if possible with a European Centre against Internet Crime or with an international police organisation "Internetpol", an online version of Interpol. Five hundred experts discussed global challenges at this conference.

*Source: Kleinreport, September 29, 2010*

### **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 – Abu Dhabi  
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  
Level 9B Wisma E&C  
2, Lorong Dungun Kiri  
Damansara Heights  
50490 Kuala Lumpur  
Malaysia  
Tel. +60 3 2080 2150  
Fax +60 3 2080 2140

#### **Muscat**

Crypto AG  
Regional Office  
P.O. Box 2911  
Seeb PC 111  
Sultanate of Oman  
Tel. +968 2449 4966  
Fax +968 2449 8929