secuview

The secunet Customer Magazine 2•2021

Preserving digital sovereignty

Dr Sven Egyedy, CIO of the German Federal Foreign Office, on the federal administration's modernised classified communication

Access for all

On the way to barrier-free IT – soon with SINA

Man or morph?

Protection against identity fraud at border control

National

International

Technologies & Solutions

News in Brief

Service

Dear reader,

Although the pandemic is still ongoing, at least the year 2021 also brought us a few months in which life was a little bit more normal. At secunet, we made the most of this time: We cultivated contacts, took part in industry events such as it-sa and organised events ourselves, namely the SINA User Days. On such occasions, it not only became clear how much we had missed the personal exchange. It also became clearer again that IT security is an industry seething with dynamism and innovation.

This is due, on the one hand, to its openness and a certain eagerness to discuss: those who attend conferences and always have a foot in the door of the developer communities constantly benefit from new insights and approaches and help shape them. Also, the open-source idea ensures transparency.

On the other hand, IT security is involved in many of the major technological topics of our time – such as AI, cloud or the fourth industrial revolution. Home office and collaboration are also strongly driven by IT security, and for this reason the pandemic that paralyses many things has rather fuelled the dynamics of IT security.

What's more, IT security concerns us all, as private individuals or as citizens of a community. In contrast to some companies that still treat the topic somewhat neglectfully, government organisations attach great importance to adequately protecting their – and our – data. In this context, I am particularly pleased with the cover interview in this issue of secuview. In it, Dr Sven Egyedy, Chief Information Officer of the German Federal Foreign Office, explains the leading role the authority will play in future in the federal administration's classified information (CI) communications.

From a global perspective, it must be an important goal of Germany and Europe to establish and protect digital sovereignty. In order to achieve this goal, it would certainly be helpful if the IT security industry received support in the form of industry policy – although it does not have to shy away from competition at the technological level.

Now I hope you enjoy reading and have a relaxing holiday. Here's to a year 2022 that may be as Corona-free as possible. Stay healthy!

Axel Deininger

German federal administration modernises classified communication

“Essential contribution to a future-proof security architecture in Germany”

Especially in times of crisis, it is evident how important it is to have functioning communication. Thus, the Corona pandemic has accelerated a project that had been planned for quite some time: the German federal administration is reorganising its communication systems for classified information. In an inter-departmental project led by the German Federal Foreign Office, a new infrastructure was set up in less than two years that enables voice and video communication up to the GEHEIM (SECRET) level. secunet is one of two companies supplying the technology for this. The system will go into operation as early as the beginning of 2022. secuview spoke to Dr Sven Stephen Egyedy, Chief Information Officer of the Federal Foreign Office.

Dr Egyedy, how did the initiative originally come about?

Dr Sven Egyedy: Until 2020, there was no general, interdepartmentally available electronic solution in the federal administration for communicating classified information (CI) of the classification levels VS-VERTRAULICH (CONFIDENTIAL) and GEHEIM (SECRET). A concrete need for action in terms of CI communication was identified in 2016 during a NATO exercise, which revealed that many systems for communicating sensitive classified information were outdated, defective or only usable with limited functionality. In 2017, a cross-departmental CI communication working group was established with the participation of the Federal Ministry of the Interior, Building and Community (BMI), the Federal Ministry of Defence (BMVg), the Federal Chancellery (BKAmt), the Federal Office for Information Security (BSI) and the Federal Foreign Office (AA) – the so-called core departments of today’s federal measure R-VSK. The goal was to lastingly strengthen the CI communication network of the federal administration. As part of the IT consolidation of the federal government, the lead management of the federal measure R-VSK was transferred to the foreign IT of the Federal Foreign Office by resolution in 2019. Since then, the entire project team of the federal measure R-VSK has made an essential contribution to a future-proof

> "In the course of the market investigation, secunet Security Networks AG emerged as one of two pioneering CI IT providers in order to comply with the dual-vendor strategy of the federal measure."

security architecture for Germany and a modern state. Within a few months, the area of secret communication in the form of telephone and video conferencing technology based on the latest crypto technology was established cross-departmentally in the federal administration.

What role did the Corona crisis play in the financing and implementation of the project?

As a countermeasure to the Corona crisis and the resulting economic damage, the economic stimulus package was passed by the federal government with a volume of ten billion euros. These were earmarked, among other things, for the modernisation and digitisation of administrations. Of this, approximately 52 million euros were secured for the financing of the project. This resulted in the condition that the implementation of the project be shortened from five to two years. This could only be achieved through a holistic reorientation of the project goals and a project management that was coordinated with this.

What is the core of the solution and how are the responsibilities allocated?

The solution includes cross-departmental communication via telephony and video communication. In 2021, a Minimum Viable Product (MVP) was developed by the Federal Foreign Office in cooperation with external suppliers and service providers and successfully tested in several trials. The solution developed is currently undergoing clearance tests in accordance with the Classified Information Directive (VSA) by the BSI, which has been supervising the project since the beginning. In 2022, operations will begin with the telephony and video communication services and the scaling of the solution to the entire German federal authorities will be started. Another part of the solution envisages the establishment of an infrastructure for the data exchange of classified information. Communication can take place in encrypted form via the open Internet as well as via government networks. For the operation, a cloud infrastructure is being developed in data centres. Overall, a large heterogeneous team is part of the federal measure and includes cooperation between the AA, BMI, BKMVg, BMF and BSI authorities as well as private-sector manufacturers of crypto components and other external service providers. The foreign IT department of the Federal Foreign Office is responsible for the coordination and control of the federal measure.

Why did you choose secunet as one of the technology suppliers?

During the project preparation phase of the federal measure R-VSK, the foreign IT department of the Federal Foreign Office conducted a market survey for CI IT communication devices. In this market survey, specific conditions were used to find out which potential providers and products are available for setting up a cross-departmental CI IT infrastructure. Taking into account the requirements of the VSA and

Dr Sven Egyedy

Dr Sven Egyedy is Chief Information Officer (CIO) of the German Federal Foreign Office and Head of Foreign IT. In addition to positions at the Federal Ministry of Finance, the Federal Ministry of the Interior and the Federal Ministry of Defence and their divisions, he was Commercial Coordinator for the construction contracts for the ITER nuclear fusion reactor at the European Joint Undertaking Fusion for Energy F4E from 2011 to 2015. Dr Egyedy is Chairman of the Board of the non-profit association NExT (Network: Experts for the Digital Transformation of Administration) and holds a PhD in social sciences.

the SÜG (Security Verification Act) and in the interest of digital sovereignty, the consideration was limited to providers whose company shares and development are predominantly located in Germany. In the course of the market investigation, secunet Security Networks AG emerged as one of two pioneering CI IT providers in order to comply with the dual-vendor strategy of the federal measure. secunet's product portfolio includes products that have been specially developed for IT security solutions for electronic classified information processing or CI communication and thus meet the specific requirements of this communication purpose. An example of secunet's product portfolio is the crypto architecture "Secure Inter-Network Architecture", or SINA for short, which was developed on behalf of the BSI. SINA enables the secure processing, storage, transmission and documentation of classified information. Differently classified data can be strictly separated. The architecture offers a comprehensive product range consisting of terminal devices, crypto gateways and Ethernet encryption technology as well as the system solution SINA Workflow (SWF).

In addition, a security partnership with the Federal Republic of Germany has existed since 2004. In various projects, secunet has gained experience in public administration, for example at the Federal Ministry of the Interior, the Federal Office for Information Security, the Federal Foreign Office, the German Air Force and the German Military Representative to the NATO Military Committee.

How was the cooperation with the other departments and with the industry partners?

As already mentioned, interdepartmental cooperation in the area of CI communication has grown historically. Since the Federal Foreign Office has been in charge of the federal measure, interdepartmental cooperation has been further intensified. The CI products for telephony and video have been extensively tested in the core departmental group and we have established constructive working groups to pool experience already gained in dealing with CI IT products and to exploit the existing level of knowledge in the federal administration. Furthermore, setting up CI IT infrastructure is highly complex, which is why we rely on the specialised CI IT expertise of our industry partners in addition to departmental experience. Through the various CI IT products and services that can be found in the product portfolio of the federal measure R-VSK, we bundle the interdisciplinary expertise of our industry partners. Our vision is to serve as a lighthouse project for functioning interdepartmental cooperation involving strategic industry partners for further IT measures within the federal administration.

> "Against the background of the particularly sensitive nature of classified information, the aspect of digital sovereignty in CI communication takes on additional weight."

Only German providers are used for the encryption technology and the end devices. Can you briefly explain the reasoning behind this?

The market for CI products is specifically geared towards the target group of public administration. The application scenarios and framework conditions differ from those of the private sector, since high secret protection-relevant requirements have to be fulfilled and complex test processes have to be gone through – keyword VSA. Against the background of the particularly sensitive nature of classified information, the aspect of digital sovereignty in CI communication takes on additional weight. Products and services from external software and hardware providers are needed to set up a CI IT infrastructure for interdepartmental

classified communication. The dimensions of sovereignty in handling data and technological sovereignty in the areas of software, hardware and architectures play an important role. Consequently, high demands must be placed not only on the products used themselves, but also on their providers. National security interests must also be safeguarded at all times when cooperating with external service providers and suppliers. In this context, independence from third countries outside the EU is of central importance and the focus was set on companies that are predominantly based in Germany.

What kind of runtime do you expect from the solution and what support services should secunet provide during operation?

As a service provider for the federal administration and leader of the federal measure, we obviously want to provide our customers with secure, durable and high-performance CI IT. That's why we only provide our customers with state-of-the-art CI IT. The end devices for CI communication have an update capability in order to be able to react dynamically to changes. Our industry partners are available to us as reliable partners for further product development.

What are the next steps?

After the operational approval by the BSI, the users of the authorities at management level will first be provided with the solution in 2022 according to a defined rollout plan. After that, all federal authorities will gradually be connected to the solution. In parallel, we are building new data centres in cooperation with the ITZBund, and their geo-redundant model will guarantee the availability of the cloud. From 2024, the "diplo version" will also provide partners and allies in other countries with a solution for direct protected information. The final stage of expansion will take place in 2025 with the "corporate version" for the secret-protected economy. When scaling the solution, the ability to integrate with other platforms is very important. In order to avoid media discontinuities in terms of user-friendliness, automated interfaces to the internal departmental networks must be created to realise seamless CI communication.

Dr Egyedy, thank you very much for the interview.

THE NEXT GENERATION RED TELEPHONE

As part of the new CI communication of the federal administration, secunet is providing a highly secure communication solution for desktop operation. The solution revives the classic "red telephone" for protected communication. However, the modern version is a hardened all-in-one PC with handset and screen for voice and video communication. The device is approved up to the GEHEIM (SECRET) level and is based on the SINA Communicator H. Two-factor authentication takes place by means of a crypto stick connected via a USB interface.

20 years of the Biometrics Institute

How eIDs and biometrics made border control efficient and more secure

Electronic identity documents (eIDs) and the biometric data stored in them form the basis for automated border controls and convenient passenger processes, as we know them today. How did we actually get this far? On the occasion of the 20th anniversary of the Biometrics Institute, we take a look back at the developments of the last two decades.

The addition of the electronic component to the established optical security features made storing biometric information in chips of eIDs possible. At the same time, biometrics created a unique link between document and document holder. In addition to a significantly higher level of forgery protection, this simultaneously opened up the use of biometrics-based automated border control. Biometrics in eIDs and the associated convenience are now taken for granted worldwide. However, the path to success was certainly not always a straight line and many steps have been taken.

Real added value can only be achieved through interoperability

The addition of biometric data to eIDs alone does not add value. First, it must be ensured that eIDs will be accepted and can be processed at borders around the world. Second, the binding between eID and its holder through biometrics enables a higher level of security and, at the same time, new digital processes. Two aspects, however, highlight the importance of interoperability:

- The dynamic market for biometric technologies: Many devices and manufacturers, short product life cycles.
- The sheer mass of eIDs: 1 billion eIDs were issued from 150 states in 2019.

Automatic border control gates (secunet easygates) at Sofia airport, Bulgaria

In numerous interoperability tests, secunet supported manufacturers of eIDs and inspection systems in optimizing components and making them fit for international use.

These tests have shown the importance of cooperation between states, sovereign authorities and industry. With the growing potential for biometrics independent organisations such as the Biometrics Institute were essential in the process – connecting all stakeholders and providing a platform to exchange innovative ideas as well as concerns.

Standardisation is the key

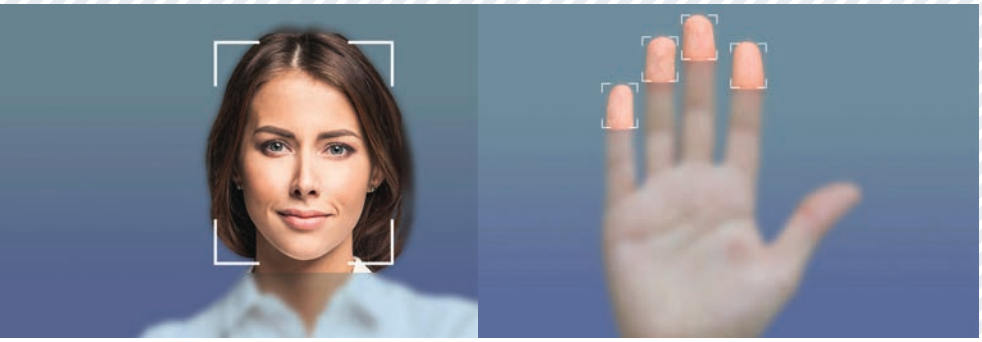
The essential parameters for the use of biometrics in eIDs and the quality and security requirements for their use in sovereign applications have been defined and further developed in international standards. They regulate a wide variety of aspects, one focus being the protection of biometric data over the entire lifecycle of sovereign eIDs, e.g. during document issuance, the security mechanisms and access rights during document verification as well as the responsible use, including appropriate and data protection-compliant handling.

One of the first important standards for automated border control was ICAO DOC9303, which is still the gold standard for eIDs but also an important prerequisite leading to the widespread use of biometrics in public sector applications.

A milestone for biometric data protection in sovereign eIDs was certainly the BSI TR-03110 of the German Federal Office for Information Security, which is still valid today. secunet was involved in its development: TR-03110 specifies, among others, Extended Access Control (EAC) for access to biometric data stored in eIDs and can be regarded as the foundation for all security protocols for sovereign eIDs – it also had a significant influence on ICAO Doc 9303 Parts 10, 11.

Standards continue to be an important tool for all stakeholders to jointly implement a consistently high level of security for handling biometric data in eIDs, on the application as well as technology side. Especially for biometric systems, standard conformity on every level assures the accuracy, thus the reliable use of the system.

Just how did these standards evolve, and what does it take to develop them?



For biometric purposes, e.g. facial images and fingerprints are used.

Experience through a valid database

A prerequisite for standardisation is data and experience – this is a lasting truth. For the use of biometrics in sovereign eIDs, this initially meant collecting a lot of data – a biometrics aficionado will certainly remember the BioP I and II projects:

Together with the German Federal Criminal Police Office, secunet conducted a large field test at Frankfurt Airport and compared biometric verification algorithms (face, finger, iris). The results formed the basis for the selection of biometric features of the electronic passport in Germany. Both studies marked the start of many subsequent projects to investigate and evaluate biometric procedures, from which the entire market profited in form of standards and technical guidelines.

These steps – data collection, standardisation, interoperability – were essential key factors for the widespread use of biometrics today. They ensure data is reliably usable in accordance with specifications in terms of quality, security and speed.

Secure eIDs in everyday life

Standards and the worldwide spread of biometric travel documents have opened up completely new possibilities: Increasing passenger numbers could now be addressed through automating border controls (ABC). Aside from the current COVID-related slowdown, the demand for biometrics in border control and passenger identification has been increasing worldwide.

In the German EasyPASS project, for example, ABC systems have increased from 70 ABC gates in operation at four airports in 2014 to more than 250 ABC gates at eight airports today with a total of 95 million users.

For biometrics-based automated border control, protection against circumvention attempts plays a major role. Current standardisation efforts and developments focus on continuously improving procedures to detect fraud attacks through, e.g. presentation attack detection (PAD) or morphing attack detection (MAD).

Plenty of challenges ahead

Biometric data is a sensitive asset that must be protected. A multitude of standards are binding in terms of which data may be collected, used and stored, and in which quality, security, usability and user convenience must always be balanced for the specific applications needs. Continuous development of corresponding standards is essential in order to meet current and future requirements for secure biometric procedures and to effectively prevent attempts to overcome them. New possibilities that arise, for example, through artificial intelligence (AI), will play a decisive role here – plenty of work for the Biometrics Institute, secunet and other important players in the biometrics community.

The **Biometrics Institute** is an international association that provides information, training, research and a network of experts on biometrics. Its mission is to promote the responsible and ethical use of biometrics and related technologies that respect the Institute's ethical guidance as an independent and impartial international forum for biometric users and other interested parties.

The Biometrics Institute was founded in 2001 and represents a unique multi-stakeholder community spreading across the globe including a large number of government agencies, banks, airlines, airports, biometric experts, privacy experts, regulators, suppliers and academics as well as international observers such as United Nations agencies, EU institutions and IGOs. It provides an unbiased and independent platform for discussion bringing together different perspectives to provide a balanced viewpoint on biometrics.

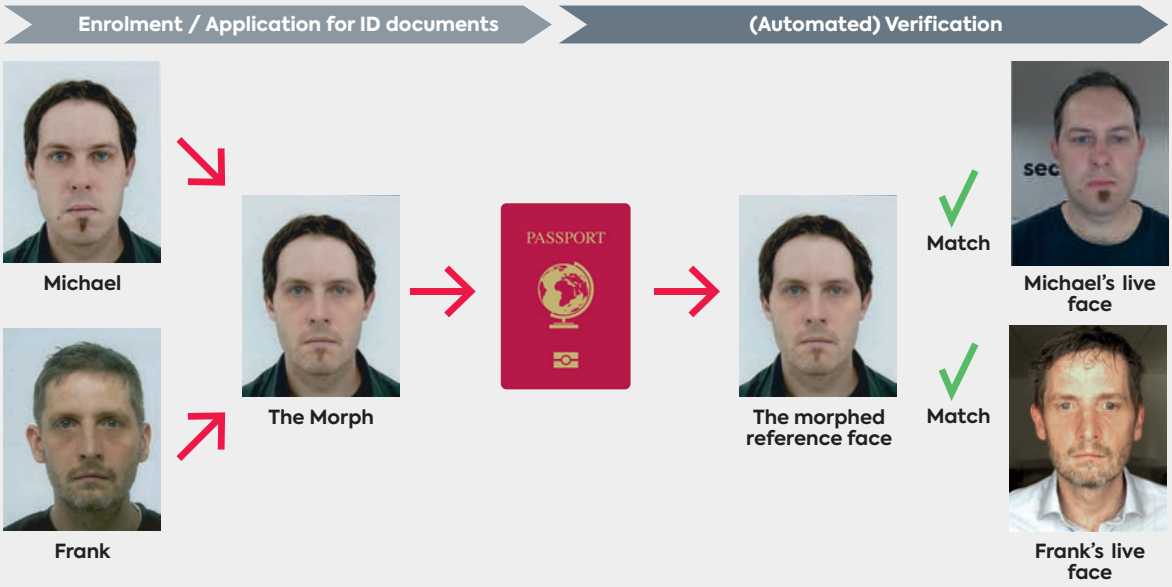
Protection against identity fraud at border control

Man or morph?

Biometrics and facial recognition have made border control more efficient and secure. However, there are types of fraud that still pose a challenge, both for border control officers and automated border control systems. These notably include so-called morphing attacks, in which fraudsters make use of ID photos assembled from the facial images of more than one person. Now there is an algorithm that can reliably recognise morphs like these.

Fictional impostors Michael and Frank use powerful image editing software to merge their biometric passport photos into a single image. The result is an image that resembles both men. Michael then uses this manipulated image for his new passport. Superficially, he's recognisable as the person in the picture, so the officials don't suspect anything when they issue the passport. Frank then goes to the airport with the new identity document. As the morph is executed well, facial recognition software – or the officer at the border control counter – mistakenly recognises him as the person in the picture, thus identifying him as Michael, the passport holder. In the worst-case scenario described here, Frank can therefore cross the border under a false identity.

The impostors in this story are fictional, but the crime is very real. Public authorities from various countries, including the Slovenian Police Force, for instance, have already reported scams involving morphing. The likely reason for this prevalence is that morphs are easy to implement. They don't require any special



This is how a morphing attack works.

expertise; a commercial image editing program and a little talent are enough.

The human security factor

Reports of detected morphs show that perpetrators predominantly target automated border control systems. However, this type of fraud also poses a challenge to humans. Research shows that, on average, people only recognise about 60 per cent of the morphs they are shown compared to a trustworthy image. However, people who take part in such a test seem to perform better and better in the course of the examination. So those who specifically deal with the subject sometimes recognise more morphs later on.

Supervised registration

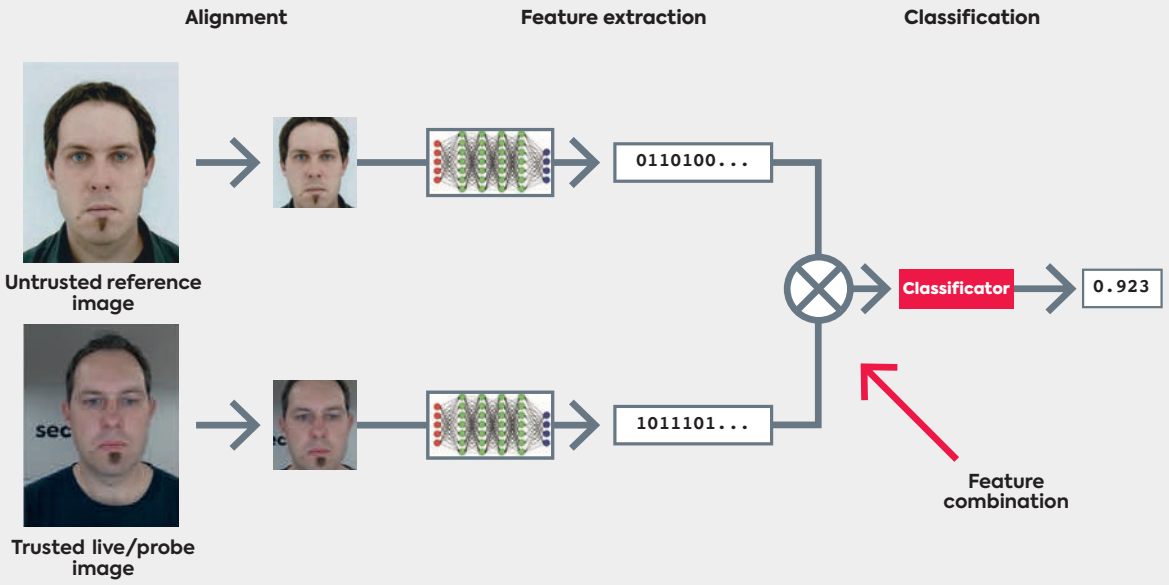
Training border control officers is therefore one way to deal with the morphing problem. Another is so-called "live enrolment". In order to prevent the forgery of personal images in identity documents at the issuing stage, authorities could no longer consider photos provided by applicants themselves. Instead, only images taken directly on-site under the supervision of the authorities would be acceptable. This would ensure that no more morphs find their way into identity documents. The problem with this is that even if all European countries were to agree on such a procedure in the future, there will probably always be countries around the world that accept images taken at home for official documents. Consequently, live enrolment alone will never truly overcome the morphing challenge.

Nevertheless, the coming European Entry/Exit System (EES) is expected to herald improvements in this area. When entering Schengen countries in the future, third-country nationals will have to register with four fingerprints and a facial image – directly at the border via live enrolment. When these individuals re-enter the Schengen area, not only the image in their identity document will be available, but also a trusted facial image in the EES database. If high-quality equipment, like the height-adjustable facial image camera secunet easytower, has been used for image capture, the result will be ideal for EES-compliant border control.

Smarter software

Another security measure is software algorithms that recognise facial morphs during automated border control. secunet's experts have been working on morphing attack detection (MAD) for several years. Strictly speaking, we are talking about "differential" MAD in this context, whereby a facial image is checked through comparison with a second, trusted image. A trusted data source is always present in the automated border control process, because this process always involves capturing a live image. This image is then compared to the image in the traveller's electronic identity document. At this point, the algorithm intervenes and detects any discrepancies. A vital prerequisite is that the live image meets high quality standards.

In partnership with the Darmstadt University of Applied Sciences, secunet has now developed a new, even more effective algorithm,[1] which has



... And this is how Morphing Attack Detection operates.

already proven itself to be suitable for everyday use. As with other algorithms like this, a threshold value can be used to fine-tune the algorithm. If set to a false positive rate of 2% (meaning two out of every hundred facial images are misclassified as morphs and have to be manually verified), the algorithm will spot 85–88% of all genuine morphs. This is very good compared to both human test subjects and previous algorithms.

A portfolio with morphing protection

The new algorithm is used throughout secunet's border control portfolio. In addition to secunet's easygate automated border control system, this includes the secunet easykiosk self-service system for easy pre-enrolment of passenger data, and the secunet bocoa border control application in combination with the secunet easytower facial image camera. These products and solutions also provide sufficiently high-quality live images for the use as trusted comparison images for differential MAD.

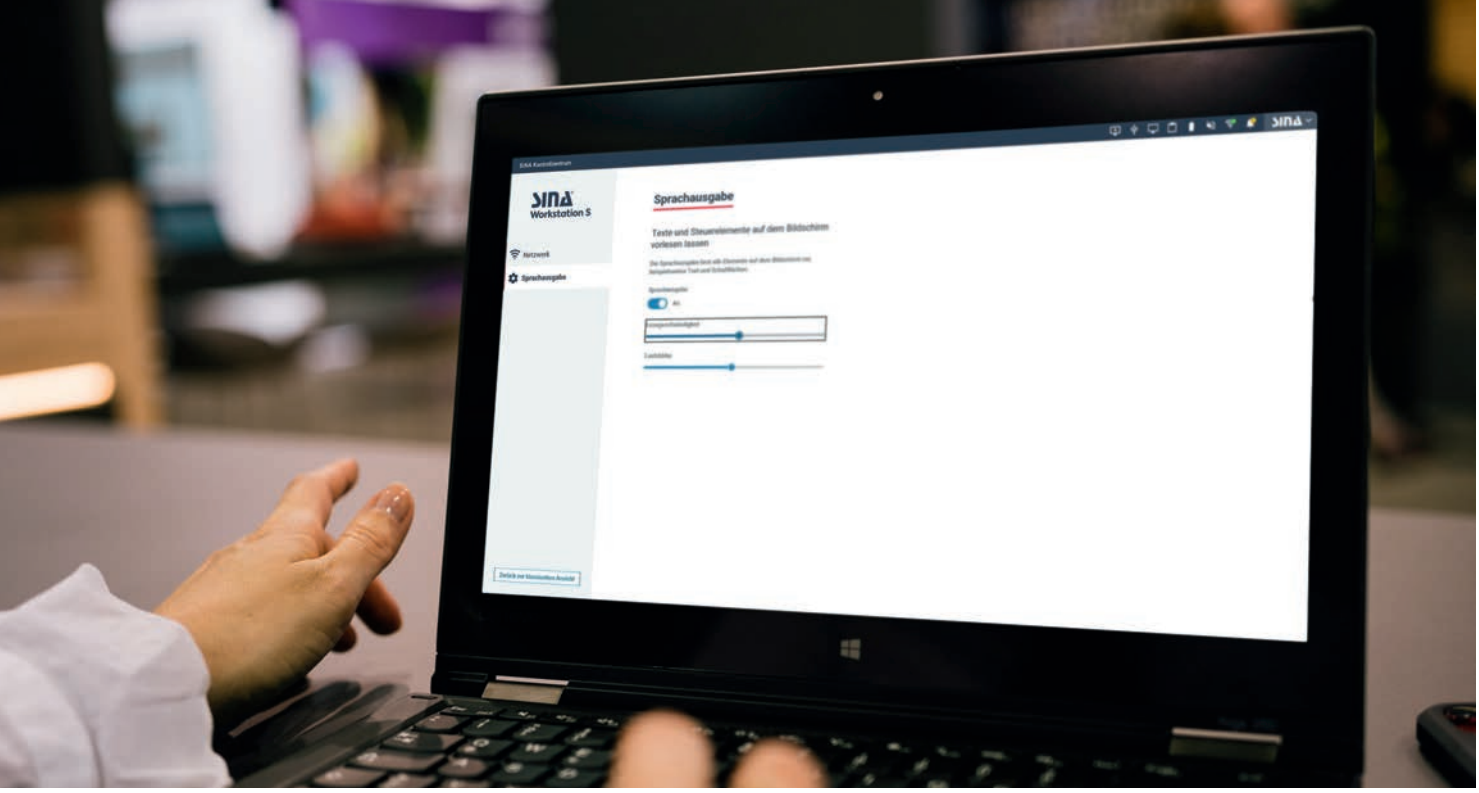
The MAD algorithm thus complements other security measures already available in secunet's border control portfolio. The secunet easygate, for instance, reliably detects a high proportion of so-called presentation attacks, whereby fraudsters attempt to present a false identity using masks.

Morphing detection: today and tomorrow

The new algorithm has allowed MAD to take a decisive step forward within a very short period of time. Despite this progress, morphing attacks will likely remain a challenge for the foreseeable future. The algorithm must therefore be continually improved, extended and retrained to further reduce error rates going forward. In addition, software-based MAD can only be part of the solution; its other cornerstones are live enrolment and the training of border control staff. After all, combatting morphing is as much about people as it is about machines.

Michael Schwaiger
michael.schwaiger@secunet.com

[1] The methodology was first described in the following publication and was subsequently developed further by secunet: U. Scherhag, C. Rathgeb, J. Merkle, C. Busch: "Deep Face Representations for Differential Morphing Attack Detection", in IEEE Transactions on Information Forensics and Security (2020).



Barrier-free IT

Access for all

Has our society already made good progress towards accessibility in the digital world? Depending on the perspective, this is judged differently. On the one hand, there are more and more laws and regulations on the subject, and the number of accessible IT products and services is also increasing. On the other hand, there is still a lot to be done, and associations for people with disabilities criticise the pace of progress as being too slow. secunet is currently developing an accessible version of the SINA user interface. In this context, secuview spoke with Robert Schäfer, software developer at the German Federal Statistical Office, who is committed to accessibility and has tested the new SINA user interface as one of several blind users.

Mr Schäfer, how do you assess the state of accessibility in IT and digital offerings in Germany?

Robert Schäfer: As far as the federal administration is concerned, there is still room for improvement from the perspective of those affected. Many things are implemented under time pressure and not consistently followed through. Let's take the example of the e-file: it itself is accessible, but the filing system and the workflows are not.

In the private sector, the gaps are even bigger. Online banking, for example, has hardly been barrier-free so far; in some cases, visually impaired people cannot even enter their customer number. There are only two or three banks that are barrier-free. The situation with online shopping is mixed: the websites of the large providers are generally easy to use, and in some cases there are information and hotlines on accessibility. On the other hand, the topic is often simply not present for the smaller ones. However, there are 10 million severely disabled people in Germany, so we are talking about a large group of potential customers.

Robert Schäfer

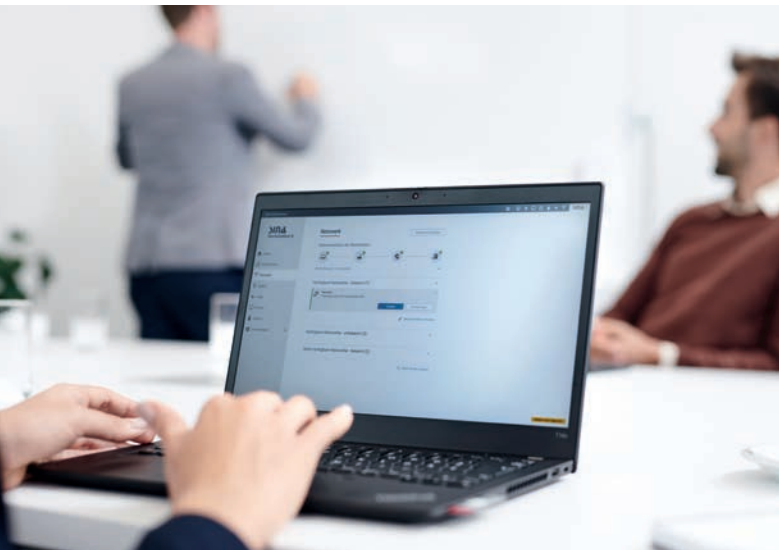
Robert Schäfer has been working at the German Federal Statistical Office since 2000, where he is responsible for application development with a focus on accessibility. He has worked in the public service since 1991. One of his earlier professional stations was the administration of the German Bundestag.

Mr Schäfer is the local representative for severely disabled employees at the Federal Statistical Office in Bonn. He is also a founding member of the VSV Bund (Association of the Representatives of Severely Disabled People in the German Federal Administration), where he is the board spokesperson for IT matters. The VSV Bund represents the interests of severely disabled employees of numerous federal ministries and their subordinate authorities.

Many people do not realise what a lack of accessibility means for those affected: they are excluded from elementary social processes. We need access for all. In the USA, by the way, things are much more advanced than in Germany. There, stricter accessibility laws also apply to the private economy.

How do you use the SINA Workstation?
I have been using it in all situations since 2013. I am a software developer. Day-to-day business runs practically around the clock, so the SINA Workstation is my primary work device. I'm on the road a lot, and in principle I can use the SINA Workstation anywhere, for example to do minor programming. Since I can't see, however, there are limitations when I'm away from home. This is the case, for example, when the device loses its connection to the network. The network settings are currently not operable for me. But that will change with the new version of the SINA user interface.

Preview of the accessible SINA user interface, of which the first functions will already be available in Q1/2022



You, among others, initiated the development of the accessible version. How was that exactly?
In 2017, at a SINA expert meeting, I approached Armin Wappenschmidt, who is responsible for the SINA Workstation S at secunet, about the topic. Mobile working is becoming more and more important, so it should at least be possible to set up the network and start the SINA guest system sessions in an accessible way. secunet responded positively to my request. Now the new version of the SINA user interface is almost finished and I took part in a user test.

How do such user tests work?
We go through predefined use cases and try out how well they can be operated. Then we discuss any queries. In my opinion, user tests are more significant than the widespread BITV tests, which only examine the points that are in the Barrier-Free Information Technology Ordinance (BITV). A good result in a BITV test does not necessarily mean that a service is actually easy to use.

Accessibility in IT and telecommunications (ICT) should ensure equal access for all people. This means that user interfaces and information must be designed to be perceptible, operable, understandable and robust for users. "Robust" means that content can be reliably accessed, regardless of which technologies (browsers, tools) users use.

Accessibility in ICT is already partly mandatory in the EU: websites, apps, intranets, extranets and electronic administrative processes must be designed barrier-free by public bodies. Uniform minimum requirements regarding accessibility are defined in the harmonised European standard EN 301549. Its application in Germany is legally fixed by the Barrier-Free Information Technology Ordinance (BITV) 2.0 and the Disability Equality Act (BGG) for the products and services mentioned and must be implemented by the beginning of 2022 at the latest.

The "European Accessibility Act" (EAA) obliges for the first time not only public bodies but also economic actors to ensure accessibility. The Barrier-Free Act (Barrierefreiheitsstärkungsgesetz, BFSG) has been the legal implementation of the EAA in Germany since July 2021. Since a transitional period is sometimes foreseen until mid-2025 and in some cases beyond, the German Association for the Blind and Visually Impaired (DBSV) criticised the law as "unambitious".

What aspects of the user interface in particular are important? How well do you think they have been implemented in SINA?

Of course, good voice output is crucial for blind and visually impaired people. This has been achieved very well with SINA. Logical menu navigation in connection with keyboard use is also important. We found room for improvement on this point in the test, which was subsequently remedied by the SINA development team. Another aspect is that basic functions of the SINA user interface such as the network settings are operable. This is now the case. Overall, the essential points have been implemented, I am very happy with the result. Of course, there are still things that could be improved.

What else would you like to see?

For example, it is currently not possible to carry out more in-depth configurations in an accessible way, for example at the individual SINA guest systems. I would like to see improvements in this and a handful of other areas in the future. But compared to the previous state, there is nothing to complain about. Generally speaking, I can now work very well with the SINA Workstation.

Other people were impressed by this too: I presented the SINA Workstation S at the VSV Bund, the Association of Representatives of Severely Disabled People in the German Federal Administration. The reactions were very positive. Especially in times of the pandemic, the SINA Workstation solves a major problem: many colleagues have hardly been able to work in a home office because there is no suitable technology for it. As a result, they either travel to the office despite being severely handicapped or require costly special solutions. SINA enables secure mobile working without special solutions – and now almost without restrictions.

Mr Schäfer, thank you very much for the interview!

Alexander Wölfel
alexander.woelfel@secunet.com

For the SINA Workstation S, a **barrier-free user interface** is currently being developed. A first version is expected to be available in the first quarter of 2022. Additions are already planned; in the future, all settings should be operable for everyone if possible. In order to prove accessibility, a declaration of conformity according to BITV 2.0 will be sought after its complete implementation.

New Work and collaboration with sensitive data

Securely into the new world of work

Under the buzzword "New Work", decentralised, flexible working had already been on the rise for years when the pandemic in 2020 abruptly forced a new form of collaboration in many organisations. Today it is clear that much of this will remain. A central element of the new working world are collaboration services that can replace face-to-face meetings in whole or in part. Handling sensitive or classified data is no obstacle to this, as secure solutions for video conferencing, messaging & co. show.

Working hours are being organised more and more flexibly, companies and public authorities want to operate more and more independently of location, and the home office will remain an integral part of the working world in the long term. According to Statista[1], the proportion of people working predominantly from home rose from around 4 to 27 per cent within a very short time during the first lockdown, then fell again and later, at the beginning of 2021, again reached a value of 24 per cent. In a survey by the German Federal Office for Information Security (BSI)[2], 58 percent of companies stated at the end of last year that they would allow their employees to work from their home offices even after the acute pandemic.

Modern office IT has paved the way for this change. Collaboration services provide the framework for effective working together even without personal contact. But in addition to the desired flexibility, new points of attack are emerging at the same time. Parallel to the expansion of home office options, the number of malware variants has also continued to grow. The BSI[3] has observed an increase of more than 20 percent from June 2019 to May 2020, i.e. including the first wave of the pandemic.

VSA-compliant collaboration workplace

Yet security concerns need not put the brakes on the introduction of collaboration services. Since the beginning of the pandemic, secunet has equipped a large number of authorities handling classified information (CI), and therefore having to implement the requirements of the German Classified Information Directive (Verschlusssachenanweisung, VSA), with secure mobile workstations. The Secure Inter-Network Architecture (SINA) is used for this purpose. As a holistic security system, it protects not only individual components, but the entire digital infrastructure.

[1] Statista 12 August 2021, survey on home office use in the corona pandemic

[2] German Federal Office for Information Security 2020, study "IT security at the home office"

[3] German Federal Office for Information Security 2021, report on the state of IT security in Germany

Video conferences from the home office are increasingly replacing physical meetings.

SINA solutions are available for different classification levels as required. The SINA Workstation S client is a central component of many SINA solutions at the protection level of VS-NfD / RESTRICTED. Despite its high level of security, it offers users a home-office-capable digital workplace with the usual operating systems and software products and also supports secure and modern collaboration via VoIP telephony, video and messaging.

Digital meetings via telephone and video conferences

With SINA, meetings can be conveniently transferred to the home office. VSA-compliant telephony with colleagues is made possible by the Voice-over-IP client, which is integrated as a softphone application in the SINA Workstation S as standard. Video conferencing is also supported: Video clients can be routed to the internal video infrastructure via dedicated VPN channels. This makes optimal use of the available bandwidths and avoids disruptions in image and sound transmission.

The architecture of SINA also allows users to use commercial tools such as Teams, Skype or Zoom. For this purpose, the SINA Workstation S provides a specially optimised guest system, secunet Desktop.

Messaging without security concerns

With the secure messenger stashcat, employees can not only exchange and connect securely via chats, but also use calendar functions, conduct surveys and implement video conferences. A file repository makes it possible to share documents in project work within the team or externally if required. All data is encrypted end-to-end and processed in accordance with the requirements of the EU General Data Protection Regulation (GDPR). With SINA, the messenger can be integrated into a CI infrastructure.

Working together on classified documents

The SINA Workflow solution is currently the only end-to-end digital management system for collaborating on CI: with just a few clicks of the mouse, classified documents such as (highly) sensitive e-files can be distributed securely. With SINA Workflow, users on the SINA Workstation can, among other things, work out content collaboratively, implement internal coordination processes with co-signatures and forward documents securely according to the principle of "need to know".

In addition, the possibilities of secure collaboration can be expanded with complementary solutions. Companies and public authorities that want to extend their secure VoIP telephony beyond the boundaries of their own network can get a solution for internal network coupling and external network connection with the secunet SBC. For highly secure voice and data communication via IP networks, the SINA Communicator H offers a suitable complement to the SINA Workstation on the desk. This is a modern terminal device in telephone format which is also approved for high levels of secrecy up to and including GEHEIM (SECRET).

Holistic security for a new working world

Today, modern collaboration is also feasible with data that requires special protection or is classified. As always when it comes to IT security, a holistic approach is advisable. Then cyber security and New Work can go hand in hand.

Aljona Wehrhahn-Aklender
aljona.wehrhahn-aklender@secunet.com

Doctor talking to a patient via a telemedicine application

Digitisation of healthcare

A cloud solution for hospitals?

Interview with Torsten Redlich, Deputy Head of the eHealth division, secunet Security Networks AG

What opportunities do cloud solutions present for the healthcare system?

Torsten Redlich: In Germany, current laws and investment programmes of the federal government are setting the course for a digital future for hospitals and other medical establishments. The policies stipulated within these regulations also mean, however, that a large number of data sources will need to be linked together. It will therefore no longer be enough to keep information to hand at isolated operating facilities or individual organisations. Rather, data will increasingly need to be made available from a central hub, which is impossible to implement without a platform approach and cloud technology. Other aspects are also important: holistic cloud solutions take the burden off IT staff, make computer resources instantly available at the click of a button, and enable healthcare institutions to focus on their core IT. When it comes to research, collaborating institutions can build shared data platforms. IT security has a crucial role to play in all of this: this security is critical for complex solutions, because one prerequisite is that the data owners retain sovereignty over their information at all times.

What questions should healthcare institutions ask themselves if they want to implement cloud-based solutions?

To start with, they need to determine which cloud solutions they would actually be permitted to use. The legislation calls for systems that are open and distributed yet meet stringent data protection and

IT security requirements. This applies in particular to hospitals, which are defined as critical infrastructures and therefore need to comply with especially rigorous security standards. However, the point at which these conditions are met is hardly for the institutions themselves to determine – especially if, as is usually the case in hospitals, they have scant IT capacity and few specialist personnel to carry out these analyses. This is another reason medical institutions require turn-key cloud solutions that meet comprehensive compliance requirements "off the shelf".

Which solutions does secunet offer in order to fulfil the requirements in the tightly regulated healthcare sector – and what must a comprehensive cloud-based healthcare concept be able to do?

It is vital to take all technical levels into account when thinking about security in cloud infrastructures. Among other things, this means that the hardware base is already secured and the virtualisation technology built on it is secure from the very beginning – the keyword here is 'Security by design'. Furthermore, at secunet we have put the emphasis on open standards and open source for decades. On the one hand, this simplifies the work for the inspection authorities and those who create the standards; on the other, users do not depend on a single manufacturer. This also applies to SecuStack, the secure cloud operating system we co-developed. This uses transparently integrated cryptographic mechanisms and numerous security modules. Specifically for the healthcare sector, we add features like confidential computing for special data classes, audit security when using machine learning or data analysis, and connection to the State health services. This approach means that complete 'Trusted Cloud Infrastructures' can be implemented for medical institutions.

Why is there a move from on-premises models towards flexible Software as a Service concepts?

On the one hand, there is increasing demand for cloud solutions in order to compensate for insufficient IT resources and experts in the healthcare sector. On the other hand, it is challenging to continually operate on-premises solutions with the necessary security and privacy features based on the existing technology. Cloud technology enables new applications and supported projects to be implemented rapidly. There are other benefits, too: in contrast to local use models, cloud-based approaches avoid information silos forming in individual institutions. Instead, they promote information sharing and make the data available across a range of interfaces. Ultimately, it is also not beneficial to carry out the necessary continuous further development of the software via hundreds of distributed and, occasionally, very different on-premises solutions. This not only costs significant time and money but also increases security risks. In contrast, a comprehensively designed cloud solution can have an overwhelmingly positive effect on aspects relating to IT security. Experience shows that, where new technologies can prove themselves by meeting stringent compliance stipulations and clearing official hurdles, they will quickly become widespread.

Torsten Redlich
torsten.redlich@secunet.com

Highly secure, multimedia communication in military settings

What does logistics have to do with SECRET-level videoconferencing?

Videocalling and videoconferencing are commonplace nowadays – almost all of us use them in both our professional and our private lives. These communications technologies have advanced a long way, especially over the past two years. Even in military organisations like the German Federal Armed Forces (Bundeswehr), videoconferences with multiple participants and large amounts of data are the norm today, whether that's in the camp, the deployment area, or in multinational federations. It's not just about a high level of security; everyday usability is also key. SCOTTY and secunet have now developed a solution that, unlike many others, can be used in a modular design and can be shipped in convenient flight cases.

Briefings in operational command, strategic coordination between generals and the Federal Ministry of Defence, regular communication between the Bundeswehr command posts and locations – videoconferences have become established and proven their worth in these and other deployment situations. Since classified information up to and including GEHEIM/SECRET level is involved, the solutions implemented must satisfy the requirements of the German Classified Information Directive (VSA). This requires high-grade encryption technology in addition to the best audio and video quality.

There are some practical challenges as a result of the stringent security requirements. Most videoconferencing solutions currently used for SECRET communications need to undergo a labour-intensive zoning and measuring process with regard to their transmission characteristics in order to preclude electronic eavesdropping. The components of these common commercial solutions cannot be measured individually due to their copper wiring. If a component is replaced and the whole system wired up its transmission characteristics can change. Thus, if one component fails, the system has to be replaced in full or measured again after it has been repaired. This sometimes results in weeks of downtime, considerable maintenance work and, depending on where the system is located, significant logistical effort.

SINA H secured video conferencing system, well packaged for transport in flight cases

secunet and SCOTTY have therefore developed a solution that addresses these and other challenges. It combines SINA's tried-and-tested security with SCOTTY's sophisticated videoconferencing technology within a comprehensive, all-in-one system, and has been specially designed to meet the logistical needs of the Armed Forces. The SINA Workstation H Client IIIa and SINA L3 Box H integrated components form the basis for secure video transmission and data exchange. They enable classified data to be processed and transmitted at classification levels up to and including SECRET / NATO SECRET. The videoconferencing components are designed to guarantee excellent video and audio quality even under unfavourable circumstances or in big spaces with large numbers of participants.

Innovative modular transmission protection

The particular advantage of the new solution is its innovative, modular system architecture, which, depending on the use case, enables a combination of versatile videoconferencing configurations. All systems are generally shipped in flight cases. This means that the videoconferencing systems can easily be brought to their intended locations or, if necessary, transported back and forth. It is therefore straightforward to operate a systems pool for operations abroad and special forces, and to send the devices immediately should they be needed. In addition to protecting the components, the flight cases also serve as a base for the monitors and audio components during operation. Once they arrive at the set-up locations, the flight cases only need to be opened and the videoconferencing modules can be connected using optical network cables.

These fibre optic cables make it possible to transmit data with simultaneous galvanic – i.e., electrical – separation. Thanks to this capability and the individual zoning of all components the system is extremely flexible and offers logistical added value. Since the system doesn't have to be measured as a whole, components can be removed or replaced at will – e.g., when maintenance is required, or to change the configuration. If a monitor fails, this can quickly be replaced with an alternative unit from the depot and the videoconferencing system remains ready for use.

Flexible configuration, from portable to semi-mobile

Several standard set-ups are preconfigured for the system, and these can be expanded or modified at any time. The portable set-up comes without its own screen and uses equipment that is already available at the place of operation. This configuration

SCOTTY Group Austria GmbH is a provider of video, audio and data communication solutions for applications in the aerospace, maritime and land mobile sectors.

SCOTTY was founded in 1993 and enables audio, video and data transmission in places where infrastructure is lacking: in field operations, in land vehicles, on ships and in the air. SCOTTY has specialist experience and expertise in the provision of solutions for critical applications operating under the most adverse conditions. Today, international corporations, peacekeeping forces, border police and civil protection authorities use SCOTTY equipment in the most remote and challenging environments in the world. SCOTTY's optimised communications solutions, which are individually customised and can be used for a multitude of applications, are the result of the company's many years of experience in satellite communications (SatCom), together with its expertise in the area of highly secure IT infrastructure.

SCOTTY's Research & Development division, production and operational headquarters are located in Graz, Austria.

can be changed to, for example, a semi-mobile set-up with one or two screens. It is also possible to connect a projector, which makes it possible to include a far greater number of participants in the videoconference.

This flexibility makes videoconferencing systems much more available, ensuring they are ready for round-the-clock use. In future, the system will become even more flexible: there are plans to have connection options for the SINA Workstation H and the SINA Communicator H. This will mean even individual workstations can be securely integrated into the videoconferencing system.

Andreas Schmidt
andreas.schmidt@secunet.com

The SINA H secured video conferencing system in portable set-up (left) and in semi-mobile set-up with two screens (right)

High-level cybersecurity

Enabling modern work practices – even at SECRET level

'As soon as high levels of secrecy are involved, both performance and usability suffer' – this opinion still persists. After all, when digitalising processes that include information classified as CONFIDENTIAL or SECRET, a plethora of specific requirements need to be taken into account. However, the latest technology shows that modern, digital, everyday working practices that encompass video conferences, collaboration and the like can also be a reality in high-security areas. secunet's SINA Workstation H Client V is an all-in-one solution that unites performance, ergonomics and practicality with classification levels up to and including the German level GEHEIM (SECRET). It has been designed with a view to the digital work processes used in today's armed forces such as the German Federal Armed Forces, in addition to public authorities operating with the highest security requirements.

When the first SINA solutions were developed immediately after the turn of the millennium, the primary focus was on the security aspect. The main aim was to use sophisticated encryption technology to build a secure network infrastructure, in order to transmit high-level classified information for the first time via potentially unsecured networks like the internet. The first SINA H end devices were hard-disk-less terminals. At the same time, the main users wanted a complete PC or fat client that they could work on using the software applications and operating systems they were accustomed to. This led to the development of the SINA Workstation, which at that point was still known as the Virtual Workstation.

This kicked off a process of continual evolution towards greater user-friendliness. The SINA Workstation H enables information from varying security classifications – up to and including SECRET – to be processed in parallel sessions on the same hardware. This functionality quickly proved popular with users, who previously had to use two or more different hardware systems for office IT and classified-level information respectively. Automated tools assist with the roll-out and administration of large SINA installations and also increase practicality.

The SINA Workstation H Client V in operation, here in dual-monitor configuration

A long story of success

The SINA Workstation H has quickly become widespread over the course of the past decade. The Client III device version, for example, operates as a highly secure end device in the German Federal Armed Forces' (Bundeswehr) HaFIS programme (harmonisation of management information systems). SINA systems form the IP Crypto backbone of the Bundeswehr, which means they are used on a large scale for processing and storing classified-level information and transmitting it via IP-based networks. It was only in summer 2021 that the Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (BAAINBw) extended the framework contract for supplying and maintaining the SINA technology.

The evolution is now going further. New user requirements have arisen again, mainly from regular, unprotected office IT. Many users would also like features such as video conferences, collaboration and telephony to be available – even at SECRET level. The new SINA Workstation H Client V makes it possible to integrate these new requirements and translate them into one coherent, overall solution. In addition to the existing approval for the German classification level GEHEIM, the corresponding international classifications (NATO and EU) are also in plan.

"As a result of conversations with our clients, we know that the desire for modern, efficient ways of working, even in high-security areas, comes a long way up their priority list," says Merlin Gräwer, Senior Product Manager at secunet. "In addition to security, we have therefore focused on making the new SINA Workstation H Client V as user-friendly as possible. For many who deal with highly classified information, efficiency in the workplace is still not a given. And that's what we want to change."

Compact hardware design

This request is already evident in the fact that the solution combines all functionalities in a single compact desktop. The client hardware is completely integrated into the primary display. This helps to keep the workspace tidy and free of cables, and improves ergonomics: for example, all slots for for smartcards and USB devices are located at the front within easy reach for the user. Its numerous interfaces mean the client can be flexibly integrated within heterogeneous network infrastructures. It is also possible to connect a local printer or scanner. The brilliant,

The SINA Workstation H Client V in dual-monitor configuration

adjustable TFT display helps reduce fatigue when working thanks to its high resolution and picture clarity. Moreover, the product design proves that even a high-security client can be visually appealing.

One factor that increases its suitability for everyday work significantly is its high level of performance. Despite the complex security measures, which predominantly run in the background, users can rely on seamless performance. This is noticeable, e.g. when using it in parallel with multiple guest systems. HD videos can run in high-performance mode, while modern applications like web and video conferences and collaboration are straightforward to use – including in combination with the high-security SINA Communicator H multi-crypto phone, which is also approved up to and including the German classification level GEHEIM (SECRET).

The new SINA Workstation E Client V client is also available for deployment scenarios where data up to medium-level classification VS-VERTRAULICH (CONFIDENTIAL) are processed.

"We're confident we have the perfect solution for IT personnel working in high-security areas who are looking to modernise," Gräwer says. "Future security is also taken care of: we're planning future updates to make the new client capable of post-quantum cryptography – something the SINA Communicator H can actually already do. To sum up, thanks to these two products we are adding a new chapter to our long story of success of working at SECRET level."

Merlin Gräwer

info@secunet.com

To find out more about the technical data for the SINA Workstation E/H Client V please go to:

https://www.secunet.com/en/solutions/sina-workstation-e/h-client-v

5G study

How secure is the Open Radio Access Network (O-RAN)?

In mobile communications, the majority of Radio Access Network (RAN) component manufacturers currently use proprietary interfaces and functions. The lack of interoperability has led to mobile network operators being heavily dependent on individual manufacturers and their products. Therefore, there are efforts towards more modularity, and thus also interoperability. The goal is Open-RAN, or O-RAN for short, in which the individual components are fully interoperable. In order to define and establish a standard according to this concept, leading mobile radio providers founded the O-RAN Alliance, in the framework of which an implementation has already been specified.

Is the O-RAN in this form associated with security weaknesses? A study commissioned by the German Federal Office for Information Security (BSI) and carried out by the Barkhausen Institute and the company AI Networks in cooperation with secunet investigates this question. The authors state that medium to high security risks emanate from a large number of the interfaces and components specified for the O-RAN. Therefore, security improvements should now be introduced into the standardisation process. The authors of the study have formulated some suggestions in this regard. secunet will accompany this process with its expertise, as these infrastructures are critical and particularly in need of protection.

The study is currently only available in German. Interested parties can download it from the secunet website:

https://www.secunet.com/5G

Axel Deininger elected as new ECSO Chairman

Axel Deininger, CEO of secunet Security Networks AG, was elected as the new Chairman of the European Cyber Security Organisation (ECSO) on October 27th, 2021. As Chairman of the Board of Directors (BoD), he will represent the interests of the association and its members, especially at the EU institutions. He succeeds Phillipe Vannier, who has acted as chairman representing the French listed IT service provider ATOS.

"I am pleased with my election and the great approval of the Board of Directors," says Axel Deininger. "IT security is a decisive success factor for successful digitisation. It is therefore crucial to further strengthen the European IT security ecosystem, which is reflected in the membership of ECSO, in order to achieve the goals set in close cooperation with the European institutions and public institutions."

secunet is a founding member of the ECSO, which was founded in June 2016 under the then EU Commissioner Günther Oettinger as a so-called contractual public-private partnership (cPPP) in the field of cybersecurity in order to promote cooperation between the public and private sectors.

Since the foundation of ECSO secunet has been actively involved in the various measures, executive and working committees of the ECSO, such as the start-up event series "ECSO Cyber Investor Days", as sponsor and promoter of the label "Cybersecurity made in Europe" and in the initiative "Women4Cyber". Axel Deininger was elected to the Board of Directors of ECSO in 2020 and has since officially represented the organization on numerous occasions.

Luigi Rebuffi, Secretary General of ECSO (left), congratulates Axel Deininger on his election as Chairman of the organisation.

The European Cyber Security Organisation (ECSO) ASBL is a fully self-financed non-profit organization under Belgian law that was founded in June 2016. ECSO is the privileged partner of the European Commission for the implementation of the public-private partnership on cybersecurity. ECSO brings together the public and private actors involved in European cybersecurity, including large companies, SMEs and start-ups, research centres, universities, end users and operators of critical infrastructures, clusters and associations as well as local, regional and national public administrations in the member states of the European Union (EU), the European Free Trade Association (EFTA) and associated countries of the H2020 program.

Further information at: https://ecs-org.eu

secunet receives the ECSO "Cybersecurity made in Europe" label

Digital sovereignty of European authorities and companies includes becoming more independent from the globally dominant IT providers when dealing with sensitive information. For this reason, the European Cyber Security Organisation (ECSO) has created the label "Cybersecurity made in Europe". secunet is a qualified and certified bearer of this label. It was issued by the European Competence Centre for Security in Information Technology, eurobits e.V.

CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

The label serves to increase the international visibility of European IT security companies as well as to confirm the trustworthiness of their products and services. To obtain it, providers must meet a number of criteria: For example, they must have a European ownership structure and meet security requirements of the European Union Agency for Cyber Security (ENISA).

Secure digital infrastructures are crucial for the development of digital sovereignty. Only those who know where their data or applications are stored and who can access them can retain control over them and adequately protect themselves from cybercrime or espionage. Labels based on European standards such as "Cybersecurity made in Europe" help to establish European digital sovereignty and offer all users solutions that meet the high European requirements.

The label initiated by ECSO is issued by authorised organisations at local level. In Germany, eurobits e.V. is the only issuing body. In the eurobits association, which was founded in Bochum in 1999, leading research institutes, established companies of the industry as well as young growth companies work together and ensure a transfer between business and science in the field of IT security and information security.

Promoting young talent

Germany is European Champion at the European Cyber Security Challenge

From 28 October to 1 November, the German national team of the Cyber Security Challenge Germany (CSCG) successfully participated in the finals of the European Cyber Security Challenge in Prague. After two exciting days of competition, they took first place, closely followed by Poland in second place and Italy in third place.

The CSCG is a German competition for young IT security talents. Up to 1,600 participants compete against each other in an online qualification. The best of these young hackers are then invited to a German final, where they compete against each other in two age categories. The tasks cover the topics of binary analysis, reverse engineering, cryptography, web exploitation, steganography and game hacking.

Despite the Corona pandemic, the ECSC 2021 was able to take place in Prague.

The competition is organised by the Bochum-based association Nachwuchsförderung IT-Sicherheit e.V., which was founded in 2020. Chairman of the board is secunet employee Falk Gaentzsch, who has already been organising the CSCG since 2015. Once funded by the German Federal Ministry for Economic Affairs and Energy, as part of the "IT Security in Business" initiative, the association brings young talent into contact with companies. "Even though the coronavirus threw a spanner in the works of some of our plans in 2020 and 2021 – for example, we wanted to organise a recruiting fair as part of the German finals – the need for young IT talent in companies continues unabated," says Falk Gaentzsch.

The European Cyber Security Challenge (ECSC), which has grown from three countries to 17 since 2015, is another exciting opportunity for the German national selection to demonstrate their skills. The selection consists of the ten best talents from the German finals. The competition had a total of 271 participants this year.

The ECSC is organised by a Steering Committee composed of representatives of the participating countries and officials of the European Union Agency for Cyber Security (ENISA).

Juhan Lepassaar, Executive Director of the ENISA, comments on the ECSC: "The cybersecurity capacity of the Union heavily relies on a workforce adequate in size and equipped with the right knowledge and skills. The European Cybersecurity Challenge encourages cybersecurity careers and attracts the young talent needed tomorrow to ensure the continuity of the EU efforts dedicated to the cybersecurity of our digital space."[1]

Despite the corona pandemic, the ECSC was able to take place in the Czech Republic's capital Prague this year. Canada and Slovakia were invited as host countries. Why Canada as a non-European country? "We are working on concrete plans to organise a world championship with the support of ENISA. We are currently discussing this with African, Asian, North and South American countries, Australia and India," says Falk Gaentzsch.

[1] ENISA, press release 1 October 2021: Germany wins the Cyber Security Challenge

The winners of the European Cyber Security Challenge 2021 with representatives of the Verein Nachwuchsförderung IT-Sicherheit e.V. (NFITS) and ENISA.

Back row, from left to right: Adrian Belmonte Martin (ENISA), Daniel Schüll, Maurice Dauer, Robert Reith, Thomas Lambertz, Sven Stegemann, Daniel Kilimnik, Alain Rödel, Dr Demosthenes Ikonomou (ENISA), Niklas Breitfeld

Front row, from left to right: Tom Dohrmann, Nils Langius, Patrick Reich (NFITS), Falk Gaentzsch (NFITS), Felipe Custodio Romero, Tim Schmidt (NFITS)

AFCEA

Spirit of optimism after forced break

Finally, the AFCEA trade exhibition could take place again. With a new location in the World Conference Center Bonn (WCCB), the most important trade fair of the Bundeswehr IT community for command support, intelligence and reconnaissance, geoinformation systems, IT security, simulation, training, logistics and SASPF opened its doors on 14 and 15 September 2021. The forced break had lasted almost two years. With a strict hygiene concept and no specialist presentations, fewer visitors came to the trade fair than in previous years due to the Corona pandemic, but secunet nevertheless welcomed a great many guests to the new booth and held in-depth discussions with customers and partners.

Lively interest under difficult conditions

Three more products from the SINA family were presented to the trade audience, which received GEHEIM approval from the German Federal Office for Information Security (BSI) during a year marked by lockdown: SINA Workflow, SINA Workstation H Client V and the new multicrypto telephone SINA Communicator H. In addition, visitors were able to convince themselves of the diverse application possibilities of the SINA Workstation by means of several application examples in cooperation with IGEL Technology, Esri and Systematic.

Last but not least, the newly announced partnership between IBM, RedHat and secunet, with the aim of developing a highly secure cloud platform for classified information, aroused great interest and ensured many discussions.

By the way, the AFCEA trade exhibition 2022 will already take place on 30 and 31 March – save the date!

The secunet trade fair stand in its new look on the eve of the trade fair

Brigadier General Armin Fleischmann, Brigadier General Rainer Simon and Major General Dr Michael Färber during the live demonstration of the SINA Communicator H by Dr Michael Sobirey and Marcel Taubert (l.t.r.)

In exchange: Florian Veit, Norbert Müller, Torsten Henn, Axel Deininger (all secunet), Prof. Dr Andreas Meyer-Falcke, Christoph Dammermann, Sebastian Barchnicki (DIGITAL.SICHER.NRW. Competence Centre for Cyber Security in Business), Christine Skropke (secunet)

it-sa

A successful new start

After the it-sa trade fair in Nuremberg had to be cancelled in 2020 due to Corona, it was able to take place again on site in October 2021. Despite its reduced size, the trade fair was generally considered a success. secunet was present with products and topics such as the secure messenger stashcat, the SECRET phone SINA Communicator H and its portfolio for industrial cybersecurity. The topic of secure cloud infrastructures for public authorities and industrial companies with SecuStack generated particularly great interest. A flight simulator, where visitors could see for themselves the performance of the graphics-accelerated SINA Workstation S, was also well received.

As in previous years, secunet welcomed numerous high-ranking guests from the fields of politics and administration at its booth. On the first day of the trade fair, BSI President Arne Schönbohm and Andreas Könen, Head of Department for Cyber and IT Security at the German Federal Ministry of the Interior, for Construction and the Homeland (BMI), were among those available for a brief exchange with representatives of the secunet Management Board.

On the second day of the event, the secunet booth was the venue for a joint discussion between representatives of the Ministry of Economics of North Rhine-Westphalia (State Secretary Christoph Dammermann and State CIO Prof. Dr Andreas Meyer-Falcke) and the Ministry of the Interior and Digital Affairs of the State of Baden-Württemberg, represented among others by Matthias Pröfrock, Head of the Department for Digitisation Strategy and Cyber Security. The discussion was initiated jointly by eurobits e.V., the IT security association of the Ruhr region, and Klaus-Hardy Mühleck, Chairman of the Cyber Advisory Board for the Ministry of the Interior of Baden-Württemberg. The focus was on the digitisation and cyber security strategies of industry-strong federal states as well as the question of how cloud strategies can be designed and implemented in the most targeted and sustainable way possible, taking into account federal and municipal structures.

European Cyber Week

The European dimension of cyber security

In mid-November, the fifth edition of the European Cyber Week (ECW) took place in Rennes, Brittany, at the Couvent des Jacobins conference centre. The event is hosted by the "Pôle d'Excellence Cyber" and its partners with the support of the French Ministry of Defence, the Regional Council of Brittany and the Rennes Métropole Council. The ECW aims to bring together companies from multinationals and MSEs (micro and small enterprises) to SMEs (small and medium-sized enterprises) and start-ups, local authorities, research laboratories, institutions, students and professionals. In terms of content, the event offers a combination of scientific and technical presentations, business meetings and high-profile European speakers. The aim is to present regional, national and international initiatives.

The European dimension was clearly visible throughout the three-day event, thanks in particular to the European Cyber Security Organisation (ECSO), which co-organises ECW. Over the past few years, ECW has continued to develop its role as a fundamental and pioneering event in the strategic areas of cyber defence, cyber security and AI – while also being a high-quality networking hub. secunet was on site this year as part of the eurobits e.V. joint stand together with the Hamburg-based start-up Quointelligence. In addition, Christine Skropke, Head of Public Affairs at secunet and Chair of the Board of eurobits, was actively involved in the discussion panels on the topics "How to build a concrete European cooperation in cyber" and "Women4Cyber".

Panel discussion at the European Cyber Week 2021 in Rennes, from left to right: Gregory Wawszyniak (Dumont, Cluster Security Made in Luxembourg), Neil Sandford (Wales Government), Oliver Väärtnou (Chairman of the Estonian Information Security Association), Danilo D'Elia (Moderator / Senior Policy Manager, ECSO), Christine Skropke (Head of Public Affairs, secunet), Giorgio Tresoldi (Armasuisse Schweiz)

Sonnenstrahl Dresden

Overcoming illness through creativity

Music therapy at the Sonnenstrahl e. V. Dresden

Sonnenstrahl e. V. Dresden is an association financed by donations that cares for children and young people with cancer and their families. It works closely with the oncological children's ward at Dresden University Hospital. "Sonnenstrahl" means "sunbeam".

Caring – that means, among other things, being there during the particularly difficult time of inpatient intensive care. Parents with longer journeys can stay at the association's parents' house free of charge and thus remain close to their child. The sick children are given the opportunity of distraction and artistic-creative processing of their cancer illness on the ward. The association also supports other family members such as siblings.

This year's secunet Christmas donation goes to Sonnenstrahl e. V. Dresden and will be used for music therapy. Together with two therapists, the sick children can sing, drum, play and strum everything off their chest that they don't want to express with words or don't know how to express.

How to contact the association:

Sonnenstrahl e. V. Dresden
Förderkreis für krebskranke Kinder und Jugendliche
Goetheallee 13
01309 Dresden / Germany
Phone: +49 351 / 315 839 00
E-Mail: info@sonnenstrahl-ev.org

Dates – January to June 2022

Due to the corona pandemic, changes are to be expected.

1–2 February 2022
BSI Kongress | digital

21–23 March 2022
GISEC | Dubai, United Arab Emirates

30–31 March 2022
AFCEA | Bonn, Germany

5–7 April 2022
Passenger Terminal Expo | Paris, France

6–8 April 2022
Intergraf Currency+Identity 2022 | Lyon, France

26–28 April 2022
DMEA | Berlin , Germany

26–27 April 2022
ID@Borders Seminar | Brussels, Belgium

4–5 May 2022
Prague, Czech Republic

11–12 May 2022
European Police Congress | Berlin, Germany

31 May–2 June 2022
GPEC | Frankfurt am Main, Germany

28–29 June 2022
Identity Week | London, United Kingdom

Do you have any questions or would you like to book an appointment with us? Please send an email to events@secunet.com.

Imprint

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

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

Design and Setting
sam waikiki GbR, www.samwaikiki.de

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

Photo credits
Title, p. 2 (bottom), 3–18, 20–26, 31 (top, bottom left), 32, 33: secunet
p. 2 (top), 19: alamy
p. 27: Adobe Stock
p. 28: European Cyber Security Organisation
p. 30 (top): Jan Bacák production
p. 30 (bottom): Amy Louise Hendry
p. 31 (bottom right): Daniel Kromberg
p. 34: Sonnenstrahl e. V. Dresden

climate neutral print
www.klima-druck.de
ID-No. 21110746
bvdm.

FSC
www.fsc.org
MIX
Paper from responsible sources
FSC® C006990

Where networks need to be shielded effectively against cyber attack, secunet is ready to help. SINA Gateways from secunet protect network infrastructures using BSI-approved encryption technology and make them ultra-secure.

secunet.com **protecting digital infrastructures**

secunet