secuview

The secunet Customer Magazine

2|2019

100,000 SINA WORKSTATIONS S DELIVERED

Modern Working in Public Administration × 100,000

On the way to the secure cloud

secustack offers cloud computing for organisations with very strict security requirements

Telematics in healthcare

Next, please: now it's the turn of hospitals

9 Military-grade information security on the go: secure remote access at a NATO IT infrastructure

National

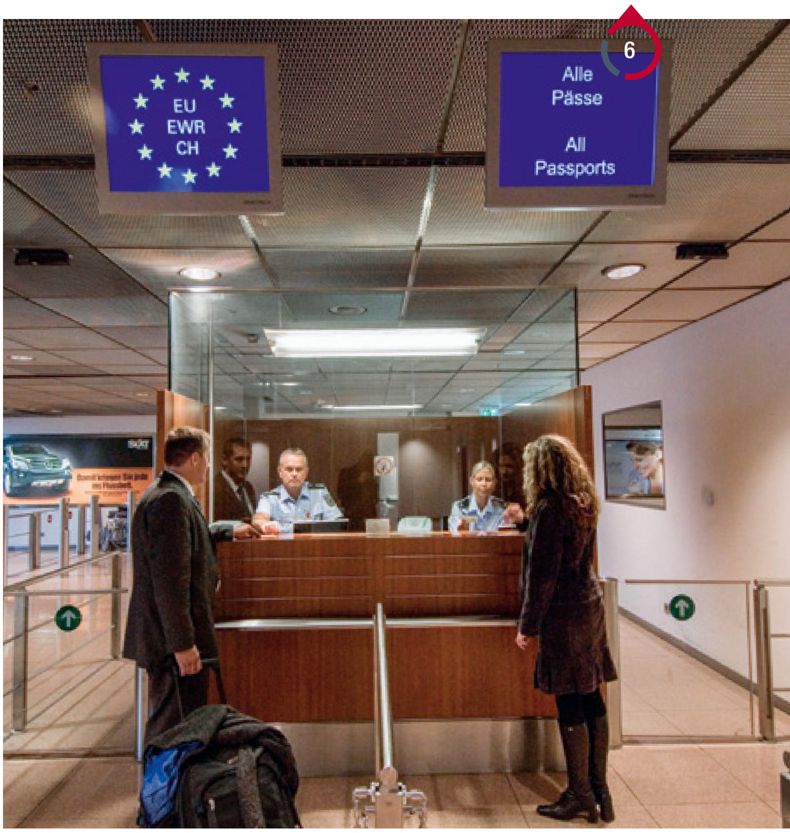
International

Science

Technologies & Solutions

Integrated border control application IGA 2.0 – fit for the border control of the future

6



News in Brief

Service

Editorial

Dear Readers,

even though, strictly speaking, the current decade includes the year 2020: we are already at the end of the “2010s”, as they’re commonly known. For the IT security industry in general, and secunet in particular, this past decade has been a time of change and growth.

High-level IT security technologies, which were originally designed for highly specialised niche markets, have become widely prevalent. An example: around ten years ago the forerunner to the later SINA Workstation S had just been approved by the German Federal Office for Information Security. Today, this crypto client is the standard workplace in numerous regional and federal authorities, and has modernised and digitalised work processes in public administration thanks to its mobility and flexibility. In our cover story we trace this development and show the diverse range of possible applications SINA Workstation offers in its different forms today.

A second example: the secunet eID PKI suite, our construction kit for public key infrastructures and a further cornerstone of our product portfolio, only left the secunet development unit in 2010. Today, solutions based on this suite can not only be found in their original deployment sphere of biometrics and identity checks, but also in industry and energy supply.

There is no end in sight for this evolution. Advancing digitalisation and connection require more and more areas of the state, economy and society needing protection to be equipped with high-performance IT security technology. Public administration, security and defence authorities have made excellent progress in this respect. Again and again, there are exciting new projects here, as the articles about secure e-files and SINA installations in military helicopters show.

The changes will be even bigger in sectors that have a lot of catching up to do. This includes industry first and foremost. Securing connected machines in production facilities is a significant challenge for the operators. Today, there are already solutions available to address this challenge. In the article in this edition of secuview on building automation we outline another topic with considerable potential with respect to IT security.

Artificial intelligence, 5G, autonomous driving – the 2020s are likewise going to be shaped by topics relevant to IT security. They are bound to be no less fascinating.

I hope you enjoy reading our magazine. Have a great 2020!

Ihr Axel

Axel Deininger

DIGITALISATION IN ADMINISTRATION

Finally Combined: E-Files and Classified Information

The transition to electronic files ('e-files') in the German Government's ministries and federal authorities will be completed over the next few years. One challenge has so far remained unresolved, however: until now, normal e-files and classified information have had to be managed separately, which has led in particular to additional costs and media disruptions where information has only been classified at a later point in its life cycle. How can this obstacle be overcome without jeopardising the confidentiality of the classified information? A joint solution from Materna and secunet has established the interoperability of e-files and classified information, and thus marks another step on the journey towards the digitalisation of administration.

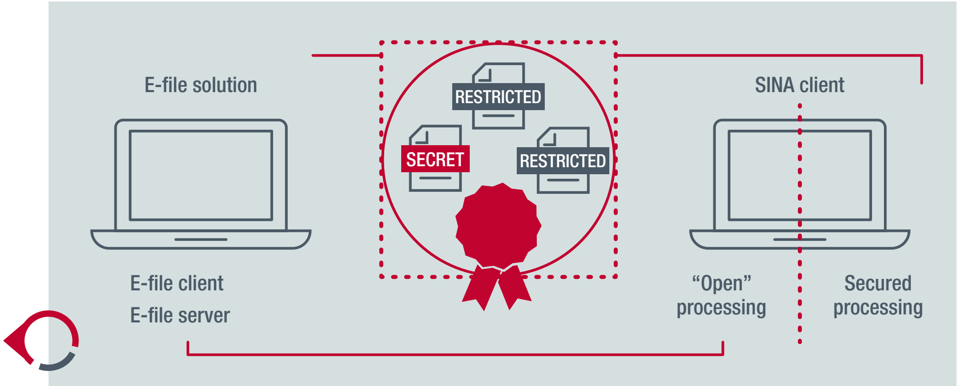
Public administration, too, is to benefit from the potential offered by digitalisation. To achieve this, in 2013 the German e-Government law was passed. This requires the majority of federal authorities to convert their previously paper-based files to electronic solutions – the aim is paperless administration. This transformation is already in full swing: the so-called "E-Akte Bund" (federal e-file) is currently being tested in various ministries and authorities through a series of pilot projects. The forerunner of the initiative is the Ministry for Justice, which is expected to have completed the majority of the conversion by the start of 2020. In other ministries and authorities the process will take place over the next few years and is expected to continue until 2024.

Germany's "Länder" (federal states) are at a similar point: they are also required to implement e-files, and North-Rhine Westphalia (NRW), for example, which brought in the NRW e-Government law, is anticipated to complete the introduction of e-files by 2022 with the assistance of Materna Information & Communications SE and Ceyoniq Technology GmbH.

Confidentiality, availability, integrity

Even more than in other digitalisation projects information security plays a significant role in the introduction of e-files: firstly, the confidentiality of the information contained within the files needs to be ensured in order to guarantee that citizens' personal data is protected. Secondly, the content needs to be available at all times in order to facilitate seamless administrative processes – ultimately the e-file is expected to become a cornerstone of efficient administration centred around citizens. Thirdly, the integrity of the e-file is highly significant in making administrative processes transparent – here the issue at stake is nothing less than the rule of law in German authorities.

These requirements apply to an even larger extent at a particular area of record keeping: handling classified information (in German "Verschlusssachen", VS). Information that it is in the public interest to keep secret is classified according to one of four secrecy classification levels – depending on the level of protection required: RESTRICTED, CONFIDENTIAL, SECRET or TOP SECRET. Authority employees who work with classified information are assigned the corresponding protection grade, which indicates which kind of documents they are authorised to view. This is also referred to as security clearance. From CONFIDENTIAL level upwards individuals must undergo a security check prior to being authorised. Even then, if someone is authorised to a particular security clearance level, the principle of a "need-to-know



Thanks to the joint solution created by Materna and secunet, e-files can now be transferred to the secured collaboration area of SINA Workflow at the point of being classified.

basis" still applies: the individual should only be granted access if this is objectively necessary – and not before, nor to a greater extent than is necessary. In addition it must be possible to prove in a legally robust way which individual has viewed and processed which classified data and when. This is stipulated in the Federal Government's Classified Information Directive (Verschlusssachenanweisung, VSA) and in the VSAs set out by the German federal states.

Standard for confidential digital information

Today, classified information can generally be stored, processed and transmitted digitally. So far, however, it has only been possible to do this separately from e-files. Many federal and regional authorities use the Secure Inter-Network Architecture (SINA), which secunet developed on behalf of the German Federal Office for Information Security (BSI), for processing classified information. Cryptographic mechanisms are used that ensure the confidentiality and integrity of the data at all times.

With the verification procedure also required by the VSA it is, however, still a common but very laborious practice to revert to paper-based documentation – or to special solutions that are not connected to the rest of the infrastructure. SINA Workflow arose to rectify this failing. The solution ensures that every piece of information in the system contains legally robust records of any processing or administrative steps that have been carried out. SINA Workflow also implements the "need-to-know" principle digitally by documenting users' statements of intent relating to specific information for the avoidance of doubt. SINA Workflow is executed technically as an integrated system of secure workplaces and special servers with integrated electronic registry of classified information and central network storage.

The secured distribution concept can also be used across different authorities and federal states. For instance, it thereby enables different security authorities who work with sensitive data to collaborate because the access permissions for processing classified e-files through SINA Workflow are implemented in accordance with the regulations.

Since up to now there has not been an interface between SINA Workflow and the systems for processing normal, non-classified e-files, the two file types have been managed separately. Files that were only classified at a later point in their life cycle therefore had to be created again.

Due to the German e-Government law, in most federal authorities paper-based files will soon be a thing of the past. But with regard to digitalising classified information, special measures have to be taken.

Avoiding additional costs and media disruptions

Materna and secunet have now put forward a solution that avoids the extra work of duplicated documentation administration: SINA Workflow and the e-file nscale from Ceyoniq can be integrated thanks to a new interface that enables seamless transmission of a normal administrative file through to classified status.

In practical terms this happens as follows: an electronic file is classified at a particular point in time. The new interface transfers it to SINA Workflow, adhering to standards for the electronic exchange and singling out of official records such as XDOMEA. The classified e-file is subsequently no longer available in the system for normal e-files, but is only available from the repository of classified information – in an encrypted form and protected from unauthorised access. Here, the "need-to-know" principle applies. The handling and transmission are regulated in an audit-proof way that ensures tracking and verifiability. The classified electronic documents can be processed in accordance with the VSA and, for example, joint underwriting can be effected by using this security environment.

Authorities that utilise SINA Workflow can in future not only avoid recourse to paper when handling classified information and collaborate across institutions and federal states; they can also benefit from the fact that interoperability with e-files leads to another hurdle to the digitalisation of public administration being removed.

Norbert Müller
norbert.mueller@secunet.com

INTEGRATED BORDER CONTROL APPLICATION: IGA 2.0

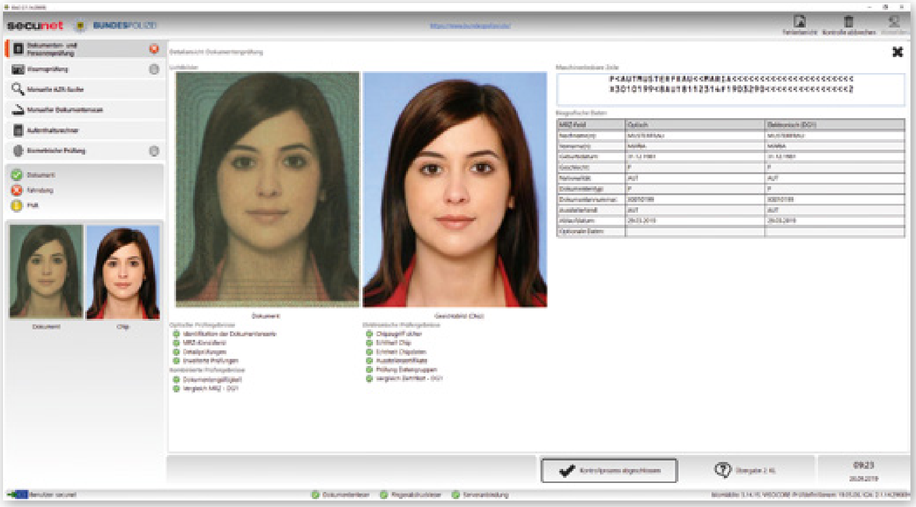
Fit for the Border Control of the Future

International travel is ever increasing; at the same time, terrorism and organised crime are raising expectations from the public and politicians regarding the quality of the checks at Schengen external borders. Despite the extensive regulatory provisions, IT systems can help to limit waiting times at border checkpoints. The complexity of the IT systems must remain manageable for officials, however, to allow the systems to provide beneficial support. The integrated border control application (IGA) 2.0 is an important step forward in this respect, and has already been used at over 1,000 German border control counters. It combines IT systems that were previously separate, delivering a genuine efficiency gain.

For members of the Schengen area crossing the EU's external borders at busy German airports handling large numbers of passengers has been faster and easier since 2014: The EasyPASS border control system has automated the process of matching the person to the electronic identity document, specifically the passport or ID card. Passengers complete the border control process by passing through automated border control systems – the secunet easygates – virtually autonomously. This results in a much faster border check and shorter waiting times.

Greater efficiency needed

Manual border control at stationary border control counters was still a laborious process, however – and therefore time-consuming for both officials and passengers: when checking people, the officials had to manually send requests to several central registers and search databases that were not connected to each other. Names, dates of birth and document numbers were queried individually in each system – from the visa database, VIS, to the INPOL search database. Having this variety of applications is not only inconvenient; but also error-prone.



In addition to the existing complexity, further requirements for stationary border control are already on the horizon: following the resolution by the EU Parliament, the EU's biometric Entry/Exit System (EES) is due to be implemented by 2022. This will eliminate the previous stamping procedure for passengers from third countries and instead will establish an electronic register. These passengers will then be digitally registered with four fingerprints and a facial image during border control at the Schengen external border. Through automatic checks can then later be determined, whether a traveller has exceeded the maximum duration of a short stay (90 days within 180 days) for example.

Read more about the planned European Entry/Exit System in the special report in secuview 1/2019: www.secunet.com/en/secuview

Compulsory biometrics from 2022

With the introduction of the Entry/Exit System, border control officials will need to add biometric data collection and maintenance in accordance with EES provisions to their existing border control responsibilities such as verifying documents and questioning and checking people. Without the supporting technology and further optimised processes it will not be possible to take on these additional tasks – at least not without the existing border control processes taking longer.

As a first step towards a supporting system to compensate respective efforts, the German Federal Police had developed the integrated border control application (IGA) 1.0: this application brought together all registers and databases relevant at that point in time. However, the solution could not, or could only with difficulty be extended to include further border control procedures and registers, such as the Entry/Exit System, databases for airline passenger data (Passenger Name

Records, PNR), or other police workflow systems such as mission control centre systems, process management systems, border control records, EasyPASS or kiosk systems.

IGA 2.0: link between different IT systems

This was the starting point for IGA 2.0. The new application did not have to be redeveloped from scratch by any means. Rather, secunet bocoa was already available as a modular solution, and the German Federal Police already had experience using it, e. g. for mobile police searches and in EES pilot projects.

IGA 2.0 conveniently brings together the results of visual and electronic document checks, the results from the background systems and analysis of biometric data, and displays them in a manageable way for the border control officials. Through appropriate filtering and visualisation of relevant discrepancies or inconsistencies the officials can comprehend and evaluate the checking procedure at a glance. If required, they can analyse the relevant details in greater depth. Furthermore, they do not have to enter the data manually several times over, and ideally won't have to enter it manually at all. The checking procedure will be more efficient, since officials will be able to concentrate on the more relevant exceptions.

Alongside those currently in existence, new, additional systems can be linked in the future: such as the planned EES and – currently – the PNR passenger data system.

Overall, IGA 2.0 acts as a central link between existing IT systems and border officials. Furthermore, it ensures seamless information flow between the federal authorities involved – i. e. the German Federal Police, the Federal Office of Administration and the Federal Office for Information Security. The solution currently handles up to 185,000 manual border controls at German airports – per day.

Staff can concentrate on core policing duties

Thanks to IGA border control officials are relieved of time-consuming routine tasks such as operating a variety of dedicated technical systems and manually evaluating data. The time gained with the collection of data can be used for plausibility and document checks, further raising the security standard.

The human factor plays an important part in the introduction and roll-out: the German Federal Police evaluated the acceptance of the system through internal surveys and pilot phases. The results of these influenced the subsequent planning and development work. The design of a graphic user interface that provides optimal support to the work of border control officials also played a key role. Here, too, user requirements and wishes were taken into consideration. The roll-out across Germany was completed at the end of October 2019; since then, IGA 2.0 has contributed to making controls at the EU's external borders future-proof and efficient.

Eyck Warich
eyck.warich@secunet.com

IGA 2.0 relieves border control officials – as pictured here at Hamburg Airport – of time-consuming routine tasks.

PKI AT THE FEDERAL EMPLOYMENT OFFICE

Trust in Cheque Card Format

The German Federal Employment Office (BA), one of the largest authorities in Germany, operates a public key infrastructure (PKI) that forms the background solution to the multi-functional personnel ID cards belonging to BA employees. secuview caught up with Holger Scheetz, Head of the trust centre at the BA, about the authority's experiences with PKI.

Mr Scheetz, where is the trust centre located within the BA's organisational structure?

Holger Scheetz: The trust centre fits within the BA's provider of trust services (VDA), which is anchored within the BA's IT systems house. This internal IT service provider operates one of the largest IT landscapes in Germany and has approximately 170,000 PC workstations. These workstations belong to the BA itself, as well as to joint facilities with municipal institutions, including job centres.

What is the trust centre's core area of responsibility?

The trust centre is responsible for issuing and administrating digital certificates. These are applied to the BA personnel ID cards, for instance. Employees use these personnel ID cards for authorisation at their PC workstations, for instance. In order to generate and distribute the certificates we operate a central public key infrastructure (PKI) in the trust centre. This solution consists of various components such as a certification authority as well as registration authorities for applying for and issuing new certificates and personnel ID cards, which are regularly audited with regard to compliance with the requirements of the eIDAS Regulation. All in all, this ensures that the certificates in use are always trustworthy.

Holger Scheetz has worked in the BA's IT systems house since 2004. During this time here he has worked in many areas of IT, including being part of the project group that built the BA's PKI. Since September 2010 he has led the trust centre and its operational team.

IN INTERVIEW

What originally triggered the PKI solution?

The BA is one of the largest authorities in Germany. Adapting to the growing and changing demands of the job market, the BA increasingly implements internet-based applications anchored in the objectives of the BundOnline initiative. Social data are transmitted as part of many of these business processes. In order to comply with the protection requirements of these data the corresponding IT security measures had to be taken. This challenge was taken up with the deployment of cryptographic processes within an intelligent solution combined with a smartcard. This necessitated building a PKI.

Which other features can you map through the PKI?

Employees can use the personnel ID cards not only to register at PC workstations, but also at applications by means of Single Sign-On. Employees can also add qualified signatures to documents using their personnel ID cards, as well as encrypt or decrypt emails. In addition, entry to the service buildings and employment-related time-keeping is controlled via the personnel ID cards. The solution therefore gives employees of the BA and the job centres everyday access to central security functions.

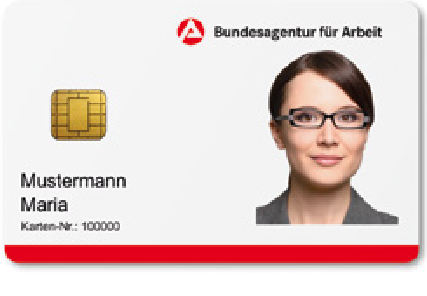
The PKI has been deployed in its current form since 2014 and, since then, has undergone continuous updating. What practical insights have you gathered using it?

First of all, the solution and the updates carried out are transparent and easy for users to apply – this aspect alone helps to keep support and administrative workloads at manageable levels. The current solution, which secunet successfully designed for us five years ago, has a modular structure and is stable to run. The interfaces provisioned allowed us to implement some enhancements. We have been working constructively together with the experts at secunet for around 15 years now.

Do you envisage enhancements at present?

Due to the service life of the solution some product updates are forthcoming. We are currently also carrying out a review of the solution with regard to amended legal and operational requirements. This is bound to result in further action being required for the future.

Head office of the German Federal Employment Office in Nuremberg



A Boeing E-3A (AWACS) aircraft at the NATO Air Base Geilenkirchen

SECURE REMOTE ACCESS AT A NATO IT INFRASTRUCTURE

Military-Grade Information Security on the Go

At the NATO Air Base Geilenkirchen which operates the Boeing E-3A Component Sentry known as the AWACS aircraft, staff members rely on a SINA solution that allows them to access classified information remotely. secuview spoke with Lt. Col Hans-Peter Kammer who is heading the CIS Plans & Policy Branch (FHCP) of the NATO Airborne Early Warning & Control (NAEW&C) Force.

The NATO Air Base Geilenkirchen is the main operating base of the NATO Boeing E-3A Component Sentry, one of two operational elements of the NAEW&C Force. It is located on German territory, adjacent to the German-Dutch border. Originally built and operated by the British Royal Air Force after World War II, the base was handed over to the German Air Force in 1968. In 1980, NATO started its E-3A Component operations at the Air Base Geilenkirchen. Today, approximately 2,000 military and civilian personnel from 16 NATO member nations work there.

The CIS Plans & Policy Branch (FHCP) is responsible for the development of NAEW&C Force's strategic communication and information systems (CIS) plans, as well as the development and operational deployment policies and orders covering the NAEW&C Force CIS.

secuview: Lt Col Kammer, what was the initial CIS challenge the NAEW&C Force had to face?

Lt Col Kammer: Nowadays operational advantage derives from the ability to collect, process, and disseminate an uninterrupted flow of information. In 2018, we were looking for a ‚secure remote access' capability to enable such information flow at the NATO RESTRICTED classification level and issued a statement for a need. The requirement was meant to facilitate remotely situated personnel, mainly during deployment or duty travel, with access to various network resources and services such as mission planning tools / data, the PILS application (Programme Integrated Logistics System), and other mission essential information.

Approximately 2,000 military and civilian personnel from 16 NATO member nations work at the NATO Air Base Geilenkirchen.

What kind of system did you have in mind?

All in all, the proposed system was supposed to enable users to securely access the NATO RESTRICTED network when they are physically outside their respective NATO environments. Specifically, the system needed to provide a secure encrypted Virtual Private Network (VPN) for transmitting NATO RESTRICTED data over an unclassified network. We also looked for state-of-the-art multi-domain, multi-tenancy workstations and secure access control mechanisms including user tokens. Also, we wanted the infrastructure to provide our system administrators with full administration capability for the clients, the capability for issuing and re-issuing the tokens for users as well as the ability to renew (refresh) and upgrade the installed base periodically.

The desired system also needed to have accreditation in accordance with the NATO security regulations and policies, be accredited to NATO RESTRICTED use and be listed on the NATO Information Assurance Product Catalogue (NIAPC) to ensure compliance.

Furthermore, the capability needed to support different user types: there are key leadership users at the NAEW & CF Headquarters, users at the NAEW & CF E3A Component including logistics and technical support personnel, deployed mission crew and other types of personnel who have to travel temporarily for duty as well as personnel at the MSEC (Mission Systems Engineering Centre).

What was the solution you ultimately deployed?

In February 2019 we made the decision to migrate to a SINA (Secure Inter-Network Architecture) solution that allows for a ‚secure remote access‘ capability. This proven, multi-domain, multi-tenancy solution, developed by secunet on behalf of the German Federal Office for Information Security (BSI), included the deployment of 30 SINA Workstations S (crypto clients in a laptop format), with a back end consisting of SINA L3 Box S devices (IPsec-secured VPN gateways) as well as a designated SINA Management solution.

What were the reasons you chose a SINA solution?

The SINA Workstation runs so-called guest systems such as Windows and their applications in a virtualised environment. Parallel operation of several isolated guest systems, which can also be assigned to different security domains, makes it possible to work with one guest system in the internal security network and simultaneously surf the Internet with another system – without running the risk of compromising your own network with malware.

Access to connected devices and interfaces detected by a guest system is carried out under the control of the SINA security operating system. All hard disk access and network connections are automatically encrypted by SINA. Users can only access the encrypted data with a PIN-protected SINA ID token which contains the configuration data and security associations for the SINA Workstation. It also serves as secure storage for cryptographic keys and certificates.

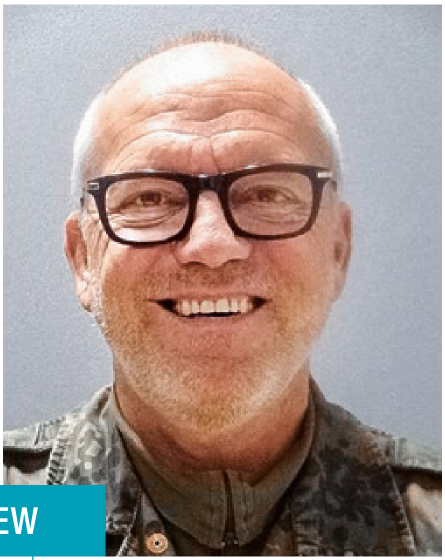
As a VPN gateway, the SINA L3 Box is a key component of the central IT infrastructure. The data exchange between the SINA components is securely transmitted via encrypted VPN tunnels.

SINA Management is used centrally for system administration, remote configuration and SINA software updates for all SINA L3 Boxes in the network. The configuration updates include network configurations and security associations. Integrated Public Key Infrastructure (PKI) with the associated user management supports critical administrative processes involving SINA L3 Box smart cards. This specifically includes customisation, generation and updating of keys and cryptographic parameters, and administration of the associated PINs and PUKs. A SINA administrator can grant or revoke rights and change the configuration from a remote location.

Could you give us a brief indication of the next steps?

Given the successful introduction and deployment of the SINA capability at the NATO Air Base in 2019, the NAEW&C Force is looking to launch Phase 2 in 2020 and expand the initial 'secure remote access' capability to more personnel on- and off-site.

Jerome Kühnert
jerome.kuehnert@international.
secunet.com



IN INTERVIEW

Lt Col Hans-Peter Kammer

Head CIS Plans & Policy Branch, NATO Airborne Early Warning & Control Force

Lt Col Hans-Peter Kammer was born on 13 May 1961 in Wuerselen close to Aachen. After graduating from High School in 1981 he joined the German Armed Forces as a conscript. In 1982 he began his career as a non-commissioned officer and platoon leader of a Signals Squadron stationed in Cologne. In 1991 he began studies in the field of electrical engineering and commissioned in 1994. He has served in different positions as a member of the NAEW&C Force since 1999. Lt Col Kammer is married and has two grown-up children.

A Geilenkirchen-based Boeing E-3A aircraft, commonly known as AWACS, in full flight

SOFTWARE INNOVATION CAMPUS PADERBORN

“We are Researching the Software Innovations of the Future”

Since March 2019 secunet has been a member of the Software Innovation Campus Paderborn, or SICP for short. Collaboration between science and industry at the University of Paderborn has led to the creation of a place for research and innovation, knowledge transfer and human resources development.

The Software Innovation Campus Paderborn (SICP) is an interdisciplinary research and innovation association where businesses and science jointly explore and put digital innovations into action. The SICP develops solutions to brand new kinds of challenges in digital society, but also implements real-world concepts and systems efficiently, securely and in a scalable way. “With the construction of the new Zukunftsmeile 2 building on Fürstenallee in Paderborn, in close proximity to the Fraunhofer Institute for Mechatronic Systems Design IEM and the University of Paderborn Heinz Nixdorf Institute, we are realising a research campus where we will be able to develop digital innovations in a particularly effective and agile way through the close interlinking of science and industry,” says Dr Stefan Sauer, Managing Director of the SICP and Manager of the Software Engineering competence area. “We see the close collaboration between science and industry as a crucial factor for success in turning research results into marketable innovations,” Sauer adds.

Digital innovations as a product of interdisciplinary collaborations

In the five competence areas of the SICP – Cyber-Physical Systems, Digital Business, Digital Security, Smart Systems and Software Engineering – around 30 working groups from the faculties for Electrical Engineering, Computer Science and Mathematics, Economics and Cultural Studies at the University of Paderborn are developing multidisciplinary new concepts, methods, technologies and tools for large distributed and intelligent systems, secure wireless communication, agile and people-centric development of interactive and socio-technical systems, digital business models, data-driven decisions, intelligent customer management and adaptive business processes. “We always view digital innovations as a close interlocking of organisation and IT: digital transformation can only be successful if we develop software and systems on the basis of the application context, transform organisational structures effectively, and empower people to create and utilise digital innovations,” explains Christoph Plass, spokesman of the SICP.

The SICP steering committee (left to right): Holger Funke (secunet Security Networks AG), Josef Tillmann (S&N Invent GmbH), Christoph Plass (UNITY AG), Prof. Gregor Engels (University of Paderborn), Dr Stefan Sauer (University of Paderborn), Jörg Wehling (Atos Information Technology GmbH), Prof. Holger Karl (University of Paderborn)

"Digital Security" at the SICP

In the era of the digital transformation, Industry 4.0 and the Internet of Things, the security aspect in particular is one of the core challenges for our modern information society. "In our area of competence we are therefore investigating methods for how security can be integrated more extensively even at the design stage, and how it can be guaranteed for the entire life cycle. Our goal is to make the concept of 'digital security' understandable, sustainable and demonstrable," says Prof. Eric Bodden, Director of the Digital Security competence area.

Distributed systems are increasingly used, e.g. in cloud computing or in service-oriented or micro-service architectures. The associated distributed computing and storage of data in virtual environments calls for more data communication on the one hand; and the use of external providers on the other. "In this situation, security vulnerabilities can easily arise from the use of complex systems and the constant connectivity. The fundamental aims of IT security for us are, therefore, maintaining information security and protecting privacy rights," states Dr Simon Oberthür, Manager of the competence area and scientist at the University of Paderborn. To this end, the SICP is researching measures such as secure IT architectures, progressive cryptographic procedures and digital identities and developing joint solutions. These topics are supported by multidisciplinary expertise in topics like agile and hybrid software development methods, static and dynamic program analysis, or software quality assurance and testing.

secunet is a member of the SICP

Since March 2019 secunet Security Networks AG has been a member of the SICP and, as one of the leading providers of IT security for businesses and authorities, has been supplementing the SICP Digital Security competence area in particular. "We are delighted to have an extremely capable partner at our side in secunet, who also regularly supports us at the Paderborn Day of IT Security, which we have staged for 14 years," says Dr Simon Oberthür. "Thanks to its many experts, high degree of specialist and methodological expertise, together with its broad panoply of innovative ideas, we see the SICP as an ideal forum for exchange and discussion," says Holger Funke, Principal at secunet Security Networks AG. The fellowship is thus building on a long-standing, trusting relationship and joint activities and project plans, including for the German Federal Office for Information Security (BSI). The aim of the SICP fellowship is to further develop this relationship, carry out joint projects, bachelor and master theses, and attract highly trained students and graduates to secunet.

You can find more information at www.sicp.de.

Dr Stefan Sauer, SICP
sauer@sicp.de

Holger Funke, secunet
holger.funke@secunet.com

SICP
Software Innovation Campus Paderborn

Zukunftsmeile 2: The SICP will be housed in this new building as of next year.
Simulation (c) Matern Architekten, Goldbeck GmbH

100,000 SINA WORKSTATIONS S DELIVERED

Modern Working in Public Administration × 100,000

The digital transformation does not stop at classified information and other sensitive data. On behalf of the German Federal Office for Information Security (BSI), secunet developed a solution that would offer the requisite security and, at the same time, be user-friendly: the SINA Workstation. The cryptographic client, which was originally conceived as a special solution for specific purposes, has since established itself as the standard PC in public administration, where it facilitates modern, mobile working. In autumn 2019 secunet announced a milestone. The success story continues, however: the solution is continually being developed and new user requirements and technologies integrated.

"The SINA Secure Inter-Network Architecture is one example of a successful public-private partnership," BSI President Arne Schönbohm stated in October 2019 at the world's largest trade show for IT security, it-sa in Nuremberg. Axel Deininger, secunet's CEO, met Schönbohm to mark a special occasion: 100,000 SINA Workstations S delivered. The cryptographic clients secure workstations within a number of authorities in Germany and Europe, including in many federal ministries. Thanks to their mobility and flexibility they have revolutionised work flows in authorities, where handling sensitive or classified documents is part of everyday responsibilities. Today, despite the stringent security requirements, their employees can fulfil their responsibilities just as independently when working from home or while out and about as employees in the private sector can. The key phrase is "new work". The security of the sensitive information is guaranteed at all times. And development is ongoing: "We will continually adapt SINA to meet users' needs and address their work scenarios," says Deininger.

SINA: a secure environment, versatile hardware

The portfolio of SINA solutions is multi-layered and always offers the right product for the different requirements. At its core SINA builds a secure environment with sophisticated encryption technology that serves to transmit sensitive and classified information over potentially unsecured networks like the internet. IPsec-secured Virtual Private Networks (VPN) are used to achieve this.

The SINA Workstation functions as the client in these secure networks. It offers the advantage that several guest systems of differing secrecy levels that are sealed off from each other can be run in parallel on one device. This is achieved through virtualisation technology. The users can easily move between the guest systems by just a mouse click, without having to use different devices to access different security domains. They can, for instance, work in a classified network and, at the same time, surf the (unsecured) internet. In addition they have access to their familiar work environment (e. g. MS Windows) at all times, without jeopardising the security of the data in the classified networks with which they work concurrently. Two-factor authentication and hard drive encryption prevent unauthorised parties from gaining access to the sensitive data.

Confidential information from RESTRICTED to SECRET

As is the case with other SINA components, the SINA Workstation is available in a range of different basic models for disparate security requirements: in principle, the SINA Workstation S (for 'standard') is approved for RESTRICTED classification level; the SINA Workstation E ('extended') for up to CONFIDENTIAL; and the SINA Workstation H ('high') for up to SECRET level. In accordance with the security requirements prevalent in the various authorities and institutions the SINA Workstation S is primarily used in public administration, while the SINA Workstation H is used in military and other contexts. The latter has, for example, become established as the standard client in the context of the German Federal Armed Forces' HaFIS programme (harmonisation of management information systems).

Concurrently with this, the SINA Workstation is available in various form factors, e. g. as a desktop, laptop or tablet. The SINA Terminal falls into an entirely separate category. This thin client only displays graphic data and emits audio signals; furthermore it accepts mouse and keyboard input. The actual processing of classified information takes place on remote terminal servers.

The SINA Workstations E and H are, in addition, available in ultra-robust versions that remain reliably usable even in unfavourable physical conditions: they are resistant to heat, cold, dust, vibrations and humidity.

Virtualisation: at the sharp end of technological evolution

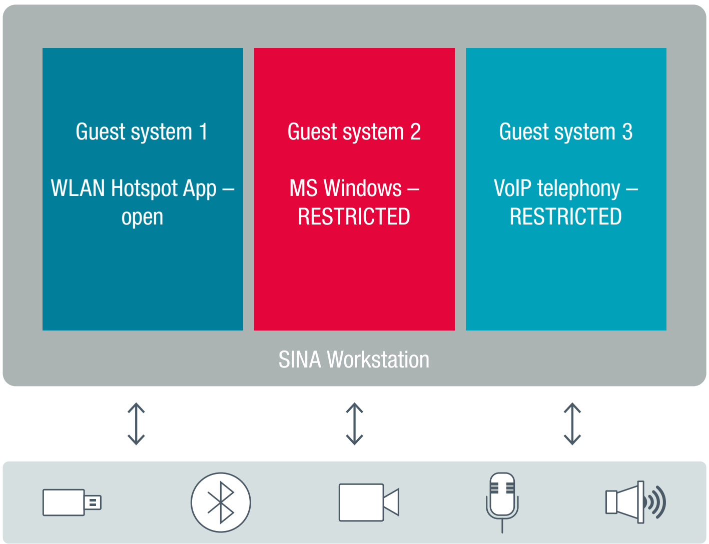
The project concept for SINA originally came about through the call for secure communication in connection with the move of large parts of the German Federal Government from Bonn to Berlin. In this context, the Berlin-Bonn Information Network (IVBB) was set up to connect the highest-level federal authorities. In addition, there was a general need for suitable encryption for classified information on an internet protocol level and, together with this, a deployment prospect for secure communication via wide area networks. At the end of the 1990s the BSI therefore drew up a draft concept for SINA. In December 1999 secunet Security Networks AG was commissioned by the BSI to develop the SINA product line.

Initially, at the start of the 2000s, secure VPN networks were set up with SINA L3 Boxes as VPN gateways and PCs were connected to them. The next step involved the SINA Terminals, which linked a SINA L3 Box and a display component. With the increasing prevalence of SINA many users were keen to have entire PCs (fat clients), with which they could work directly in their usual Windows environments. secunet experimented subsequently with virtualisation technologies and ultimately developed the concept for the SINA Workstation together with the BSI. A virtualisation solution from manufacturer InnoTek brought about a breakthrough, which secunet extensively adapted and developed for SINA – and which continues to be developed. InnoTek later went to the technology provider Sun Microsystems, which was in turn taken over by the Oracle hardware and software corporation. The virtualisation solution is marketed under the name VirtualBox.

> › The success principle of the SINA Workstation is based on client virtualisation. secunet is driving this technology forward significantly with SINA Workstation, like cloud computing is driving forward server virtualisation. ‹
>
> Armin Wappenschmidt, Head of Network & Client Security, Public Authorities Division, secunet

En route to an authority standard

When the SINA Workstation was first brought to life the supposition was that there would be demand for around 1,500 workstations. Today it is clear that the market has evolved rather differently than had been anticipated. With 100,000 installations of the SINA Workstation S alone, the SINA product family has become an authority standard.



One milestone on this path came in the mid-2010s, when several federal ministries were fully fitted out with SINA Workstations. This gave rise to brand new challenges again: previously, the spotlight was purely on security; now the question was also how a mass roll-out and the administration of very large SINA installations could be successful without entailing an excessive workload. The answer lay in automation: the new challenges were tackled with the SINA Install Server and the SINA Remote Admin Server. Their successful implementation proved that SINA was suitable for mass roll-outs.

Users demand a variety of applications

The SINA Workstation spread very rapidly within Germany's public institutions, which soon led to a concomitant rise in users' demands. Users expected that more and more of the applications that they were reliant on as part of their day-to-day work should also be mapped in the SINA Workstation: from the connection of printers and scanners to USB support for headsets for audio conferences, right through to video telephony with Skype for Business. Implementing these requirements within the secure, virtualised SINA environment was often challenging, yet these challenges were overcome time and again.

A further example: since 2015 SINA has been compatible with the biometric middleware secunet biomiddle. This enables those in specialist roles – such as border control officials – to hook up biometrics hardware like passport readers and fingerprint scanners. The SINA Workstation is also used successfully in mobile identity control and for registering people.

On the occasion of delivering 100,000 SINA Workstation S representatives from the BSI and secunet met at it-sa 2019. From left to right: Dr Günther Welsch, Arne Schönbohm (both BSI), Axel Deininger (secunet), Dr Gerhard Schabhüser (BSI), Dr Kai Martius (secunet)

100.000 x SINA Workstation S
Entwickelt im Auftrag des BSI
Success Made in Germany
SINA
secunet
100.000 x SINA Workstation S
Cybersecurity for Defence and Space

The SINA Workstation is available in various form factors – the picture shows a version in a laptop format.

The SINA Workstation presents users with a range of software applications through its SINA apps, which were originally developed in response to requests from individual clients. These applications can be started as separate guest systems and fulfil defined tasks. One example is the SINA WLAN Hotspot app. This enables users to establish a secure VPN connection even at unsecured public hotspots.

Convenient and secure internet access

At the top of the list of many office IT users is convenient internet usage that is as free as possible of restrictions. Unsecured access to the internet does, however, represent one of the biggest gateways for malicious software, which not only affects the target system, but which can also jeopardise the confidentiality of the data. Many users in public authorities therefore used to have to switch to a separate PC workstation if they wanted to conduct research on the internet. Other, more convenient solutions were always merely a compromise when it came to security aspects.

The SINA Workstation opens up an elegant way forward here by making a version of the secunet safe surfer solution available, which is based on the BSI's ReCoBS (Remote Controlled Browser System) architecture. The internet browser is not itself implemented on the local Windows system requiring protection, but within a quarantine system that is implemented outside of the sensitive network area – in the case of the SINA Workstation, as a further virtualised guest system. The user controls the browser within his Windows workstation remotely, as it were, and can thereby work with sensitive data or critical networks, and simultaneously access the internet – without the former limitations. Even functions like uploads and downloads, as well as a printer connection are conveniently available thanks to a data lock.

The option of starting individual Windows applications in their own virtualised environments, which potential malicious code cannot break out of, provides additional security. This principle underpins special partner solutions such as Bromium Secure Platform, which can be integrated within the SINA Workstation. The tried and tested external protection of the SINA environment is thus enhanced by a further, internal protection mechanism for Windows applications.

The future: small, mobile, intuitive

The increasing popularity of the SINA Workstation is leading to more and more new user groups coming into contact with it. This is one of the reasons that the evolution of SINA is moving in the direction of simple, intuitive interfaces, which take away the need for specialist training for SINA users. For example, a new graphical user interface is currently in progress, which will further improve the user experience. The aspect of accessibility is also on the agenda.

In addition to the simple usability of the SINA Workstation, users are also focussed on mobile usage. Tablet solutions are already available and other mobile form factors will follow.

So what does the future of the SINA Workstation look like? The old contradiction of security and convenience has increasingly fallen away. The objective is a cryptographic client that can hardly be differentiated from conventional user systems, but that still meets security requirements from high to highest.

Armin Wappenschmidt
armin.wappenschmidt@secunet.com

ENCRYPTED VIDEO COMMUNICATION NOT ONLY WITH HELICOPTERS

Exclusive Live Transmission from Several Kilometres Up

Digital communication has featured in military infrastructures in a big way. The requirements are becoming ever more exacting: today, airborne platforms such as helicopters, reconnaissance aircraft and drones not only need to be connected to IT systems and, for example, transmit image data; they also need to deliver high-resolution video footage in real time while on deployment – at RESTRICTED secrecy level. To achieve this, several of the German Federal Armed Forces' helicopter models carry the SCOTTY Communication Platform on board, which is fitted with SINA encryption technology. The high security solution SINA, which has formed the IP cryptographic backbone of the Federal Armed Forces for years on the ground, is thereby now tapping into the vertical dimension too.

In the armed forces increasing demands with respect to agility and flexibility on deployment have led to a growing need for live video communication. This enables missions to be coordinated, supported and led dynamically. On a practical deployment, such as on reconnaissance and monitoring missions, HD video material is streamed live to central command. Status reports are therefore far more accurate and up-to-date.

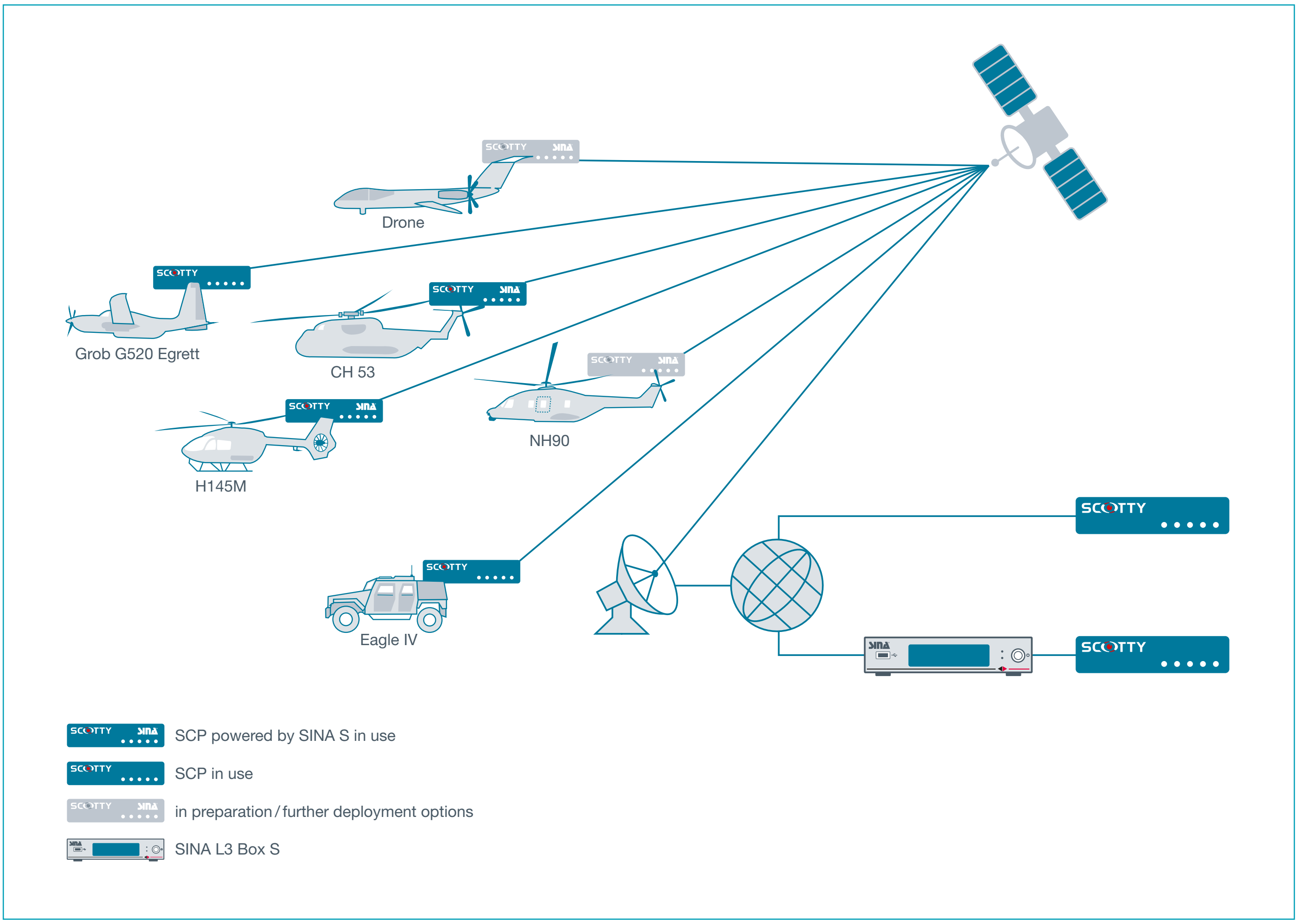
In the area of medical service support the encrypted video and data transmission in real time enable a plethora of different telemedicine applications. In addition to the transmission of vital data in emergency situations, teleradiology, teleparasitology and teledermatology, it is also possible to provide support with a sonographic examination in real time via a specialist in the country of origin.

One traditional use case is bi-directional video and speech transmission in the form of a video conference used as a modern leadership tool. Last but not least, the system also serves to transmit media reports from the deployment territory, whether for internal communication or external reporting purposes.

These types of scenario are executed technically with the assistance of separate computer systems on board of aircrafts or vehicles. SCOTTY, a company headquartered in Austria, produces solutions for this purpose. The SCOTTY Communication Platform (SCP) enables data, photos, audio and HD video material to be beamed live from the air, land and high seas – preferably via satellite communication, because this ensures continuous network availability irrespective of the environment infrastructure. Moreover, the SCP supports terrestrial networks. With both types of connection there is the challenge that the networks available on the deployment usually only have moderate bandwidth available and have high latency. The SCP therefore prepares the video data in such a way that they can be transmitted in high quality despite the unfavourable conditions. If necessary, the users can decide whether an optimal image resolution or optimal motion dynamics should be achieved when processing – depending on the tactical benefit.

The SCP is made up of two components: a hardware decoder / encoder and a processor unit. The combination of these two

The Sikorsky CH-53 is a medium-weight transport helicopter that has been operational on a large number of the Federal Armed Forces' foreign deployments in recent years.



elements enables a series of applications, including bi-directional video communication, unidirectional video streaming and video recording. The transmission of technically less challenging information arising through the deployment, such as audio material or simple data, is effected over the SCP too.

In order to transmit the information not only so it is readily available and of sufficiently high quality, but also so it is tap-proof, one version of the SCP is equipped with the SINA cryptographic system. As part of the “SCOTTY Communication Platform powered by SINA S”, SINA is now leaving the ground and boarding the Federal Armed Forces helicopters on deployments at heights of up to several kilometres above ground. The joint solution by SCOTTY and secunet is approved for the German VS-NUR FÜR DEN DIENSTGEBRAUCH secrecy level, as well as for NATO RESTRICTED and EU RESTRICTED / RESTREINT UE levels internationally.

How is communication protected specifically? The SINA component in the SCP in the helicopter functions as an IPsec secured VPN gateway. As a counterpart, one (or more) SINA L3 Box S is required on the ground and integrated within the respective military IT infrastructure there. The data exchanged between the SINA components are securely transmitted in encrypted VPN tunnels. In doing this it is immaterial which potentially unsecured network is used for the data transfer – e. g. the internet, or, in the present instance, via satellite-based connections. RESTRICTED level-compliant cryptography ensures that only the SINA components affected can decrypt the data – even with high data throughput, in order to enable applications such as video communication.

The SCP's hardware platform

For the time being, two types of Federal Armed Forces helicopter models in Germany's air force are flying missions with SCP powered by SINA on board. One of the two is the Sikorsky CH-53, a medium-weight transport helicopter that has been operational on a large number of foreign deployments in recent years. For many years the CH-53 has been the Federal Armed Forces' beast of burden in Afghanistan. From transporting troops to connecting flights, transfer of special forces to the deployment territory through to medical

SCOTTY Group Austria GmbH provides a comprehensive range of communications solutions, specifically tailored to application in defence, civil protection and surveillance. SCOTTY facilitates audio, video and data transmission where there is no infrastructure: in the field, on wheeled vehicles, ships, and in the air.

SCOTTY, founded in 1993, has tremendous experience in providing solutions for critical applications under challenging circumstances. Armed forces worldwide use SCOTTY equipment and rely on the long-standing experience and know-how to take communication to remote locations which are difficult to access. SCOTTY products can be integrated into aircraft, helicopters and vehicles. The transmission of video recordings in real time to the command centre makes surveillance operations as well as reconnaissance missions more efficient and allows rapid action.

The encrypted video and data transmission in real time enable a plethora of different telemedicine applications.
(c) SCOTTY

The SCP is not only designed for use in helicopters, but also in aircraft (such as the Grob G520 Egrett pictured here), land-based vehicles and ships.
(c) SCOTTY

evacuation: the platform has been used for many years for a host of missions in this deployment territory, which is challenging not only because of the climatic conditions.

A further type of helicopter with SCP powered by SINA S on board is the new lightweight multi-purpose Airbus Helicopters H145M. The scope of application for this helicopter includes supporting land-based and maritime special operations, as well as, in future, fire support, evacuation support and reconnaissance missions. The German navy is also planning to implement the SCP powered by SINA S: in future, the IT security solution will transmit and safeguard video communications in the new tactical NH90 Sea Lion marine transport helicopters.

As a hardware component for aviation, special requirements apply to the SCP: ultimately, the solution needs to function securely even under extreme conditions, such as those in play within a plane or helicopter. The standard DO-160G sets out requirements for tolerance with respect to environmental factors, as well as for the electromagnetic compatibility. This includes the temperature range in which the system has to function faultlessly, the air pressure, the resistance in terms of electromagnetic radiation as well as, in particular, the resilience to cope with vibrations and knocks, which, especially when it comes to helicopters, can be very extreme. The SCP passed the test procedure for this standard successfully.

In principle, the SCP is not only designed for aviation, but also for land-based vehicles and ships. The same applies to the product versions with SINA functionality. There is currently a project in plan to integrate the system into land-based vehicles.

IT systems have become integral components within overarching military systems, which alter their capabilities and, in turn, generate new requirements. This is especially evident in the example of live HD video communication: where flying platforms are equipped with this functionality their deployment capabilities are extended. This in turn leads to new requirements, specifically with regard to the quality, availability and confidentiality of the data transmitted. To cover future requirements for military IT infrastructure as well, SINA is continually being developed in close collaboration with the Federal Armed Forces.

✉ Dr Michael Sobirey, secunet
michael.sobirey@secunet.com

Dr Mario Polaschegg,
SCOTTY Group
M.Polaschegg@scottygroup.com

Dr Michael Sobirey
Head of Defence division, secunet

Dr Mario Polaschegg
Head of Customization, SCOTTY Group

TELEMATICS IN HEALTHCARE

Next, Please: Now it's the Turn of Hospitals

The digital transformation of German healthcare is picking up speed. The telematics infrastructure, the digital backbone of the healthcare system, is being enhanced with additional applications step by step. At the same time, a second connector design is in the starting blocks: the secunet konnektor for data centres is primarily intended for use in hospitals.

The telematics infrastructure (TI) is the digital network of the healthcare economy, through which the electronic health card gets its digital connection. Often described as a data highway for the healthcare sector, in future the TI will support a series of digital processes that offer real added value for policyholders too, such as electronic patient files and e-receipts.

The connector acts as the centrepiece for secure communication between the medical providers' IT systems and the TI. Since the approval of the first connector by gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) in November 2017 medical practices in Germany have been equipped with a connector.

This was only the first wave of the TI connection though. In accordance with the will of the legislator, all pharmacist stores are to be connected to the data highway by 30 September 2020 and, by the end of 2020, all hospitals too.

In the case of hospitals in particular the connection requirements differ considerably from those of a medical practice, however. Today, hospitals operate large data centres. The one box connectors previously available on the market, including the secunet konnektor, have a format reminiscent of DSL routers. What is recommended for medical practices will not necessarily be the right fit in a data centre setting: here, powerful components in closed 19" housings are anticipated, which are adapted to data centre operation both in terms of electricity connection and power supply as well as in terms of their cooling concept.

Connector for data centres

secunet has therefore decided to develop and offer a version for exactly this type of scenario. The secunet konnektor for data centres is based technically on the one box connector, but delivers double the performance and is in addition equipped with management software that makes it far easier for administrators to operate several connectors in combination.

The new connector design is expected to gain approval in December 2019 (this is the case at the moment of going to print with this secuview issue). If these timings remain unchanged the roll-out in hospitals will be able to start as early as January 2020. For around 2,000 hospitals in Germany the secunet konnektor for data centres is a tailor-made solution; it can also be an interesting alternative for large pharmacist stores.

The German electronic health card gets its digital connection through the telematics infrastructure (TI).

Added value in view

For the moment the new connector design is supplied with 'VSDM' software (policyholders' master data management), until the next software upgrade has undergone the approval process. This is expected to happen in the second quarter of 2020. The upgrade, which can be brought in online, will supplement the connector with the electronic medication plan (eMP), qualified electronic signature (QES) and emergency data management (NFDM) applications. The QES functionality will also enable electronic doctors' letters via the specialist KOM-LE (secure communication between providers) application. The electronic patient file (ePA) is anticipated to come in at the earliest by the end of 2020.

The introduction of the TI has made superb progress over the course of 2019. The second connector design now facilitates the secure connection of hospitals and large pharmacist stores. At the same time, applications are appearing on the horizon that will clearly demonstrate why the major TI project will ultimately pay off.

Markus Linnemann
markus.linnemann@secunet.com

SWIFT ROLL-OUT

The secunet konnektor for medical practices (one box connector) was only approved by gematik in December 2018, since secunet had only decided late in the day to enter the healthcare market. Barely a year later, over 45,000 medical practices have already been equipped with the secunet konnektor. A very high value in relation to the overall market as well: there are roughly 140,000 medical practices in Germany, of which approximately 115,000 are currently connected to the TI.

The secunet konnektor is available in one design for medical practices (right) and another design for data centres (top). Both versions are optimised for their respective deployment scenarios.

DATA SECURITY IN CLOUD COMPUTING

Joint Venture secustack for Secure Data Processing in the Cloud

secunet Security Networks AG has combined its know-how with that of Dresden-based Cloud&Heat Technologies GmbH and founded a joint venture. secustack GmbH offers infrastructural cloud solutions that provide the users with sovereignty over their data. The offer is primarily aimed at the public sector and all companies that either do not yet want or simply are not allowed to process their sensitive data in the cloud due to security concerns. In this interview, Dr Marius Feldmann, CEO of secustack GmbH, gives insights into the cooperation and talks about the goals and challenges that were decisive for the cooperation between the two companies.

Dr Feldmann, are you so kind as to describe to our readers what secustack does and who is behind it?

secustack GmbH is a subsidiary company of secunet and Cloud&Heat, which was found in May this year. Our team consisting of passionate cloud experts from Dresden are being dedicated to the development of a cloud operating system, which meets highest security requirements and, thus, makes cloud computing for all kinds of sectors not only more attractive but secure.

Dr Marius Feldmann

COO Cloud&Heat Technologies GmbH, CEO secustack GmbH

Can you tell us more about the cooperation between secunet and Cloud&Heat? What was initiating this cooperation?

The cooperation has already begun several years before the foundation of the joint subsidiary. With the initial goal of exploring the market with regard to secure cloud infrastructures, we first came into conversation. Cloud&Heat was a particularly interesting partner due to its many years of experience in the operation of OpenStack-based cloud infrastructures. Additionally, our expertise in green IT and sustainability drew attention at secunet: Technology by Cloud&Heat makes it possible to use waste heat of servers in data centres for heating. In a joint project that ran in 2017 and 2018, we identified potential measures that would contribute to hardening the security of OpenStack infrastructures and implemented them in a targeted manner.

For what kind of industries is secustack's solution especially interesting and why?

The use of cloud computing offers many advantages in reducing costs and complexity and creates high operating standards through automation. That's fact that no one will contradict. The problem is that there are industries that do not use cloud environments because they are subject to very strict security requirements. However, this is a waste of essential competitive advantage. For example, this affects organisations that process sensitive data, such as government agencies, but also operators of critical infrastructures, for whom an attack on the infrastructure could have catastrophic consequences. However, there was no solution on the market that takes this particular problem into account. To increase cloud security and to provide a solution that meets these requirements, secustack was founded.

How exactly does secustack contribute to increasing the security of modern digital infrastructures?

With its product of the same name, "SecuStack", secustack offers a solution that not only makes the storage and processing of data secure, but also more transparent. Based on the platform OpenStack, SecuStack offers additional mechanisms for end-to-end encryption, access control, data sovereignty and defense-in-depth. Thus, SecuStack contributes to various security issues, such as securing infrastructure access or comprehensive control over cryptographic material. The proven SINA technology from secunet is used to implement infrastructure access. In addition to the general development of security enhancements, SecuStack covers the entire lifecycle management and also offers a solution for secure container orchestration.

Why is the Open Source platform OpenStack a suitable basis for SecuStack?

There are many ways to build a cloud environment. In this context, OpenStack is the de facto standard for open source solutions. It offers a modular architecture to provide a set of core services that enable scalability

Dr Feldmann has been working for Cloud&Heat Technologies GmbH in Dresden since 2013 – and since 2015 in the role of Chief Operating Officer. Here he is responsible for the operation of the OpenStack-based cloud installations at Cloud&Heat. His current research projects include cloud security and data protection in the cloud. This includes AUDITOR, which is striving to develop an EU-wide cloud certification system. When secustack GmbH was founded in May 2019, Dr Feldmann and Dr Kai Martius from secunet Security Networks AG assumed the role of CEO of the joint venture.

Dr Marius Feldmann (left) and Dr Kai Martius. Both are CEOs of secustack GmbH.

and elasticity as core design principles. Open source platforms offer many arguments such as flexibility, vendor independence, the ability to verify and improve code, and the implementation of short-term innovations by a broad group of contributors. These characteristics also contribute to a high degree to the trustworthiness of digital infrastructures. And this is exactly what secustack is all about.

What are the next milestones and where does secustack see itself in five years?

In addition to the constant development of the security stack, we will expand our marketing and sales activities. SecuStack has already been successfully put into operation in Cloud&Heat projects, for example in its data centre in Frankfurt's Eurotheum. Together with Cloud&Heat, we are striving not only to make all future data centre projects more energy-efficient and thus more sustainable, but also to equip them with SecuStack distributions. In addition, we want to strengthen the cooperation between secustack and its mother companies. Our overriding aim is to make the cloud world more secure, and we hope that this will make it easier for many companies across all industries to switch to the cloud. In five years we see ourselves as an established enabler for secure cloud computing with a strong network.

secustack was founded in May 2019 by the IT security specialist secunet Security Networks AG and the IT infrastructure provider Cloud&Heat Technologies GmbH. The two partners are pooling their many years of expertise in the field of IT security solutions and the operation of OpenStack-based cloud infrastructures. The Dresden-based team of passionate cloud experts develops mechanisms to provide a secure cloud operating system based on OpenStack. The SecuStack solution has various functions for securing data and the cloud infrastructure. The core element here is strict, cross-functional client separation. SecuStack can be used in any environment with security-critical processes and sensitive data.

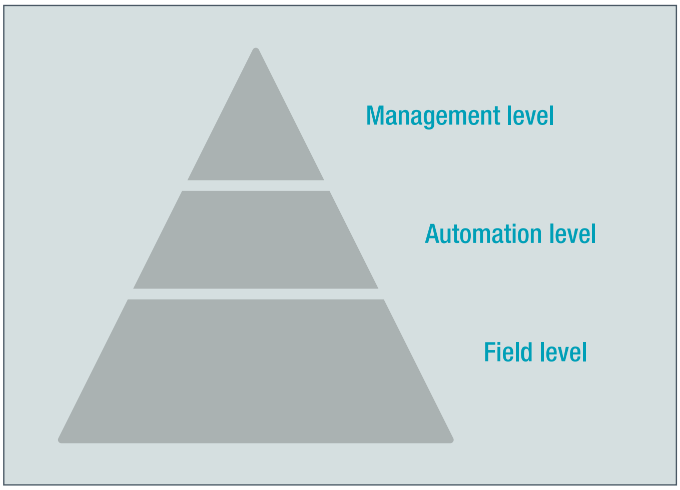
BUILDING AUTOMATION

How to Secure a Smart Building

IT systems are increasingly used to control commercial or public buildings. In building automation (BA), however, there is traditionally a different understanding of security than in IT. This has led to the issue of IT security in BA being neglected until now. The risks to smart buildings entailed by this approach are growing all the time. The situation requires a rethink and, above all, interdisciplinary collaboration between BA and IT.

Flats, houses and buildings are becoming ever more intelligent: smart technology is enabling more efficient use of energy and spaces of all kinds to be utilised in a more convenient way. Smart lighting control can be adjusted to suit human biorhythms, voice assistants make it possible to control all kinds of devices, and intelligent temperature regulation ensures a comfortable room temperature – when someone is in the room.

These types of scenario are not just a feature of the 'smart home'; they also have their equivalent in the commercial and public spheres. The concepts of the 'smart building' and 'building automation' have become established here. This refers to the connection and automatic control of technical BA systems in non-residential buildings – including office buildings, but also airports, hospitals, factories and shopping centres. Building automation is one of the most complex ways the Internet of Things (IoT) is utilised.



High degree of complexity in building automation

Since non-residential buildings are generally significantly larger than private real estate, the automation technology they depend on is also much more extensive and complex. To bring structure to the myriad of individual elements and control circuits a three-level classification system is often used, as illustrated in the graphic showing the 'automation pyramid':

Sensors and actuators – for instance temperature gauges and heating regulators – are located on the lowest level, the field level. The devices on the automation level analyse the measurements from the sensors and generate the corresponding settings in the actuators. The control centre, from where the results of this complex interplay are operated and managed, is located on the management level.

Communication between the components and devices in one level and between the various levels is not necessarily uniform: especially in older and modernised buildings there are often a variety of protocols, bus systems and interfaces in operation. Communication between the various components is predominantly achieved via cables, but increasingly also carried out wirelessly.

The age of the components differs as widely as the technology. Even more than in other areas of application of digital networking, in building automation, structures that have in part been around for decades are equipped with retrofitted technology, in some instances, even brand-new technologies. When the majority of the buildings that exist today were in the planning stages, computer-aided control did not yet play a significant role. The corresponding components – such as the older connection-programmed control elements or the newer programmable logic controllers – are traditionally considered part of automation technology and not information technology. This is even the case with control systems which essentially are composed of PC technology with a PC operating system.

Safety vs. security

While for specialists in automation technology the spotlight is on safety, i. e. operating safety in terms of protecting life and limb, in the IT world security plays a key role with its traditional protection objectives of integrity, availability and confidentiality of information. This is not only a conceptual differentiation, but also entails cultural differences between the two specialist areas.

Whether or not IT in building automation is officially considered to be automation technology and treated as such, it does not change the fact that, in practice, it is treated similarly to IT systems in other areas: components from technical BA systems are connected to the internet, technicians' notebooks, or office communications networks for a wide range of reasons. The hurdles to connection are rendered lower by the fact that the communication protocols in building automation are also increasingly becoming standardised – and these standards are often taken from IT, such as the internet protocol family (TCP/UDP/IP). "Internet comes to building automation" came the announcement back in 1999; and "cloud management" for the BA of large buildings has been a reality for some time now.

This growth in communication options has so far only rarely been matched by a corresponding increase in security measures. The following is often the case for BA systems: standard passwords remain unchanged, or cannot be changed at all. External laptops belonging to maintenance technicians represent an unknown quantity when it comes to malware infections. Log files are either not written, or at any rate not analysed. And affordable OEM components from the Far East not only have security vulnerabilities in the sense of unintended deficiencies, but may also be delivered with spyware.

This is where the dual role of information security for smart buildings is in evidence:

- On one hand, information security is becoming increasingly important for people's physical safety, too. Unidentified security vulnerabilities and unauthorised access routes open the door to tampering with systems such as fire protection equipment or boilers, for instance.
- On the other hand, with the appropriate networking the information security of the BA technology in a smart building can have an impact on the information security of those based in the building in question. For example, confidential data handled by those renting an office building can be jeopardised if the locking system is open to attack due to vulnerabilities in the surveillance cameras. Conversely, a compromised server in an office network can become a gateway for attacks on the building automation technology. These types of attacks are not out of science fiction – they are happening right now.

Phased plan for information security in smart buildings

The challenges of IT security in building automation are tremendous. How can we make a start pragmatically? The experts at secunet follow the following phased plan for relevant projects:

1. Documentation

The first step, in order to manage the complexity effectively, is up-to-date and complete documentation (insofar as possible) of all technical systems used, including site, connection, manufacturer, software versions, configuration and parameterisation and, where applicable, maintenance service provider. Frequently, only incomplete information is available – and even this is not stored in a central location.

Once created, this logging of the current status should be kept continually updated and all authorised personnel given access to it. It also makes sense to use external sources of information that, for example, supply information about currently identified security vulnerabilities in components and software.

2. Establishing the level of protection required

In building automation the critical processes such as, for instance, the power supply, fire protection, air-conditioning, leak detection and emergency evacuation (incl. safety lighting) must be protected as the top priorities. The protection requirements for the critical business processes determine the protection requirements for the technical systems with which they are implemented. Determining the protection requirements for business processes is the responsibility of the management level.

3. Ascertaining the need for action

Based on the previously ascertained protection requirements for the business processes and technical systems, and additionally taking into account the emergency management, the requisite further security measures now need to be determined and prioritised. These can be both organisational and concrete technical measures. It is necessary to obtain information from service providers and manufacturers as part of this process.

4. Implementation
Implementation of the security measures must take place on the basis of the priority level determined beforehand and the available budget. This can either be done as part of regular maintenance or planned modernisation measures – or, where urgent action is required – on an unscheduled basis.

To ensure security measures are managed, controlled and, where applicable, adapted, it is recommendable to set up an information security management system (ISMS) for BA, which is familiar from the context of German IT baseline protection.

IT baseline protection is the means of choice

Ensuring security in building automation can be achieved not only via an ISMS, but also using other IT baseline protection methods and processes from the German Federal Office for Information Security (BSI). IT baseline protection is tried-and-tested and is the best approach currently available.

The building blocks for industrial IT of modernised IT baseline protection, which contain the requirements for the information security of technical systems, are especially relevant. In future versions additional components will be added in the domain of industrial IT to make IT baseline protection for smart buildings even more universally applicable, as per the components for control centres and safety systems, for example.

secunet's practical experience has shown that the BA of a smart building can be initially safeguarded using approximately 20 components from the IT baseline protection catalogue. Around 40 components are generally required for comprehensive protection.

In future: Safety and Security by Design

The earlier the IT baseline protection catalogue comes into play in the life cycle of an automated building, the more efficiently and effectively it can be implemented. Ideally, the concept of information security should already be considered at the point of planning the building's automation technology, in the sense of 'Security by Design', which complements 'Safety by Design' – for example planning fire protection at an early stage.

Cultural change is needed

Moreover, cultural factors are also of fundamental importance: the apparent borders that still exist between the 'worlds' of IT and BA in people's minds and the real borders within organisational structures need to be identified and removed as a problem and security risk. Instead, what is required is a 360-degree understanding of building automation that avoids suppressing its IT nature – along with IT problems and security issues. Fundamental improvements to the situation will only be enabled if real cultural change comes about.

For the further development of IT baseline protection the question remains whether its application in the sphere of building automation will become as much of a success story as it has been in the domain of traditional IT. The foundations have been laid with modernised IT baseline protection. As mentioned above, however, it also requires a cultural change in building automation in order to ensure the necessary IT security.

✉ Robert A. Gehring
robert.gehring@secunet.com

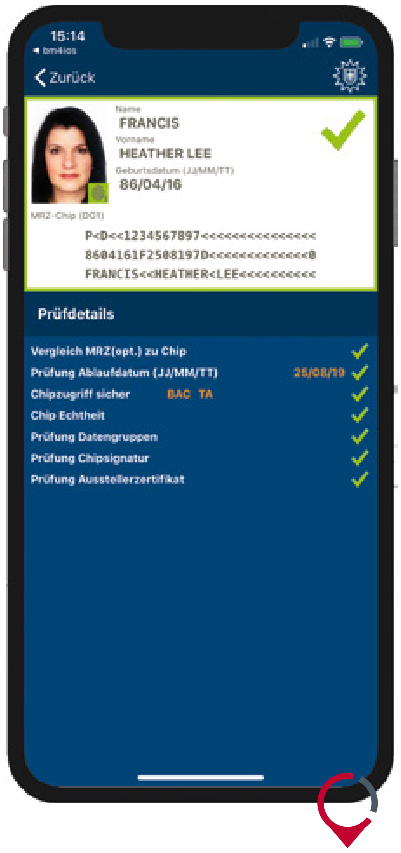
The article is based on the talk entitled 'Herausforderungen der IT-Sicherheit im Bereich der Gebäudeautomation' ['Challenges in IT security in the domain of building automation'] by **Robert A. Gehring, Christina Helbig and Markus Stark,** which was given at the sixteenth German IT security congress in May 2019 in Bad Godesberg, Bonn. The conference transcript was published by SecuMedia and can be purchased from booksellers (ISBN: 978-3-922746-82-9).

One of the benefits of building automation is saving energy. Some smart buildings can do without air conditioning; they use intelligently controlled sun shields and ventilation instead.

GERMAN FEDERAL POLICE

Mobile Document Checks via a Smartphone App

secunet has been working with the German Federal Police for several years to develop a modern information architecture for digital policing. One outstanding result of this collaboration has been the development of a Smart Police app based on the secunet biomiddle software platform. The application allows users to access and manage police information anywhere and from any device. The app is now available for iOS as well and can be used by federal as well as regional German police forces.



15:14
◂ bm4ios

‹ Zurück

Name
FRANCIS
Vorname
HEATHER LEE
Geburtsdatum (JJ/MM/TT)
86/04/16
✓

MRZ-Chip (DG1)

P<D<<1234567897<<<<<<<<<<<<<<<<

8604161F2508197D<<<<<<<<<<<<<<0

FRANCIS<<HEATHER<LEE<<<<<<<<<<<

Prüfdetails

Vergleich MRZ(opt.) zu Chip		✓
Prüfung Ablaufdatum (JJ/MM/TT)	25/08/19	✓
Chipzugriff sicher	BAC TA	✓
Chip Echtheit		✓
Prüfung Datengruppen		✓
Prüfung Chipsignatur		✓
Prüfung Ausstellerzertifikat		✓

The “BPOL Document Check” app gives German Federal Police officers a flexible and secure way to read and check electronic identity documents (eIDs) using a smartphone during mobile police operations.

Since 2018, the German Federal Police has been successfully using apps to verify documents and identify persons in mobile identity checks. The “BPOL Dokumentenprüfung” (“BPOL Document Check”) app gives federal police officers a flexible and secure way to read and check electronic identity documents (eIDs) using a smartphone during mobile police operations. Further, it allows the verification of biometric data such as comparing the facial image stored in the chip against the live image of the person. The app also offers important aspects of stationary passport and identity card checks to be performed via smartphone. secunet developed the app for the German Federal Police on the basis of the secunet biomiddle platform and tailored it to suit the police force’s day-to-day requirements. It allows to also conduct checks in offline mode, for example. The app improves the overall availability of police information and thus plays a significant role in maintaining domestic security.

With the NFC interface in iOS13 which was recently opened up to third party providers, the app is now available on all major mobile platforms and can read eIDs without the need for any additional hardware. This will benefit police forces which use both Android and iOS devices and are using, or planning to use, the “BPOL Document Check” app.

The German Federal Police and secunet are also offering regional police forces the results of their successful partnership at federal level to develop apps for mobile document checking and biometric identity verification. In addition to the “BPOL Document Check” app, several regional forces are already successfully using other apps developed with secunet in their everyday business.

All of secunet’s smart police apps are based on the secunet biomiddle software platform, which was developed together with the German Federal Office for Information Security. It offers a wide range of functionality in the fields of document verification, biometrics and OCR. It is the core element of multi-faceted document authentication and identity check applications used by law enforcement. Through service-oriented interfaces, secunet biomiddle implements the process logic on an application-specific basis and manages the components and the communication with background systems required for the relevant law enforcement procedure (e. g. Fast-ID).

The mobile version of the secunet biomiddle platform can be incorporated into existing apps of police forces or other providers as a Software Development Kit (SDK), e. g. for case processing. With versatile platform support and SDK availability, the German Federal Police and secunet have taken an important step towards providing unified mobile IT across police forces.

Thomas P. Schäfer
thomas.schaefer@secunet.com

Another Record Year for it-sa

This year, too, it-sa has managed to set some impressive new records: with approximately 15,600 trade visitors and over 750 exhibitors the trade show is growing year on year and acts as the European meeting place for the international IT security community. A 20 per cent increase in trade show visitors from other countries and many transnational shared stands demonstrate the growing international significance of the show.

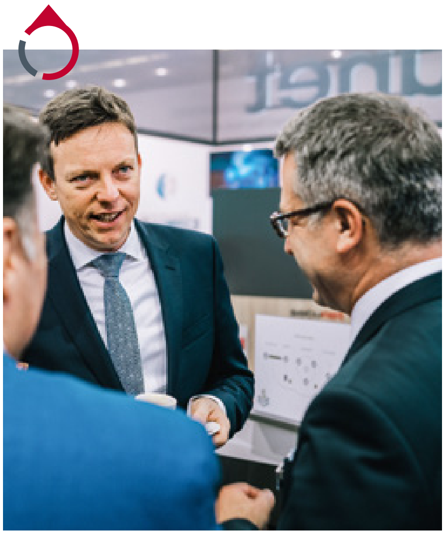
"it-sa is the trade show home for all those who operate professionally in the IT security sector. The clear uplift in exhibitor and visitor numbers and the re-enlarged exhibition area confirm the relevance of it-sa as a leading international platform for cyber security," says Petra Wolf, member of the executive board of NürnbergMesse, the company that organises the trade show.

Around 350 forum contributions and 30 separate events in the Congress@it-sa enrich the trade show with insights into IT security and data protection. Last but not least, a highlight from the last trade show day was a special keynote speech by British investigative journalist Misha Glenny.

For 11 years secunet has been involved in the specialist trade show, which is now the largest in the world for IT security. At a redesigned trade show stand secunet presented a wide spectrum of solutions for state and military organisations, security authorities, critical infrastructures, industry and healthcare. The trade show appearance was rounded off by diverse talks that spanned a number of different themes. This year, too, secunet was pleased to have lively discussions with visitors to the stand.

Dr Kai Martius, CTO of secunet and CEO of secustack, before his talk on secure cloud computing

secunet CEO Axel Deininger (right) greets Tobias Hans (centre), Saarland's Prime Minister, at the trade show stand.



The secunet trade show stand at it-sa 2019

secunet expert Mustafa Alaa Eddine speaks about secure transfer of ISDN to all-IP

secunet expert Jens Kulikowski explains how machines in the industrial IoT environment can be networked securely with secunet edge

Dates – January to June 2020

20 January 2020
ELSTERdialog | Munich, Germany

20–22 January 2020
Omnisecure | Berlin, Germany

4–5 February 2020
Europäischer Polizeikongress | Berlin, Germany

11–12 February 2020
StrategieTage IT Security | Bergisch Gladbach, Germany

11–13 February 2020
e-World | Essen, Germany

18–20 February 2020
General Police Equipment Exhibition & Conference (GPEC) | Frankfurt am Main, Germany

24–28 February 2020
RSA Conference | San Francisco, USA

10 March 2020
SINA Anwendertag | Berlin, Germany

17 March 2020
SINA Anwendertag | Bonn, Germany

20–22 March 2020
Chemnitzer Linux-Tage | Chemnitz, Germany

23–24 March 2020
Rethink! IT Security | Hamburg, Germany

25 March 2020
Polizeitag | Düsseldorf, Germany

31 March–2 April 2020
ICAO TRIP Symposium & Exhibition | Montreal, Canada

31 March–2 April 2020
Passenger Terminal Expo | Paris, France

1–2 April 2020
AFCEA Fachausstellung | Bonn, Germany

16–8 April 2020
GISEC | Dubai, United Arab Emirates

20–24 April 2020
Hannover Messe | Hannover, Germany

21–23 April 2020
DMEA | Berlin, Germany

28–29 April 2020
ID@Borders Conference | Brussels, Belgium

5 May 2020
ITS.Connect | Bochum, Germany

12–14 May 2020
KELI | Bremen, Germany

3–4 June 2020
FTE EMEA | Dublin, Ireland

9–11 June 2020
Identity Week (SDW) | London, UK

15–17 June 2020
Zukunftskongress Staat & Verwaltung | Berlin, Germany

Would you like to book an appointment with us? Just send an e-mail to events@secunet.com

Imprint

Publisher
secunet Security Networks AG
Kurfürstenstraße 58, 45138 Essen, Germany
www.secunet.com

Chief Editor, Head of Design, Content and Advertisement (Press Law Representative)
Marc Pedack, marc.pedack@secunet.com

Design and Setting
sam waikiki, www.samwaikiki.de

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

Photo credits
Cover, p. 5, 8, 18/19 bottom, 27, 28: iStock
p. 2 bottom, 7: alamy
p. 3, 6, 15, 16, 17, 19 top, 21 bottom left, 23, 24, 25, 29, 30: secunet
p. 8: Bundesagentur für Arbeit
p. 9, 10, 11: NATO
p. 12: SICP
p. 13: Matern Architekten, Goldbeck GmbH
p. 20, 21 top and bottom right: SCOTTY Group
p. 22: Fotolia

For reasons of legibility, in many cases the male form is chosen in the text. The information refers nonetheless to members of both genders.

SUBSCRIBE TO SECUVIEW

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

www.secunet.com/en/secuview

There you can also change your preference or unsubscribe.

climate neutral print
www.klima-druck.de
ID-No. 1986664
bvdm.

FSC
www.fsc.org
RECYCLED
Paper made from recycled material
FSC® C006990

Official secrets don’t fall into the wrong hands.
With SINA, public authority networks are ultra-secure.

Source: Geoportal Berlin / [DOP20RGB]