

# CRYPTO MAGAZINE

N° 1 | 2018

The course  
is set for  
growth





## Dear Readers

Quite a lot has happened since the last edition. In the intervening period, Crypto AG has separated its national and international operations into two new companies: Crypto Schweiz AG and Crypto International AG.

What are the advantages of this? The new structures allow us to better serve the different needs of Swiss and international customers and to expand our market offerings with a greater focus on customer requirements. We explain this in greater detail over the next few pages.

In this edition, we also highlight the extent to which states and civilian and military organisations depend on information and communications technology (ICT). Without these increasingly interconnected systems, they are barely able to operate.

What requirements do governmental organisations and armed forces place on ICT? Moreover, what challenges does this "networking of the world" present in terms of Information Security? You will find more information on these topics in this edition of CryptoMagazine.

Giuliano Otth  
CEO  
Crypto Schweiz AG

Anders Platoff  
CEO  
Crypto International Group AB

### 3 | FOCUS

## Crypto AG is gearing up for growth

- 6 | Information and communications technology as a driver of efficiency
- 9 | Security to the power of four – journeys in the world of networked data
- 12 | Armed forces need crisis-proof ICT systems
- 14 | INTERVIEW  
Safeguarding integrity at all times
- 18 | Estonia – a digital role model
- 22 | SUCCESS STORY  
A highly secure workstation as the basis for efficient policing

#### Publication details

Published twice a year | **Print run** | 3,750 (German, English, French, Spanish, Russian, Arabic)

**Publisher** | Crypto International AG & Crypto Schweiz AG, Zugerstrasse 42, 6312 Steinhausen, www.crypto.ch

**Editor-in-chief** | Anita von Wyl, Crypto Schweiz AG, T +41 41 749 77 22, F +41 41 741 22 72, anita.vonwyl@crypto.ch

**Reproduction** | Free of charge with the consent of the editorial office. Courtesy copies requested. Copyright Crypto International AG & Crypto Schweiz AG

**Illustrations / photo credits** | Crypto AG: Cover, pp. 2, 3, 4, 5 | Getty Images: p. 9 | Jean-Paul Theler: p. 15 | Shutterstock: pp. 6, 10, 12, 16, 20, 21 | Grisha Bruev/Shutterstock: p. 18 | Maciej Bledowski/Shutterstock: p. 8



# Crypto AG is gearing up for growth

Crypto AG is dividing its national and international business into two new companies. The international business is being taken over by the Swedish cyber security veteran and entrepreneur, Andreas Linde, and will be further developed by the Crypto International Group. The Swiss business, Crypto Schweiz AG, is being taken over by the management, led by long-time CEO of Crypto AG, Giuliano Otth, through a management buyout that includes the former sister company InfoGuard AG.

CryptoMagazine met with the owner of the Crypto International Group, Andreas Linde, the co-owner and CEO of Crypto Schweiz AG, Giuliano Otth, and Anders Platoff, CEO of the Crypto International Group, to talk about how they are gearing up for growth in their new, focused businesses.

#### Why did you decide to separate the Swiss and the international business of Crypto AG?

Giuliano Otth: We had two business models with very different customer needs within Crypto AG. Separating them is the logical step to enable each to reach its full potential. In particular, it will enable us to better serve the different needs of our Swiss and international customers by developing each market offering with greater focus. This move will strengthen both companies, and both groups of customers.

#### What does the new ownership mean for the customers?

Giuliano Otth: The operational division into the two new

companies will be implemented in the course of 2018. With the new ownership structure, each company can focus on its business model, and each will be able to make targeted investments in future technologies and sales channels. Both the Swiss and the international business will be enhanced thanks to the expansion of their respective market offerings. Our customers will notice that our products match their needs even better!

#### Why did you choose Andreas Linde to take the international business ahead?

Giuliano Otth: Andreas Linde is a true entrepreneur and strong strategic partner with a wealth of experience in the sector. We intend to cooperate closely in the future, in particular on product developments. The new Crypto International AG, a subsidiary of Crypto International Group AB, is taking over all the international customer relations and will develop its range in the direction of comprehensive cyber security solutions, in addition to the existing product portfolio in the high security



encryption systems sector. His visions for the business, as well as his solid experience in the sector, make us confident that he is the right person to maintain and develop the international business.

**Why did you choose to take over the international business?**

Andreas Linde: The employees of Crypto International – as well as Crypto Schweiz – have unique knowledge that cannot be found elsewhere. The combination of a state-of-the-art product and service portfolio as well as an outstanding global customer base makes it extremely appealing. The Crypto brand represents high assurance at its best, respect for our customers' privacy and feedback, whether it is positive or in need of improvements. These are values that I take great pride in. After a few weeks in office, this sentiment of mine has grown even stronger. We bring in the best of Swedish innovation and Swiss engineering to provide our customers with the very best cyber security.

**Which areas will you make further investments in?**

Andreas Linde: The international business will further strengthen its crypto offering and develop a comprehensive cyber security portfolio, tailored to the increasingly complex cyber security needs of our international customers. Zug, Switzerland, will remain the long-term, strategical R&D knowledge site of the Group. This year, we will open a second R&D site in Lund, Sweden. The ambition is to build a truly international cyber security company. The Group will be headed by Anders Platoff, an experienced executive.

**What is your vision for the international business?**

Andreas Linde: We have started a new, exciting journey in an almost 100-year-old business operation that saw its first light in Sweden in the 1920s, when the textile engineer Arvid Damm

established a Swedish crypto company. A few years later, the business was taken over by another well-known Swede, Boris Hagelin, who successfully transformed the small business into a global leader in the crypto industry. Crypto AG has been leading the way in the sector ever since. It is now time for the next era in the history of Crypto AG, where we align its Swiss identity with its Swedish roots and make great leaps into the cyber security world. The international business will further strengthen its crypto offering and develop a comprehensive cyber security portfolio tailored to the increasingly complex cyber security needs of our international customers. The fusion of our unique high assurance expertise and cyber security is something that will be highly valuable for our customers who understand the true value of protecting their nation and citizens against attacks.

Anders Platoff: We are working intensely on developing the next generation of comprehensive cyber security solutions in order for our customers to feel secure, gain better control and be prepared for new cyber security threats. Our ambition is to launch our first cyber security proposal by the end of 2018. However, I urge all our customers to contact us if they have any urgent or specific requirements in the cyber security field – we will do our utmost to accommodate their ideas and requirements.

**What is the exciting news from Crypto Schweiz AG for the Swiss customers?**

Giuliano Otth: With over 150 staff, the newly created group with Crypto Schweiz AG and InfoGuard AG is the largest purely Swiss cyber security company. In addition to our well-known state-of-the-art encryption systems, by joining together we can offer our customers the full range of cyber security solutions and services, which will also be tailored more

---

"We are seeing strong market growth in cyber security. With the newly formed companies, we can take a pole position in our core markets."

---

strongly to Swiss requirements. In future, the specialised security knowledge that was built up over a period of decades will also be made available to IoT applications. In this way, we want to take a leading role both as a service provider for our customers and as a technology partner for other companies from other industries.

**So, looking ahead, we understand that there is a lot for customers to gain. Could there be any negative impacts for customers in the transition phase?**

Anders Platoff: We will do our very best to make the transition phase as smooth as possible for our customers. The very idea of this transition is to provide an even better service to our customers in the future. However, we know that there are difficulties to overcome in a transition phase, and we will of course do our utmost to ensure that there will be no inconvenience to our customers.

If our customers do encounter any problems in the transition phase, please rest assured that both Giuliano and I are here to solve any such issues swiftly.

**What areas will the two new companies cooperate in and benefit from each other?**

Giuliano Otth and Anders Platoff: Both companies want to maintain a close partnership and work together in the future. We intend to cooperate closely on Crypto product developments. Both of us will be offering the entire crypto product portfolio, though the focus will certainly be different by being tailored to the respective needs of each market.



**Andreas Linde**

The entrepreneur, Andreas Linde, is the owner and Chairman of the Board of Directors of the Crypto International Group AB based in Lund, Sweden. Linde has a long career in the cyber security industry. At the end of 2015, Andreas Linde founded the company Famco, which, as an external service provider for government organisations, implements turnkey projects with a cyber security core.

Until 2015, Linde was CEO of the Swedish company Advenica, founded by his father in the early 90s. Linde is the largest shareholder of Advenica. Advenica offers a variety of certified cyber security solutions for governmental and critical infrastructure organisations. In 2000, Andreas Linde also co-founded 4C Strategies, a risk management solutions company that helps clients build and develop skills in risk management, crisis management and business continuity management.

Linde is an enthusiastic entrepreneur with a drive to build successful long-term businesses. He has broad experience of cyber security, Information Security and business development within the sector.

Linde is 43 years old, married and father of two daughters, 3 and 4 years old.

# Information and communications technology as a driver of efficiency

Information and communications technology (ICT) has a profound influence on the state, the economy and society. In recent years, advances in this field have proven to be a driving force in the modernisation of public authorities and associated processes. Keeping pace with and benefiting from technological development calls for a strategy that takes Information Security into account.

Nowadays, it is impossible to imagine a world without computer systems. In everyday life, it is only when a system breaks down that the extent to which information and communications technology shapes the modern world becomes clear. If the payment terminals in shops stop working, for example, long queues form in front of the checkouts. If the system controlling the traffic lights at a crossroads fails, traffic can temporarily be brought to a complete standstill.

In situations requiring a higher level of protection, failures and breakdowns of systems have a far more serious impact. The more critical a system is to the way processes function, the more clearly its failure demonstrates how dependent the state, the economy and society have become on information and communications technology – or ICT for short. This includes everything from administrative processes at public authorities to industrial manufacturing machines and IT-based control systems in nuclear power plants.

## ICT's penetration is expanding

Recent years and decades have witnessed a steady increase in the importance of ICT systems. This was first mentioned in the late 1970s and early 1980s, when the transmission of digital information using telecommunication technologies began in earnest. With the transmission of digital information, traditional information technology (IT) and communication technology gradually started to come together. Today, these once-separate technologies have irreversibly merged into one.

In essence, ICT encompasses three basic functions:

- Communication, or the transmission of information from one place to another
- Information storage, or the holding of data from one point in time to another
- Information processing, or the conversion of data on the basis of defined rules, which could generally be referred to as computing

For the state, the economy and society, information and communications technology is essential. Without ICT systems, they are simply no longer able to operate. Dependence on these technologies has increased significantly over the course of time – in parallel to the ever-greater networking of individual systems. The advantages of networking are obvious: it simplifies and speeds up processes. In this way, ICT has made a fundamental contribution to modernisation in all areas of life.

## Modernisation spurred on by ICT

In organisations and public authorities, ICT has also had a decisive influence on the way that processes are structured. Even the simplest of actions could no longer be carried out

without technical systems, and a large part of the information is now stored only in digital form, meaning the data can only be read and edited using suitable equipment. As technology has advanced, the volume of data being recorded, transported, stored and processed has grown enormously, exacerbating this dependence to the extent that processing and transmitting the volumes of data that are commonplace today would be inconceivable without ICT. Conversely, modern ICT is responsible for creating the large volumes of data in the first place.

There are no signs or reasons why technological development might slow down or come to an end – and it shows no signs of doing so. On the contrary, information and communications technology is likely to remain a key driving force in the continuing process of modernisation. The keyword here is digital transformation. In this context, it is essential that companies, organisations and public authorities consider and plan their use of ICT carefully.

In Switzerland, the first efforts to plan the use of ICT date back to 1998. ICT was seen as an important tool for boosting prosperity on a lasting basis. Since then, two IT strategies have been formulated. Today, Switzerland is in the midst of implementing the strategy for 2016 to 2019, with the long-term objective of making the Confederation's ICT more business-oriented, more integral, more reliable and more focussed.

It is essential that companies, organisations and public authorities plan their use of ICT carefully and take Information Security into consideration.

## The vision predefines the measures

An ICT strategy is also indispensable with regard to cost. Within public authorities, modern technologies and process automation have played a key part in making procedures and processes cheaper and faster to carry out. At the same time, however, ICT also created the need to collect and analyse certain data in the first place. The entire development process has given rise to gigantic volumes of data that must be processed, stored and maintained, as well as a multitude of interfaces that need to be managed and monitored. The cost of ICT is and will remain a decisive factor, even though technological development has steadily brought down the price of the physical infrastructure for processing, transmitting and storing data and information.



Given the cost of implementing ICT projects and the ongoing operating costs of ICT applications, which are not to be underestimated, efficiency and cost-effectiveness are key components of any ICT strategy. The aim should always be to take a holistic view; in other words, cost-effectiveness and efficiency must be evaluated within the wider context. In addition, the evaluation of costs should not only take account of a project's length but also the expenditure that is likely to arise over the entire useful life of a system.

#### Taking all requirements into consideration

Besides efficiency and cost-effectiveness, however, numerous other aspects deserve at least equal attention in ICT strategies. One such aspect could be paraphrased as "appropriateness". In other words, it is important to ensure that ICT is always geared towards the requirements of an administrative or organisational unit and helps it to perform its role. At the same time, the ICT must take account of the needs of users as well as those of other stakeholders – especially citizens and external service recipients and providers, as well as other public authorities. A conflict of interest is therefore unavoidable: if cost and practicability considerations lead to a focus on ICT solutions that are as standardised as possible, it is impossible to fully satisfy the specific requirements of individual administrative units. Solutions that are too standardised also carry a risk that the ICT might no longer be able to fulfil its role as a driver of efficiency.

In ICT strategies, particular emphasis should be placed on Information Security. This is the key to ensuring continuous, failure-free operation of the systems and to guaranteeing the security of the state. Information Security is one of the critical success factors to which appropriate attention should also be paid in the area of risk management. After all, a system failure – or the loss or theft of data – can have serious consequences.

Although the severity of the risks always also depends on the entities involved, neglecting Information Security can have devastating repercussions for a state in many areas. Such issues must therefore be afforded sufficient scope at the stage of the ICT usage strategy. When it comes to safeguarding the confidentiality and integrity of data, or rather protecting it against unauthorised access and modification, cost-effectiveness can no longer be the most important criterion.

---

Traffic control must be ensured following a power outage

---



## Security to the power of four – journeys in the world of networked data

---

We are heading towards a hyperconnected world. With the increasing penetration of IT comes a growing need to protect the underlying systems and the circulation of digital information. Crypto SmartProtect technology takes account of this development, allowing up to four completely isolated security zones to operate on one device in order to ensure extensive protection of sensitive data at all times.

---

Today, information and people can travel faster than ever before. A number of applications and areas of activity have already broken free of their local moorings and made the move into cyberspace. Given the dangers lurking there, it is imperative to design information and communications technology (ICT) systems in a way that ensures the reliable protection of security-critical components, processes, interfaces and information at all times.

#### Constant change increases vulnerability

Modern ICT offers huge potential for standardisation. This potential should be utilised as far as is sensibly possible, as stipulated by the Swiss Federal ICT Strategy, for example. Of course, given the diversity of specialist fields in the public

sector, it is never possible to achieve total standardisation. As a result, up to 6,000 different specialist applications are currently in use in Switzerland. Meeting these specific requirements of different stakeholder groups is a key objective. To make matters worse, the number of networked systems and devices is rising constantly – and it remains almost impossible to estimate the consequences of this development. One thing is for certain: overall, digitisation has led to an increase in vulnerability. Even governments and organisations with well-developed IT protection have recently fallen victim to cyberattacks. On multiple occasions, attackers have succeeded in gaining access to sensitive data by exploiting misconfigured infrastructure components or weaknesses that were not identified until it was too late.

Safeguarding operational security in conjunction with maximum ease of use is a central challenge that must be overcome. At the same time, it must also be taken into account that the structures of the Internet are subject to constant change. Technical progress is rapidly paving the way for new potential applications that must be integrated into existing IT infrastructures. In the near future, these applications will likely be joined by non-IT components, such as the Internet of things (IoT). Moreover, the recording and linking up of huge volumes of data (big data) is opening up previously unknown possibilities.

Safeguarding operational security in conjunction with maximum ease of use is a central challenge that must be overcome.

#### Eradicating security risks

The use of mobile technologies has already become established on a widespread scale. Nowadays, efficient working is no longer possible without incorporating mobile devices, and the secure networking of stationary and portable systems has become one of the key factors for success. However, this relies on the availability of ICT infrastructures that allow and ensure boundless communication and unrestricted collaboration – that is, Unified Communication and Collaboration (UCC). Whether the information is public or confidential, users require access to their data and documents everywhere and at all times. This aspect is worthy of particular attention, especially if the situation requires sensitive data to be shared in a network or with individual partners.

For example, if a citizen of a state is kidnapped abroad, the foreign ministry of the victim's home country is usually in charge of finding a solution. Depending on the specific case, an operation of this kind may require the involvement of instruments only loosely linked to the foreign ministry, such as external advisers or units of the police force. Ensuring that information is exchanged securely via this network necessitates technologies that support parallel data traffic.

The same applies to operations involving the military: for example, when the armed forces conduct subsidiary operations whose success is dependent on the secure exchange of data. At the same time, it is crucial not only that military leaders have access to internal information channels but also that information is exchanged with partners properly and securely.

Situations such as these generally also involve exchanging information at different classification levels. This exchange must therefore always take place on completely separated networks, as total Information Security can only be ensured



User-friendly working on one device

through consistent separation. For a long time, this could only be achieved by using multiple devices, but this approach is no longer in keeping with the times. Not only is it inconsistent with today's user requirements, it also takes up valuable time.

#### Up to four user environments – one workstation

These hurdles can be overcome with Crypto SmartProtect technology, which allows the secure processing of information on a single device. The user has the option to work with up to four completely isolated security zones (Compartments). On the one hand, the two standard Compartments allow access to the Internet (classification level: public). On the other hand, the second Compartment is used to run the applications required for editing internal information (classification level: internal). Furthermore, the Crypto SmartProtect technology also allows solutions with further Compartments: a third Compartment for confidential documents (classification level: confidential) and a fourth Compartment for data and applications that are classified as secret (classification level: secret).

Depending on the specific requirements, different restrictions can be defined for the Compartments – for example, no printer connection or use of USB sticks at the secret classification level (fourth Compartment). These options remain available to the user in the second Compartment, however. The advantage of this solution is that the user can work in their familiar user environment and – in the event of a crisis – does not need to access a system that is rarely used.

#### Targeting devices

Knowing what is necessary to meet security requirements is one thing – taking appropriate action is another. However, the risks to sensitive information can be consistently eradicated by providing staff with devices that allow them to operate in familiar user environments in isolated security zones. This is important because devices have recently become an increasingly popular target for hackers, serving as a "springboard" for penetrating other levels of an IT system.



# Armed forces need crisis-proof ICT systems

**In the digital era, it is more important than ever for armed forces to ensure that their operational independence remains intact. The trustworthiness, integrity and availability of communication channels must remain under seamless control. Guaranteeing this security of ICT systems is an increasingly important challenge as it is vital to their operational capabilities.**

Armed forces must maintain their ability to operate and act at all times and in all situations. Here, communication within the unit and the secure forwarding of information play a vital role, and growing importance is attached to the use of modern IT tools in the provision of command support. Especially in crisis situations, confidential communication must function effectively. Under no circumstances must sensitive information be allowed to fall into the wrong hands or be tampered with. Information and situation reports must remain confidential even years after the mission is complete.

Rapid technological development is increasing the density of information and demands on its availability – and this greater availability is accompanied by rising demands on Information Security. In particular, field sensors and effectors – such as drones, body cams or radar – now deliver high-resolution picture information that requires a higher bandwidth in transportation systems. In the tactical arena, this can be achieved using modern IP radios, satellite communication, or military mobile communication over 3G or 4G. Fixed

network structures are currently based on microwave networks and increasingly also on high-speed fibre optic cables.

Until now, a variety of older systems have often operated in parallel. These systems are based on different programming languages and technologies, and the data is usually stored in an isolated and decentralised manner. In general terms, the problem with this outdated technology is that it provides too little integration and bandwidth to meet the new demands for extensive command and control information in real time.

## **Safeguarding the ability to act**

In order not to restrict their ability to act in a crisis situation, armed forces must have systems that are resistant to outside attacks. The hardening and protection of these crisis-proof networks and data centres is achieved through physical hardening, as well as through corresponding encryption and protection of the information. In order to encrypt communication and to protect networks, Crypto International AG and Crypto Schweiz AG offer a variety of solutions that meet the

---

The independence of the military network is of paramount importance

---

corresponding requirements and that are based on Crypto's Security Architecture. As a result, attacks are always averted using the strongest available security measures. For connections from one location to another, Crypto cProducts use cryptography (logical/cryptographic) to protect information from attacks at the information level during transmission.

At least since the Snowden affair, there has been a general understanding that relevant systems should be kept separate even within the base network in order to achieve zoning of the information. For example, logical/cryptographic methods are used to separate the air force's radar system from telephony, a biometric access system, and a command support and information system. This ensures that, in the case of failure, or in the event of deliberate tampering, no information can be exchanged between zones. Last but not least, end-to-end encryption is required for part of the information. This is achieved using end-user solutions that allow the secure transmission of voice or paper or electronic documents up to the maximum level of confidentiality.

Armed forces aim to be autonomous and not to depend on civilian providers in emergency situations. In crisis scenarios, this approach also ensures that the secured networks can act as connections between the military and the government, as well as with operators of critical infrastructures (nuclear power plants or airports), so that basic services operate properly in a crisis. Often, systems are highly interconnected to allow optimum assessment of the situation and scenario planning. Extensive information is collected about a mission and processed centrally in order to derive the operational picture. This not only helps to ensure optimum preparation and effective operational command but also serves as documentation afterwards.

## **Armed forces in the 21st century**

Many armed forces are currently making the transition into the 21st century, and a key part of this modernisation process is the safeguarding of system security. This also includes monitoring networks and detecting cyberattacks on ICT systems, as well as triggering any necessary countermeasures.

In addition to new data centres, the plans often also include the establishment of a single, independent telecommunications network that brings the different systems together. Old networks based on copper cables and directional radio are being replaced by optical fibres, allowing encrypted data transmission between many individual locations. This network is intended to serve not only the armed forces, however, but also civilian organisations with security-related functions. Thanks to the solutions from Crypto International AG and Crypto Schweiz AG, it is even possible to share infrastructures while operating them separately and in a highly secure manner.

**In order not to restrict their ability to act in a crisis situation, armed forces must have systems that are resistant to outside attacks.**

Updating the network technology allows both voice and data to be transmitted from the armed forces' fixed and protected transportation network out into the field via mobile and partly mobile components – and independently of private telecommunications providers. Another objective of modernising ICT systems is to reduce the sheer number of systems and to introduce standard platforms.

Smooth logistics are indispensable if armed forces are to function properly. Limited resources such as vehicles, troop supplies and food should be provided quickly and promptly. In emergencies, the armed forces' pharmaceutical centres can take over community responsibilities and help ensure the provision of medical care. These material movements and logistics services aimed at supporting resource planning are now virtually impossible to handle without an ERP-based IT system. Armed forces' operational capabilities are ensured if the logistics can provide the operating resources on time and in line with demand. Naturally, this requires not only availability (planning and a stock of resources) but also a functioning logistics process, including the associated IT logistics solutions. Linking this process to crisis-proof networks improves availability and guarantees the logistics process. State-of-the-art technology and hardened ICT components with appropriate, up-to-date protection ensure that such systems operate efficiently.

# "Safeguarding integrity at all times"

Nowadays, the armed forces' operations are primarily supported by information and communications technology (ICT) tools and can no longer be conducted effectively without them. In addition to the numerous advantages and opportunities that ICT brings, we must also be keenly aware of the new risks and dangers involved in its use in the military setting.

## *What demands does ICT face in a military environment?*

Compared with the civilian environment, the requirements in terms of robustness, availability and Information Security are viewed and weighted differently from a military perspective. The armed forces must perform their duties in all situations and take account of all possible threats. ICT is never an end in itself in the military setting. Rather, it supports the military actors in performing their duties and functions. I emphasise this because, as a consequence of incorrect or insufficient ICT services, there is a considerable likelihood of people coming to harm. These aspects essentially also determine the different and stricter demands that are imposed on ICT in the military setting. Specifically, in the military environment, we need ICT infrastructures that continue to function in all situations, both after a military attack and after major natural events or a widespread power shortage so that the necessary ICT services can still be used.

## *Which fields of action present the greatest challenges? What strategies do the Swiss Armed Forces consider useful in order to meet these challenges, and how are they implemented?*

The primary task of the Swiss Armed Forces is to protect the Swiss population and to ensure Switzerland's territorial integrity. By that I mean that the armed forces are primarily geared towards operating within their own borders. Likewise, that means that we also essentially have to deliver and safeguard our ICT services within the territory of Switzerland. At present, the greatest challenges we face are in the following fields of action: the secure and robust networking of systems and actors, ensuring the delivery of the necessary information at the right time, and cyber defence – that is, detecting and defending against threats in cyberspace.

As the armed forces, we are required to provide our services in all situations – that is to say, continuously. We therefore have our own hardened and autonomous infrastructures and systems in the area of ICT services, which we can operate and utilise with our own personnel – defence staff and members of the militia. We also have to ensure that our staff have the

necessary knowledge and experience to perform these tasks independently and autonomously.

With the FITANIA programme, we're currently in the process of renewing our ICT infrastructures and adapting them to current requirements and threats. The programme includes three major projects for the construction of the Swiss Command and Control Network, the renewal of the armed forces' telecommunications, and the construction of new data centres. In addition, the head of the Federal Department of Defence, Civil Protection and Sport (DDPS), Federal Councillor Guy Parmelin, has approved the action plan for cyber defence. Once implemented, this will create the necessary conditions within the department so that the armed forces can also deliver the necessary services in this area.

## *Rapid technological progress requires constant adaptation of the ICT landscape. How do the Swiss Armed Forces fare generally and in comparison with other countries?*

Even the Swiss Armed Forces cannot escape from technological progress. Unlike in the civilian world, however, the requirements in the military world – and especially in Switzerland – are driven not by technological trends and possibilities but rather by emerging, changing threats and the requirements these create. Of course, new technologies and the products based on them are also used in the military setting with a view to exploiting these new opportunities to support the fulfilment of military requirements and orders.

With their militia system, the Swiss Armed Forces have a significant advantage. Our soldiers, or rather the members of the armed forces, are now growing up alongside technological progress. For them, using these technologies and products is nothing out of the ordinary. On the other hand, the use of modern systems is becoming increasingly complex and requires a strong and competent professional organisation with specialists who can configure, maintain and repair these systems so they can be used by troops (members of the militia). The big challenge here is that, in order to recruit ICT specialists

for the professional organisation, we're competing with large civilian IT companies on the Swiss labour market.

The integrity and authenticity of data are of fundamental importance.

## *There is a broad trend towards standardisation of ICT structures and processes. Does that also apply to the military?*

Correct, that also applies to the military setting. Standardisation is necessary, especially in order to ensure interoperability with our military and civilian partners. Since the Second World War, military operations have generally been conducted jointly with other armed forces or, when dealing with major natural events, with civilian emergency personnel. To ensure our joint success and cooperation, it was necessary to find a common language and to define procedures, processes and interfaces. This work was especially important for the collaboration between partners in the western world, leading to a huge effort in relation to the military standardisation of structures and processes and ultimately to a large number of technical standards. Without standardisation, it simply wouldn't be possible to utilise today's technologies, such as those in the area of telecommunications. Incidentally, this also applies to the civilian world.

## *Which threat scenarios rule out universal standardisation from the outset? And what are the main risks facing the armed forces' ICT systems?*

In principle, the primary purpose of standardisation is to ensure interoperability and cooperation. However, it also boosts transparency as a result. In other words, a potential attacker knows how I do things and can therefore plan how to attack and injure me more effectively. On the other hand, if I use a standardised procedure, such as a specific protocol, I also have



**Jean-Paul Theler** studied economics at the University of Lausanne before going on to obtain a Master of Science in Mathematical Economics from the London School of Economics and Political Science (LSE) and a doctorate (oec. publ.) from the University of Lausanne. In 1996, Jean-Paul Theler joined the Training Corps and was deployed in a variety of roles, including at the Armed Forces College and as Head of Military Doctrine. As Head of Armed Forces Personnel, he was promoted to the rank of brigadier. From 1 January 2013 to 31 December 2017, he led the Armed Forces Command Support Organisation (AFCSO) as a major general and was responsible for services in the area of information and telecommunications technology and electronic operations within the armed forces.

Within the context of implementing the Armed Forces Development Programme, he has served as Project Manager for Support Command since 1 January 2018. Based on the parliamentary decision regarding the organisation of the armed forces, Support Command will bring together the current duties of the Armed Forces Command Support Organisation and the Armed Forces Logistics Organisation.



Soldiers are also using an ever-greater number of technical aids

a better idea of where the weak points and risks lie. According to the threat situation, I can therefore take appropriate measures to minimise or even eliminate these risks. The important thing is that I recognise the risks that could make it harder or even impossible for me to carry out my duties. If I recognise these risks and then consider what threats and dangers I'm exposed to, I can take appropriate measures to evade or avert these dangers. As already stated, the ICT systems serve to support the armed forces in carrying out their duties. In summary, we can say that the armed forces' ICT systems serve to generate, process, store, transport and present data or information. Based on this, we can identify two fundamental risks: firstly, the risk of information being lost, meaning it can no longer be used, and secondly, the risk of my systems' operational capabilities being diminished or destroyed. Specifically, these are risks from cyberspace:

- Data leakages or the impairment of software-based functions and processes
- Human misconduct, such as the intentional incorporation of errors or weak points in software (backdoors)
- Deliberate tampering with data and processes
- Physical threats due to forces of nature and kinetic forces (such as earthquakes, explosions or impacts of weapons)
- Failure of the energy supply (electrical energy or water)

Here, I'm seeking to highlight that, in addition to significant risks from cyberspace, the armed forces' ICT systems also face equally important risks in other areas. This is a key difference from the perception of risks in the civilian setting.

**What specific significance is attached to Information Security?** Information Security is of vital importance – primarily, of

course, in relation to protecting data or information. In the military setting, the system for classifying information – SECRET, CONFIDENTIAL, INTERNAL – creates a structure that also determines the approach to handling information. Measures to protect information at the SECRET level, ranging from ICT infrastructures to the processes for handling information, are more extensive and restrictive than at the INTERNAL level.

In addition, the integrity and authenticity of data are also of fundamental importance. Commanding officers' decisions are based on the information available to them. If, for example, an enemy succeeds in manipulating the information, this can have a profound influence on the decision. Consequently, the integrity and operational capability of ICT systems are a basic requirement for Information Security.

**In your view, what are the primary threats to Information Security?**

From the armed forces' perspective, the following fundamental threats can be distinguished: firstly, the leakage of information, secondly, the destruction of information or prevention of access to it, and thirdly, the manipulation or corruption of information. By "stealing" information, the other side seeks to obtain information (e.g. planning documents, access information such as passwords, or certificates) that gives them information superiority and access to IT systems, before using this access to seize control of the systems or tamper with them. By destroying this information or preventing access to it, the aim is to make it impossible for their enemy to deploy its resources. For example, if the images from a reconnaissance drone can be prevented from reaching the operations centre, the use of weapons can be obstructed. Furthermore, by

manipulating information and data, they can bring about incorrect decisions or even cause systems to crash.

The armed forces' current guidelines forbid the networking of private devices with the ICT infrastructures of the armed forces and administration.

**Technologies such as the Internet of things (IoT) are still in their infancy, but in future they will allow devices to communicate with one another directly. What is the armed forces' position in relation to the IoT? Or rather where do you see the greatest potential for the IoT in the military environment?**

Like many other topics, the IoT is surrounded by hype that is not directly relevant to the military setting. However, if you view the topic from a general perspective, as a way to network many different IT resources so that they can communicate with one another directly, then it is also undoubtedly relevant to military applications.

In the military setting, we also use the term sensor-to-effector loop – that is, the networking of sensors with effectors in a more or less automated process. Today, it is still the case that humans represent the central and primary intelligence in this loop and therefore make the decisions. Soldiers on the front line are also being equipped with an ever-greater number of sensors that transmit data to central command centres directly and autonomously. The consolidated information is then transmitted back to the soldier, allowing weapons to be used more efficiently in the field. The automation of this loop will be intensified in future as part of the trend towards reducing the exposure of humans, who are highly vulnerable and represent the weakest link on the front line. In my view, however, it's crucial when using weapons that the human always makes the final decision and therefore assumes responsibility. We must never let fully automated warfare become a reality.

I expect that, as in the civilian setting, the IoT will become an increasingly important technology, primarily in the area of support, and could bring about even greater automation of logistics processes, for example.

**What security risks does this present for communication, and how might effective protection be designed?**

When processes become more automated as a result of the IoT, end-to-end security in particular becomes more important. The need to ensure the authenticity and integrity of information becomes much more pressing and, in parallel to this, there's also a massive increase in the number of possible targets for cyberattacks. A necessary consequence of this is that all information must be packaged so that it contains identification elements. These allow identification and authentication in order to safeguard the integrity of the transported information.

**To what extent do private devices present a security risk in military applications? And what protection measures do the armed forces take to combat this risk?**

Private ICT equipment presents a security risk per se in military applications because it is used for the same activities as military equipment with identical or similar functions but is not equipped and used with the same – or at least equivalent – protection measures.

Certainly, the assessment of security risks must make a distinction based on the type of private device and the place of use, but we know that in most cases these devices are not used in isolation. Rather, they are networked with their environment via one infrastructure or another. Networking private equipment with military infrastructures is a clear no-go area, but even if it is used independently of the military ICT infrastructures, it leads to a risk of uncontrolled data leakages. It also poses a risk as an uncontrolled sensor – for example, via the positioning function in a smartphone or the microphone or camera in a laptop or smartphone.

The armed forces' current guidelines forbid the networking of private devices with the ICT infrastructures of the armed forces and administration. In addition, the ICT infrastructures are protected against unauthorised network access by a variety of mechanisms. Those entering classified military facilities have to pass through access control and a baggage check similar to those at airports. However, the most efficient protection measure is still self-discipline and monitoring by superiors and comrades.



## Estonia – a digital role model

The small Eastern European country of Estonia is seen as a pioneer of digitisation, having put its faith in these new technological capabilities earlier and more consistently than other countries. Although this approach is not without its risks, Estonia is seen as a role model – also in regard to the protection of data and IT infrastructure.

Estonia seized its opportunity. When the country gained its independence from the Soviet Union in summer 1991, it was able to create new structures of government on "greenfield land". The young politicians who rose to power were quick to recognise the potential of new technologies and the dawn of the Internet. In the mid-1990s, they began their first broad IT education initiative, in which all schools were given suitable hardware and software. The government itself has been paperless since the end of the 1990s.

Today, Estonia holds first place in the European Union's ranking of the digitisation of government. This is hardly surprising, for almost all interactions between the state and its citizens can now be carried out online. The only three exceptions are marriage, divorce and buying a house, which still require citizens to be physically present and provide signatures.

Estonians are taking advantage of the new capabilities. For example, in the 2014 European elections, almost 10 percent of voters submitted their votes online, and more than twice as many did so in the national parliamentary elections held the following year. Almost all Estonians now submit their tax

return online, and significant parts of the return are completed automatically anyway thanks to the networking of tax authorities, banks and employers.

A perfect example of the high level of digitisation can also be found in the healthcare sector. For around 10 years, the Baltic state has had a unified system of electronic patient records that stores the medical histories of all residents. These can be accessed by doctors and patients alike. The e-Health platform is also used to make doctors' appointments, conduct simple consultations and prescribe medication.

### Internet as a basic right

The foundations for all of this were laid at the turn of the millennium, when the parliament in Tallinn amended the country's constitution to include a basic right to Internet access. Rather than simply paying lip service, this actually led to the construction of robust broadband infrastructure that

undergoes regular upgrades. Mobile Internet coverage is also excellent in this relatively sparsely populated country of some 1.3 million inhabitants.

According to EU figures, the country scores above the European average for all indicators used to measure the level of digitisation. For example, approximately 86 percent of those aged 16–74 use the Internet regularly (EU average: 76%), and 87 percent of households have a broadband connection (EU average: 80%).

The government also continues to invest considerable resources in boosting digital skills. At schools, for example, programming is a normal subject. Nevertheless, the country believes it still has a long way to go, and its Digital Agenda 2020 is a road map for further improvements.

### X-Road and Digital ID

The backbone of Estonia's digital society is the decentralised X-Road platform, which is linked to around 1,000 institutions. X-Road allows the secure exchange of data between authorised databases, with some data stored using the blockchain principle – that is, in database systems where the administration of data is decentralised. In these systems, the data sets are interlinked using cryptographic methods.

In addition, all Estonians have an electronic ID card that can be used with a card reader and two-factor authentication to allow secure online identification and for all e-services. This also allows people to "sign" documents electronically. Over 90 percent of the population use the card – not only for government services via the e-Estonia platform but also for banking transactions.

### Gaps and attacks

However, all of this is not without its dangers – and, sure enough, security gaps in the electronic ID card system became public knowledge in autumn 2017. The media reported that hackers had managed to access the data of around 750,000 people. According to experts, however, the problem was given top priority. The prime minister himself made an immediate statement on the matter, and a technical solution was soon found to close the gaps in defences.

Over 10 years ago, Estonia made headlines with one negative consequence of digitisation. For a period of several weeks, hackers repeatedly paralysed various websites, including the government's online portal and the websites of various banks.

Electronic security therefore became part of national defence at a relatively early stage. In the wake of the attack 10 years ago, the authorities introduced a new system for securing data. In addition, every Estonian can now check whether and when their data has been accessed – so that attacks can be spotted quickly.

### NATO centre for cyber defence

Estonia has become a pioneer in matters of cyber defence, not least because of the attack a decade ago. Immediately after joining NATO, it proposed the creation of a corresponding centre of excellence. Since 2008, the country's capital, Tallinn, has been home to the Cooperative Cyber Defence Centre of Excellence (CCDCOE), a sort of think tank for cyber defence.

The institution's key document is the "Tallinn Manual", a collection of legal texts on the topic of cyber defence. Some experts see this as a possible basis for extending the law of armed conflict in relation to electronic warfare. However, the CCDCOE also conducts specific defence exercises in which specialists from the participating armed forces – from NATO countries and neutral states – are required to tackle massive cyberattacks.

Last but not least, the CCDCOE compiles reports on individual countries – including on Estonia itself. According to the report, the high level of digitisation and corresponding vulnerability means that the topic of cyber security enjoys higher priority than in most other countries.

Even the youngest in society deal intensively with digital tools



### Cyber security strategy

The authors go on to say that the country was one of the first to establish a cyber security strategy, in 2008, and renewed this in 2014. Naturally, the measures set out in the strategy are secret, as is the amount the armed forces spend on cyber security. Nevertheless, there is a commitment to making this topic a high priority.

### Partners play an important role

Overall, however, experts agree that Estonia serves as a role model for digitisation. Among other things, they point to the fact that processes are more efficient and therefore more economical. Estimates suggest that the small country saves around two percent of gross domestic product simply thanks to the widespread adoption of the digital signature.

However, experts warn that countries hoping to emulate Estonia must also bear in mind the risks of such a digitisation strategy. Data must be adequately protected at all levels. For highly sensitive data that is vital to the country's survival, highly secure Information Security Solutions are indispensable. This applies first and foremost to Diplomacy and communication within the security forces, as well as to the areas of State Governance, Defence and Internal Security. According to the experts, the key thing here is to bring the right partners – with the corresponding knowledge – on board at an early stage.

For highly sensitive data, highly secure Information Security Solutions are indispensable.

The strategy's aims, however, are made public, and they include greater awareness of cyberattacks and improved capabilities to combat them. The organisational structure of cyber defence is also disclosed. However, the CCDCOE's report was not unqualified in its praise for Estonia, noting that the country's top cyber security committee had, at times, fallen short in its supervisory role and that there was a lack of political support.

Secure access control using a card reader



## SUCCESS STORY

# A highly secure workstation as the basis for efficient policing

Police organisations often operate nationwide. In this context, the exchange of sensitive information must be ensured at all times in order to safeguard their ability to act. Moreover, efficient policing also requires unrestricted access to classified information in the core network at all times regardless of location. At the same time, the confidentiality, authenticity and integrity of this information must never be put at risk.

Police organisations have a diverse range of requirements, and information plays a key role in their ability to act. For example, when police officers are out conducting checks as part of their everyday work, they require access to data stored in a central location. The system must therefore allow the fast retrieval, easy editing and highly secure transmission of sensitive information such as personal details quickly, everywhere and at all times, as well as simultaneously providing access to information that is publicly available.

There is a need for Information Security Solutions that take account of the new threat scenarios, in which devices are the primary target of attacks, as well as offering a highly secure working environment both inside and outside the organisation.

The two Compartments can be operated simultaneously, while consistent separation ensures total Information Security at all times.

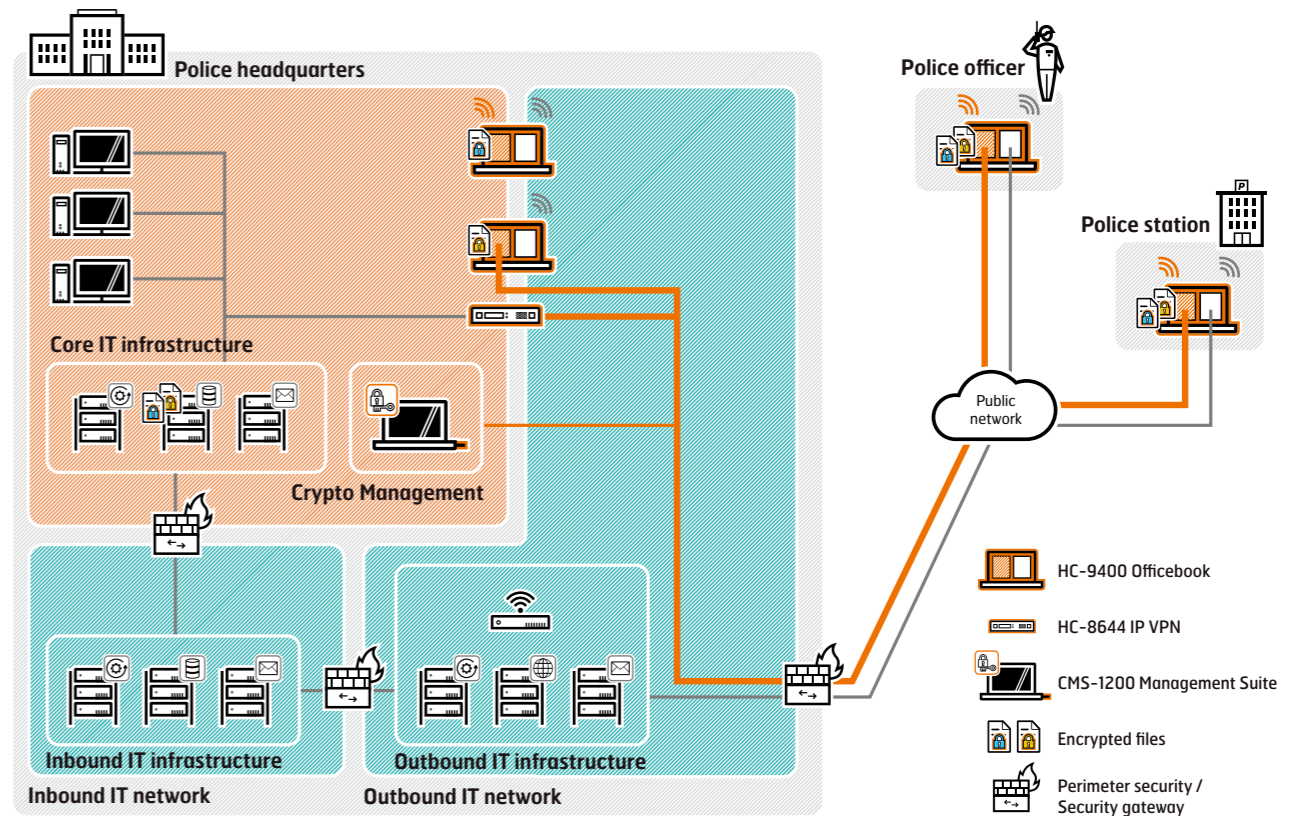
Police organisations therefore want a solution that allows them to work without compromising on ease of use and to run common operating systems such as Windows, as well as Microsoft Office applications and web browsers. In addition, it should be possible to administer communication relations and users through a central security management system. In many cases, tailor-made management infrastructure is also required for the purposes of system configuration and administration.

### cOffice Workplace is the solution

Based on Crypto SmartProtect technology, the cOffice Workplace system fully satisfies all these requirements and allows for convenient and highly secure working in a familiar user environment at all times – both inside and outside the organisation. This means that highly secure communication operates continuously in a comprehensive nationwide network with connected field offices.

The HC-9400 Officebook is a central system component of cOffice Workplace, which is suitable for both stationary and mobile use. With two Compartments, it offers two completely separated user environments. The first Compartment can be used to access the organisation's centralised information and applications, allowing secure access to the police headquarters' IT infrastructure that is secured by the high-performance HC-8644 IP VPN encryption solution. The second Compartment allows the user to access publicly available information via a web browser. The two Compartments can be operated simultaneously, while consistent separation ensures total Information Security at all times. Configuration and administration of the overall system is ensured via the CMS-1200 Management Suite and the HC-8644 IP VPN gateway.

With cOffice Workplace, Crypto International AG and Crypto Schweiz AG offer uncompromising protection against cyberattacks.



cOffice Workplace allows secure and convenient working in a secure user environment – both inside and outside the organisation

## Uncompromising protection against cyberattacks

### Total security

Based on Crypto SmartProtect technology, cOffice Workplace provides the best possible protection of sensitive information against third-party access without compromising the working process.

### High efficiency and flexibility

Two completely isolated user environments can be operated at the same time, allowing users to work in an efficient and

flexible way. Sensitive internal information is protected even when a public network is accessed at the same time.

### Maximum ease of use

Users can work in a familiar user environment regardless of their location. Furthermore, the Compartments can be switched between easily without putting sensitive information at risk.

### Easy integration

Integration into the IT environment does not require any major changes to infrastructure.



Crypto International AG  
Zugerstrasse 42  
6312 Steinhausen  
Switzerland

Crypto Schweiz AG  
Zugerstrasse 42  
6312 Steinhausen  
Switzerland

T +41 41 749 77 22  
F +41 41 741 22 72  
crypto@crypto.ch  
www.crypto.ch

### **Crypto cSeminars**

**cSeminar Information Security Specialists**  
10 to 14 September 2018

**cSeminar Contemporary Cryptography**  
17 to 21 September 2018

The seminars are held at the Crypto Academy  
in Steinhausen.

**Contact and further information**  
[www.crypto.ch/seminars](http://www.crypto.ch/seminars)