

A portrait of Professor Christof Paar, a man with short grey hair and glasses, wearing a dark patterned button-down shirt. He is standing with his arms crossed, looking directly at the camera. The background is a blurred office or laboratory setting with blue and white tones.

**PROFESSOR CHRISTOF PAAR ON  
THE NEW CLUSTER OF EXCELLENCE  
AT THE RUHR-UNIVERSITÄT BOCHUM**

## IT Security in Research, Education and Industry

### **At LEAG cyber security is of prime importance**

One of the largest German energy suppliers protects its IT infrastructure

### **Law, legislation and cyber security**

Information security at the Ministry of Justice of the state of North Rhine-Westphalia



Secure Internet access in a business context: The tool manufacturer PFERD relies on secunet safe surfer

## National

- 4 Official Online Authentication: E-Government – as Easy as Online Shopping
- 6 **Ministry of Justice of the state of North Rhine-Westphalia: Law, Legislation and Cyber Security**
- 8 Bavarian Ministry of Economic Affairs, Energy and Technology: Knowledge protects
- 10 **Energy supplier LEAG: “Cyber security is one of the top priorities”**

## International

- 12 NAPMA further expands its SINA Secure Remote Access capability

## Science

- 17 **New Excellence Cluster for IT Security in Bochum: Cutting-Edge Research with Team Spirit**

## Technologies & Solutions

- 20 **Secure Internet Access in a Business Context: Surfing Without the Risk**
- 22 The Evolution of the Electronic Driving Licence
- 24 PKI: the Key to the Future
- 26 Encrypted Voice Communication: SECRET Telephony: What Comes After ISDN?
- 28 High-Performance Site Networking and Data Backup for Geo-Redundant Data Centres: Networked up to SECRET-level – at Gigabit Speed
- 29 secunet protect4use: Digital Keyring for Access to Web Portals

Cover:  
Professor Christof Paar, holder of the Chair for Embedded Security at Ruhr Universität Bochum (RUB)

## Miscellaneous

- 30 Enigma Model, Built 2018

## News in Brief

- 33 First iPhone App for electronic ID checks
- 34 Everything Secret, Complete Insecurity?
- 35 finally safe Presents AI Solution at Digital Summit
- 35 Marcel Taubert Strengthens secunet’s Defence Division
- 36 World’s Largest IT Security Trade Show: it-sa Sets New Records
- 37 Axel Deininger Elected to the TeleTrusT Executive Board
- 38 secunet Ilmenau: Compelling Proximity to Research

## Service

- 39 Dates – January to June
- 39 Imprint



Enigma, built 2018

## Dear Reader,

Today, cyber security is one of the most pivotal factors in the sovereignty of nations and societies, and also one of the most exciting fields of research. So it is entirely logical that the issue has now also become the focus of government funding: from 2019 the Ruhr-Universität Bochum will house a cluster of excellence focussing on IT security. Professor Paar, one of the speakers at the cluster, explains the reasons behind the move inside this issue of *secuview*.

In addition, we see that cyber security is increasingly being taken seriously within industry and critical infrastructures and not just seen in its traditional role of importance within public authorities and military organisations. Also in this edition, LEAG, one of the largest German energy suppliers, and the tool manufacturer PFERD describe how they already rely on a high level of IT security and have done so for some time.

In recent decades we have come a long way in this regard. Since the Nineties, when the World Wide Web first began its ascent to prominence, the societal relevance of IT security was only gradually starting to seep into the public consciousness.

The early IT security specialists were able to fall back on the experiences of, among others, cryptologists who had already practised encryption before there was any such thing as IT: in this issue we give the briefest of outlines of the history of the famous Enigma cipher machine, which was used during World War II and whose codes were ultimately cracked by the Allies.

Just a few decades later cryptologists made use of what were then new types of asymmetric encryption procedures to lay the foundations for today's world of Internet-based processes that we all use on a daily basis – such as online payment, or the German electronic ELSTER tax return system. Progressive cryptography is packed into sophisticated technology for homeland security, for example in solutions for automated border control. With SINA, we have developed and established a product range that uses applied cryptography to satisfy even the most stringent of security requirements.

How will things evolve over the next few years? The contours of future challenges are already coming into focus. A key buzzword will be 'quantum computer'. In order to adapt to these and other developments we need high-level interdisciplinary research and training, effective collaboration between the scientific community, politicians and industry, plus a good-sized pinch of entrepreneurial vision.

I would first like to wish you a relaxing Christmas holiday season and very best wishes for 2019!

**► To adapt to future challenges,  
we need a good-sized pinch of  
entrepreneurial vision. ◀**



A handwritten signature in blue ink that reads "Rainer Baumgart". The signature is stylized and includes a long horizontal stroke at the end.

Dr. Rainer Baumgart

## OFFICIAL ONLINE AUTHENTICATION

# E-Government – as Easy as Online Shopping

While many other countries have long since offered their citizens easy-to-use state online services, the construction of an appealing and standardised e-government offering in Germany has made slow progress up to now. One reason for this is that federal government, states and municipalities often work on their separate offerings independently. This multiplicity makes it complicated for users, however. With its award-winning EKONA concept the Bavarian State Office for Taxes (BayLfSt) has now achieved a breakthrough.

EKONA can significantly contribute to the standardisation of the German e-government landscape: the solution supplies an important element that, in future, will enable citizens and businesses to utilise various e-government services across Germany via a single account. The basis for this is the ELSTER platform, for many years a tried-and-tested online authentication service.

For years there have been efforts to make Germany fit for the future in terms of e-government. In 2017 the German Bundestag adopted the Online Access Act (OZG), whose objective is to accelerate the development of a Germany-wide, standardised offering for official online services. The act obliges the federal government and states to combine their online portals to form a portal network, which then provides all the services to citizens and businesses.

The aim is to achieve this within five years – a time frame that many consider ambitious. This is because fundamental prerequisites still need to be drawn up for the new e-government model. These include standardised user accounts: to ensure the process requires minimal effort from citizens and businesses each should have their own user account from which they can access all services on the network. This in turn requires a nationwide online authentication system.

This is where BayLfSt comes in with its EKONA project (Elster Konten Identifizierungs- und Authentifizierungsdienst/Elster Accounts Identification and Authentication Service). Two essential requirements apply for online authentication in the public sector: it must demonstrate a sufficiently trustworthy level of security for citizens and municipalities; and it must be easy for users to manage. The authentication service from the ELSTER platform, developed and operated by BayLfSt, has fulfilled these two points for many years. ELSTER is the largest and probably the most successful e-government project in Germany and has continued to break records ever since it was launched in

1999. In 2016, the 21 million income tax declarations submitted were authenticated via the electronic interfaces at the tax authority.

## Secure data exchange for citizens, officials and businesses

The ELSTER authentication service, which was launched by secunet in 2004 with the attached Trust Center ensures secure authentication of the users by means of certificates. The pivotal concept for EKONA was to utilise this service that had proven itself a million times as the basis for cross-portal authentication. This is why BayLfSt and secunet are currently jointly developing the interface for KOLIBRI accounts (Konten-Link für Bürger- und Unternehmens-Identitäten/Accounts Link for Citizen and Business Identities). To be able to use the identity data from the tax administrations as part of the ELSTER certificate for other e-government services – and, accordingly, also for authentication – KOLIBRI enables a secure exchange of data between the tax administration and the 17 user accounts of the federal government and the states across the country that are currently being set up on behalf of the IT Planning Council. There is potential for the online authentication via KOLIBRI to be available to all municipalities and officials in Germany – without this involving a huge amount of work.

As a “Made in Germany” authentication process KOLIBRI uses the tried-and-tested security level of the ELSTER platform, making it totally trustworthy. Moreover, the process is convenient for citizens: in future, they will easily be able to unlock their ELSTER certificate from their personal ELSTER account, even for non-tax-related purposes. They will then be able to use processes for e-government applications that they are already very familiar with from online shopping.

All that is required for this is a certificate file, which can be saved and is then usable everywhere and at any time. There is no need for further hardware such as, for example, a

card reader. Users who already use signature cards or security sticks for ELSTER will also be able to use these within KOLIBRI.


### Good starting conditions thanks to six million ELSTER identities

Another aspect entails a significant advantage, especially in the context of the tight schedule stipulated by the OZG: there are already approximately six million ELSTER certificates belonging to citizens and businesses in existence that are available for online authentication. The starting position for a rapid, Germany-wide dissemination of the procedure is therefore favourable, because KOLIBRI is easy for the authorities to adapt. In addition, anyone subject to taxation in Germany can participate in ELSTER and, as part of this, obtain authentication via KOLIBRI too.

### New services for businesses

In addition, KOLIBRI features a unique selling point when compared to other systems internationally: the procedure also enables non-natural persons to authenticate themselves, such as companies, communities of heirs or associations. For example, this would enable companies to apply to register company vehicles via online services. In principle, even processes such as corporate takeovers, spin-offs or changes in legal status could be carried out via online portals. For the authorities, apart from connecting to their user account no additional effort would be incurred.

The development of KOLIBRI, which is taking place as part of the EKONA pilot project, is expected to be finalised over the course of 2019. If the interface is then quickly integrated into the 17 user accounts of the

federal states and the federal government that are currently being set up, then all municipalities and authorities throughout Germany will in the near future have a secure and user-friendly authentication procedure at their disposal with which they can offer their services online. 



Martin Fechtelhoff  
martin.fechtelhoff@secunet.com

## EKONA HONOURED AT THE FUTURE CONGRESS STATE & ADMINISTRATION

At the 6<sup>th</sup> Future Congress State & Administration, which took place from 18–20 June 2018 in Berlin, the EKONA project team received a special award: together with technology provider Cisco, BearingPoint consultancy honoured the six winners of this year's e-government competition. The Bavarian State Office

for Taxes (BayLfSt) was the category winner in the "Best design for implementing the Online Access Act (OZG)" category with its submission: "EKONA with the interface for KOLIBRI user accounts". The jury praised the solution as affordable, user-friendly and pioneering.

Martin Fechtelhoff took part in the award ceremony together with representatives from BayLfSt. He heads up software development, web & application security for secunet's Public Authorities division and is involved in the development of EKONA.

The award ceremony of the 17<sup>th</sup> e-government competition took place on 20 June 2018 in Berlin on a grand stage. The EKONA team, from left: Paul-Alexander König (Vice President BayLfSt), Markus Geiger (mgm), Dr. Susanne Seibert (Project Leader EKONA), Martin Fechtelhoff (secunet), Roland Krebs (BayLfSt)



## INFORMATION SECURITY IN THE LEGAL SECTOR

# Law, Legislation and Cyber Security

Digitisation doesn't stop, even before the judiciary. The successive introduction of electronic processes offers clear efficiency benefits; yet also entails challenges for information security. secuvie spoke with Markus Ausetz, Chief Information Security Officer (CISO) at the Ministry of Justice of the state of North Rhine-Westphalia.

**Mr Ausetz, you are the appointed CISO for NRW Justice and entrusted with managing information security in your department, that is, in the Ministry of Justice and downstream authorities.**

**How important is information security for you and the work that takes place in your department?**

As CISO, alongside the Ministry of Justice I also look after the divisions of the ordinary courts, the four specialised courts, the public prosecutors' offices and law enforcement in all matters pertaining to information security. In line with the state's guidelines and NRW Justice, I have set myself the objective of driving forward information security, coordinating measures for improvements and, with regard to the employees of the state Ministry of Justice, further sharpening their awareness of the importance of information security.

**Many of our state's citizens probably mostly have images of paper and mountains of files in their heads when they think of the Ministry of Justice and laws; the concept of cyber security is likely to be less prominent.**

The Ministry of Justice has always been aware of its responsibility in dealing with the sensitive and personal information entrusted to it, and treats this information in accordance with its requirements of confidentiality and correctness. There is a long-standing tradition of paper-based file management and it has proven its reliability. We are also going through a transformation, however, and we want to harness the benefits of digitisation. An example of this would be the introduction of electronic legal communication and electronic files. Our aspiration in so doing is not only to bring the security and reliability of previous processes into the

digital era, but also to meet the particular challenges of digitisation. It is, therefore, absolutely critical to make information security a central theme.

**You have already been working together with secunet for well over a year to achieve these goals. Which activities were implemented previously and which successes have you already achieved on the path to improving information security?**

We originally started to implement our information security management (ISM), appoint information security officers in the divisions and establish the organisational requirements for ISM a long time ago. In doing so, we are particularly concerned to preserve our constitutional independence in this area as well, and to establish an independent security organisation for the Ministry of Justice, in order to fulfil the resulting special requirements.

**As per any management system, ISM is of course subject to a process of continuous improvement, which form does this CIP take for you?**

We, too, understand information security to be an ongoing process; with secunet's support, therefore, we have carried out brief audits across the board in the Ministry, as well as in the divisions of representative courts, public prosecutors' offices and penal institutions.

These brief audits have supplied us with valuable insights into the status of information security implementation against the backdrop of the requirements of the IT protection standard as certified by the German Federal Office for Information Security (BSI). The results represent an important basis for the planning and implementation of further security measures, and enable us to improve



### Markus Ausetz

Chief Information Security Officer (CISO) at the state of North Rhine-Westphalia's Ministry of Justice

## IN INTERVIEW

**Markus Ausetz** has served in many areas of the judiciary of the state of North Rhine-Westphalia as a judge in case law and administration, most recently as District Court Director. Since November 2016 he has held the role of Chief Information Security Officer (CISO) at the state of North Rhine-Westphalia's Ministry of Justice.

the level of security in a targeted way both locally in the areas monitored and from my higher-level view as CISO.


In parallel to this, and also with the support of secunet, we have begun to develop security concepts for central electronic procedures, such as electronic files. In addition, a skills centre for information security has been set up in the Ministry of Justice to support and work alongside the improvement and modernisation process.

**As well as a functional information security management system and the implementation of technical and organisational measures, the users also play an important role in the implementation of information security of course, so, in your case, the Ministry of Justice's employees working in administration**

**and case law. What is your strategy for involving the members of the judiciary in the state of North Rhine-Westphalia, who number almost 40,000?**

In addition to strengthening our internal ISM organisational structures we have also started to include members of the judiciary in the state of NRW in information security. In collaboration with secunet, one of the measures we are planning to undertake is a comprehensive sensitisation and awareness campaign for our leadership and management teams. This enables us to harness the multiplier function of this group of individuals and to convey the objectives surrounding information security to the various branches of the judiciary, too.

To do this we are using the existing, proven structures and processes within our internal information, training and professional

development system. Moreover, we are working on extending and expanding our training programmes with relevant topics on the subject of information security, and thus achieving a lasting impact by addressing our new employees directly. 

## BAVARIAN MINISTRY OF ECONOMIC AFFAIRS, ENERGY AND TECHNOLOGY


# Knowledge protects

Cyber attacks, disruptions and IT failures pose risks to citizens, the economy and the state. Protection provided by information and communication technologies is, therefore, a fundamental requirement for being able to harness the opportunities of digitisation successfully. As a result of this, the Bavarian Ministry of Economic Affairs, Energy and Technology (StMWi) has decided to invest in IT security. State-of-the-art perimeter protection for the Ministry's systems was already guaranteed. This does not offer all-encompassing protection from cyber attacks, however. In order to have ongoing protection from attacks on or via your own network, direct and continuous monitoring of network traffic is essential. This is the only way to detect and analyse regulation breaches (compliance) and discrepancies (anomalies). Communicating devices are likewise detected by means of constant monitoring – a sign of a continuing attack. Those who always know what is happening

in their networks are also in a position to react appropriately and, should the worst happen, to take countermeasures.

To this end the StMWi decided to collaborate with the finally safe GmbH firm from Essen. In October 2017, as part of the award of contract process, finally safe prevailed over a number of other competitors. In April 2018 an "advanced security analytics platform" was installed to monitor the Ministry's complex network and analyse the network traffic. The strict confidentiality regarding the highly sensitive information held by the StMWi made it necessary to carry out security checks on the experts working on the implementation. Specialists from secunet offered support on site.

Due to the size and complexity of the network, implementing the solution for the collection and analysis of the information was not a straightforward undertaking. The experts accomplished this via two high-performance test access points (TAPs) through

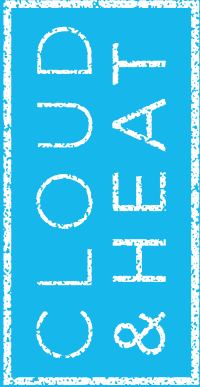
which both inbound and outbound network traffic is monitored. Following implementation the first results were quickly available: the analysis platform detected both regulation breaches and discrepancies or irregularities that the StMWi's IT specialists were able to follow up. The solution provided by finally safe thereby contributes to protecting the IT systems and sensitive data, and delivers measurable results regarding information security. 

After the editorial deadline of this magazine issue, the structure of the Bavarian government was altered, and the ministry was renamed **Bavarian Ministry of Economic Affairs, Regional Development and Energy.**

The premises of the Bavarian Ministry of Economic Affairs, Energy and Technology (StMWi)







# The future of compute



Cloud&Heat Technologies is secunet's  
Cloud partner for SecuStack.



## Secure

We deliver a security-hardened software stack based on OpenStack.



## Sustainable

We offer energy efficient infrastructure solutions, allowing up to 30% reduction of operational costs.



## Scalable

We deliver turnkey solutions that can be deployed in any locations and at any scale.



## Simple

We provide services across the entire datacenter lifecycle, including planning, construction, operation and support with designed SLA.

## PROTECTING CRITICAL INFRASTRUCTURES

# “Cyber security is one of the top priorities”

As critical infrastructures, energy suppliers are particularly crucial to society. An important element of maintaining supply security is protecting their IT systems – especially in the context of advancing digitisation and interconnect- edness. LEAG, one of the largest energy suppliers in Germany, has been investing in cyber security for a long time. secuvie spoke with Hubertus Altmann, member of LEAG's board of directors and responsible for the Power Plant division.

**Mr Altmann, what significance does the topic of cyber security hold for you as a board member of a major German energy supplier – including in comparison to other commercial challenges?**

Cyber security is one of our top priorities at LEAG. Long before the Federal Government identified the theme of cyber security for Germany and made this manifest in its IT security law of 17 July 2015 we were concerned with technical and organisational measures designed to protect our process IT. Together with the manufacturers for control technology systems, solutions were sought for a secure system environment that would protect us from attacks from cyberspace, but also from errors occurring in business processes. All this involves a lot of effort. Nevertheless, we face this challenge as well as many others that come with our business. Information security and supply security are as crucial

to us as protecting the environment, safe working conditions and efficiency.

**Which priority cyber security risks do you see, especially in the context of advancing digitisation?**

Digitisation is an important buzzword in view of the continuous progress of our flexible and efficient energy production. Topics such as “Industry 4.0” and the “Internet of Things” are ubiquitous and also present in our company. To enable our power plant and control technology engineers to use lots of technical opportunities for monitoring or collecting and evaluating measurement values the different systems need to be networked to each other. This can result in risks to LEAG's information security. It is therefore our job to keep a watchful eye on compliance with the existing regulations and processes and to use the security systems available.



### ABOUT THE COMPANY

**LEAG** is the joint brand of Lausitz Energie Bergbau AG and Lausitz Energie Kraftwerke AG, as well as their subsidiaries. The LEAG Group, based in

Cottbus, employs 8,000 people and is the largest energy supplier in eastern Germany.

As one of the two parts of the LEAG Group, Lausitz Energie Kraftwerke AG operates four power plants, which, purely for the purposes of illustration, together generate enough electricity annually to reliably supply around 15.6 million households. In addition to electricity the company also produces district heating, which is used to supply thousands of households, companies and municipal facilities such as hospitals, schools and public offices; as well as process steam for industrial customers.

**Is LEAG well-armed against this? Which steps have you taken lately as regards cyber security?**

Our company is well-positioned in matters of information security. There are regular checks and we then derive the necessary measures from these results and implement them. We are currently engaged in implementing an information security management system (ISMS). We are also actively supported by the secunet Security Networks AG in this undertaking. Furthermore, our personnel receive ongoing training on information security. By doing this we can meet the high demands that arise in relation to cooperation with the German Federal Office for Information Security.


**Can you tell us more about the connection between the cyber security strategy and the general security strategy at LEAG?**

One of our corporate principles is that occupational safety, health, environmental protection, fire protection and corporate safety have top priority. When we started work on the project to implement an information security management system at Lausitz Energie Kraftwerke AG in May 2016 this was a further component. Once

the project is successfully completed and certified, the ISMS complements our existing management systems for operational and environmental protection, as well as quality and energy management.

**What sort of support would you like to see from other stakeholders with respect to cyber security, e.g. politicians, the IT industry, or even the energy sector?**

Our common objective is to guarantee safe, affordable and disruption-free energy supply for our society. We expect politicians to

create reliable framework conditions. Just as we also, of course, need planning and legal certainty from developers and manufacturers of control systems in order to be able to develop and produce secure systems equipped with long life cycles. 



**Hubertus Altmann**

Member of the board of Lausitz Energie Bergbau AG and Lausitz Energie Kraftwerke AG

**IN INTERVIEW**

**Hubertus Altmann** is a member of the board of Lausitz Energie Bergbau AG and Lausitz Energie Kraftwerke AG and is responsible for the Power Plants division. He has held this position since 2010 on the joint board of Vattenfall Europe Mining AG and Vattenfall Europe Generation AG. Previously, he spent seven years at Vattenfall Europe Generation AG as Head of Technology in the Power Plants management board division, then as Head of Power Plant Management. On his way there, Hubertus Altmann held various responsible positions at the Hagenwerder/Hirschfelde, Schwarze Pumpe and Jänschwalde power plants.

He joined the Boxberg power plant in 1980, where his last position was as head of department for boilers, equipment and conveyor technology.

Hubertus Altmann acquired his professional qualification with the academic degree “Diplom-Ingenieur” by studying energy plant engineering, specialising in energy conversion, at the Technical University of Dresden.



NE-3A type reconnaissance aircraft are also known as NATO AWACS. They are part of the NATO Airborne Early Warning & Control (NAEW&C) programme. The NATO agency NAPMA is responsible for managing the programme – from procurement to provisioning and life cycle management of the NE-3A.



# NAPMA further expands its SINA Secure Remote Access capability

The NATO agency NAPMA uses a SINA solution, enabling staff members to securely work with classified and unclassified data simultaneously. In December 2017, the specific NAPMA infrastructure which includes the SINA solution was granted security accreditation by the NATO Office of Security. Furthermore, the

agency recently decided to extend the solution. These were two good reasons for securview to talk with Mr. Stephan Sauer who is heading NAPMA's Information Management Branch.

**Mr. Sauer, thank you for taking the time to talk to us. For those not familiar, let us start out by introducing NAPMA to our readers. Who and what is NAPMA and what is the organization's mission?**

The NATO Airborne Early Warning & Control (NAEW&C) Programme Management Organization (NAPMO) was created in 1978 as a NATO Production and Logistics Organization to implement the NAEW&C Programme. This organization comprises of 17 NATO nations and is responsible to the North Atlantic Council for the NAEW&C Programme – which, in short terms, is the NE-3A aircraft, the NATO AWACS.

The NAEW&C Programme Management Agency (NAPMA) is the executive agency of NAPMO. Its 116 posts are filled by seconded military officers and civilian personnel drawn from the Nations participating in the NAEW&C Programme. Within the responsibilities granted to NAPMA, the agency manages all aspects of the Programme from acquisition through delivery and on through

In parallel, NAPMA is preparing a potential Final Lifetime Extension Programme (FLEP) for the NE-3A, which the NAPMO Nations are currently deliberating.

**Within NAPMA, what do you and your team look after? What are your key operational responsibilities, goals and objectives?**

NAPMA's Information Management Branch is the Information Management (IM) and Information Technology (IT) service provider of the agency. Its mission is to enable NAPMA with IM/IT services and capabilities needed to perform NAPMA's executive, administrative, and project management functions in an effective and efficient manner. Emphasis is on ensuring timely availability as well as quality of the relevant business information from a technical perspective.

The availability and control of information is critical to NAPMA's organizational success, because NAPMA's business is not to manufacture a product or capability, but, in the

As with other NATO entities, NAPMA shall comply with NATO-wide IT related and CIS Security policies, directives, and guidelines. At NAPMA those policies, directives, and guidelines are further tailored to NAPMA's business requirements while maintaining a security accreditation by the NATO Office of Security (NOS). NAPMA differs from other NATO bodies e.g. regarding the requirement to be able to handle information that is classified commercially sensitive, export controlled or proprietary to industries.

In daily work this means on the one hand to refresh and increase staff awareness of their personal CIS Security responsibilities and, on the other hand, to operate and maintain technical safeguards (e.g. boundary protection, secure e-mail gateway). A prominent milestone was achieved in December 2017 when NOS granted security accreditation authorizing the NAPMA NR Main CIS to store, process, or transmit information up to and including NATO RESTRICTED (NR). This accreditation included the SINA implementation at NAPMA.

With regard to the capability to securely store, process, or transmit sensitive data, it is mandatory for NAPMA to keep control and ownership of the information. Likewise, supervisory control of all external IT services/support shall remain with NAPMA. From this perspective, SINA is a great capability for NAPMA's IT to meet this requirement.

**All SINA components**, authorized and accredited for use within the classified NATO environment (RESTRICTED & SECRET), are published in the NIAPC (NATO Information Assurance Product Catalogue), which is being maintained by the NATO Communications and Information (NCI) Agency.

For more information visit: [www.ia.nato.int/niapc](http://www.ia.nato.int/niapc)

Life Cycle Management of the NE-3A. As such, NAPMA is responsible for planning and coordinating acquisition strategies and for managing contracts associated with modernization of the NE-3A fleet.

In addition, NAPMA ensures Technical Airworthiness and in this regard is responsible on engineering matters and is safeguarding that Operational, Safety, Suitability, and Effectiveness (OSS&E) requirements are adequately addressed in the Programme.

NAPMA's current modification programme is called the Follow-on Upgrade Programme (FUP) to the NE-3A, which includes mandated enhancements of the platform's air-to-air interrogation system with Mode-5 and Enhanced Mode-S capability and upgrades to the NE-3A cockpit from legacy analogue technology to a full digital "glass cockpit" environment that will enable the platform to meet current and emerging air traffic management requirements in the dense European airspace.

end, to manage information and knowledge e.g. to accomplish modernization projects, to secure technical airworthiness or to support NAPMO Governance.

Currently, NAPMA operates a small secure dedicated CIS environment centered on Microsoft technology to provide office automation and external connectivity located at one site in Brunssum, The Netherlands. The main services provided to the users are e-mail (MS Exchange), document management (MS SharePoint) and an enterprise resource planning system (SAP). With the extension of the SINA laptops and secure smartphones, around 70 % of the NAPMA staff is now equipped with a SINA laptop.

**When working in such an operational environment you need to be able to securely receive, store, work on and transmit sensitive and/or highly-sensitive data. What kind of CIS policies and processes do you need to follow to ensure compliance?**

**When you and your team formulated your requirements for a secure remote access capability, what were the key objectives and challenges you were seeking to address?**

NAPMA's objective regarding a Secure Remote Access (SRA) capability was to establish, maintain, and operate a SRA capability that can achieve a security accreditation by the NOS as an integral part of NAPMA infrastructure. Intent was to enable staff to work on- and off-site, on- and off-line with the same functionality as the in-house NAPMA NR workstations and with a similar performance. The challenge was to implement a service that not only meets the user requirements, but also fits into NAPMA's framework regarding e.g. pricing, quality of service, and implementation timelines. In addition, NAPMA strived for a system that provides the user with two strictly separated workspaces:

1. A managed workspace for NAPMA business like on any other NAPMA workstation for up to and including NATO RESTRICTED.
2. A low cost (e.g. license free) and low maintenance workspace allowing web-browsing and basic office applications during business travel (e.g. no content filtering on internet access to allow check-in for flights, etc.)

An initial SRA capability has already been in place at NAPMA since around 2012 but needed to be replaced in the autumn of 2015. Therefore, NAPMA conducted an international competitive bid, where 15 potential providers were asked for an offer. The award of contract finally was with CONET Services GmbH, who maintains and operates the SINA solution for NAPMA.


**In 2015, you obtained the SINA 'secure remote access' capability and, in 2018, you and your team decided to invest into that and triple the size of the infrastructure. How did this expansion come about and what were the key drivers and motivating factors behind it?**

The expansion of NAPMA's SRA implementation had mainly three reasons:

First of all, the NAPMA users have been very pleased with the SINA devices regarding performance and user handling. The pool of six devices, which were just temporarily assigned to staff, was almost always completely booked.

Second, when updating its IT strategy, NAPMA envisioned that working practices over the next decade will move towards a more mobile, agile approach to business processes based on mobile and remote access

solutions. Therefore, NAPMA determined the detailed requirement for mobile phones and SRA devices in early 2018 based on a functional justification (e.g. required availability of staff, work assignments outside NAPMA premises, access in case of urgency or emergency). This led to the number of around 90 SINA devices being required now.

Third, NAPMA strives to technically enhance internal collaboration. Therefore, a Wi-Fi service will soon be implemented within the NAPMA building, which – amongst others – will allow NAPMA users to work in small ad hoc teams or attend internal meetings with online access to NAPMA data. Since Wi-Fi services are limited to NATO UNCLASSIFIED, the SINA technology allows NAPMA staff to securely reach back to the classified NAPMA CIS domain from any place in the building. 

NAPMA is based at NATO's Allied Joint Force Command (JFC) premises located in Brunssum, in the Netherlands.





**Stephan Sauer**  
Chief Information Management  
Branch, NAPMA

**Stephan Sauer** is a DEU Air Force General Staff Officer currently seconded to NAPMA. From 2014 to 2017 Mr. Sauer had been the Executive Officer of the NAPMA General Manager, BrigGen Michael Hain. As a subsidiary job during this period he established the Information Assurance Section at NAPMA deriving initial Information Assurance requirements for the Final Lifetime Extension Programme of the NE-3A. Since 2017, on an interim basis since 2015, he has been the Chief Information Management Branch responsible for providing IT services to the agency. Current projects are the technical refresh of the IT infrastructure and services as well as the adjustment and optimization of the SAP-based ERP system. Mr. Sauer's last national assignment was in the German Ministry of Defence as desk officer for NATO Defence Planning.

**In terms of administering and using the SINA SRA, what are the key benefits your network and system administrators as well as your daily users have encountered and voiced back to you? Did areas such as quality-of-service, interoperability or manageability play a role in their evaluation?**

Criteria regarding performance, quality-of-service, interoperability, and manageability were key requirements for NAPMA's SRA capability and have therefore been determined prior to the bidding and included within the requirements statement. After three years of operation I may summarize that the SINA solution has fully met the users' as well as administrators' expectations regarding these criteria. The fact, that in three years of using 30 SINA devices NAPMA just had to open 12 support tickets, speaks for itself. Support tickets in this case are all service requests that NAPMA could not solve internally. These tickets included e. g. the request to assess the impact of "Meltdown and Spectre" on SINA, the plea to "whitelist" drivers for a USB peripherals (e. g. Smart-Board) or the support in migrating the SINA management server to new hardware.

With regard to the extension of the SINA devices at NAPMA, it is a fair statement that the new SRA users have fewer difficulties handling their "unknown" SINA device than they have with adapting to the software change that took place in parallel from Win 7 to Win 10 and to the new version of MS Office.

The network and system administrators benefit very much from the smooth integration of the backend and the devices into the existing IT infrastructure. Managing


the capability does not require a lot of effort. Using the same software images on the SINA, as well as remaining desktop computers, is more than beneficial. Positive feedback is also coming from CIS Security staff, who is pleased to see the separation of the restricted business workspace and the less protected session for Internet access.

**Let us change gear for a moment. With you leading the Information Management branch at NAPMA, what are some of the current and ongoing IT trends that you are seeing in your daily work? How do some of these trends affect what you are trying to accomplish?**

For a small entity it is optimistic to look for current and ongoing IT trends and technologies. However, we have to stay realistic and do not lose sight of our organizational needs. NAPMA's IT Strategy constitutes a solid baseline focused to support and enable NAPMA's mission and business requirements. Hence, after having technically refreshed the IT infrastructure and services in 2018 to a very good state-of-the-art environment, NAPMA will shift its focus in the following years on the procedural and cultural changes regarding enhanced collaboration. It has been acknowledged that working practices over the next decade is moving towards a more mobile, agile approach to business processes and are based on mobile and remote access solutions. Therefore, NAPMA's information architecture shall evolve towards meeting the next generations' approach to business engagement as a social interchange, whether from the office, home, or on the road, that supports conversation.

NAPMA's IT strives to improve or implement real-time synchronization of information, chat and user-based Video-Tele-Conferencing (VTC), cross-application workflows, enhanced retrieval functionality for business information and, not forgetting the catchwords, Business Intelligence and Knowledge Management.

**Looking into the future: What is the next step for NAPMA and the NATO Airborne Early Warning & Control (NAEW&C) Programme as a whole?**

Regarding the NATO E-3A capabilities (aircraft and related ground systems) studies and analysis on a potential Final Lifetime Extension Programme (FLEP) were conducted to determine feasible technical solutions to meet unfulfilled operational requirements, maintain the platform's operational relevance, and extend the NE-3A fleet's lifetime to support NATO operations to 2035. If approved by the NAPMO Nations, the programme will begin execution in 2019 and be completed by the end of 2026. FLEP will address mandated upgrades to the NE-3A's data link and voice communications capabilities, enhance the Wide-Band Beyond Line-of-Sight airborne networking capability and refresh the NE-3A's mission computing hardware and software infrastructure, while simultaneously addressing known and emerging Diminishing Manufacturing Source issues. 





Students at the campus of the Ruhr-Universität Bochum

## NEW EXCELLENCE CLUSTER FOR IT SECURITY IN BOCHUM

# Cutting-Edge Research with Team Spirit

**Ruhr-Universität Bochum (RUB) has been very successful in Germany's nationwide Strategy for Excellence and, from 2019, the University will become the site of two clusters of excellence, one of which will be focused on IT security. This will enable RUB to further build on its existing lead role in this field of research. secuview spoke with Prof. Christof Paar, one of the speakers at the excellence cluster.**

Germany's national and regional Strategy for Excellence is designed to strengthen Germany's profile as a hub for scientific endeavour for the long term, and continue to improve its degree of international competitiveness. The aim of the excellence cluster funding series is to bring together prominent scientists from a variety of disciplines in a location where they can work together on an area of research that has significant social or economic relevance. Out of the 195 proposals for excellence cluster topics received from all areas of science 57 were selected for

funding in a competitive selection process. 'Cyber Security in the Age of Large-Scale Adversaries' (Casa) is one such proposal and is the only cluster of excellence in the field of IT security. It offers a framework within which, between 2019 and 2026, 21 research groups will work at the Horst Görtz Institute for IT Security (HGI) at the Ruhr-Universität Bochum (RUB). The research studies will be supported by funding subsidies to the tune of tens of millions of Euros. RUB professors Thorsten Holz, Eike Kiltz and Christof Paar are speakers at the excellence cluster. 



**Prof. Dr. Christof Paar**  
Speaker at the excellence cluster

**Prof. Dr.-Ing. Christof Paar** is an expert for applied cryptography. Since 2001, he has been the holder of the Chair for Embedded Security at Horst Görtz Institute for IT Security (HGI), Ruhr Universität Bochum. From 2004 to 2007, from 2010 to 2012 and from 2016 to 2017 he was the managing director at HGI.

Prof. Paar is co-founder of the conference CHES – Cryptographic Hardware and Embedded Systems and founder of ESCRYPT GmbH – Embedded Security which is now part of the Bosch Group. Since 2009, Paar is an Affiliated Professor at the University of Massachusetts, USA. Some of his main research topics are hardware security, fast hardware and software technologies for cryptography as well as security in practical systems, i. e. vehicles or access systems. Prof. Paar has been honored several times for his research work, i. e. he was named an IEEE Fellow (2011), received the ERC Advanced Grant in the field of hardware security (2016) and was appointed IACR Fellow (2017).

### **Professor Paar, what goes on at the Casa cluster of excellence?**

Cyber security has become a central societal issue, because the type of threat posed has changed drastically in recent years. Today, many attacks on IT systems are carried out by large-scale attackers, especially by governmental organisations. Governmental adversaries are particularly alarming, since they act for the long term and have considerable technical capabilities and resources at their disposal. As can be seen from the almost weekly incidents that we are aware of the conventional security solutions against these types of attackers are, to a large extent, currently inadequate. The Casa project is focussing on countermeasures targeted at the most powerful of these attackers.

### **In your opinion, will the funding have long-term consequences for the region's IT security industry? How can it benefit from this?**

In Bochum and its environs we already have the best-developed ecosystem for cyber security in Germany. The ecosystem is based on the three pillars of cutting-edge research, education and practical application. Casa will lead to stronger cutting-edge research and application in particular. In addition, it is possible to expand the theme to current developments – such as the interplay of people and cyber security, or security and machine learning. The second crucial aspect for the region will be the Casa TransferLab. This will involve testing promising research findings with practical partners in real-world applications at a very early stage. We are concentrating on industries that are very important to the state of North Rhine-Westphalia, including Industry 4.0, logistics and eHealth.

### **What do you have planned in practice for the next steps?**

The key element of Casa is for the various research approaches in the field of cyber security to be amalgamated, with the aim of working on one of the most important security issues – possibly even the most important – in a targeted way: how can we offer long-term protection against very powerful, governmental attackers? For this purpose we have identified 11 fundamental research issues. We will be commencing our scientific work by means of selected pilot projects as early as the start of January.

### **In your view, does the Ruhr region occupy Germany's top spot when it comes to IT security?**

There are certainly still various other outstanding locations for cyber security in Germany. What distinguishes Bochum and its surroundings, however, is its aforementioned triad of cutting-edge research, education and application, combined with a cooperative team spirit that is so typical of the Ruhr region. Alongside cutting-edge research another equally important factor for long-term success is that, with approximately 1,200 students on its four specialist IT security study programmes, the Horst Görtz Institute for IT Security at RUB is the largest education facility for IT security in Europe by far. In global terms, too, the institute is already in the top 5 facilities thanks to its 20+ research groups and 200 scientists working in a broad spectrum of fields around modern cyber security. We are also leaders when it comes to application: with 20 start-ups in the field of cyber security to date, which have been taken over by companies like Bosch, Google and the TÜV (which carries out testing and product certification), we are also at the forefront nationally. In the past year Cube 5 has started work and operates as an incubator specialising in start-ups in the field of IT security.

Furthermore, it was announced in November that a new Max Planck Institute for cyber security and privacy will be established in Bochum, further strengthening the location.

### **In your view, what should effective collaboration between science and industry look like?**

Our experience over the past 20 years has shown that knowledge transfer in the field of cyber security can be very diverse. To this end we have developed various forms of collaboration. Firstly, we carry out “traditional” industry research that involves working on practical issues that arise within the industry. The second method is to carry out R&D projects in consortia with one or more companies. The projects are often funded by the BMBF [Federal Ministry of Education and Research] or the BMWi [Federal Ministry of Economics and Technology]. The third form of collaborative transfer is where research findings form the foundations for start-ups. Such spin-offs have meanwhile developed into a particular strength of the Bochum location.


### Please tell us more about your research approach to cyber security!

The special thing about the Casa cluster is its holistic approach. Although it is generally known that strong cyber security needs to safeguard all system components, science (and often industry, too) generally only pursues partial solutions. In contrast, within Casa we develop security concepts at all system levels. For this purpose we use a highly innovative concept to conduct cutting-edge research in four areas: cryptography, software security, hardware security and the human aspects of cyber security. Another factor specific to Casa is its interdisciplinary team, unique worldwide, in which professors of information technology, mathematics, engineering and experimental psychology work in close collaboration with each other.

### The availability of highly-trained specialists continues to be a priority concern in the industry. How can educational institutions and companies help generate even greater levels of enthusiasm among young people for IT security?

At the Ruhr-Universität we have been training specialists in IT security since the year 2000. Over time we have learned that cyber security ought to be taught as a separate discipline. That means that it is not enough to offer a handful of special lectures on computer security or cryptography as part of Masters programmes. Instead, cyber security must be taught in specially designed courses. It is important to teach students to think security as early as possible. It is also, of course, just as important to teach the technical security concepts at all system levels.

### What do graduates today expect from a potential employer?

To cut to the quick: an exciting work environment. Today, graduates in IT security can target virtually any employer. In my experience, the substance of the work gives most graduates the leading edge. In particular candidates with a five-year Bachelors plus Masters degree in IT security anticipate having a job that doesn't fall into a routine within a few months – and to which they can bring and build on their extensive technical expertise. In conjunction, the softer aspects are also important of course, such as the company's reputation and working atmosphere, not forgetting the salary. 

With approximately 1,200 students, the Horst Görtz Institute for IT Security is the largest education facility for IT security in Europe.



## SECURE INTERNET ACCESS IN A BUSINESS CONTEXT

## Surfing Without the Risk

**An unsecured Internet connection is still the biggest entry point for malware. The secunet safe surfer solution closes this gap by giving the browser a secured quarantine environment to work in and, to an extent, remotely controlling it. August Rüggeberg GmbH & Co. KG, the company behind the well-known tool brand PFERD, uses the solution successfully. secuvie spoke with Tim Meurer, System/Network Administrator at PFERD.**

In a four month long test phase that began in January 2017, secunet safe surfer was put through its paces at August Rüggeberg GmbH & Co. KG. The key question: will the solution fulfil the requirements of an international company?

Following the test phase we were sure that we were backing the right horse, and we decided to roll out secunet's safe surfer across the whole company. The joint introductory project, in which the Internet access architecture for all employees was transferred to safe surfer, was designed over a period of several months, during which time safe surfer terminal server cluster installations were constructed for three international locations: Marienheide (Germany), Johannesburg (South Africa) and Melbourne (Australia).

All servers are controlled centrally from Marienheide via an overarching management system. In addition, other of the company's international locations are linked to the safe surfer system via the three aforementioned locations.

**Mr Meurer, which issue was it that prompted you to start searching for an IT security solution for secure Internet access?**

We didn't just start searching two years ago. Even right at the start when we built the IT for PFERD, when the Internet was nowhere

near as important as it is today, we had our minds on security. It was clear to us that we wanted to circumvent potential threat scenarios from the Internet from the very beginning. Even the firm's first Internet access was done remotely. Using an image and keyboard/mouse transmission, which we achieved with infrastructures we had developed ourselves in a Citrix ICA terminal server environment, we created our own individual solution. We now needed a replacement for this – our system had aged considerably in the interim; it required a significant level of maintenance and could no longer fulfil all the requirements.

**How did you come across the secunet safe surfer system?**

We looked on the market for a suitable solution. The secunet safe surfer is unique. Moreover, we found the feature set very appealing, especially the ability to manage from a central hub via the management server. Previously, we had three stand-alone solutions in Germany, Australia and South Africa that had to be managed separately. This was elaborate.

Now, everything is automated and controlled centrally from Germany using safe surfer: Marienheide, Johannesburg and Melbourne serve as the three locations for safe surfer terminal server cluster installations in Germany, South Africa and Australia. Different sales offices are connected to each of these. The one in Germany not only looks after various sales offices and factories, but also other European countries such as Italy, Spain, Belgium, Sweden, Poland, France, Turkey and the United Kingdom. Plus it does so with no loss of performance! Employees there have the same latency period as I do on my computer in the central hub.

PFERD offers a combination of quality tools, drives and personalized consultation.





## IN INTERVIEW

**Tim Meurer** has a degree in Computer Science and works as System/Network Administrator within the IT department at August Rüggeberg GmbH & Co. KG. After starting out working in the administration of Microsoft products and systems, since 2008 he has mainly worked on projects and infrastructures in areas such as firewalls, VPN connections, network, segmentation and secure Internet communication in the company's IT Infrastructure and Service Management team.

PFERD maintains its tradition of over 200 years of operating as a tool manufacturer.

### How is this implemented in technical terms?

The sales offices in Germany and South Africa each use Citrix terminal services to access the internal IT infrastructure and start safe surfer within this Citrix session. In Australia, clients from the sales offices have direct access to safe surfer.

### Were there any special challenges or difficulties when carrying out the implementation process across state borders?

Well... No real difficulties... But, for example, nobody had considered that the automatic restart of the system at three o' clock in the morning German time would mean Internet access being frozen in the middle of the day in Australia. The Australian employees didn't find this very funny, naturally.

The standard language used for the web-pages in the browser was automatically set up in German, so this was quickly changed

to English. The differing keyboard layouts, too, in Turkey, France, Sweden and also in Belgium, where there are still differences even inland, had to be taken into account and adapted.

### Where in the business is the secunet safe surfer used?

It is actually used in all areas of the business, right through to management. We make no exceptions. Where direct Internet access is absolutely critical due to business requirements, e. g. with creative jobs with Adobe products, the employee uses a PC within the demilitarized zone (DMZ). In addition, employees with laptops can connect directly to the Internet via Wi-Fi, but they then do not have direct access to resources from the internal network, nor to protected systems. Even mobile phones and tablets can be used in this way. Overall, safe surfer is used throughout 98% of the company.

### How do you find using secunet safe surfer for day-to-day requirements?

#### What is the feedback from employees?

We have received lots of feedback saying that safe surfer is better than the old infrastructure, and for us in the IT department, too, this solution has fulfilled all expectations. The URL handler in particular is a giant step forward. The data lock is also used extensively.

Of course, there are various small hindrances in day-to-day work that annoy some people – depending on what their individual Internet usage looks like. We are still working on solutions. These minor inconveniences have always existed, even if they were different before. You probably have to accept this if you want to achieve this level of security and therefore have to avoid native Internet access.

## ABOUT THE COMPANY

**PFERD** is leading in the development, production and support, as well as in the distribution of tool solutions for work on surfaces and material cutting. In keeping with a tradition that dates back more than 200 years, PFERD operates as an independent, internationally oriented, family-owned company geared towards the long term. With currently 25 subsidiaries around the world, six production sites and more than 1,870 employees, PFERD Group is broadly positioned.

The combination of individual advice and innovative quality tools with the users' know-how provides the best

result for every task. As a manufacturer of hand-guided tools, PFERD feels especially obliged to tool users and would like to contribute to more safety, health, comfort and efficiency at work. The PFERDVALUE program systematically factors in working ergonomics and economic efficiency.

As an employer, PFERD stands out in terms of reliability, fairness and social responsibility. Services like PFERDBIS-TRO which offers several healthy and fresh dishes every day, a company-owned day care centre or the health and fitness initiative PFERDVITAL all contribute to making PFERD a great company to work for.

# The Evolution of the Electronic Driving Licence

**As is the case with other identity documents we are seeing an evolution of the driving licence from paper, to a chipped ID card, to a smartphone app. Due to being in wide circulation the driving licence has the potential to assert itself as the most-used means of electronic identification of individuals. Will customers at supermarket checkouts be able to use their digital driving licence in future as proof of age? Having a “mobile Driving Licence” (mDL) on a smartphone will make this and other scenarios a real possibility. What is the current state of affairs and where will the journey take us?**

We are using digital and mobile means to deal with more and more tasks in our daily lives. Even now, a standard smartphone comes with a plethora of features that make everyday life easier for us: we use it to save travel tickets or admission tickets, make mobile payments, check in to flights, participate in loyalty programmes and much more. All this is made possible thanks to a host of apps that, in combination with the smartphone hardware, are increasingly evolving to become our mobile “ID wallet” that we can use to carry out transactions requiring proof of identity.

Key signposts in the further technological development in line with this trend are factors such as user-friendliness and ease of use. In respect of this, the good old driving licence – one of the most widely utilised documents for ascertaining proof of identity – is once more at the heart of the discussion, especially since it seems to be ideally suited to mobile use.

Only a few years ago the driving licence was solely a paper document in many countries. A photo of the licence holder served as the biometric link between the document and the holder. At the start of 2013 a standardised, credit card-sized driving licence was introduced across Europe. It was then incumbent upon each individual Member State to decide whether or not to safeguard this driving licence with a chip as per other sovereign documents such as the country's official ID card or passport. In Germany the driving licence takes the form of a simple card with no integrated chip. On the contrary, many other European countries, e.g. the Netherlands, add an RFID chip to the licence card in order to provide the driving licence with greater protection and equip it with additional features.

## **International standards**

With regard to the electronic driving licence the system in question is an open one with a large number of stakeholders. These include chip producers, system integrators, the issuing authorities as well as the institutions that read the driving licence for the purposes of ascertaining proof of identity, e.g. the police. To ensure that the whole “electronic driving licence” ecosystem operates seamlessly the separate interfaces need to be standardised, from the format of the driving licence through to the structuring of the data on the chip. The International Organization for Standardization (ISO) sets out mandatory standards that enable cross-border and cross-application utilisation of the (electronic) driving licence. The relevant set of standards that numerous companies are involved in creating and maintaining is called ISO/IEC 18013. Alongside the physical properties of the driving licence this set of standards also specifies the security protocols that are used on the chip. These are designed to comply with the protocols defined in Technical Guideline TR-03110 issued by the German Federal Office for Information Security and are also in use in the context of sovereign documents.

The most recent section of this standard goes a step further and describes a mobile, digital driving licence that is liberated from the actual physical card and stored on a smartphone. In this way a smartphone can be used in combination with an app that contains the data and security protocols as a replacement for the actual physical document. In practice this could be implemented in one of two ways: either the data can be saved to the smartphone directly by a governmental authority; or the data could be loaded to the smartphone from the chip of a physical document. In the latter instance,



## THE DRIVING LICENCE

has entered the digital age and not only provides licence holders with greater convenience and security but also new features.

known as the “derived identity” method, the holder of the driving licence still owns a physical document that can be used in parallel, e. g. if the smartphone or corresponding digital reading device is not available.


### Digital, mobile driving licences in practice

Mobile driving licences will soon be used in reality within the Republic of Kosovo. In future, when having their driving licence checked drivers there will simply need to show their smartphone. To do this they would open an app and the transport police can then read and check the data electronically.

The first pilot projects have already been initiated within some states in the USA in order to analyse the technical feasibility of a digital driving licence. The assumption was that the virtual examples should retain some of the properties of a physical driving licence, e. g. displaying the licence holder’s personal information such as their name, address and date of birth, as well as a photo. For this purpose different technologies are being considered; security and usability are the key factors here too. Contrary to in the majority of European states, in the USA driving licences are often used as the primary form of ID document, since there is no official ID card. The digital version of the driving licence is, therefore, of particular interest to citizens of the USA.

Do we still need driving licences at all in the short-term, however? Won’t we all simply be chauffeured around in self-driving cars? In the view of many experts this is still a long way away from being a reality and, until that time, we humans will still be able – and will need to be able – to intervene as the last point of safety to control the car. Driving licences will still be required in the years to come, therefore.

### Completely new scenarios

As driving licences enter the digital age they not only provide licence holders with greater comfort and security but also new features. Use of a smartphone in particular offers new possibilities beyond checking individuals in traffic: driving licences are also of interest to the private sector, for example as a low-data means of checking an individual’s age when buying alcohol at the supermarket. In addition, the mobile driving licence is already designed so that other data can potentially be saved to it for the purposes of completely new usage scenarios that no one has yet thought of. 



Holger Funke  
holger.funke@secunet.com



Only a few years ago the driving licence was solely a paper document in many countries.


# PKI: the Key to the Future

Business processes are increasingly carried out electronically and confidential information is exchanged via open, internet-based platforms. For relationships based on trust to function in modern everyday life the confidentiality and the integrity of data must be ensured at all times. A public key infrastructure (PKI) is the best solution for achieving this. PKI has already become established in a wide range of applications – others will follow.

Digital certificates are used for authenticating users and technical components, as well as for signing and encrypting data and communications: they ensure, for example, confidentiality and integrity when transferring data at border control. Digital certificates are also used in the interaction of machines in the context of the Internet of Things (IoT), e.g. for authentication, integrity checks and the secure communication of electronic devices and in connected cars. A public key infrastructure (PKI) is required to generate, use and manage these digital certificates.

A typical PKI consists of a set of elements that automatically issue, distribute, and check digital certificates. These include, for example, a certificate authority (CA), which signs the certificate; a registration authority (RA), which registers the users in the CA; and a directory service (DIR), which, among other things, contains a list of invalid public keys. Taken as a whole, these and other elements make sure that the certificates in circulation are reliable at all times.

Since a PKI usually entails a high degree of complexity, applications in which the solution runs automatically in the background and the end user does not come into direct contact with the PKI are most common. A good example for this is the TLS (transport layer security) encryption protocol, which is used in HTTPS-based web servers. Largely unnoticed by the user, the browser uses the PKI for secure online banking and online shopping, for example.

This trend is also continuing in new areas of PKI applications. These include, for instance, update processes or the installation of configurations, as well as (remote) maintenance access, protecting value-added services (e.g. map updates in vehicles) or ensuring compliance between interfaces. All these are PKI-supported processes where the PKI runs in the background yet users do not come into direct contact with them. 



Andreas Hellrung  
andreas.hellrung@secunet.com

## THE SECUNET eID PKI SUITE – ONE SOLUTION FOR EVERYTHING

secunet has used its extensive expertise from over 350 projects combined with its experience from over 20 years of working in PKI design and implementation to develop its own PKI solution: the secunet eID PKI Suite is a proven, fully modular public key infrastructure not only in the domain of official documents ('eID' stands for electronic identity documents)

but also for all other purposes, including commercial applications. Individual software modules can easily be integrated into existing infrastructures or when combined can form a high-performance overall system.

Whether for security organisations, operators of critical infrastructures, the armed forces or clients from the auto-

motive sector – the eID PKI Suite acts as a reliable and highly available security framework and proof of identity in the digital world for all of them.

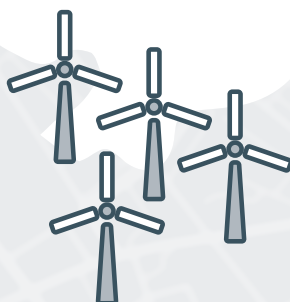
The secunet eID PKI Suite is a tried-and-tested standard solution that can nonetheless be customised to suit a very wide range of client requirements.



At **border control** PKI operates in the background as a security framework to ensure that the authenticity of identity documents can be determined efficiently, reliably and in a highly secure way, and that fingerprints can be read and verified.



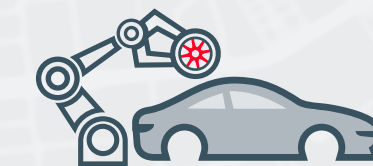
With **industrial control systems**, for example, the process control technology for wind turbines, the PKI supports remote maintenance access and manages the secure transmission of process and configuration parameters, as well as the validation of updates for a range of different systems in critical infrastructures.



For **manufacturers of control and measuring components in mechanical engineering** the PKI takes over the protection of communication interfaces between infrastructure and machine for the transmission of process parameters, machine and diagnostic data.



In **gambling machines** the PKI protects the billing data and issues device-specific certificates. In addition, there is a close linkage with the manufacturer's ERP system via a specific interface.



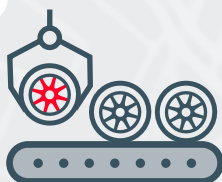
With **vehicle manufacturers** a set of certificates is created for each control unit in production during the assembly of the vehicle. Systems in production facilities around the world are equipped for this and issue certificates around the clock. Moreover, certificates are issued centrally and used in combination with value-added services (e.g. weather data, breakdown assistance, traffic and navigational data) for the purposes of mutual authentication.



Well-known applications for protecting electronics in the **automotive** sector, such as, for example, secure flashing of control units, over-the-air software, diagnostic protection, secure onboard network communication (SecOC) and secure smart charging communication (ISO 15118) can be implemented, as well as new and future tasks in the area of data services, mobility services or car-2-car communication.



In the **agricultural industry** PKI enables communication between different manufacturers' systems and is thereby the foundation for protecting the interoperability of agricultural machinery.



**Suppliers to the automotive and agricultural sectors** use PKI for, among other things, generating device-specific encryption keys in control units for diagnostics purposes, as well as for the signature of firmware updates and configuration data.

## ENCRYPTED VOICE COMMUNICATION

## SECRET Telephony: What Comes After ISDN?

The days of ISDN technology are numbered. However, crypto phones which are currently used by German government authorities still rely on ISDN for the communications and switching network. Alternatives are already on the horizon but will only be available after a transitional period. Interim solutions are therefore being sought.

For secure voice communication the public administration, the German Federal Ministry of Defence and, in a non-tactical context, the Bundeswehr (German Federal Armed Forces) currently use various ISDN encryption systems that are now outdated: in the foreseeable future, German network operators will be deactivating the 'Integrated Services Digital Network' (ISDN), which was introduced back in 1989. In an international context, ISDN has already been partially unavailable for several years now. ISDN technology is currently gradually being replaced by IP networks.

It is anticipated that the migration of open ISDN networks to exclusively IP networks will be completed more quickly than replacement devices will be available for the cryptosystems used to date. There are therefore many attempts being made today to extend the service life of the systems used by means of ISDN IP gateways. There are nonetheless issues with compatibility here, since the ISDN network uses a circuit-switched method and IP networks a packet-switched one. With ISDN networks the time of the information is always retained, which is not a given when using a gateway to an IP network. When jitters occur, i.e. packet loss or inconsistencies in the data transmission due to differing

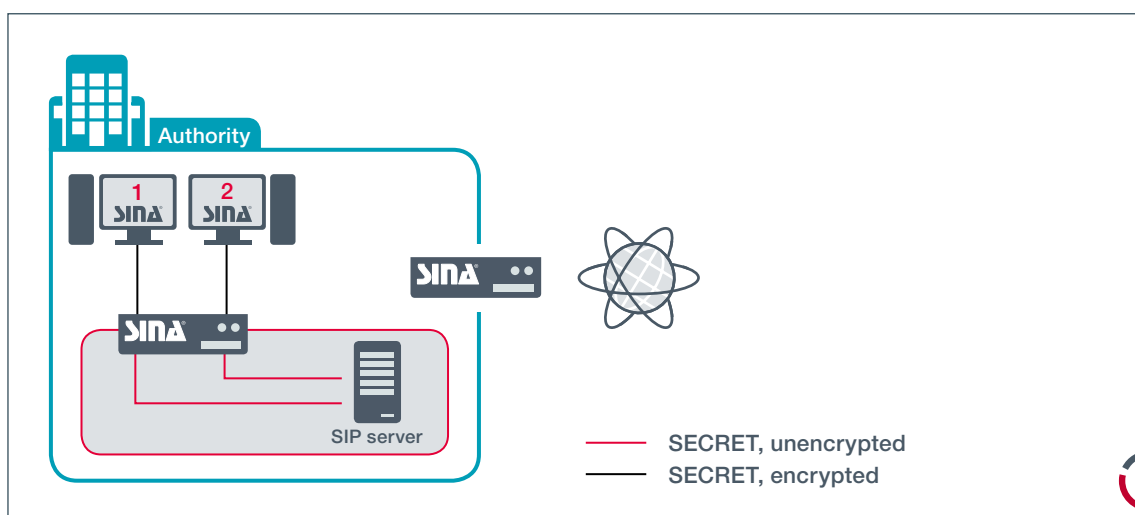
packet runtimes, it can lead to a bit slip, a loss of bits, in the ISDN connection that has been converted into IP data. This then leads to the encrypted connection collapsing.

In addition, ISDN video conference systems can only be operated to ISDN IP gateways in a limited fashion, which can also be traced back to their susceptibility to jitters. In combination with a cryptosystem, which requires a perfect bit time and cannot re-synchronise itself following a bit slip, frequent connection failures can also be expected.

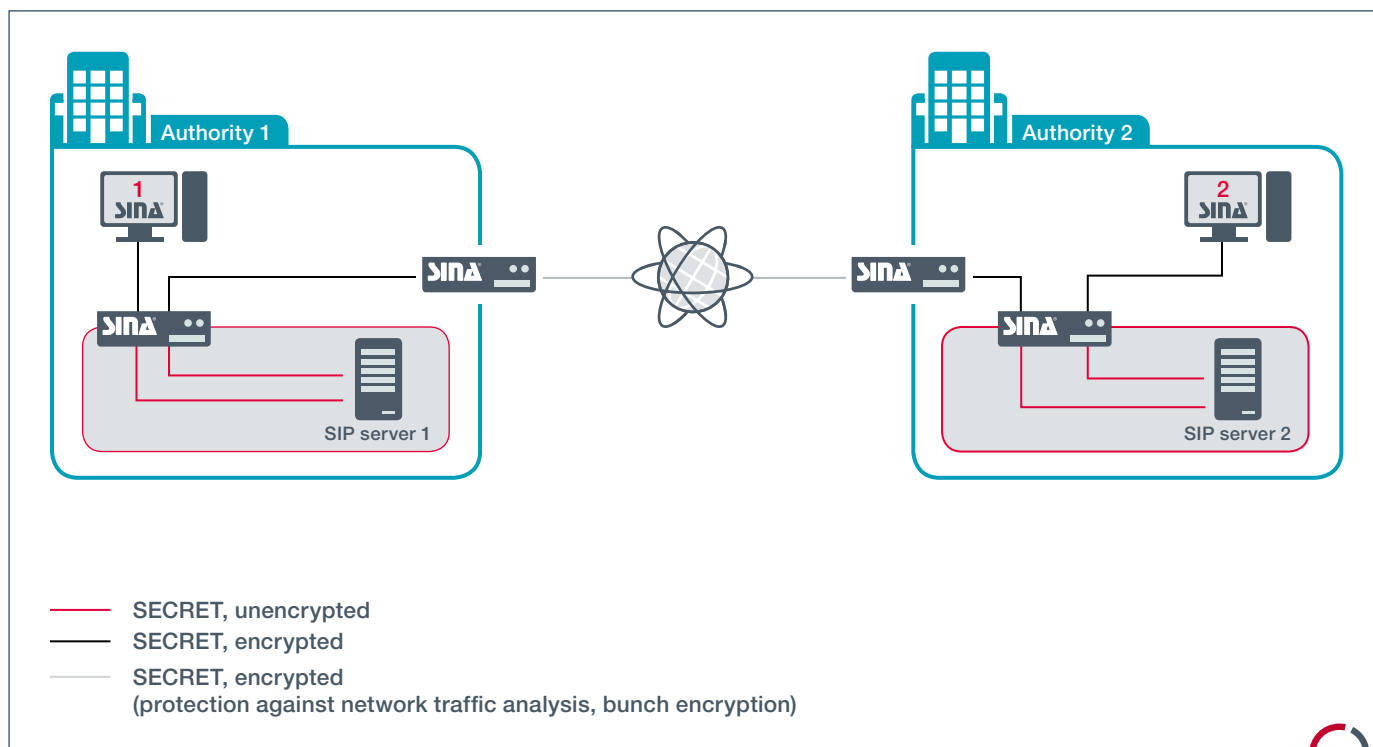
#### Commercially available interim solutions with SINA H

Today, SINA technology already offers the possibility of IP-based voice communication up to classification level GEHEIM (SECRET). With the SINA Workstation H using its integrated, dedicated VoIP session, or by connecting standard VoIP phones to the SINA L3 Box H, it is possible to communicate by VoIP using a secure IPsec connection.

We shall illustrate the first method now. With the VoIP session of the SINA Workstation H a voice over Secure IP (VoSIP) connection can be turned "red", i.e. into a network intended for classified information. The process uses the mechanisms of the



**Illustration 1**  
Functional sketch for SECRET-level voice communication with a SINA Workstation H within an authority – end-to-infrastructure

**Illustration 2**

Functional sketch for SECRET-level voice communication between two authorities with SINA Workstation H – end-to-infrastructure

SINA Workstation H and SINA L3 Box H that are authorised for GEHEIM/SECRET. The SINA Workstation H establishes a VPN tunnel to the SINA L3 Box H via a network. This provides the SINA Workstation H with access to the protected network area and the SIP telephone system can then establish a voice session between two SINA Workstations H via the SIP server. The voice data are exchanged between the SINA Workstations H and the SIP server via the Real-Time Transport Protocol (RTP). The data are transmitted unencrypted within the protected network area. However, outside of the trustworthy infrastructure, the data are encrypted in a highly secure way. This use case is shown in Illustration 1.

In the use case in Illustration 1 the integrated VoIP session is used both on SINA Workstation H “1” and on SINA Workstation H “2”. The existing IPsec mechanisms of the SINA Workstation H are used for encryption, i. e. the signalling and voice data are transported over a secure network. In this configuration there is no end-to-end security of voice communication, since the SINA Workstations H can establish security relationships with the central infrastructure

but not directly with each other. This infrastructural peculiarity is addressed by placing the VoIP server in a network segment protected by a SINA L3 Box H, as shown in Illustration 1. Within this network segment the signalling and voice data remain unencrypted. In addition, in the current implementation of the dedicated VoIP session of the SINA Workstation H, both the signalling and voice data must be routed via an authority’s SIP server.


The data and user settings of the VoIP session are stored on the SINA Workstation H within an encrypted file system. The call list, the local telephone directory, the configuration and the user settings, for example, are stored safely within it. In addition, a global directory can be set up centrally based on the Lightweight Directory Access Protocol (LDAP) and used in the session or softphone. Telephone calls can also be made between two different authorities with the SECRET level-enabled VoSIP mechanisms available, as shown in Illustration 2.

It is important to note that, as an alternative to direct routing between the SIP servers through the use of so-called session border controllers (SBC, very roughly simplified: VoIP firewalls), it is possible to achieve a

substantial separation of the different authority networks. The secunet SBC that is currently going through the Common Criteria certification process is recommended for this.

The second method of an interim solution with SINA technology functions in an equivalent way: with this option, only the SINA Workstation H needs to be replaced by standard VoIP phones in combination with the SINA L3 Box H.

### Outlook

In future, the interim solutions described above with commercially available SINA H components will be replaced by the functionally equivalent SINA Communicator H, which is currently in development. The SINA Communicator H is based on an innovative device concept for GEHEIM/SECRET communication, which unites modern communication possibilities in a compact system that meets the most stringent security requirements and which can be adapted flexibly according to future requirements. 



Jan Leduc  
 jan.leduc@secunet.com

## HIGH-PERFORMANCE SITE NETWORKING AND DATA BACKUP FOR GEO-REDUNDANT DATA CENTRES

# Networked up to SECRET-level – at Gigabit Speed

Following more than two years of seamless pilot operation of the SINA L2 Box H 1G Ethernet encryptor for a German national security organisation, type approval for classified information up to German classification level GEHEIM (secret) is expected to arrive in January 2019. This acts as the green light for a broader deployment of the powerful SINA component, which combines high security with high data throughput.

The high-performance encryption device is specified for the secure exchange of information in networks on OSI layer 2 (Ethernet) and supports point-to-point connections. Due to the low latency – this refers to the device's internal data throughput time – the SINA L2 Box H 1G is especially suited to scenarios involving high quality of service and/or real-time requirements. With a data throughput of 1 Gbit/s full duplex the device is also the highest-performing encryptor available for GEHEIM.

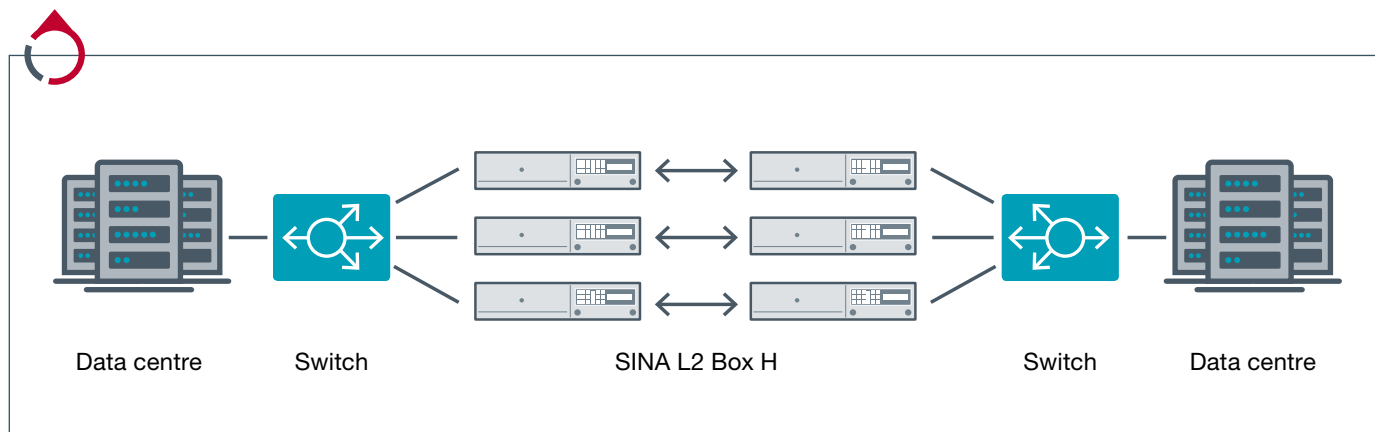
These performance features predestine the SINA L2 Box H 1G for applications where highly secure yet fast transmission of large quantities of data is required. For example, this includes broadband networking of sites, protection of backbone networks and the mirroring of data in high-availability architectures. Other use cases are data centre backup – for instance as part of the HaFIS program that the Bundeswehr

(German Federal Armed Forces) are using to implement an extensive harmonisation and modernisation of the military management information systems, as well as in the NuKomBw military message handling system.

Line encryption with the SINA L2 Box H 1G creates virtually no overheads. This means that, alongside the actual data that need to be transmitted, only a small amount of additional information that is required exclusively for the transmission process needs to be generated and sent. The solution thereby offers high data rate efficiency and is thus especially suited to satellite-based communication, for example.

The figure on this page illustrates the application of a backup of geo-redundant data centres. The data streams are distributed via switches to an appropriate number of SINA L2 Box H 1G channels (pairs) and merged again.


The figure illustrates the application of a backup of geo-redundant data centres.



This approach enables data backup architectures with a considerably more moderate number of encryption devices than is required when using SINA L3 Boxes H 200M, for instance.

The configuration of all SINA L2 Boxes H on the network is done centrally by the SINA Management. This set-up has been tried and tested in many network infrastructures over the years. An integrated Public Key Infrastructure (PKI) with associated user management supports a large number of essential administrative processes relating to the SINA Smartcards. These include customising these SINA Smartcards, generating and updating keys and cryptographic parameters, as well as managing the associated PINs and PUKs.

In operation, the SINA L2 Boxes H record data relevant to operations monitoring. These data can be imported into network management systems and be appropriately prepared and visualised there.

All initial configuration data and security links for the SINA L2 Box H 1G are stored in a protected area on the SINA Smartcard. When starting the system the SINA L2 Box H 1G software is loaded from a flash memory, while its integrity is protected. The security links are then set up in accordance with a point-to-point mode and the device is ready to use. This simple start-up and network integration constitutes an advantage under operating conditions, increasing the device's usefulness. 




Jörg Rösch  
joerg.roesch@secunet.com

## secunet protect4use: Digital Keyring for Access to Web Portals

Operators of web portals and online services can offer their users secure and convenient authentication with secunet protect4use. The new app for android and iOS transforms smartphones into digital keyrings which portal users can use to verify their identity and therefore their access authorisation. Alternatively, users can also authenticate themselves using other security mechanisms such as soft tokens, USB tokens, or smart cards. The authentication solution can be used with any browser and operating system.

secunet protect4use enables secure access to employee and customer portals operated by public authorities, or suppliers of energy, telecommunications, or insurance for example. In home banking scenarios, both the login process and two-factor authentication with secunet protect4use can be used for secure transactions which were

previously processed using TAN procedures. In contrast to those traditional methods, authentication with protect4use does not generate any costs for additional tokens or other means of authentication. The high level of security that the solution offers enables many usage possibilities, for example in authentication to comply with the written form requirement in citizens' portals, the triggering of remote signatures, or the encryption and signature of data. The flexible client/server solution provides both the user and the portal operator with a wide range of convenient login options, including secure multi-factor and multi-channel authentication.

The secunet protect4use app is available to download now from the Apple App Store and Google Play Store. Clients for Windows, Linux and MacOS are also available. 



Gregor Boeckeler  
gregor.boeckeler@secunet.com

# Enigma Model, Built 2018

**Klaus Kopacz builds functional, faithfully reproduced replicas of the famous historical Enigma encryption machine. One of these now takes pride of place in the showroom at secunet's Essen headquarters.**

Klaus Kopacz slowly opens the wooden casing. A device emerges that, at first glance, resembles a typewriter. This is a brand new encryption machine that Kopacz has just finished making and is now presenting to his client. A logo familiar to anyone interested in cryptography is emblazoned on an open-out section at the front of the device: within an oval-shaped outline the word "ENIGMA" is visible. This is not a scene from the Twenties or Thirties of the last century but happening now in 2018, and the machine in question is a replica, a faithfully reproduced copy of the original. The client is nonetheless impressed – possibly not so much by the device's cryptographic ability, which is approximately 80 years past its prime; the historical accuracy of the replica is captivating, however – and, on top of this, it is fully functional.

It's not only since the novel of the same name by Robert Harris and the cinematic thriller of 2001 based on it that the Enigma machine has been seen as the most well-known encryption machine. The coding machine developed in 1920 by Berlin-based electrical engineer Arthur Scherbius made it possible to have extremely strong codes for the time given the state of cryptography at that point. It was used by the German armed forces during World War II but also by other organisations within the National Socialist regime for communicating secretly. With considerable effort the Allies managed to crack the codes, however, and to decrypt the Germans' radio messages. In addition, the British built a whole industrial enterprise – originally based on the findings by Polish mathematicians – around the Bletchley

Park country estate close to London, which was dedicated to decrypting the Enigma messages with the help of specially designed machines (known as "Turing bombs"). This "Ultra organisation" at times involved up to 12,000 people, who were sworn to the strictest secrecy.

Even though some German soldiers might have suspected in the latter years of the war that the Enigma codes had been broken, members of the German Reich generally proceeded on the basis that they were trustworthy. The device was therefore manufactured in large quantities and used up until the end of World War II. The Allies used the advantages they gained from decrypting the Enigma codes for military benefit, ultimately shortening the duration of the war. This remained secret for a long time though: the German Federal Intelligence Service only found out in the Seventies that the Enigma had been cracked.

This baffled a large number of experts at the time, since, even in the Seventies, the Enigma codes were still seen as a "tough nut to crack". One of the later models that the navy had used during World War II utilised a key space – the number of possible keys – of  $10^{23}$  possible combinations. Even with today's computing technology it is impractical to crack these types of keys using the "brute force" method alone, i.e. using an automated method to try out all the possible combinations. What helped the British and Polish in their decryption efforts were cleverly applied statistical processes, as well as errors by the Germans when using the device. In addition, the Allies succeeded in capturing some Enigma machines.

**The showroom at the secunet headquarters in Essen (Germany)** is home to a replica Enigma machine built by Klaus Kopacz. Registered visitors to the company can therefore learn more about both the past and the present status of cryptography.



This Enigma reproduction is identical to the original down to the last detail.

from simple encryption methods. The possible settings included the capability to exchange the rotors and adjust their rotation patterns; furthermore, the current flow could be modified by plug-in cable connections. The latter option was the strongest cryptographic element. The operator used a secret table to check which Enigma settings should be set each day.

The Enigma M4 model, which featured the addition of a fourth rotor, demonstrated how significant the rotors were as it considerably increased the number of possible options. When this model was deployed in the navy in 1942 it caused a setback for the Allies. For ten months they were unable to read and decipher the encrypted radio messages sent using the M4 until the cryptologists in Bletchley Park managed to crack this method too with the help of coding documents they had seized.

### An encryption device as a collector's item

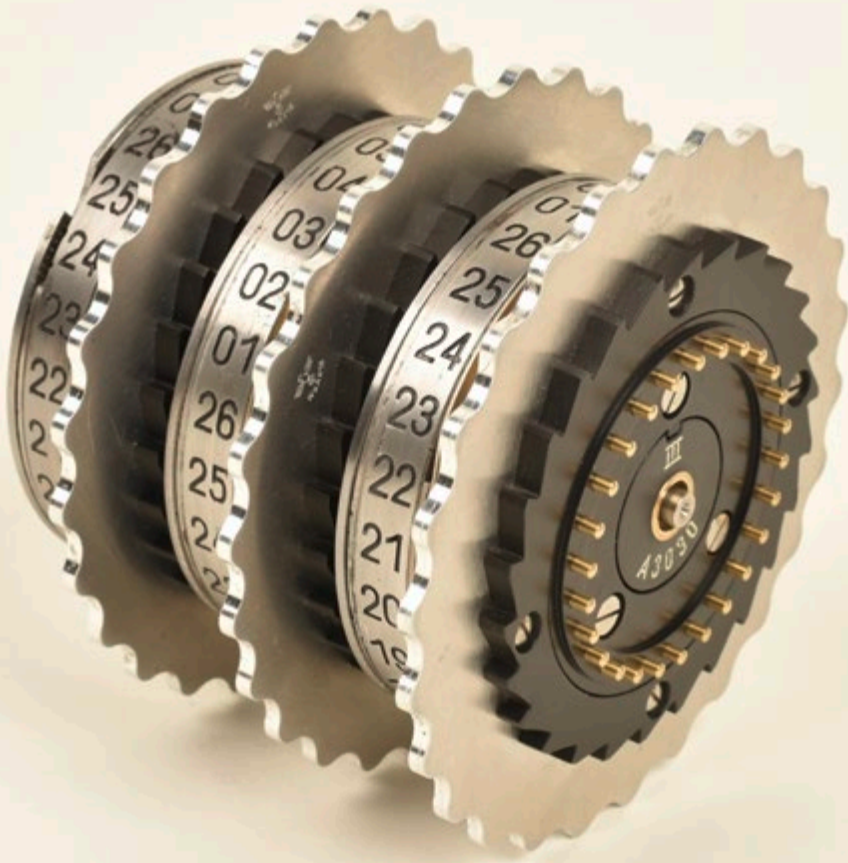
An estimated 46,000 models of the Enigma were built in all. Today, only around 300 still remain in existence. This is mainly due to the fact that the German soldiers were instructed to destroy their Enigma machines rather than let them fall into enemy hands – though this did happen on occasion. As the Enigma turned into a collector's item long after the war its limited availability pushed prices up.

Klaus Kopacz, who worked with modern encryption devices, therefore had the idea of constructing new, replica Enigma machines. "Enigma became my hobby in the Eighties," recalls Kopacz. "I then had the opportunity to renovate and restore museum pieces, which enabled me gradually to acquire incredibly detailed knowledge of these devices. As the Enigma became more popular as a collector's item counterfeit devices entered circulation and I was asked to identify them. A friend from the automotive industry then called me and told me about computer

### Complex inner workings

At the heart of the ostensibly high encryption performance of the Enigma were its rotating discs, or rotors. Depending on the model, an Enigma had either three or four rotors. Every time a button was pressed a current of electricity flowed through the rotors and, depending on its current position, illuminated

one of 26 character lights. An "A", for example, became a "G". At the next press of a button the rotors turned, so that this time, entering the letter "A" no longer resulted in a "G", but, depending on a series of settings, might become a "C", for example. The turning of the rotors and the manifold possible settings were what distinguished the Enigma



Rotors in a reproduction Enigma

small-scale production series. “An Enigma is composed of 3,200 parts and 378 different part types. Most part types require specialised tools and moulds to be manufactured, for instance. This can’t be justified for just one or two Enigma replicas. It was therefore the plan right from the start to follow our first example with a series of others.” There is certainly demand for Enigma copies that are faithful to the original: museums, universities, companies, collectors – all are among Kopacz’s clients.

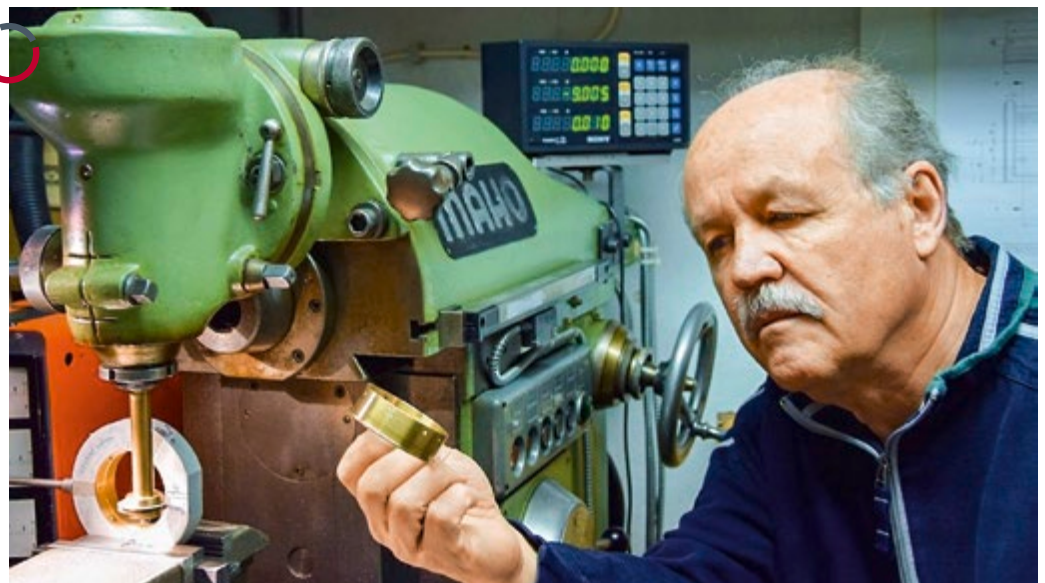
Ten replicas have so far been created; another small-scale series is in production. It is not possible to create many more, since the meticulous and detailed work swallows up many hours of work. It is also challenging to procure faithfully reproduced small parts in comparatively small quantities. “My partner in the automotive industry has good contacts with suppliers, which is very helpful. It’s not always easy, though, to convince a manufacturer to supply us with 5,000 screws made according to historical specifications; and to do this at a cost that is halfway reasonable. This type of company normally produces in batch quantities of upwards of 100,000 units,” explains Kopacz.

models that are based on scanning a real object by laser beam. Together we developed the idea of using this method to reconstruct an Enigma machine. We then actually put the project into action: after five years we had finished the first replica. That was in 2013.”

### The Enigma goes back into production

The copy was identical to the original down to the last tiny screw and was fully functional. Kopacz then quickly learned, however, that the enormous effort was only really worth it if the Enigma replicas were manufactured as a

Klaus Kopacz in his workshop






### Database for Enigma components

The parts that Kopacz doesn't build himself come from 123 different suppliers in all. This shows the high amount of organisational effort needed alongside the actual construction work, and it is also very time-intensive. Kopacz maintains his own database of the various part types and manufacturers. Even establishing the specifications for the parts is a science in itself. Since the genuine Enigma models varied slightly over the years there are no universally correct Enigma specifications. Kopacz therefore calculated the average values and it is these that form the basis of his replicas. In addition, Kopacz had to opt for one of the many historical Enigma models. His copies are based on a 1935 model featuring three rotors that was used by the army and the air force and was widely in circulation.

Kopacz is convinced that the effort is worth it when you look at the result of all the work. "My copies are truer to the original than many of the originals," he says. "This is because some museums are home to poorly restored Enigma machines that are not even functional. I have even had collectors who already own original machines commission me to construct a replica anyway because they want to own an Enigma that actually works."

Kopacz is delivering the final machine in his first small-scale production series to a sponsor who is loaning the machine to the British National Museum of Computing. The museum is located in a very special place: Bletchley Park. 




**Klaus Kopacz**  
Builder of the Enigma replicas

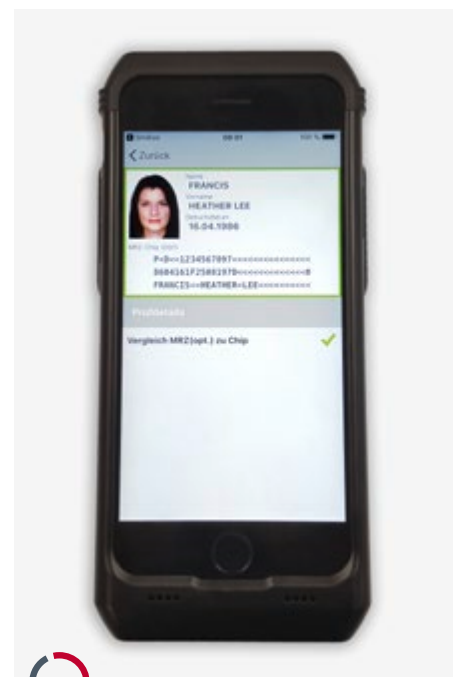
## First iPhone App for Electronic Identity Checks

The secunet app for mobile identity checks, secunet bocoa, is now available for the iOS platform. For the first time, police forces will be able to use iPhones for mobile identity verification, taking advantage of the proven solution for checking electronic identity documents (eID). With Android and iOS, secunet bocoa now supports the two most common operating systems for smartphones.

In a matter of seconds, the secunet bocoa software application reads the data from the RFID chip of the electronic ID document and clearly displays document check results on the smartphone. The app is based on the proven secunet biomiddle platform, which allows a flexible integration of the verification processes as well as software and hardware components via standard interfaces.

The hardware for the new iOS-based solution is provided by secunet's partner Dataphone, an international company based in Switzerland. Dataphone develops innovative and reliable mobile soft- and hardware solutions for warehouse management, transport and retail.

For the iOS-based solution, Dataphone provides the necessary innovative hardware sleeve including NFC module and spare battery. Combined with the appropriate certificates, smartphone sleeves from the Linea Pro series make it possible to read and subsequently also check the RFID chips contained in eID documents (e.g. ID cards, passports, residence permits). 



The iOS-based secunet bocoa app displays the data read from the RFID chip of the electronic identity document.



At the AFCEA Europe Cryptography Workshop in Brussels, 13 September 2018, Dr. Kai Martius moderated the panel “Technological Challenges Today: Benefits and Disadvantages of Classical Crypto Technologies”.

## Everything Secret, Complete Insecurity?

### Commentary on the Cryptography Workshop at AFCEA Europe by Dr. Kai Martius

In September AFCEA Europe hosted a rather different sort of workshop in Brussels. The spotlight was not on the applications, but rather much more on a fundamental debate over regulations and processes for future cryptographic processes in security and defence. Approximately 90 experts and interested participants from the industry, management, defence and scientific sectors came from all over Europe and the USA to convene and exchange ideas.

Interoperability – the buzzword par excellence! But how does it work? There are high expectations of the NATO standards, for instance. Many of those involved do not always ensure the best (and therefore most secure) result, however, and sometimes not the fastest either. Once the standard has been defined and laid down the industry product development cycles begin, ideally already accompanied and flanked by the certification process. At the same time, the product life cycles of standard hardware and software (commercial off-the-shelf) become shorter. How then does high security still fit within the modern product landscape? With a high development dynamic internationally – 5G, quantum computers, etc. being imminent – the challenges of subjecting cryptography to new policies in order to cope with this dynamic are significant. The critical factor is, as ever, “time”.

Or shouldn't we integrate security into standard products straightaway, as far as possible? In any event, a secure supply chain is essential: it is critical that components required for security also come from a trustworthy source.

The dynamic of technology developments could, however, lead to effective and tested industry standards also becoming the standards used in highly secure areas of application, such as the protocol interoperability with IETF (Internet Engineering Task Force). Industry standards work because, due to the market volume, many rely on these same standards and interoperability is achieved as a result of this. At the same time, shortened standardisation processes enable faster availability.

At the end of the workshop day there were many findings and proposals, no finished solutions – and yet there was a shared understanding and awareness of the issue. A good start for initiating this process of change further, which does not weaken the level of security but which triggers measures to make crypto policy more flexible and thus enable faster production for industry and faster provision for the user. 

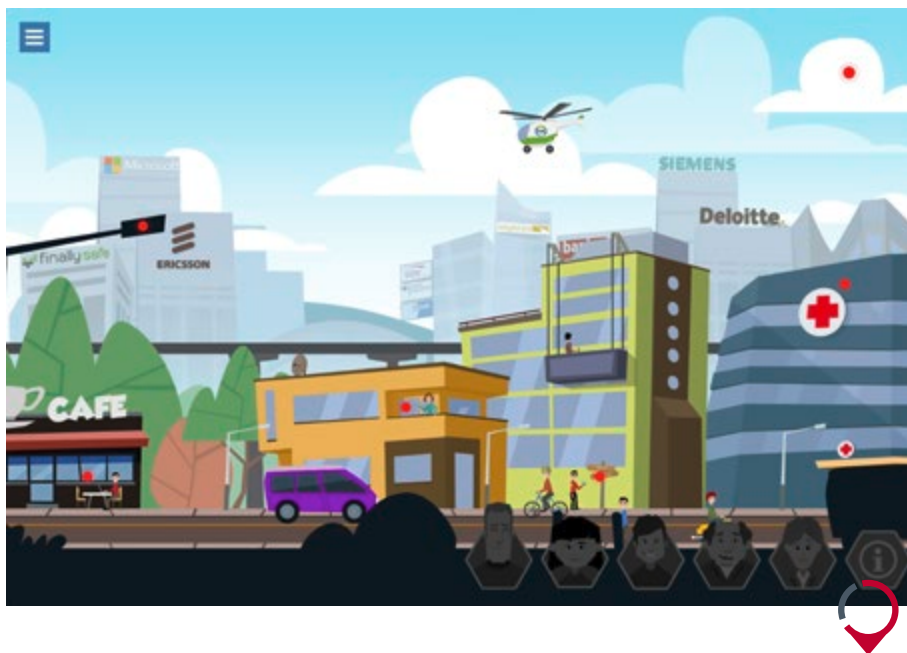


**Dr. Kai Martius**  
CTO of secunet Security  
Networks AG

# finally safe Presents AI Solution at Digital Summit

There are now intelligent solutions to the most stringent requirements for IT security thanks to the Advanced Security Analytics Platform from finally safe GmbH. At the Digital Summit in Nuremberg finally safe presented a solution that uses artificial intelligence (AI) to detect unwelcome network traffic. Through the use of Deep Learning unusual traffic can be recognised more efficiently, allowing behavioural discrepancies to be identified more rapidly.

You can find further information at: [www.kinsights.de](http://www.kinsights.de) or [www.finally-safe.com](http://www.finally-safe.com)



The website [Kinsights.de](http://Kinsights.de) – which is currently only available in German – provides information on artificial intelligence and how it is already used in everyday life.


## Marcel Taubert Strengthens secunet's Defence Division

The defence division at secunet Security Networks AG has achieved strong growth in recent years, as shown by the latest major contracts with the Bundeswehr (the German Federal Armed Forces) and BWI GmbH, for example. At the same time, the German Federal Ministry of Defence (BMVg) has made the decision to use secunet's SINA technology as its IT security architecture in future, both within the Ministry and the whole of the Bundeswehr.

This is the reason behind secunet's decision to expand the division's management team: on 1 October 2018, Dr. Michael Sobirey, under whose leadership the division has grown exponentially, was joined on the leadership team by Marcel Taubert.

Taubert has both a degree in Business Informatics and an MBA. He also brings over 13 years of experience of active service as a naval officer operating on a variety of assignments in the German Bundeswehr

and most recently held the rank of Kapitänleutnant (Captain Lieutenant). In recent years Taubert has worked at Rohde & Schwarz Cybersecurity, most recently as Director IoT and Strategy Executive Officer. Furthermore, he is involved with national IT security associations. As a member of the division's leadership team Marcel Taubert will not only bring his many years of experience in the Bundeswehr and take responsibility for sales activities; thanks to his experience in the IT security market he will also inject the division with considerable inspiration to further develop its remit.

The division's leadership deputy will continue to be Matthias Neef, who has headed up the consultancy area for over a decade. 



**Marcel Taubert**  
Head of Defence Division,  
secunet Security Networks AG

## WORLD'S LARGEST IT SECURITY TRADE SHOW

## it-sa Sets New Records


The 2018 edition of it-sa set new records. With a total of 696 exhibitors this is now the largest specialist trade show for IT security in the world. The show also recorded a big increase in the number of visitors attending, attracting 14,000 visitors this year. "Our exhibitors are enthusiastic. In parallel with the dynamic development in their industry, they have developed it-sa at the Nuremberg exhibition venue into the central platform for IT security," says Petra Wolf, Member of the Executive Board of organizer Nürnberg-Messe.

secunet has been exhibiting here from the word go and joined in the celebrations in Nuremberg this year for the show's 10<sup>th</sup> anniversary. The trade show was an unmitigated success once again, with a new trade show stand and exciting cyber security solutions for e-government, public authorities, critical infrastructures and industry. In addition to plenty of fascinating client conversations the secunet team was delighted to receive a group of distinguished visitors on the opening day, when the VIP tour stopped at secunet: Andreas Könen, Head of Cyber and Information Security at the German Federal Ministry of the Interior, Building and Community, together with BSI President Arne Schönbohm

and CEO of Bitkom Susanne Dehmel, spoke with the team about the latest secunet developments on the subject of mobile identity document checks, among other topics.

### The significance of it-sa as the "home of IT security" in Nuremberg

In parallel to it-sa, the fourth IT-Grundschutztag 2018 (IT baseline protection day) took place at the Nuremberg Exhibition Centre – secunet was authorised to organise the event for the German Federal Office for Information Security (BSI). More than 250 visitors spent a day learning in depth about modernised IT baseline protection.

The it-sa lecture programme drew in the visitors once more. A total of five fora and around 350 talks covered the entire spectrum of IT security. For international guests there was also a forum held exclusively in English for the first time. To ensure that the much-needed next generation of IT security experts didn't miss out, students on degree courses related to IT security and adjacent subjects were given the opportunity to contact and engage with companies and potential future employers at MesseCampus@it-sa. 

### SEVENTH GERMAN IT SECURITY AWARD PRESENTED AT it-sa

Five teams and their projects made it to the final of the seventh German IT Security Awards. The award was presented on 9 October 2018 at it-sa in Nuremberg for the first time. Consisting of a prize fund totalling EUR 200,000, the award granted by the Horst Görzt Stiftung is one of the highest-value, privately donated business awards in Germany. Entries were evaluated by a jury of experts via a dual-stage process based on three criteria: "Degree of innovation", "Usability" and "Real market opportunities". Dr. Rainer Baumgart, CEO of secunet Security Networks AG, was part of the jury.

The winner of this year's German IT security award is the Bochum-based start-up Physec, a spin-off from the Ruhr-Universität Bochum (RUB). The expert jury chose Physec's unique security concept for the Internet of Things as the best innovation submitted.



More than 14,000 people attended it-sa 2018.



At it-sa 2018 secunet presented solutions for mobile identity document checks, among other things. From left to right: Torsten Henn, Thomas P. Schäfer (secunet), Arne Schönbohm (German Federal Office for Information Security, BSI), Dr. Rainer Baumgart (secunet), Andreas Könen (German Federal Ministry of the Interior, Building and Community) and Dr. Holger Mühlbauer (TeleTrust).

## Axel Deininger Elected to the TeleTrust Executive Board

At the TeleTrust General Meeting on 30 November 2018 Axel Deininger, member of the secunet Security Networks AG board, was elected to the TeleTrust executive board with a large majority. Other executive board members appointed are Karsten U. Bartels (HK2 Lawyers), Dr. Kim Nguyen (Bundesdruckerei GmbH) and Prof. Norbert Pohlmann (Westphalian University of Applied Sciences/Institute for Internet Security).

The IT Security Association Germany (TeleTrust) is a widespread competence network for IT security comprising members from industry, administration, consultancy and research as well as national and international partner organizations with similar objectives. With a broad range of members and partner organizations TeleTrust embodies the largest competence network for IT security in Germany and Europe.



From left to right: Karsten U. Bartels, Dr. Kim Nguyen, Axel Deininger, Prof. Dr. Norbert Pohlmann

## One of Eleven secunet Locations

## SECUNET ILMENAU


## Compelling Proximity to Research

After introducing the secunet site in Paderborn, East Westphalia, in the last issue, this time we are travelling to the northern edge of the Thuringian Forest, more specifically to Ilmenau. The city of Goethe and the University, Ilmenau is located around 33 kilometres from the state capital of Erfurt and has a population of circa 26,000 – including 6,000 students currently studying at the Technical University (TU).

The existing collaboration with the TU, which has already been going for several years, was another factor that motivated secunet to set up the site at Ilmenau a good 18 months ago. Innovative functionalities for SINA technology, such as SINA SOLID for example, are being developed as part of joint telematics/computer networks projects run by secunet and the Department of Computer

Science and Automation under Dean Prof. Schäfer. SINA SOLID enables complex IPsec networks to be configured in a flexible and automated way. The highly qualified graduates enrich the project work on upgrading the SINA product family to make it future-proof.

In addition to prestigious research the Ilm-Kreis district has yet more to offer: the region is prized in particular for its countryside, which features a wealth of hiking trails and castles, the highest mountain in Thuringia and a UNESCO biosphere reserve. The Rennsteig, for example, is not only one of the best known, but also one of the most popular high-level hiking trails in Germany. Anyone who has ever hiked to the heights of the Thuringian Forest will understand where the city's slogan, "Ilmenau himmelblau" ("sky-blue Ilmenau") comes from.

secunet's bright, friendly premises are situated very close to the University, in the midst of lots of small high-tech firms that have established themselves as spin-offs from the TU – a sort of mini 'Silicon Valley'. The site is continuing to focus on sustainable growth and benefits from excellent transport connections, especially towards Dresden, Berlin and Munich. The premises also have their own beach volleyball field – something no other secunet site can offer. Students who want to get involved at a practical level are just as welcome as industry professionals. You can find details of current vacancies (in German language) at <https://jobs.secunet.com>. 



On the first anniversary of the site's opening Prof. Udo Helmbrecht (right), Director of the European Network and Information Security Agency (ENISA), visited the Ilmenau site. secunet's CEO, Dr. Rainer Baumgart (left), highlighted the successful scientific collaboration with the TU in his presentation.



# Dates – January to June

21–23 January 2019  
**Omnisecure** | Berlin, Germany

7–8 February 2019  
**ManuSec Europe Summit** | Munich, Germany

12–13 February 2019  
**StrategyDays IT Security** | Bergisch Gladbach, Germany

17–21 February 2019  
**IDEX** | Abu Dhabi, United Arab Emirates

19–20 February 2019  
**22<sup>nd</sup> European Police Congress** | Berlin, Germany

26–27 February 2019  
**3<sup>rd</sup> European GeoInformation Symposium** | Berlin, Germany

4–8 March 2019  
**RSA Conference** | San Francisco, USA

12 March 2019  
**SINA User Day** | Bonn, Germany

16–17 March 2019  
**Chemnitz Linux Days** | Chemnitz, Germany

26–28 March 2019  
**Passenger Terminal Expo** | London, UK

8–9 April 2019  
**Rethink! IT Security** | Hamburg, Germany

9–11 April 2019  
**DMEA** | Berlin, Germany

10–11 April 2019  
**AFCEA Exhibition** | Bonn, Germany

11–12 April 2019  
**ID @ Borders & Future of Travel Conference** | Vienna, Austria

15 May 2019  
**secunet Annual General Meeting** | Essen, Germany

21–23 May 2019  
**BSI Congress** | Bonn-Bad Godesberg, Germany

11–13 June 2019  
**Security Document World (SDW)** | London, UK

18–20 June 2019  
**ID4Africa** | Johannesburg, South Africa

25–27 June 2019  
**ICAO Trip Symposium** | Montréal, Canada

Would you like to book an appointment with us? Just send an e-mail to [events@secunet.com](mailto:events@secunet.com)

## Imprint

### Publisher

secunet Security Networks AG  
Kurfürstenstraße 58, 45138 Essen, Germany  
[www.secunet.com](http://www.secunet.com)

### Chief Editor, Head of Design, Content and Advertisement (Press Law Representative)

Marc Pedack, [marc.pedack@secunet.com](mailto:marc.pedack@secunet.com)

### Design and Setting

sam waikiki, [www.samwaikiki.de](http://www.samwaikiki.de)

The contents do not necessarily reflect the views of the publisher.

### Copyright

© secunet Security Networks AG.  
All rights reserved. All content herein is protected under copyright law. No part of this magazine may be reproduced or otherwise used without the prior written consent of secunet Security Networks AG.

### Photo credits

cover: © Simon Bierwald/INDEED Photography  
p. 2 top left/20/21: August Rüggeberg GmbH & Co. KG  
p. 2 bottom right/31/32/33 top: Klaus Kopacz  
p. 3/7/33 bottom/34 bottom/37/38: secunet  
p. 5: Roland Krebs  
p. 8: imageBROKER/Alamy Stock Foto. Fotograf: hwo  
p. 10/11 right: LEAG/Andreas Franke  
p. 11 left: Rainer Weisflog  
p. 12/13/16: NAPMA  
p. 15: Source & Copyright©, Luchtopnames NATO HQ JFC Brunssum, Flickr: Allied Joint Force Command Brunssum  
p. 17: © RUB, Marquard  
p. 18/19: © Simon Bierwald/INDEED Photography  
p. 23: shutterstock  
p. 34 top: AFCEA Europe  
p. 35 top: Screenshot KInsights.de/ Deutschland sicher im Netz e.V.  
p. 35 bottom: Marcel Taubert  
p. 36: NuernbergMesse – Thomas Geiger

## SUBSCRIBE TO SECUIVIEW

Would you like to receive secuvieview on a regular basis, free of charge? Choose between the print and electronic versions and subscribe at

[www.secunet.com/en/secuvieview](http://www.secunet.com/en/secuvieview)

There you can also change your preference or unsubscribe.



## **Trusted IT Security** **Made in Germany**

We work wherever the stakes are high. Where sensitive data and identities are fundamental values for companies and public authorities. Where our clients face complex security challenges.

Our specialists offer the government, society and the economy reliable protection against cyber threats. We offer IT security solutions for digital and networked infrastructures – catering to the highest levels of confidentiality.

[www.secunet.com](http://www.secunet.com)

**secunet**

IT security partner of the Federal Republic of Germany