Federal Office
for Information Security

BSI Magazine 2021/02

Security in focus

Online Elections

Cyber Security

Certified into the Quantum Future: For More Confidence in IT Products

IT Security in Practice

The IT Security Label: Transparency for Consumers

Digital Society

Crash Test for Cyber Security: How IT Security Is Driving the Shift in the Mobility Industry

EDITORIAL

IT Security: A Top Priority

In the second half of 2021, the coronavirus pandemic continued to dominate the headlines. In spite of the progress made in fighting the virus, it still affected many people's everyday lives. We participated in events virtually rather than in person, worked from home and set our children up for remote lessons, and organised video conferences and digital family get-togethers. When it comes to information security, the events of recent months have seen us living more digital lives than ever before. And this process of digitalisation is set to continue – in government, in industry, and in wider society. This shift will bring many benefits, but it also means we have some major work to do on cyber security.

This is why the passing of the German IT Security Act 2.0 was an important milestone not just for the BSI, but for cyber and information security in Germany as a whole. By implementing this crucial update, the country's legislators have laid important foundations for a secure digital future. This can only be achieved when information security is considered right from the start. We need to stop misunderstanding the topic of information security as an obstacle and start seeing it as an investment in the future. We all have to understand that information security is key to a successful digital transformation.

This fact has become evident in recent elections and elections processes. Due to the restrictions imposed as a result of the pandemic, demand for digital solutions has skyrocketed. In-person events such as association or shareholder meetings, company meetings or plenary and committee meetings of parliaments or political parties were unable to take place for several months – or, if they did, only to a very limited extent. In our special feature on online elections, we explain the various aspects of this new approach and share our recommendations on organising secure elections in the digital realm. This issue also features articles on security requirements in the post-quantum age, our new IT Security Label and the importance of IT security in the automotive sector.

I hope you enjoy this edition and stay healthy.
Yours faithfully,

Arne Schönbohm,
President of the Federal Office for Information Security

TABLE OF CONTENTS

NEWS

Consumer Protection Goes Digital

New Committee: The Digital Consumer Protection Advisory Board

Since June 2021, the BSI has been supported by the Digital Consumer Protection Advisory Board. This independent expert committee, which was established to boost cyber security in the everyday digital lives of consumers, develops and implements appropriate practical measures according to the needs of each target group. Each year, the Advisory Board chooses a focus topic as a basis for compiling its recommendations. Its ten members ensure that the perspectives of consumers, civil society, consumer science, information technology and business are all incorporated into the process. Prof. Dr. Martina Angela Sasse, a professor of human-centred security at Ruhr-University Bochum, was appointed the spokesperson of the Advisory Board. Further information on the new committee, its members and its remit is available at www.bsi.bund.de and from the office of the Advisory Board itself (beiratdigitalerverbraucherschutz@bsi.bund.de).

Information Security in Transition

Migration to Post-quantum Cryptography

The BSI has taken an important step in the migration to post-quantum cryptography. The SINA Communicator H has become Germany's first IT product to successfully deploy a quantum-computer-resistant key agreement and achieve the highest level of approval for handling strictly confidential communications. The functions of the device were successfully demonstrated in a telephone conference with leaders from the Federal Ministry of the Interior, the Federal Foreign Office, the Federal Ministry of Defence, the German Chancellery and the BSI.

The SINA Communicator H enables organisations to make telephone calls and hold telephone conferences in line with the "Strictly confidential" and "Restricted" security standards. It can also be integrated into restricted client networks to ensure their secure separation. In addition to IPsec support for conversations and integration into existing SINA infrastructures, end-to-end security can already be achieved in strictly confidential conversations using the SCIP protocol. In the future, the SINA Communicator H will support a range of usage scenarios, including as a 64 kbit/s SATCOM telephone, a video telephone or a thin-client workstation comprising a monitor, mouse and keyboard. The first batch of devices was delivered to the Federal Administration in September.

The R&S®ELCRODAT 7-FN from Rohde & Schwarz SIT – another classified communication IT product that uses quantum-computer-resistant cryptography – is also expected to be deployed in the future.

Further information:

https://www.bsi.bund.de/PQ-Migration

A Strong Partner

First Co-operation Agreement in Germany: Lower Saxony and the BSI

On 17 November 2021, BSI President Arne Schönbohm and Boris Pistorius, Lower Saxony's State Minister for Interior and Sports, met in Hanover to sign a co-operation agreement to fight cybercrime – the first such agreement between a federal state and the BSI.

"Working as a team is the only way that Germany can strengthen its information security defences and sustain the highest possible security levels to detect and defend itself against cyber threats. The state of Lower Saxony has been a strong partner in this regard from the very beginning", said Arne Schönbohm.

The partnership – which was first launched in 2018 – now encompasses seventeen fields of collaboration. In addition to supporting one another in response to specific security incidents, the partners also set up work shadowing arrangements and collaborate on the development of information security standards.

Minister Boris Pistorius emphasised the importance of this agreement for Lower Saxony: "Threats from cyberspace don't stop at state or national borders. This agreement will bring us even closer to the BSI, enable us to get better and better at combining our efforts and help us learn more from one another!"

Stepping Up at the BSI

First Three Sites – Then the Whole World!

The coronavirus pandemic continues to be a challenging time for us all, not least because it has made it more difficult to stay fit and remain connected with colleagues. In summer 2021, department manager Jörg Pieper thus recruited 35 teams to join him in taking on an ambitious challenge. Dubbed the BSI@walk – Three Site Challenge, it involved colleagues from various departments coming together to pay a "virtual visit" to the other BSI sites. They did so by clocking up enough combined steps to cover the distance between Bonn, Saarbrücken and Freital. Each team walked 1,300 kilometres – that's around two million steps! – with members urging one another on in a group chat.

An all-female team was the first to make it back to the starting point. But it's the taking part that counts, of course, and having fun while getting fit was the main point of the challenge. Together, the teams racked up an even greater achievement: In eight weeks, they covered a total distance of 43,388 kilometres, which is equivalent to walking around the equator!

At the closing ceremony, the participants all agreed that the challenge was a great way to stay fit – and connected.

CYBER SECURITY

The Accelerated Security Certification

For More Confidence in IT Products

By Dr. Helge Kreutzmann, Section Recognition and Certification of Bodies and Persons and Dr. Kai Redeker, Section Certification of Network Components and Accelerated Security Certification

Two central trends have been emerging in recent years in products that use information technology: first, the rate of change due to digitalisation is accelerating in the most diverse areas of life; secondly, however, the constant appearance of new vulnerabilities is having an increasingly severe impact on our lives and commodities, as products are continuously more deeply integrated into our (business) lives and are also connected worldwide.

In order to obtain assurance statements about the "trustworthiness" of IT products, the BSI has been offering product certifications for more than 30 years. Alongside French partner authority ANSSI (National Cybersecurity Agency of France), the BSI is now unofficially the global champion in certifying products for governmental use or those with very high security requirements. However, what was missing during this time was the ability to offer a service to broader market segments that were not reached by Common Criteria, which had been used exclusively for this purpose up to now.

Reducing the effort required for the manufacturer

Drawing inspiration from concepts in the French CSPN certification (First Level Security Certification), the BSI asked itself how it is possible to convince broader groups of manufacturers to certify products for mission-critical areas, for example. It was imperative that the certificate

still achieved the well-known high-level (security) statement from the BSI. However, a key objective was also to reduce the requirements placed on the manufacturer and to focus testing on the aspects that contribute most to the security statement. At the same time, additional areas to take into account included the dynamic continuous development and the disclosure of new vulnerabilities (and the associated patches) in information technology. This resulted in the creation of the Accelerated Security Certification (Beschleunigte Sicherheitszertifizierung, BSZ).

In order to reduce the effort needed from manufacturers (including the financial expenditure), no highly specialised or formal information about the design is required, as is regularly the case with Common Criteria certification. Tests are carried out instead via the interfaces, involving only minimal information about the internal design of the product. At the same time, confidence in the product is no longer defined using abstract levels. Instead, an experienced attacker with a limited period of time helps determine this. To achieve this, the evaluator carries out the test in the fixed time period that has been set at the start of the procedure. This ranges from 15 to a maximum of 60 days, and is usually 35 working days. This also makes turnaround times of three months from the start of the procedure to the certificate being awarded a realistic prospect – something that is very beneficial with respect to time to market considerations.

At the same time, dynamic development has not been thrown out the window; experience has shown that security updates are required. With this in mind, BSZ-certified products must provide an update mechanism, whose security is tested. In addition, manufacturers are required to deliver updates via this mechanism as necessary for the entire period that the certificate is valid. These targeted updates may also be tested and certified without taking up too much time if the applicant wishes to do this.

Initial scope: network components

Following a feasibility study and several pilots, the BSZ programme was launched in October and the initial scope will be network components (e.g. routers and industrial control systems). In the future, further scopes will continue to be developed.

A BSZ procedure is as follows: first, the applicant, usually a manufacturer or vendor of a product, prepares the few documents that are required. The security target is key here, and it is usually presented in a relatively short document of about 10 pages and describes the product's operational environment and security features. In addition, the applicant must commission a test laboratory accredited by the BSI to evaluate the product as part of the procedure. At this point, the applicant may submit the application and all supporting documents to the BSI's certification body.

Next, both the certification body and the test laboratory review the documents to determine if they and the product meet the requirements for a BSZ procedure and whether an evaluation is possible. If everything turns out fine, a kick off meeting is arranged. At this meeting, the evaluation of the product is discussed, the required evaluation time including a fixed schedule is determined and all outstanding issues are clarified. The testing then begins and no more changes may be made to the product or documentation. The test laboratory documents the tests, results and assessments performed and presents them to the certification body in the closing interview. The certification body makes the decision whether to grant the certificate based on these findings.

Only then are the test results and the decision shared with the applicant. In the event of a positive decision, the applicant is awarded the certificate for use. A BSZ certificate is usually valid for two years. If the outcome is negative, a new, shortened procedure is available, where applicable, and the applicant also has a good overview of the problems identified. ■

Further information:

https://www.bsi.bund.de/bsz

Certified into the Quantum Future

Towards Secure Quantum Key Distribution

By Dr. Tobias Hemmert, Dr. Manfred Lochter, Stephanie Reinhardt, Section Information Assurance Technology Requirements, Dirk Fischer, Section Hardware Certification

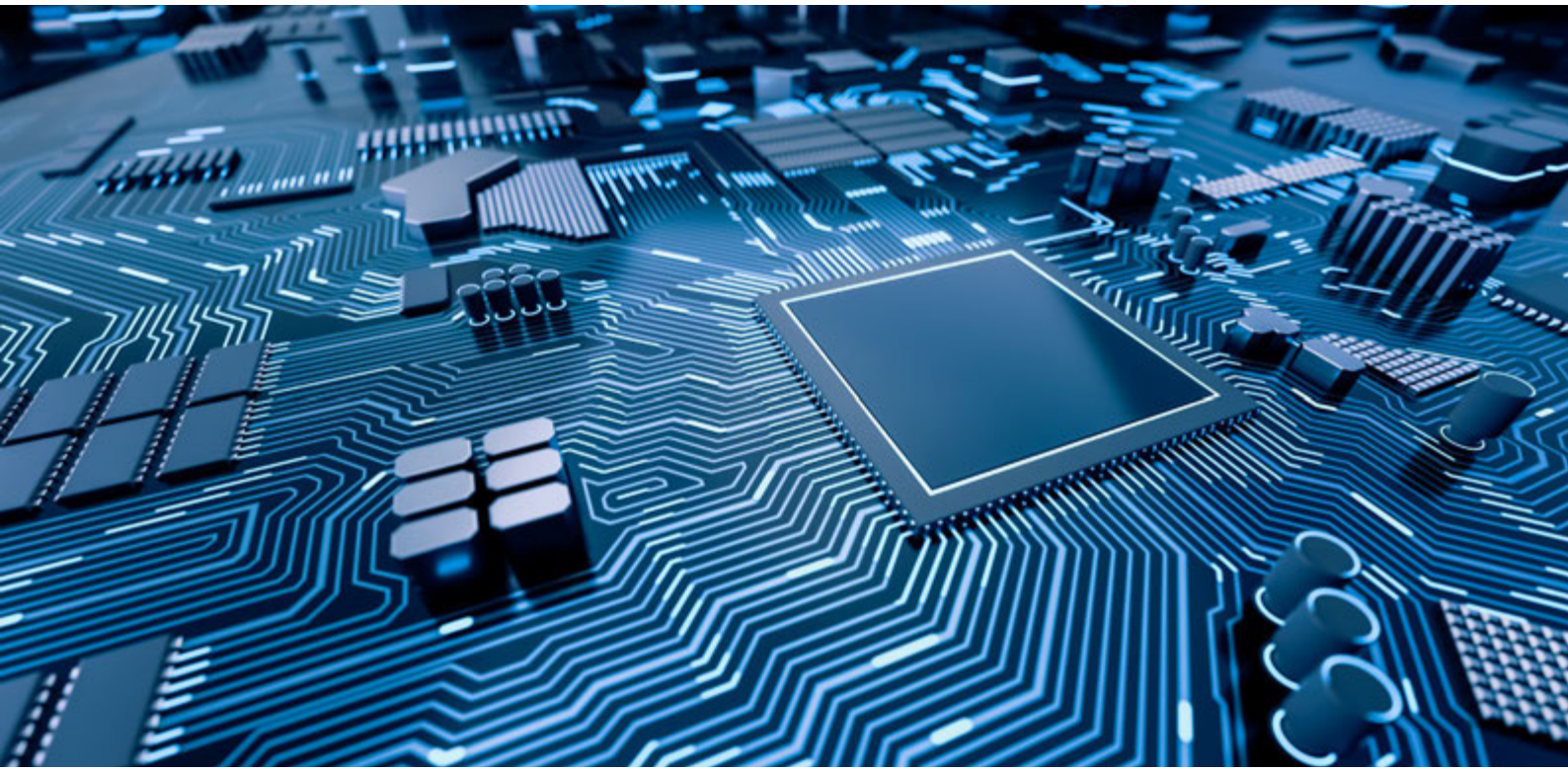
Quantum computers are the subject of in-depth research worldwide and in large scale would threaten the public-key cryptography used today. Post-quantum cryptography and quantum key distribution (QKD) have been proposed as key exchange schemes that are resistant to both classical and quantum attacks. To pave the way for the secure use of QKD, the BSI has commissioned a first Protection Profile (PP) for QKD devices.

The rapid progress in the development of quantum computers threatens the public key cryptography in use today. The implementation of scalable quantum computers is currently the subject of in-depth research. This is not only the case for large companies such as IBM and Google, but also in Germany, where the German government is providing huge amounts of funding. Looking ahead, it is therefore already important to migrate to cryptographic algorithms that will also be resistant to attacks by quantum computers. In the domain of high-security applications, the BSI is acting based on the working hypothesis that by the early 2030s, there will be quantum computers that threaten the security of public-key cryptography used today. This statement should not be interpreted as a prediction of when quantum computers will be available, but represents a guideline for risk evaluation.

Two fundamentally different approaches have emerged for secure key exchange schemes: post-quantum cryptography and quantum key distribution. The security of post-quantum cryptography is based on the assumption that certain mathematical problems are hard to solve for classical and quantum computers, whereas the security of QKD is based on purely quantum mechanical, and therefore physical, principles. For QKD, specialised hardware such as photon sources and detectors is required to suitably employ quantum mechanical effects.

The BSI has already started the migration to post-quantum cryptography and considers QKD a possible future addition to post-quantum key exchange schemes. However, as it stands, QKD is restricted to special fields of application, as the technical requirements for QKD are still very limiting and no certified products are available to date.

There are already a large number of activities under way worldwide relating to the introduction of QKD, such as the European Quantum Communication Infrastructure initiative (EuroQCI). This initiative intends to establish a European quantum communication infrastructure within the next few years. In July 2021, Ireland became the last EU member state to join EuroQCI. The network that the initiative plans to build is supposed to employ QKD to provide secret keys for highly secure applications. The QuNET project funded by the Federal Ministry of Education and Research (BMBF) (see the box on the demonstrator) can be considered to an extent the German counterpart of EuroQCI. In addition to the EuroQCI and QuNET projects, there are numerous other German initiatives. Considering the significant investments in QKD and international, extensive plans to build QKD networks, the BSI is also already working on the security assessment of QKD. The objective is to ensure security by design.



The "Protection Profile for Quantum Key Distribution" project

With the advent of a new technology such as QKD, the issue of conducting a security assessment of the IT security products in question comes up naturally. The Common Criteria (CC) represent an internationally recognised standard for security evaluation. As a first step in the development of evaluation criteria, in 2020 the BSI commissioned the security evaluation facility of Deutsche Telekom Security to create a Protection Profile (PP) for QKD. In a sense, this PP represents a blueprint that helps manufacturers looking to achieve a certain security level to create a product-specific Security Target. The commissioned PP is initially limited to what are known as prepare & measure protocols and to point-to-point connections. This means that network aspects are not taken into account. In order to involve the scientific community and manufacturers as early on as possible and to create a globally recognised PP, the PP is being developed in collaboration with a technical subgroup of the European Telecommunications Standards Institute (ETSI) and should eventually result in an ETSI standard. The next step is the certification of the PP. A certified PP with suitable additions can then also be used as the basis of an approval process for devices processing classified information. For approvals there may be additional requirements, particularly regarding the origin of products.

The PP should also facilitate the development of products that meet the EU's objective of a "certified secure end-to-end quantum communication infrastructure (QCI) composed of space-based and terrestrial-based solutions, enabling information and data to be transmitted and stored ultra-securely" (EU19). The aim is therefore for the Protection Profile to require an evaluation assurance level of EAL4+ (augmented by AVA_VAN.5 and ALC_DVS.2).

The PP should have an open design so that countries involved can still make their own decisions regarding nationally regulated or defined aspects. In Germany, these aspects would relate to cryptography and random number generation, for example BSI TR-02102 Cryptographic Mechanisms: Recommendations and Key Lengths and AIS 20/31.

Outlook

While significant progress has been made, the upcoming finalisation of the BSI/ETSI Protection Profile is not the end of the journey towards a comprehensive QKD infrastructure. In the future, various other QKD variants will come along, for example entanglement-based QKD protocols. These protocols will be used for satellite communication in particular. In addition, quantum networks and the integration of traditional cryptography are crucial. As the technology advances, it is possible that additional PPs will be developed.

On top of the prospect of additional versions of the Protection Profile, our work also lays the foundations for creating the required European certification ecosystem. Within the European framework, the creation of a technical domain for QKD is desirable, in which

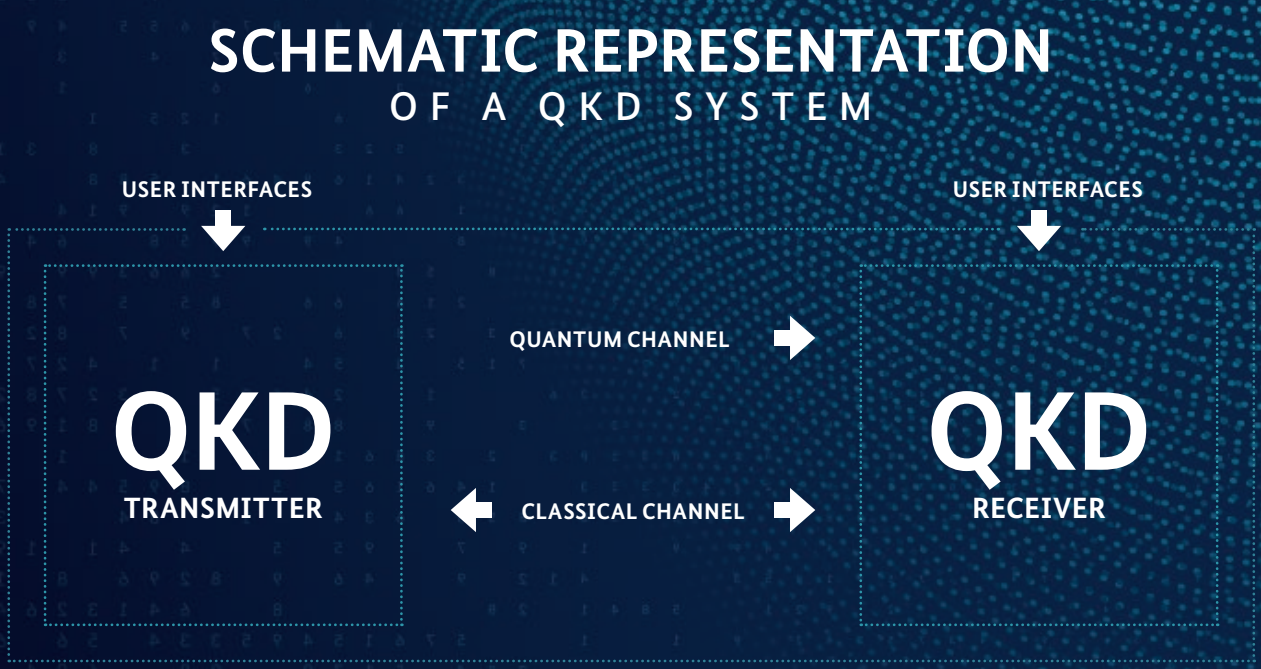


Figure: Schematic representation of a QKD system

the internationally standardised supporting documents required for fast and successful certification can be created. A technical domain can be made up of joint working groups of certification bodies, evaluation facilities and industry – i.e. all of the stakeholders involved in a product certification process. The supporting documents that still need to be drafted include, for example, the definition of test methodologies, standardised frameworks for vulnerability assessment, requirements for the expertise of evaluation facilities and in-depth work on technology-specific attack methods, such as side channels.

The standardisation of QKD protocols is also an area that still requires work. Ideally, a QKD standard should also include a security proof with a quantitative security statement. As the Federal Cyber Security Authority, the BSI therefore also promotes and closely follows this topic in order to ensure QKD is securely implemented. ■

Further information:

https://digital-strategy.ec.europa.eu/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

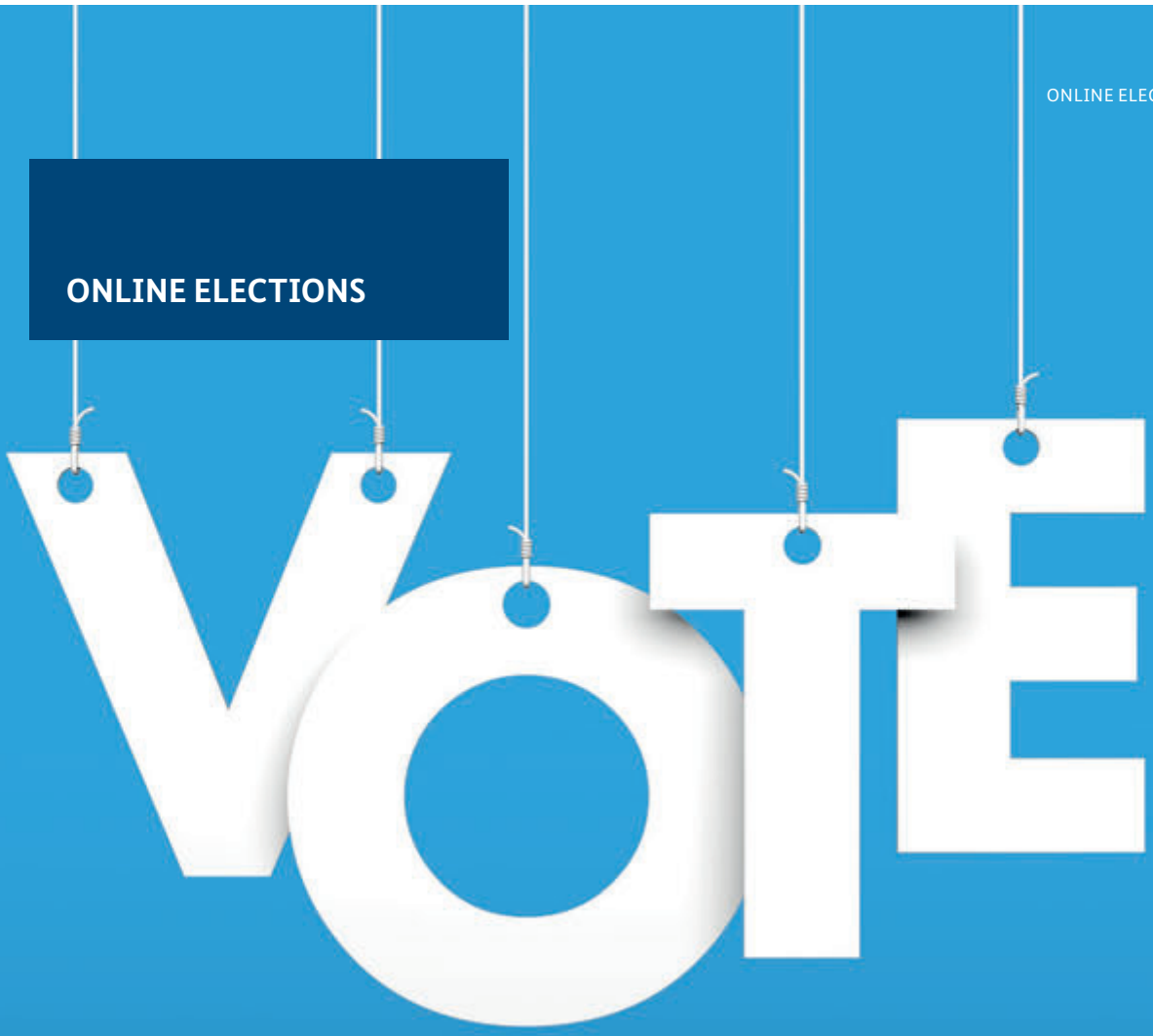
www.bsi.bund.de/Quanten

Dr. Martin Schell, Head of the Fraunhofer HHI.

QuNET demonstrator

On 10 August 2021, Federal Minister of Education and Research Anja Karliczek opened the first quantum-secured video conference between two federal authorities, the BMBF and the BSI. The demonstrator was set up as part of the QuNET initiative that was launched two years ago and in which Fraunhofer-Gesellschaft, the Max Planck Society and the German Aerospace Center (DLR) are researching the basis for a pilot network for quantum communication. The BSI is represented on the QuNET advisory board and advises on security issues in particular. During the demonstration, all participants shared the common goal of a quantum ecosystem in which certified and approved products are able to ensure reliable communication.

ONLINE ELECTIONS



Special Section: Online Elections

The Covid-19 pandemic has led to a situation in which events such as club or shareholder assemblies, company meetings or plenary and committee sessions of parliaments and political parties can only be held with major restrictions, if they are possible at all. This has quickly made digital solutions more popular as a means of conducting virtual meetings, voting rounds and elections.

This special section on online elections shows how these kinds of formats can be made as secure as possible in light of the worsening threat landscape in cyberspace. What kinds of threats to online elections have been observed? Which technical and organisational measures can offer corresponding protection? How can the basic principles of electoral law also be upheld in online voting formats?

On the topic of online voting and virtual elections, the BSI has already developed a wide range of specific recommendations for action from its various fields of expertise. Its Technical Guidelines and protection profiles, for example, provide guidance on how to secure such events. In developing these resources, the BSI completed important background work during the model project "Online Social Elections in 2023" (p. 12).

Corresponding certification is an important way to establish minimum standards for the security of online elections (p. 14 and p. 20). IT-Grundschutz also offers some important basic guidance on designing online elections (p. 22). In addition, the virtual event and election project group ViVA (p. 24) provides further tips, recommendations and key topics for organisers to consider.

This special section also includes a guide to the cryptographic tools that help secure voting processes in the digital realm (p. 16). Some initial field reports from businesses and political parties are available, as well – see p. 26 for details.

Digitalisation of Online Elections

Model Project: Online Elections for the Governing Boards of Social Insurance Institutions in 2023

By Jennifer Breuer, Section eID Solutions for Digital Administration

In Technical Guideline TR-03162, the BSI has defined the technical IT security requirements for implementing online elections. This has established a key pillar for the secure digitalisation of the governing board elections for German social insurance institutions in 2023. These specifications can also be applied to the digitalisation of other elections.

Online elections for the governing boards of social insurance institutions in 2023

As part of this model project, health insurance companies will be given the option to implement online elections alongside conventional postal votes in the 2023 elections for the governing boards of social insurance institutions. In Technical Guideline TR-03162 ("Technical IT security requirements for implementing an online election within the framework of the model project in accordance with Section 194(a), Social Code, Book V (online election)"), the BSI provides specifications for information security as a key pillar for the secure digitalisation of the governing board elections for Germany's social insurance institutions in 2023.

Applying the principles of electoral law

In digitalising elections, there are legal requirements that must be met, but it is also important to implement the principles of electoral law that apply to all elections. It is not possible to apply every principle of electoral law in the same way through digitalisation. The biggest challenge in an online election is to sufficiently ensure that elections are secret and public in equal measure. In particular, following a judgement of the Federal Constitutional Court, the possibility for voters to determine whether their online vote has been saved as specified in the (electronic) ballot box needs to be considered.

On the one hand, this means that the casting of votes must be protected so that there is a high level of security when it comes to protecting the secrecy of the ballot. On the other, there must be an adequate level of transparency regarding the election process. The public must be given extensive powers to track the key stages of this process, as well as the result and how it was determined (*see article on p. 16*).

When it comes to the digitalisation of elections, it is therefore important to consider how the principles of electoral law have previously been weighted. The goal should always be to implement the principles of electoral law as effectively as possible. In order to trace how these decisions are made, documentation should be drawn up if a principle of electoral law can be implemented only to a limited extent due, for example, to the implementation of another principle and/or the effort to safeguard the election against manipulation.

Technical IT security requirements to safeguard the election

To fulfil the principles of electoral law and to obtain a valid result, security is presumably the most important factor. Online elections in particular contain sensitive information and are exposed to a host of threats. Any type of manipulation of the election process must be ruled out. The term "manipulation" includes any form

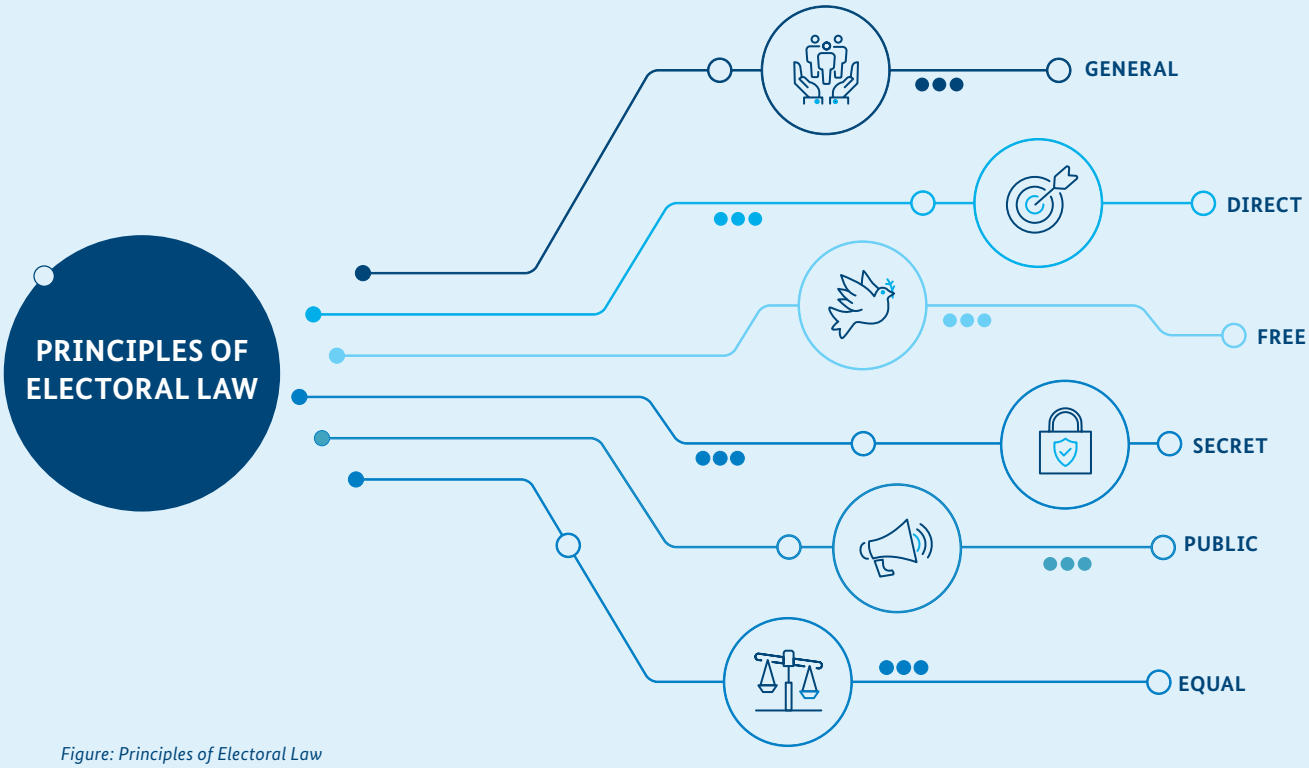


Figure: Principles of Electoral Law

of unauthorised reading, modification, or addition or deletion of information, as well as efforts to influence access.

The threats in the context of online elections can be divided into different categories: Attacks by external attackers vs. internal attackers; Attacks on IT systems vs. efforts to influence eligible voters.

Unlike elections in person or via postal ballots, the worst-case scenario is that the overall result of an election could be manipulated rather than just individual votes.

Minimising these threats entails implementing both technical and organisational measures. Cryptography plays a key role in this regard. Along with transport encryption, other encryption mechanisms, signatures and time stamps are particularly important in protecting online elections. Appropriate key management is also essential. Technical and organisational safeguards must be put in place to ensure that no one gains unauthorised access to private keys, whether for decryption, time stamps or signatures. These are just two examples of appropriate measures for protecting online elections.

For the model project involving the online elections for the governing boards of German social insurance institutions, protection methods have been defined in TR-03162. Based on this project, some generally applicable technical security requirements have been developed for the digitalisation of other elections, such as for the equal opportunity commissioner. These will be implemented at the BSI by creating protection profiles for online elections products and a Technical Guideline that covers the supervision of online elections *(see article on p. 14)*, which is expected to be published by the end of 2022. ■

Further information:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03162/TR-03162_node.html

Certification of Online Elections Products

Interaction of Protection Profiles and TR-03169

By Jennifer Breuer and Sebastian Palm, Section eID Solutions for Digital Administration

The certification of online elections products through protection profiles is an important way to set minimum standards for online elections. Specifications for such products are formulated in these protection profiles. The certification of these products can help election supervisors choose the ones right for them. Before they can use these certified products, however, supervisors must make certain decisions and preparations. The BSI is set to offer help with TR-03169.

There are currently various online elections products on the market. If an election or vote is to take place online, the supervisors need to decide which product is the right one. In particular, online elections must be protected by technical IT security measures. As you might expect, every provider of online elections products states that their offering is secure. IT security certification can give process owners the certainty that a specific number of security objectives are covered. This certification provides several pieces of information, including whether state-of-the-art cryptographic methods are used to deliver an authentic election result while safeguarding the secrecy of the ballot. Another example is the assurance level at which voters can register for an online election and cast their vote. If a high assurance level is required, the product must support the use of the online ID function with an ID card or equivalent form of identification.

What is not covered by the protection profiles?

Besides deciding which assurance level is the right one for the election or vote at hand, election supervisors also need to answer a number of other questions to prepare an online election properly. First of all, they must check whether the legal framework is in place for an online election. There may be a corresponding regulation containing requirements that the election must meet (e.g. the Online Elections Regulation for the model project involving online elections for the governing boards of social insurance institutions). These requirements apply not only to the online elections product used, but also to the framework conditions in which it is used. An online election project may encompass many tasks and processes depending on its size and complexity. These may have to do with preparing and following up on the election rather than actually carrying it out. In addition, organisational and operational precautions must be taken that play a role in the secure use of online elections software. These framework conditions cannot be covered by product certification.

Why is TR-03169 needed?

For this reason, the BSI intends to provide Technical Guideline TR-03169 (on technical IT security requirements for implementing electronic elections) by the end of 2022, in addition to product certification. To cover all the aspects of holding secure online elections in a manner suitable for all the entities involved, this

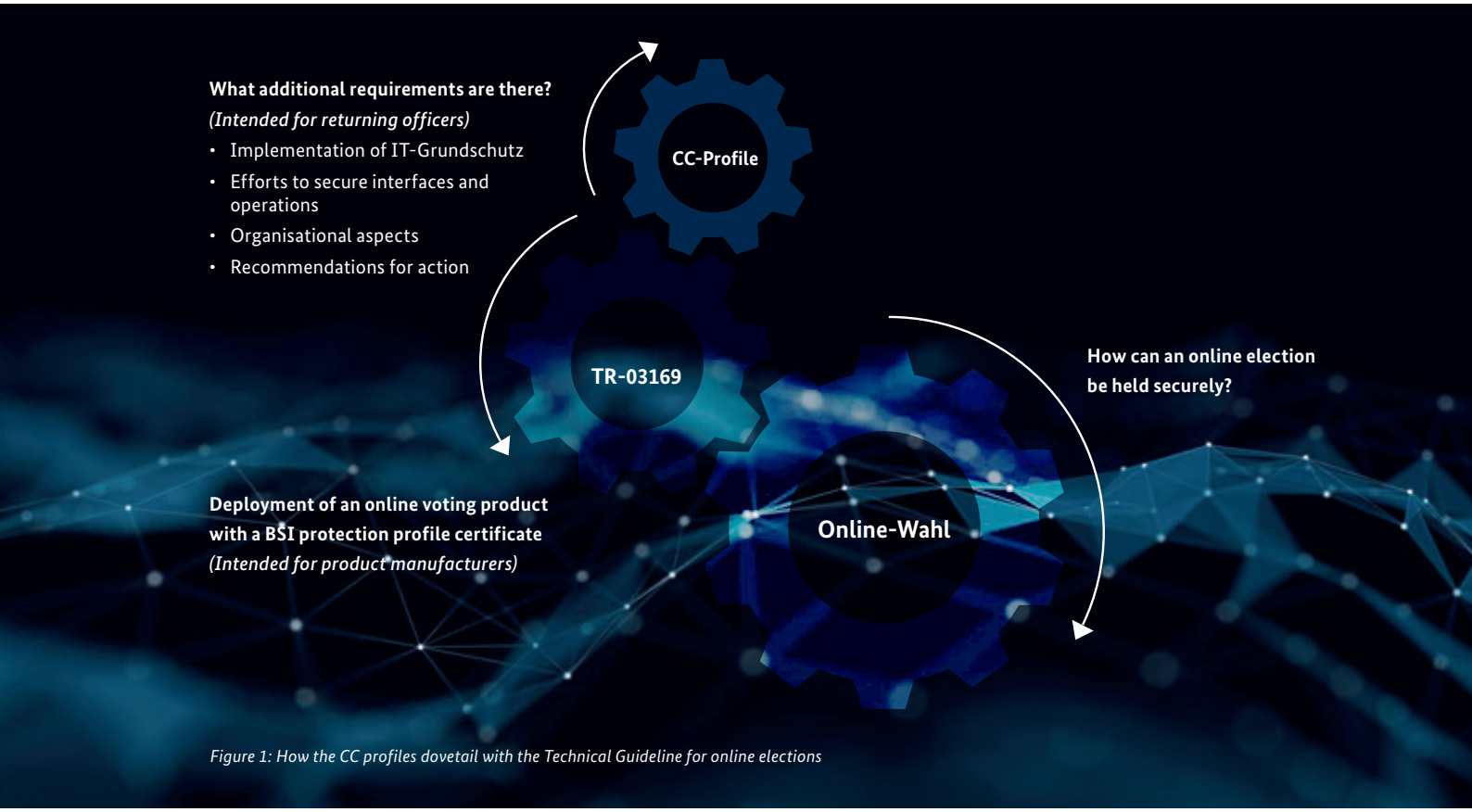


Figure 1: How the CC profiles dovetail with the Technical Guideline for online elections

Technical Guideline is aimed at election supervisors and/or other decision-makers in organisations that intend to implement online elections.

The Technical Guideline covers a number of areas, including:

- Preparatory work for online elections, such as collecting data and coordinating content related to setting dates for the elections period, voter ID numbers, electoral rolls, and candidates or electoral lists. This work must be done outside the online elections system. The information that is gathered must then be transferred or transmitted securely to the online elections system.
- The application of IT-Grundschutz, particularly with regard to the specific requirements of online elections (*see article on p. 22*).
- Recommended actions for process owners in preparing, implementing and following up on online elections.
- Important points to consider when using external data centres to operate applications in the context of online elections.

The Technical Guideline therefore focuses on giving election supervisors the information they need to implement an online elections process that is as secure as possible from beginning to end. It is especially important that election supervisors receive clear information about the options available to them and the duties they must fulfil. To reduce the complexity of certain topic areas for election supervisors, the Technical Guideline also provides information on possible monitoring methods, such as certification or audits.

Certifying a product for online elections ensures that the basic requirements for the secure implementation of online elections are met at the application level. The Technical Guideline describes the additional framework conditions required for the secure implementation of online elections. Together, product certification and TR-03169 offer all the tools needed to take on the issue of online elections in all the key sub-areas. ■

Secret Online Elections

Balancing Transparency and the Secrecy of the Ballot

By Dr. Gottfried Herold, formerly Section Information Assurance Technology Evaluation and Lea Nagler, Section Information Assurance Technology Requirements

Digitising elections: How does the process work and what are the challenges that need to be overcome? An insight into the cryptographic toolbox.

For electoral decisions to be democratically legitimate, the corresponding votes have to possess certain characteristics. These may include the principles of electoral law, namely that a vote must be general, free, equal, direct and secret. In addition, the vote must be public in way that gives the voters confidence that the overall system meets these characteristics. In the context of online elections – or elections processes in which at least the actual casting of a vote takes place online – some of these characteristics are achieved through cryptographic methods. The building blocks used in cryptographic elections protocols are highly diverse and complex. The article below provides a general description of two approaches for these protocols based on a simplified protocol, with a focus on counting votes. The two approaches are among the generally discussed solutions proposed for the problem of secret online elections.

Open ballot

An open ballot involving only the voters and a elections server could be implemented in the following way: to check elections eligibility, the elections server has a list of eligible voters with their public signature keys. The voters transmit their votes to the elections server together with a signature and a reference to their identity. The elections server can then correct the list of votes cast so that only one valid vote with a valid signature is included for each voter. The server uses this corrected list to determine and publish the result. If the server also publishes all the corresponding lists (public signature keys, votes cast, corrected votes), everyone involved can check whether their votes have been cast and the correct overall result has been determined.

If this process were to be expanded and applied to secret ballots, one initial idea would be to cast the votes in encrypted form with a public key procedure. The vote would then be secret with respect to third parties, but not necessarily to the elections server, which must check the validity of the results and evaluate them. The difficulty here is that the elections server must establish a link between the casting of a vote and the voter's identity in order to check elections eligibility, but should not be able to associate the voter's actual decision with their identity. In other words, a way to separate a voter's identity from their encrypted vote after checking their eligibility must be found.

Either the result needs to be determined in an encrypted state (homomorphic counting) or the mixing process in the physical ballot box needs to be simulated (verifiable mixing).

Homomorphic counting

Homomorphic counting methods avoid any decryption of individual votes. In a vote with two options (e.g. yes/no), it would be possible to define that a "yes" vote corresponds to 1 and a "no" vote corresponds to 0. The total number of votes cast then indicates the number of "yes" votes. It is sufficient to compare this total number of votes against the number of valid votes cast. There are special homomorphic encryption methods available that perform a summation of this kind with the encrypted votes without having to decrypt the individual votes. The result is the number of "yes" votes in encrypted form, and only this result is decrypted.

However, this does not solve the problem of secrecy towards the elections server. Anyone with access to the key for decrypting the result can also decrypt individual votes. Using a homomorphic method with threshold decryption may solve this problem. This can be understood as the digital version of the dual-control principle: trust is distributed across several servers, each of which has only one sub-key. Each server executes a sub-operation so that the key is never actually available as a whole. If enough servers are honest and operating only on the result, dishonest servers are not able to violate the secrecy of the ballot.

This ensures protection against dishonest servers. The method is not secure against dishonest voters, however, as there can be no direct check of the validity of the vote format. In the example above, voters could attempt to send a 2 in encrypted form instead of a 1 and thus double the weight of their vote. Therefore, evidence of the vote format that does not result in the vote itself being revealed needs to be provided. One way to achieve this is with non-interactive zero-knowledge proofs.

A disadvantage of this approach is that the only elections systems that can be implemented are those whose results can be determined with an operation such as addition. This is not the case with every elections process, however, which is the reason behind the second approach – where individual votes are decrypted to determine the result.

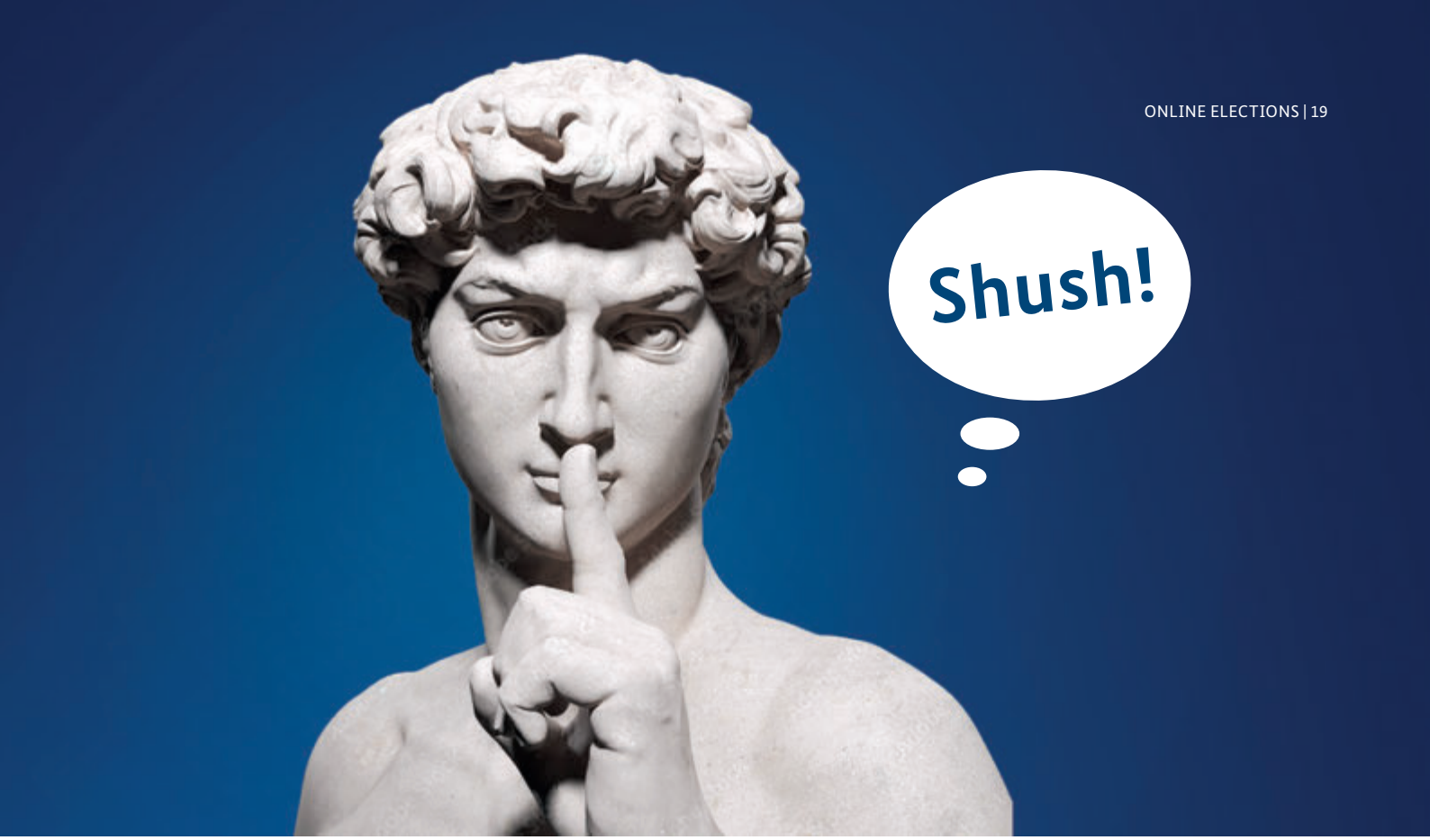
Verifiable mixing

Here, the elections server first separates the encrypted votes from the signatures and identities. It then puts them in a new and random order. This is an important step, and not simply because the signature and identity represent a link between the elections decision and the voter; it is also because the time of sending influences a vote's position in the list of all those cast. This could

Signature	A digital signature that protects against subsequent manipulation.
Public-key procedure	An encryption method that has separate keys for encryption and decryption. Encryption is possible for anyone who has the public key, but this does not enable to decrypt information.
Homomorphic encryption methods	Encryption methods that permit operations such as addition in an encrypted form
Threshold decryption	A decryption method that must involve several parties working together
Bulletin board	A public protocol of messages sent and operations executed
Non-interactive zero-knowledge proof	Proof of a characteristic of a secret that does not disclose the secret and requires no interaction between prover and verifier
Re-randomisation	Renewal of the random component contained in a ciphertext
Mix-net	Multiple servers working in concert to re-randomise ciphertexts and permute them in a random order
Individual verifiability	The opportunity for the voter to check that their own vote has been counted correctly
Universal verifiability	The opportunity to check that the overall process is correct

enable observers to obtain information about the voter, even without any identity information. This process becomes even more important if all actions are logged in a publicly visible way (e.g. on a bulletin board) with the aim of ensuring transparency.

In this context, it also becomes clear that simply mixing the specified information is not an adequate solution: the ciphertexts are still the same and could be compared against the submitted ciphertexts that can be assigned to an identity. To prevent this, they must be modified without changing or revealing the corresponding plain text. One way to do this is through “re-randomisation”,which is based on the fact that encryption methods are generally non-deterministic. This means that two ciphertexts pertaining to the same plain text and key are generally different. In case of elections processes that are protected with a public key procedure, the need for this method quickly becomes clear: if attackers observe the distribution of ciphertexts and compare them against the published result of the vote, they can identify which ciphertext stands for which plain text, thus breaking the secrecy of the ballot for all votes in one go without even knowing the public key. To ensure that this does not happen, the ciphertext must be disguised by a random component during encryption. The idea now is to renew this random component. From an observer’s perspective, the relationship between an encrypted vote and the corresponding identity is destroyed. To ensure this applies to individual elections servers, several servers (which together form a “mix-net”) are used that execute this operation independently in succession.



As a result, the votes are secret, but there is a risk of a dishonest server deleting votes and adding new ones in their place instead of mixing them. To prevent this from happening, a zero-knowledge proof is used, as in the case of homomorphic encryption. At the end of the mixing process, all votes can be decrypted with threshold decryption and then evaluated.

A question of trust?

The approaches above focus primarily on counting votes. However, there are many sub-steps to a elections process that should be verifiable as a whole. The option for every individual to check that their vote has been cast and counted is known as “individual verifiability”. This comprises the following three sub-verifications:
(1) transfer of the elections decision in the form of an encrypted or non-encrypted vote (cast-as-intended),
(2) transmission and saving (stored-as-cast) and
(3) counting (tallied-as-stored).

The option for independent auditors to check that the entire elections process is correct is known as “universal verifiability”. Both of these characteristics are important, as they increase trust in a elections system.

The encryption of votes results in parts of these characteristics being lost, meaning they must be restored through other means. In the case of homomorphic encryption, for example, the ability to review the validity of votes is restored by zero-knowledge proof, thereby ensuring universal verifiability.

However, the problem with this approach is that it makes the protocols, which already comprise many sub-steps that require protection, much more complex. This reduces transparency, which in turn reduces trust when the opposite is the goal. Even if the protocol and its implementation are openly accessible, only a very small proportion of the public will be capable of checking it. Ultimately, an online elections product can be regarded as a special IT security product. For these products, there is always the question of how their security can be assessed in a trustworthy way. ■

Further information:

https://oparu.uni-ulm.de/xmlui/handle/123456789/22747?locale-attribute=de

Shaping Security

How Online Elections Products Are Advancing Software Certification

By Fritz Bollmann and Michael Meissner, Section Software Certification

Products used for online elections are subject to high IT security requirements and rely on certifications to prove that these requirements have been met. However, these products are usually released in very short release cycles. The legally compliant use of certified products subject to regular, short release cycles requires forward planning when it comes to product certification.

The The Common Criteria (CC) are one of the few internationally recognised IT security criteria with which high assurance statements can be made. The CC are flexible, so manufacturers or authors of Protection Profiles can freely define both the assurance level and the choice of security features based on their individual requirements.

A high assurance level and thus a high security statement automatically increase the evaluation effort since verified security can only be based on knowledge and facts. Public criticism often revolves around the idea that CC certifications are costly and take a long time. However, this is not usually due to CC, but rather to the effort required for high-level assurance requirements.

Obvious ways to reduce the effort involved in certification are therefore to choose lower evaluation levels and to limit the security functions to be evaluated.

In addition to the CC, the BSI offers other certification procedures, such as the Accelerated Security Certification (BSZ, see article on page 6) and the IT Security Label, which allow appropriate security statements to be made for a wide array of security product types and application scenarios. For example, the BSZ uses a risk-driven sampling based evaluation to make security statements.

However, there is currently no alternative to the Common Criteria certification for high assurance levels. Other acceleration strategies are required here.

Managing product changes: re-certification

The first time a manufacturer seeks product certification is usually the most time-consuming. Essential tasks include adapting and documenting development processes and creating evaluation documents. Those responsible for evaluating and certifying become familiar with the real workflows and processes on site through audits and manufacturer visits. They talk to developers and see how much they know and to what extent they adhere to the security processes in development (and production). Experience indicates that proof of security for a product cannot only be obtained by reading documents, but also by experiencing the security processes that a manufacturer actively uses on site.

This means those involved in the process can prioritise and reuse aspects for future re-certifications. The evaluation process becomes more efficient. These foundations grow stronger with each re-certification and audit. Naturally, re-certification projects become faster. The disadvantage is that this approach is usually based on many years of collaboration between a manufacturer, an evaluation lab and the certification body.

CC community solutions

A new CC methodology called patch management aims to achieve the feat of speeding up the re-certification process without compromising security. Specifically, it is a process that focuses more on confidence-building in the patch and software quality processes at the manufacturer.

The goal is to accelerate the confidence-building process. To achieve this, some additional assurance requirements for product maintenance and development security are defined, comparable to the experiences on site. The results can then be reused directly in a re-certification procedure. In practice, there are currently two approaches to this methodology. One of them comes from the International Security Certification Initiative (ISCI) Working Group, while the other comes from ISO standards (Towards Creating an Extension for Patch Management for ISO/IEC 15408 and ISO/IEC 18045). The fundamental motivation of the approaches is similar but they differ in terms of the modelling of the additional requirements. The ISO methodology has already been piloted in a certification project by the BSI.

In the software sector in particular, the version cycles are short due to a rapid development rate. This has been regarded as a disadvantage of the CC, as certification under high-level assurance often could not keep up with fast version cycles. For the first time, the patch management methodology now presents the opportunity to fix this disadvantage.

Online elections products

More than almost any other product, online elections products, for which Protection Profiles will also be available, are the focus of critical public and security scrutiny. In addition, these products must be ready for use at a specific time and operate to the latest security level. An election cannot be postponed just because a certification process has not yet been completed. The combination of high public focus, the need for certified IT security, a strict time frame and fast update cycles make patch management the ideal tool for the CC certification of online election products.

With this in mind, the BSI will continue to test and introduce the new approach of patch management in certification. As well as delivering the above benefits, this will also help meet the requirements in the area of online elections. At the same time, this should also give CC certification a new impetus for other product types in order to speed up project durations while maintaining the expected high level of assurance. ■

Protecting Information and Elections Securely

IT-Grundschutz in Online Elections

By Sebastian Palm, Section eID Solutions for Digital Administration

Online elections is a complex issue with many unique characteristics that need to be taken into account. How compatible is it with IT-Grundschutz, and what factors need to be considered?

Technical Guideline TR-03169 (on technical IT security requirements for implementing electronic elections) is intended to help election supervisors protect online elections processes in various contexts. The aim is to enable various votes (such as elections for equal opportunity commissioners or works councils) to be conducted online using TR-03169. Online elections is a special application scenario. There are different legal provisions (such as elections regulations) depending on the context of the vote. In addition, it is necessary to fulfil specific processes and requirements, such as those relating to the electoral register, voter ID numbers and ballot papers. The risks and damage scenarios characteristic of online elections must also be assessed (to ensure that elections are general, direct, free, equal and secret, for example).

A key component of TR-03169 is the implementation of IT-Grundschutz, which offers the opportunity to tailor information security requirements to the needs of a defined information domain. When it comes to the substantial issue of online elections, the more extensive Standard Protection (as opposed to Basic or Core Protection) must be chosen as the method of applying IT-Grundschutz to the corresponding information domain.

This figure shows the individual steps involved in implementing the Standard Protection afforded by the IT-Grundschutz methodology.

What is actually special about implementing IT-Grundschutz for online elections has to do with its modelling. The question arises as to how this can be done on the application side, since there is no module in the IT-Grundschutz Compendium for the special application scenario of online elections. The following takes a closer look at how to tackle this issue.

IT-Grundschutz contains a number of more general modules for modelling applications. Of these, “APP.3.1 Web Applications” and “APP.6 General Software” are the ones that could be applied to most application scenarios in online elections. APP.3.1 only makes sense if the online elections product being used is actually a web application as defined in the corresponding module. If it is an in-house development, further modules may need to be applied (e.g. APP.7).

The available modules may not be adequate for modelling purposes due to the complexity of online elections. They do not take account of all the potentially relevant application scenarios and risks, such as the processes for creating and transferring particularly sensitive data from the elections process (e.g. electoral registers, ballot papers) to the elections application. To tackle this problem, IT-Grundschutz provides for a risk analysis of the target object in question (in this case, the application for online elections), as it cannot be covered adequately by the modules in the IT-Grundschutz Compendium.

Alternatively, a separate, user-defined module can be created for a target object for which there is no appropriate module in IT-Grundschutz. Since a certain amount of work is involved in creating a user-defined module, considerations should be made as to whether the module is likely to be used again. If the application scenario is unique or rare, it may not be worthwhile to create a separate module. User-defined modules can be created in coordination with the IT-Grundschutz Section of the BSI. The BSI website provides a template, implementation guidance and other information on user-defined modules.

An IT-Grundschutz profile entitled "Rapid Reporting of Elections Results" is currently being drawn up in which elections support will be a key module. It is expected to be completed by the beginning of 2022.

Common Criteria Protection Profiles and Technical Guidelines (see article on page 20) provide a good basis for selecting measures in drawing up a risk analysis. They are not intended to be exhaustive, and other suitable measures must be evaluated for the risks identified. This is particularly important because every application scenario, operating environment and application is different, and these differences and the resulting requirements must be taken into consideration in risk analysis. ■

Further information:

www.bsi.bund.de/IT-Grundschutz

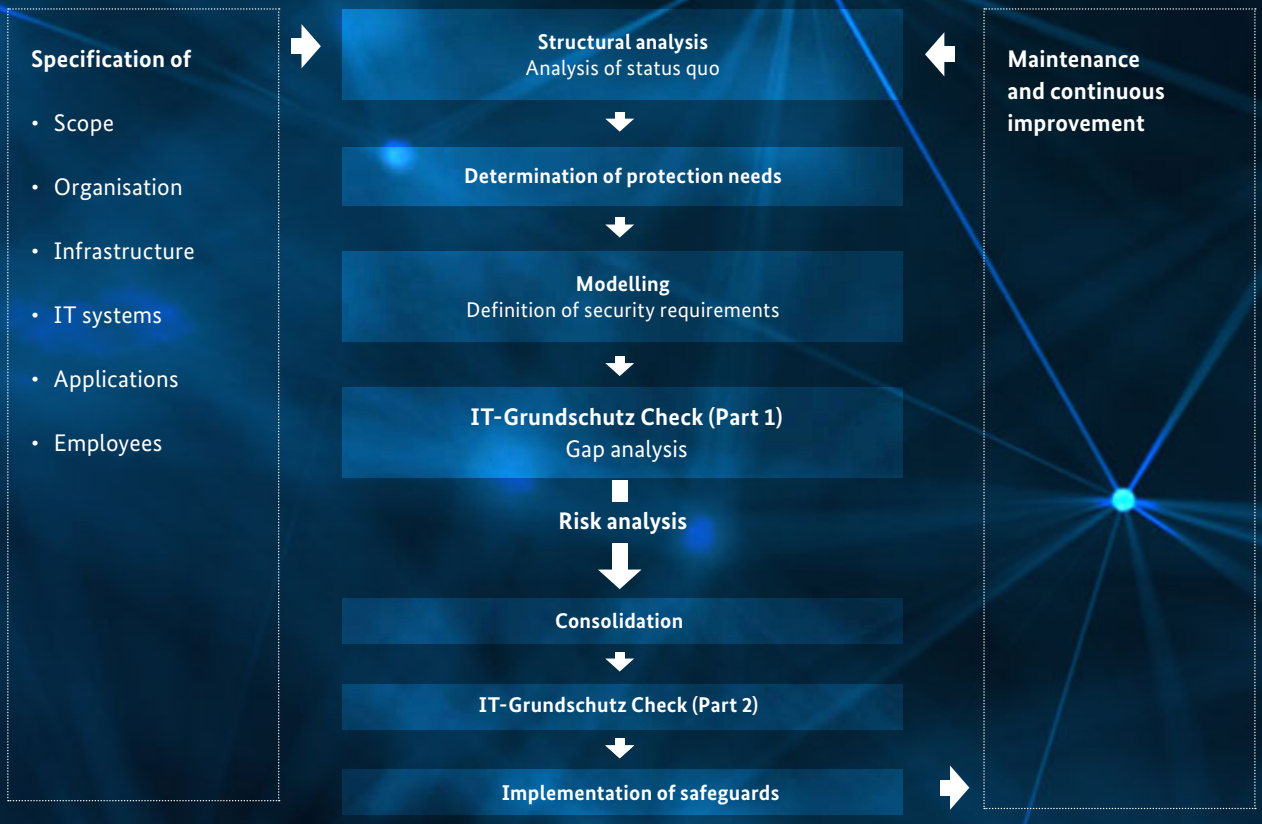


Figure: IT-Grundschutz method: Standard Protection (source: BSI Standard 200-2)

Online Events and Elections

Practical Information and Support for Successful Digitalisation

By Michael Amler, Section National Liaison Office and Dr. Florian Seiller, Section Strategic Approaches to Information Security

During the coronavirus pandemic, the demand for solutions for online meetings and elections has grown dramatically. But how can these formats be implemented as securely as possible against the background of the growing threat landscape in cyberspace? To help with this, the BSI has published scenarios, guiding questions, tips and practical assistance and also provides advisory support.

The coronavirus pandemic has given digitalisation a huge boost. In-person events of various sizes, such as association or shareholder meetings, lectures and seminars at universities, company meetings or plenary and committee meetings of parliaments or political parties were unable to take place for several months – or, if they did, only to a very limited extent. As a result, the use of web and video conferencing tools and platforms for collaborative work has increased dramatically and is probably now a permanent part of the new normal. But what is the IT security situation of online or hybrid conference or meeting formats? What aspects need to be considered to ensure that information in the digital world can be transferred and exchanged securely? What security risks are there and how can the key security objectives (availability, authenticity / integrity and confidentiality) be sufficiently protected? In short, how can online meetings and elections be conducted with a level of security that is appropriate for the occasion or individual requirements?

BSI Online Meetings and Elections (ViVA) project group

Since April 2020, the BSI has been intensifying efforts on the topic of "Online Meetings and Elections" (ViVA) and has formed a cross-departmental project group for this purpose. This work has produced several publications with scenarios, guiding questions, information and practical tips that can be accessed on the BSI website and can provide assistance for manufacturers, operators and organisers from the planning stage through to implementation.

The paper "Ideas and Scenarios for Government, Business and Society", which is intended as a starting point, includes ideas and scenarios related to online meetings as well as (non-secret) elections. It also provides initial answers on how small, medium and larger digital meeting formats with normal protection needs can be held securely.

There are certain risks associated with implementing electronic elections. In particular, this applies to secret elections. The publication "Approaches to Risk Assessment in Digital Secret Elections in the Context of Meetings" mainly focuses on the electoral principles involved and raises fundamental questions that need to be addressed by the organisers before a secret ballot can take place electronically.

The paper "Requirements for Products for Online Meetings and Online Elections" is available in English and required the BSI to be in contact with various domestic and foreign partners and providers. It contains a comprehensive catalogue of product requirements divided into the areas of performance parameters, security features as well as proof of security, testing and detection. The requirements catalogue primarily addresses manufacturers and operators of products and services for online meetings and online elections, but can also serve as a guide for product selection.

Further BSI recommendations for improving information security

The BSI's trusted guidance documents also provide systematic approaches for substantially increasing the security level of online meetings and elections. These focus on technical aspects but also on infrastructural, organisational and personnel aspects. These documents include the IT-Grundschutz with the IT-Grundschutz Compendium and the IT-Grundschutz Profiles, the Compendium of Video Conferencing Systems and the BSI Criteria Catalogue C5 (Cloud Computing Compliance Criteria Catalogue, *see also page 22*).

Practical example: party conventions

Organising secure digital party conferences is particularly challenging. In 2020, parties represented in the Bundestag had to meet, discuss, determine positions and also elect persons and offices entirely online for the first time.

As well as requiring changes to the law, questions regarding information security suddenly came to the fore: How can secret elections be organised? What risks do the parties run? How can several hundred delegates take part?

In addition, the political focus of the event should not only be viewed in terms of its content, but also in terms of politically motivated attack attempts and political implications. This is why the goal of technical resilience often coincides with the goal of democratic resilience.

To help achieve this, the BSI offered general assistance and supported the parties in securely hosting these digital events when requested through an on-site liaison officer, for example. The experience gained was in turn transferred into the public papers referenced above. Most importantly, the key component of a secure party conference is the ability to prepare functioning incident management and crisis communication protocols as well as sufficient backup and mitigation measures.

Party convention – additional radio link to the Berlin TV tower to act as a backup in case of a network failure

Further development

Regardless of the type of meeting or vote, users must carefully consider the risks and purpose and define the desired requirements before IT security solutions can be developed. There is no system that can guarantee total protection.

The development of the entire field is very dynamic and has been characterised by cross-sector learning from one another for more than a year. The BSI and the ViVA project group are certainly playing their part in this. Through the papers they have produced and the practical tips, guiding questions and recommendations they contain, they are offering a comprehensive guiding framework to enable online events and elections to take place with a high level of security. ■

Further information:

https://www.bsi.bund.de/viva
Contact: viva@bsi.bund.de

Digital Elections and Elections Processes

Opinions from the Field

By Agnieszka Pawlowska, Section Cyber Security for the Private Sector and Alliance for Cyber Security

The transfer of analogue coordination processes into digital ones represents a great opportunity but also a challenge for companies and for parties. The Alliance for Cyber Security (ACS) has captured voices from the field in its two formats, the Cyber Security Web Talk and its podcast CYBERSNACS.

Can in-person meetings and analogue elections processes simply be transferred to the digital realm? This was the question faced by Germany's political parties in 2020 and 2021 as they considered how to organise their party congresses. New ground has been broken in various ways in the last two years due to the COVID-19 pandemic. In September 2020, the Green Party held its first hybrid congress. In January 2021, the CDU faced the challenge of organising its first fully digital party congress and electing a new leader. In the fourth episode of CYBERSNACS, the moderators had the opportunity to learn more about this by interviewing Dr. Stefan Hennewig, responsible for planning and implementing the congress in his role as Federal Executive Director of the CDU.

Since the beginning of the pandemic, many organisations found themselves facing this new challenge of organising digital events. As we all know, however, digital events are somehow very different from in-person events. One common conclusion, after over a year of the pandemic, their organisation involves even much more work than their analogue counterparts do.

This was the case for the CDU party congress, which had to meet various legal requirements given that it also involved online leadership elections. The first task was to ensure coordination between more than 12 different technical and organisational units. This applied in particular to the software provider of the digital plenary hall and to the company commissioned to carry out the elections. A simple public vote – similar to a traditional show of hands in a conference hall – can nowadays be carried out with standard video conferencing systems. The challenge begins with the secret ballot. This is why another specialised service provider was tasked to organise the online leadership election. Besides ensuring the process was secure and protected against attacks, the provider had to offer methods of guaranteeing the transparency of the elections process in accordance with Article 21 of the Basic Law.

In addition, party votes are subject to stricter rules than would be the case for votes at an AGM, for example. For this reason, the election of the CDU's new leader followed a two-step procedure. A change in the law in October 2020 allowed a digital preselection process to take place. Once the digital vote had been taken, the result had to be confirmed by the delegates in a postal vote.

The benefits of digital meetings are obvious: there is no need to travel long distances, which makes participation easier. But what about exchanges that take place outside the regular programme of events? Networking is usually at least as important as the speeches and other official items on the agenda. Some creative methods have been identified through the use of multiple devices. While attending a party congress on one device, participants could get to know each other and exchange perspectives in smaller groups in privately organised Zoom meetings.

Two hours on cyber security for AGMs and secure elections

ACS presented further perspectives on secure digital elections in March 2021 in the "Cyber-Sicherheits-Web-Talk" (Cyber-Security-Web-Talk). The guests were Anna-Maria Palzkill from POLYAS GmbH, who reported from a provider's perspective, and Prof. Dr.-Ing. Andreas Mayer from the Heilbronn University of Applied Sciences, who offered his experiences from a participant's point of view. In their presentations and the subsequent discussion, they looked at what needs to be done to ensure that information is transferred and exchanged securely and how the security objectives of authenticity, confidentiality and availability can be guaranteed. ■

Stay up to date on the latest news in cyber security with two monthly formats: the "Cyber-Sicherheits-Web-Talk" and "CYBERSNACS", the podcast of the Alliance for Cyber Security. Find out more on our website.

Further information:

Cyber-Sicherheits-Web-Talk:
https://www.allianz-fuer-cybersicherheit.de/webtalk

CYBERSNACS:
https://www.allianz-fuer-cybersicherheit.de/cybersnacs

CYBERSNACS #04: Conversation with Dr. Stefan Hennewig (Federal Executive Director of the CDU)
https://cybersnacs.podigee.io/4

THE BSI

The BSI and State Elections

Increasing Resilience and Safeguarding Elections

By Michael Amler, Section National Liaison Office

Digital solutions are increasingly being implemented as part of parliamentary elections, which entails a rise in threat exposure for the 2021 federal elections and a total of five state elections. Democratic and technical resilience coincide. The BSI provides support through webinars, workshops and availability around the clock.

In times when fundamental democratic values are being boldly questioned, it becomes even more evident that the resilience of these values needs to be reinforced. Parliamentary elections play a key role in this. They are the fundamental act of legitimisation in a representative democracy, in which elections are of primary significance.

While the act of elections with pen and paper in the elections booth or by postal vote, is a highly analogue process, the BSI is starting to play a bigger role in the election process. Citizens are increasingly accessing information online, yielding to election campaigns taking place online progressively. Political parties are using virtual platforms to present their programmes and allocate party list positions. Accordingly, election results are being communicated and recorded digitally. In short, the digital sphere is playing an increasingly major role in electoral contexts.

Threat landscape and BSI election support

Threat exposure during elections is both multifaceted and complex. The attack scenarios range from cyber stalking, online abuse and identity or data theft – including the publication of captured information (known as doxing) that can gain a lot of media attention – to disruption and sabotage using encryption Trojans, all the way up to spreading disinformation. To combat this, the BSI is taking on a leading role on both federal and state level, next to returning officers, the Ministry of the Interior and the Federal Office for the Protection of the Constitution. It is worth remembering that digitalisation is only one side of the coin, the other is information security. Both elements are inseparably linked to each other.

The BSI provides comprehensive assistance in safeguarding elections. With the “National Liaison Office” in Berlin, Hamburg, Stuttgart and Wiesbaden and the “Information Security Consulting Unit for State and

Local Governments", the BSI also offers support to the responsible government agencies to retain safe elections through a cooperative and complementary approach. After all, successful information security can only be possible on a national level if not across state borders.

The BSI has also gained valuable experience for state elections through the groundwork it has carried out strengthening the integrity and availability of the core electoral process as well as increasing resilience against technical manipulation attempts during federal elections. Taking into account legal and resource framework conditions, this expertise is the cornerstone of a diverse set of services that allows state returning officers, IT security officers and further roles to find the most suitable solution for their requirements.

The core of the services are workshops that discuss the existing concepts and security measures for the state elections, map out the threat landscape and set up crisis management. It further offers room to discuss open questions and information packs and other support related matters.

On-site presence and technical support

The first state elections in 2021 have already demonstrated the diversity of the BSI's range of services. For example, a BSI liaison officer provided on-site support at the Federal Statistical Office on election day until the preliminary election results were announced after the counting of all constituencies had been completed after midnight. This provided a direct connection to the BSI and enabled any technical questions to be settled. But most importantly, being on location provided valuable insight the processes and security safeguards. Over the course of a long night – up until the last constituency had been counted – a number of personal stories about self-developed and self-hosted software in connection with the elections came up in conversations.

In addition, webchecks of the election results publication page enabled proposals to facilitate improvements to the system.

Information security for the first release process

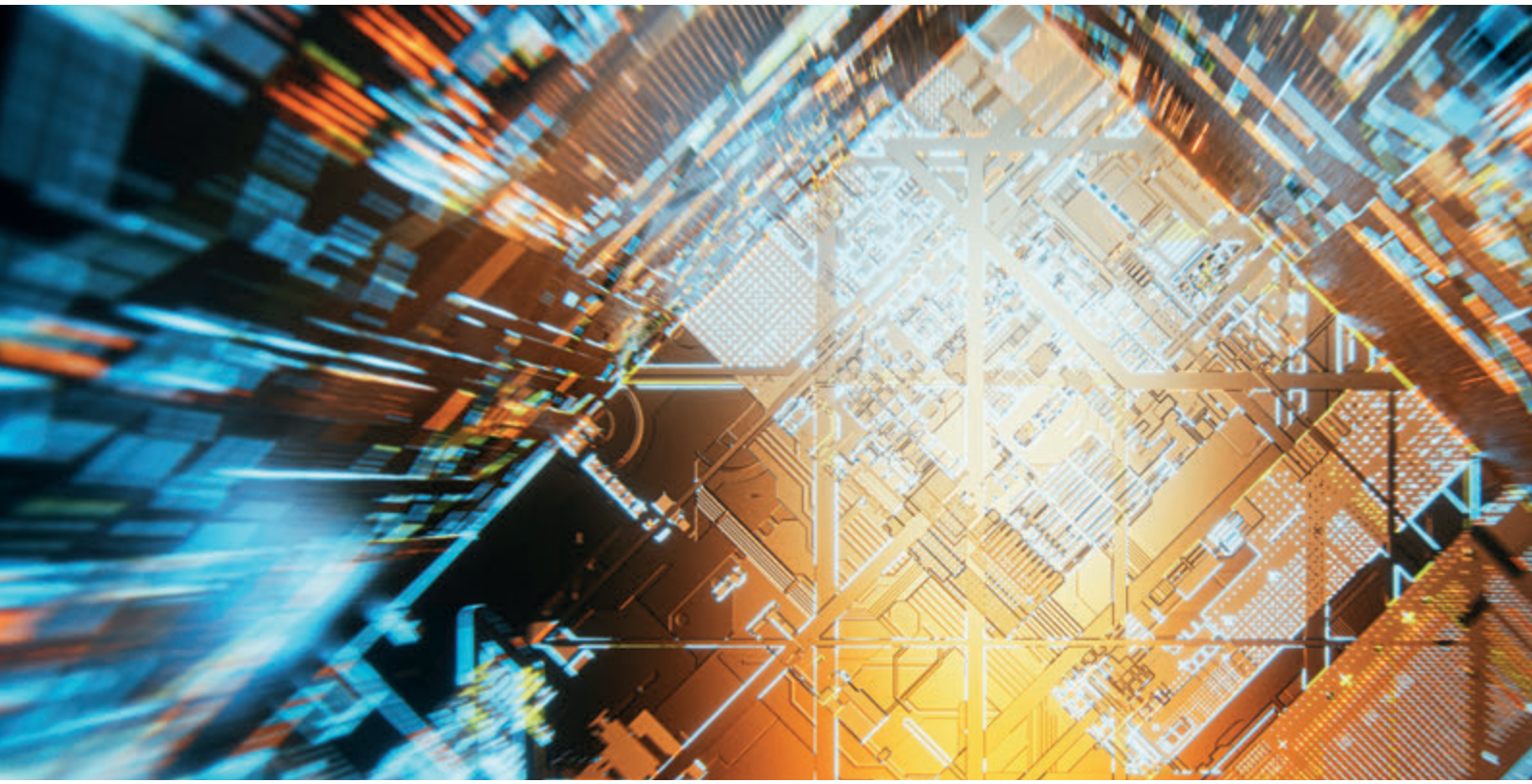
However, one of the most important BSI support services for the federal and state elections is probably the "Compliance Catalogue for Information Security in the Determination of Provisional Election Results", which is aimed at federal and state returning officers as well as municipalities. Commissioned by the Federal Election Commissioner and compiled by the BSI, it contains very specific and practical security criteria, guidance and checklists that can ensure information security around election day for the first release of the preliminary election results (Section 71 – Federal Election Code (BWO) for elections to the German Bundestag). In addition, the Compliance Catalogue is to be upgraded to an IT-Grundschutz profile from the beginning of 2022 and will be available at a state and national level.

In addition, a webinar series on "Information Security for Securing the Rapid Reporting Process" was arranged in August this year in cooperation with the Federal Election Commissioner and welcomed almost 2,400 attendees from local government. This in itself was a major challenge from an information security perspective given the highly varied IT structures and requirements involved.

Outlook

These processes and services only touch the surface on the work the BSI has conducted in the context of the 2021 elections. They are constantly evolving and being developed. In 2022 alone, there will be four more state elections. The BSI would also like to provide support for these elections and intends to share the common experience gained in the context of future parliamentary elections (state and federal), to arrange more specialised webinars with representatives from the federal states and the municipal umbrella organisations, and of course to provide specific support. ■

IS web check: the security status of the website of a public authority or an institution can be checked using the BSI IS web check feature. These tests are largely performed using automated methods online.



Shaping Digitalisation in Germany – and at the BSI

A Federal Authority Sets the Course for the Future

By Tim Griese, Head of the project group Digitalisation at the BSI

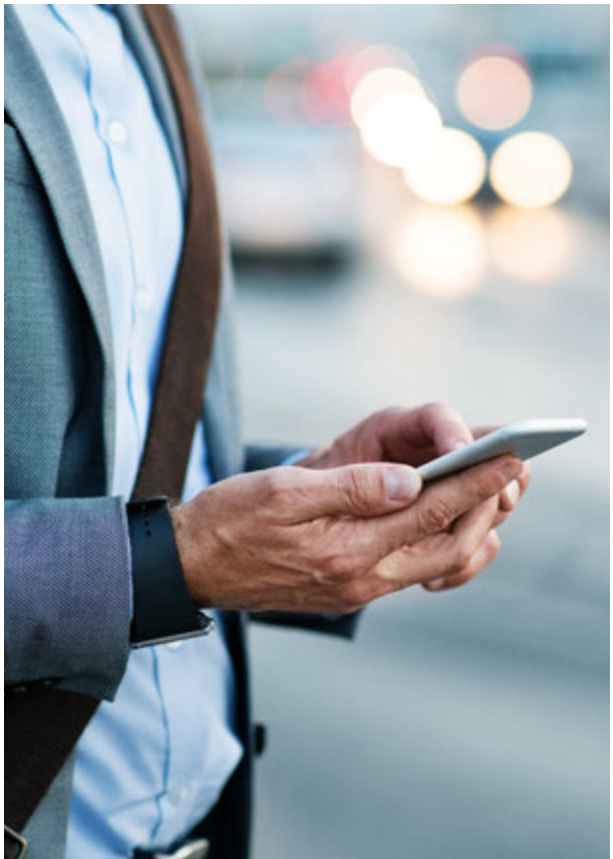
The BSI is the federal cyber security agency and the chief architect of secure digitalisation in Germany. This role has been clearly strengthened and expanded by the legislative authority with the German IT Security Act 2.0, which came into force in 2021. However, even prior to this, the BSI had been assigned new tasks and the number of employees had grown due to the steadily increasing importance of digitalisation and cyber security as its prerequisite. The number of BSI employees has almost trippled between 2016 and 2021. New tasks, target groups and more employees also require further development of the internal processes as well as the organisational structure. This means that the BSI is not only the chief architect of secure digitalisation in and for Germany, but digitalisation is also being actively promoted within the BSI itself.

The requirements of target groups in government, business, research and society that the BSI must meet as part of digitalisation are increasing every day. Public authorities at federal, state and municipal levels, politicians, companies, institutions, research institutes, associations and, last but not least, consumers expect the BSI to provide concrete solutions and support for the problems and challenges they face. Job applicants with exacting technical requirements as well as all BSI employees expect to be provided with highly functional ways of working together, along with a modern workplace befitting of the excellent reputation that the BSI has earned in recent years as one of the best employers in the IT sector.

The BSI of the future: procedural and digital

In order to meet these expectations and to provide services of a consistently high quality in an efficient and scalable manner as well as across multiple sites, the BSI needs to adopt a procedural and digital approach across the board. By 2025, the BSI aims to be a public authority that provides practical and target-group-oriented products and services based on scalable, reliable and digital processes. In doing so, the BSI will fully comply with its legal obligations as well as its high level of social responsibility.

As far back as 2017, the BSI had already started documenting existing processes and modelling them in a process map that is continuously being developed and adapted – for example, when the BSI is assigned new tasks or new framework conditions emerge. Based on the process map, the BSI continuously analyses its internal processes, exploits possible digitalisation potentials and promotes its transformation into a process- and impact-oriented organisation.



New organisational structure

The focus on processes is also reflected in the BSI's organisational structure. The "Technical Centres of Excellence" division was established in 2019 and combines expertise and processing of central, technical long-term projects, such as artificial intelligence, secure semiconductors or cloud computing, and makes its results available to the other BSI departments. The departments use these results in order to provide customised products and services to particular target groups in government, business and society.

To support and expedite the ongoing shift to a process-oriented approach, the BSI created a "Digital Agenda" in 2019 to identify and capitalise on existing digitalisation potential. Digitalisation involves more than just the transfer of paper-based processes into the digital world. In fact, it provides the opportunity to rethink and optimise processes and – through relevant performance indicators – to make success measurable. In addition, digital solutions pave the way for more flexibility and scalability when implementing new tasks or when faced with increasing demand from the stakeholders involved. Lastly, digital databases or digital knowledge management with high synergies lay the foundations for standardised service provision at a consistently high level.

Initially, creating efficient, digitalised processes requires investments by the BSI departments, as well as by many employees. In the long term, however, this investment will pay off, as internal digitalisation will help the BSI to further enhance how it fulfils its legal obligations by positioning itself as a leading example of a digital public authority. Employees will be able to focus on their professional duties with more clarity, enabling the various teams at the BSI to continue to provide their diverse products and services to a high standard and with a strong customer focus. ■

BSI Boosts Presence and Networking

New Base in Saarbrücken and New Office in Freital

The BSI has opened two new sites over the past year. With the Saarbrücken base, the BSI is connecting with the Saarland Informatics Campus and strengthening its cooperation with European institutions. At its new site in Freital, the Federal Cyber Security Authority is taking advantage of synergies with the nearby innovation cluster around Dresden.

The BSI in Saarbrücken – a further step in shaping secure AI technology in Germany and Europe

Artificial intelligence (AI) is a key driver of digitalisation. It is increasingly being used in critical applications: be it in medical diagnostics and prognosis, for biometric identification, driver assistance systems in cars, fraud detection in the financial industry or in operation of autonomous agricultural machinery. In these and similar scenarios, security is crucial. The BSI is actively and constructively accompanying this dynamic development to ensure that AI technologies in Germany and Europe are as secure as possible. On 14 June 2021, the BSI opened a new base in Saarbrücken. The 30 team members who will eventually be employed at the site will intensify the authority's work in the field of artificial intelligence. The city is home to a number of high-level scientific institutions and research facilities that specialise in IT security and artificial intelligence, and its geographical location is perfect for forging close partnerships with other European partners.

BSI President Arne Schönbohm explains the choice of location: "Saarbrücken is the perfect base for us to research one of the most important topics of our time:

artificial intelligence. As the Federal Cyber Security Authority, we actively forge links with national research bodies. In addition, Saarbrücken is an ideal place to continue and intensify our partnerships with other European institutions, bodies and states. The BSI strives to take a worldwide leading role in shaping the design of secure AI technology. We are delighted about our new base and the opportunities it offers for our organisation. I would like to express my sincere thanks to the Saarland State Government for its assistance in setting up the new base in this wonderful city!"

The BSI in Freital – new offices in Saxony

On 1 July 2021, Federal Minister of the Interior Horst Seehofer, Saxony's Interior Minister Prof. Dr Roland Wöller, Freital mayor Uwe Rumberg, district authority head Michael Geisler and BSI President Arne Schönbohm celebrated the opening of the BSI's second office in Freital. In recent years, "Silicon Saxony" – as the region of Chemnitz-Freiberg-Dresden is known – has become a major location for the microchip industry and one of the most important centres in the European micro-electronics sector.

Saarland Minister-President Tobias Hans and BSI President Arne Schönbohm

Digitalisation and information security go hand in hand

A number of large industrial players and new research institutions have chosen the region as their base, sowing the seeds for a new centre of digitalisation in Germany in the process. As a major competence centre for information security, the BSI is helping shape the future of secure digitalisation in Germany. The team in Freital will focus on the development of secure 5G, digital consumer protection and the introduction of the IT Security Label, which is designed to create transparency around the basic security features of digital products sold to consumers. Freital is the perfect place for closely monitoring not only the development of technology, but the future of the IT security landscape. as well. The site's other focus areas will include penetration tests and technical analyses, and in it will also eventually serve as the home of the BSI Service Centre. Saxony's Interior Minister Prof. Dr Roland Wöller adds: "For the process of digitalisation to be a success, high levels of information security are essential – particularly when we are relying on technology to protect our own security. Digital consumer protection is an important topic that is relevant to all of us. This is what the BSI works on each and every day at its offices in Freital."

New opportunities for employees

The new BSI office in Freital brings synergies and benefits for many parties – and they extend far beyond the topic of cyber security. The location is another example of the Federal Government's effort to site new official buildings in areas that need infrastructural development or have been affected by infrastructural change. The creation of high-level jobs helps to guarantee a consistently high standard of living and to safeguard the future of (largely rural) regions like these. "These kinds of structural changes are the only way the state can help ensure that people can live where they want to live", said Federal Minister Seehofer at the opening of the new site in Freital. "The type of structural policy we see in action here really is a service to the people in this region."

Saxony's Interior Minister Prof. Dr Roland Wöller; Federal Minister of the Interior, Building and Community Horst Seehofer; and BSI President Arne Schönbohm

Besides strengthening IT security in Germany, the measure is expected to create a total of 205 jobs. BSI President Arne Schönbohm comments: "If the BSI site in Freital can help the entire region's ecosystem flourish, it will be a great thing for Germany as a centre of technology, for Silicon Saxony as a key location for the microchip industry in our country, and of course, for the BSI itself." The new location will open up important new possibilities for young people, too, as Freital mayor Uwe Rumberg explains: "After 1990, many towns were left facing enormous demographic decline. This new site will be a great opportunity for young people in the area." With structures like these in place, the BSI will be able to monitor technological shifts and adapt its security efforts accordingly both now and in the future. ■

Getting Better Every Day

Using the Employee Survey to Shape the "New Normal"

By Anna Breise, Section Human Resources Development

"The BSI's strength as an organisation relies on the strength of its employees. This is why it's so important that we provide a healthy working environment in which our colleagues enjoy what they do. The employee survey is a great opportunity for them to help actively shape the future of the BSI, whether openly or anonymously".

– Dr Gerhard Schabhüser, BSI Vice-President

There's an old saying that the only constant in life is change, and this is especially true of the field in which the BSI operates. In the world of cyber security, the rapid pace of digitalisation means that the demands placed on IT security are always evolving. For the BSI, this change brings a never-ending flow of new tasks and new responsibilities. Our organisation is also competing for the top talent, and prospective employees like these have specific ideas and expectations for their workplace. Since motivated employees are the backbone of the BSI, we actively examine how these challenges affect collaboration and well-being in the workplace, as well as our employees' ability to do their jobs.

The employee survey helps us evaluate these developments in a structured and holistic way. In the November 2020 survey, employees not only responded to the mandatory questions included to assess mental health risks; they were also asked to share their opinions on a number of other cultural aspects.

In the employee survey process (which is managed by the HR Development team), there are three central considerations:

1. Participation: We are enabling our employees to reach their full potential and providing opportunities to participate.
2. Holistic view: The various topics covered are interrelated and viewed as part of a connected system.
3. Transparency: Communication is designed to be open and oriented towards specific target groups across different channels and hierarchical levels.

Participation – shaping the future of the BSI

The time we spend at work accounts for a significant portion of our lives. This fact alone should be enough to encourage all employees to actively shape their chosen working environment. Topics such as health and safety and work satisfaction affect us all, regardless of our role, location or age. For this reason, employees' opinions and the diversity thereof are particularly important to the BSI. Each phase of the employee survey is designed to encourage as many employees as possible to participate. As part of the preparations for the survey, a working group was set up with representatives from the departments and committees. In a number of exploratory workshops, participants had the opportunity to discuss the challenges and come up with ideas for solutions. With the help of video conferences and digital boards, they were able to collaborate in groups effectively and interactively despite working from home.

"The results of the employee survey are a valuable source of input for us as we develop our new normal and learn more about how our employees want to work in the future. Recognising their needs is an important aspect of being able to offer attractive conditions as an employer".

Dr Ildiko Knaack, permanent representative of the Division Central Tasks

82 %
participated in the
employee survey

84%
are able to achieve a good
WORK/LIFE BALANCE

87%
think that the BSI makes
an important contribution
to society

83%
CAN TALK TO THEIR MANAGERS ABOUT PROBLEMS AT WORK

86%
can rely on
THEIR COLLEAGUES

83%
would recommend
the BSI as an employer

"As an organisation that's shaping information security in the age of digitalisation, the success of the BSI is based on respecting and valuing the contribution of each individual and on a leadership culture characterised by transparency, innovation and responsibility at all levels. The results of the employee survey will also be taken into account in the leadership development process Leadership@BSI_2025, which was launched back in 2019. This will allow us to take action where necessary while also making the many positives even better".

Anke Gaul, Head of Section Human Resources Development

Holistic view – tackling the bigger picture together

Alongside a great deal of positive feedback – including on the BSI's meaningful work, high levels of identification with the organisation, and the friendly atmosphere and good work/life balance it provides – the survey highlighted a number of topics in need of attention, such as increasing workloads. The survey showed that the organisation is on the right track in many areas and is already initiating solutions in areas such as knowledge management. In other fields, the employee survey opened up new perspectives, including on current developments such as working at the BSI during the pandemic. The fact remains, however, that singular solutions can only have a limited effect in periods of change. When deciding on such actions, it is important to take a holistic view of the BSI as a whole and identify where the findings of the employee survey need to be integrated into ongoing or planned activities. The synergies among the different areas at hand are what enable measures like these to remain effective over the long term.

Transparency – the why and the because

It isn't easy to maintain an overview of the BSI's topics and how they are all connected. Clear and continuous communication around the employee survey is critical to achieving lasting improvements, which is why our organisation always aims to include all employees in the process. Before the survey got under way, the "100 Good Reasons for the Employee Survey" campaign summarised the issues that are important to employees and what matters most to them in offering their opinions. Articles in the internal BSI News and wiki, along with video messages from senior management, showed that employee feedback was being taken seriously and factored into the BSI's decisions. At the same time, it is important to communicate that both teams and individuals can effect change in their own environment. ■

The State of IT Security in Germany in 2021

Reporting Period: 1 June 2020 to 31 May 2021

With its report on the state of IT security in Germany, the Federal Office for Information Security (BSI), acting in its role as Germany's Federal Cyber Security Authority, provides a comprehensive and in-depth annual overview of cyberspace threats.

IT security situation remains tense to critical

This year's report has again been marked by the effects of COVID-19. The impact of the pandemic throughout society has also had consequences for the working environment at almost all public authorities, organisations and businesses. Meanwhile, new challenges have arisen in information security, not least because of the tremendous increase in people working from home. In the area of malware, rapid growth has been observed in the number of malicious variants in circulation, with up to 553,000 new variants recorded on just one day – the highest number ever. The ever-widening threat landscape in ransomware remains the dominant topic.

Cyber extortion attempts becoming the number-one threat

Last year saw a significant expansion in the blackmail methods utilised by cyber criminals, who are encrypting data held by businesses and organisations in complex, multi-stage attacks aimed at extorting ransom money. While the infrastructure for the Emotet malware was successfully taken down in January 2021, the underlying threat remains. The situation report clearly shows how cyber criminals continue to hone and refine their attack strategies, and how damaging a ransomware attack can prove to be for an affected organisation. DDoS attacks, which are also used in extortion attempts, further increased in intensity and number as well.

Vulnerabilities remain one of the greatest challenges

Weaknesses in hardware and software products are and will remain one of the major challenges in the field of information security. With the technical means at their disposal, cyber criminals are capable of exploiting these vulnerabilities – often without any further input on the part of the user. A security hole in Microsoft Exchange servers that was closed in March 2021 can be seen as emblematic of the magnitude of the task at hand. Immediately after news of the hole was published, a wave of attempts at sniffing out and compromising vulnerable Exchange servers was observed. In response, the BSI raised the IT alert level to its second-highest tier for only the third time in its history. After two weeks, the number of vulnerable servers detected had been reduced from an alarming 98 percent to under 10 percent. For weeks or even months afterwards, however, servers that had already been compromised could still be used to launch damaging cyber-attacks.

The human factor

Human users of IT continue to offer an all-too-easy point of access for attacks. During the reporting period, criminals capitalised on the various uncertainties and challenges posed by recent COVID-19 developments – as well as objective and subjective time pressures and the overall dominance of the topic in society and the media – by using phishing attacks and other forms of fraud to motivate victims to disclose sensitive or personal data. Security incidents resulted not only from data leaks, cyber-attacks on video conferences, poorly secured VPN servers or the use of personal IT in a work context. They also arose due to elaborate attacks on carefully selected individual targets that had been planned over a long

RANSOMWARE/DDOS

Significant expansion of cyber-criminal extortion methods

+ 360 % data leak pages

Hush money extortion

Ransom money extortion

Protection money extortion

New trend

144 million

new malware variants

+22%

compared to 2020:
117.4 MILLION

AN AVERAGE OF
394,000
2020: 322,000

new **malware variants** every day

WITH A PEAK OF
553,000
2020: 470,000

period of time. Another crop of incidents was caused by DDoS attacks, weaknesses in cryptographic methods and hybrid threats from foreign powers and their proxies.

Without cyber security, the digital transformation will fail

Developments over the last twelve months have emphasised the growing seriousness of the threat posed by cyber criminals to our digital society and the networked world of work. The adoption of the IT Security Act 2.0 in April 2021 has further strengthened the role of the BSI and also widened its remit in detecting vulnerabilities and thwarting cyber-attacks. German lawmakers have thus recognised the growing importance of cyber and information security and worked to establish the environment needed for a secure digital transition. What we need now is a determined effort to continue pursuing this course in the face of a rapidly evolving threat landscape – one that is now also benefitting from our increasingly interconnected society. While a digitalised world offers a wealth of opportunities, it also creates many risks and a growing pool of potential targets. A new approach to digitalisation is therefore needed. Information security must be placed front and centre and form the basis of any and all digitalisation projects we undertake. The 2021 State of IT Security in Germany report is a stark reminder that the successful digitalisation of government, business and civil society can only succeed with the proper commitment to cyber security. ■

Further information:

https://www.bsi.bund.de/lageberichte

Cyber Security over the Past 12 Months

June

- Agreement between BSI and consumer protection agency
- BSI brings the topic of cyber security into Germany's EU Council Presidency
- Presentation of the Corona-Warn-App
- BSI and VDA work together for more cyber security in cars

July

- BSI publishes audit specifications for broadband routers
- BSI contributes to European standard for networked smart home devices
- Proof of security deficiencies in telematics infrastructure due to misconfigurations

August

- Argentina: Ransomware attack at immigration office results in outflow of passport data
- New Zealand: Blackmail attempt via DDoS attacks on New Zealand's Exchange (NZX)
- Blackmail attempts via DDoS attacks in the financial sector and on payment service providers
- Security requirements published for telecommunications networks
- Recommendations for the migration to post-quantum cryptography updated

September

- Ransomware attack on a university medical centre in North Rhine-Westphalia
- EvilQuest: malware targeting the Apple macOS operating system
- DDoS blackmail of Internet service providers (also in October)
- BSI team succeeds at the CHES-Challenge crypto conference
- BSI and EASA work together for more cyber security in aviation
- BSI and ProPK publish Digital Barometer 2020
- Launch of the BSI ‚Update available' podcast

October

- Cyber blackmail with sextortion campaign
- BSI and Federal Motor Transport Authority reach administrative agreement on cyber security in automotive sector
- Publication of the Cyberfibel by BSI and the'Deutschland sicher im Netz' ('Germany safe online') association
- ECSM: livestream series with the Federal Agency for Civic Education on cyber security, disinformation and deep fakes
- BSI publishes ‚Guidelines for Your Virtual Event'
- BSI publishes security requirements for online social elections

November

- Ransomware attack on Saarbrücken Airport
- Official cyber security conference for the German EU Presidency by BMI and BSI
- Symposium on digitalisation, cyber security and first-person perspectives in healthcare at University Hospital Bonn
- Cooperation agreement between BSI and Fraunhofer IAIS on joint development of audit processes

2020

Global *DDoS* blackmail campaign

2021

December

- Cyber attack on the European Medicines Agency (EMA)
- Ransomware attack on a major German media group
- USA: APT attack on monitoring provider SolarWinds
- Information Security Guideline agreed as part of the German federal government's IT consolidation project
- Chief Information Security Officer appointed for the German federal government's IT consolidation project
- First version of the Artificial Intelligence roadmap presented at Digital Summit

January

- Emotet malware infrastructure smashed
- Cyber blackmail with sextortion campaign
- Bundeskartellamt (Federal Cartel Office) and BSI work together to protect digital consumers
- Draft of the new BSI Standard 200-4 on business continuity management published

February

- Highest average daily increase in new malware variants ever measured: 553,000
- ‚Smishing' (SMS phishing) messages sent using the Android malware MoqHao
- BSI organises 17th German IT Security Congress – first to be held digitally
- Publication of the Criteria Catalogue for AI-based cloud services (AIC4)

March

- Security update for vulnerabilities on Microsoft Exchange servers
- Cyber blackmail with sextortion campaign
- BSI publishes ‚Minimum Standard for Video Conferencing Services'
- Launch of the BMI-BSI campaign #einfachaBSIchern (‚simply secure')

April

- Adoption of the German IT Security Act 2.0
- Deep-fake manipulation: successful deception of several European politicians
- EU Commission and 18 other states succeed in integrating online ID function into eID scheme
- Launch of eMergent project for digitalisation in emergency services
- Alliance for Cyber Security reaches 5,000-participant milestone
- Presentation of results of BSI business survey on working from home

May

- USA: Cyber attack (DarkSide) on IT infrastructure of Colonial Pipeline Company
- Belgium: DDoS attack on major internet service provider
- Cyber blackmail with sextortion campaign
- UP KRITIS: 750 organisations now participating in the platform
- IT-SiG 2.0 comes into force

The German IT Security Act 2.0

Second Act on Increasing the Security of IT Systems

By Dr. Martin Hecheltjen, Section IT Security and Law

> "We want to expand the BSI as the Federal Cyber Security Authority and strengthen its role as a neutral and independent advisory body for IT security matters".

This was the mandate set by the governing parties of the grand coalition in Germany in their coalition agreement dated 7 February 2018. In early 2019, Federal Minister of the Interior Horst Seehofer announced the new German IT Security Act 2.0. However, more than two years would pass before a final version was presented in the Bundestag and Bundesrat and the law came into force. Over that time, the specific content of the law was the subject of technical and political debate. The long and technically complex discussions at all levels and the significant public interest in the new rules illustrate that IT security is no longer an area of special interest for technically astute IT professionals. As the process of digitalisation continues apace, the issue has become a major point of debate in society, not least because of the large number of IT security incidents in recent years and their impact on many citizens.

The German IT Security Act 2.0 is the most comprehensive extension of the BSI Act since its inception in 2009. It represents a significant step towards strengthening network and information security in Germany. The mandates and competencies of the BSI have been expanded or refined in virtually all of its areas of work in government, business and society.

The BSI is the German body responsible for information security at the national level.

The BSI works to ensure information security in the area of digitalisation through prevention, detection and reaction. Since it was founded in 1991, it has developed from a federal IT security service provider to an inter-departmental centre of excellence for information security issues in government, business and society. The continuous development of the task areas at the BSI is now reflected in Section 1 of the BSI Act (BSIG), which states that the BSI is "the body responsible for information security at the national level".

Consumer protection and the IT Security Label

In addition to protecting federal communication technology and overseeing critical infrastructure, the BSI's tasks have included providing advice and warnings to citizens in relation to IT security issues since before 2021.

The new statutory task of "consumer protection and consumer information in the field of IT security" makes it possible for the BSI to place an even greater focus on consumer protection issues in the field of IT security in the future. In view of the increasing level of networking between everyday IT products, the responsibilities to inform consumers and develop fundamental requirements in relation to IT security for the purpose of consumer protection are crucial elements in promoting IT security in Germany.

One initial concrete measure to be taken by the BSI in the context of consumer protection is issuing IT Security Labels. In accordance with Section 9(c) BSIG, the BSI can use IT Security Labels to inform consumers about the IT security of products from specific categories it has defined.

The mark comprises two parts: a manufacturer's declaration regarding specific IT security requirements and security information from the BSI about security-related IT characteristics. Combining this information in a standard IT Security Label gives consumers a transparent, up-to-date and straightforward way to take account of the aspect of IT security when deciding to purchase IT products or services.

Improved protection for the Federal Administration

The new rules in the German IT Security Act 2.0 also markedly improve the protection the BSI provides to the Federal Administration.

Section 4(a) BSIG, for example, tasks the BSI with monitoring federal communication technology. This new rule enhances the role of the BSI as the body responsible for IT security within the Federal Administration. It also enables the BSI to actively promote a consistently high security level across the federal IT systems.

These powers of oversight are complemented by the BSI's responsibility to define binding minimum standards for federal IT security in consultation with the relevant departments. Working together with the departments will make it possible to establish a fundamental IT security level that is consistently high across the board.

Alongside these preventive competencies, the options available to the BSI in detecting and protecting against IT attacks on government networks have been expanded. In recent years, the types of attack have become increasingly complex and diverse. In particular, analysis of past attacks within the Federal Administration has shown that specialised cyber attacks known as advanced

persistent threats (APT) can take place over a period of years. The retention period for log data relating to federal communication technology has been extended to 18 months to effectively counter the subtle methods intrinsic to such attacks and of address incursions that are discovered at a later point in time. The BSI has also received additional powers regarding the processing of internal public-authority log data, which is highly significant when it comes to detecting and analysing ongoing attacks and reconstructing past attacks on federal IT and communication technology.

Expansion of detection measures and operational cyber defence

The analysis of malware and vulnerabilities for the purpose of advising and warning affected parties is a fundamental task of the BSI. To ensure such advice and warnings are even more comprehensive and effective in the future, the BSIG has expanded the BSI's authority to detect and analyse malware and methods of attack. In accordance with Section 7(b) BSIG, the BSI is thus now able to implement measures to find known vulnerabilities in public interfaces of federal IT systems, critical infrastructure, digital services and companies that are of particular public interest. In line with the BSI's fundamental conviction that every vulnerability must be addressed, the results of these measures may be used only to immediately inform the affected parties.

The BSI has also been given the authority to issue instructions to telecommunications and telemedia providers to avert specific IT security threats. Even before the German IT Security Act 2.0 came into force, service providers had the power to restrict, redirect or prohibit the use of telecommunications services in the event of a fault in order to repair or prevent an impairment under Section 109(a) of the Telecommunications Act (TKG, Telekommunikationsgesetz). To protect against particular risk situations, the German IT Security Act 2.0 gives the BSI the option to use this existing mechanism by requesting that providers implement the measures required in each case.

Until now, the BSI did not have the authority to request that telemedia providers take measures to safeguard telemedia services in an appropriate manner in line with the current state of the art. Section 7(d) BSIG now enables the BSI to request that the operator of a telemedia service – e.g. a website – take appropriate protection measures if this service has inadequate protection and represents a considerable threat. This gives the BSI an effective way to counter threats such as "drive-by downloads" from malicious online ads.

Extension of KRITIS competences

The German IT Security Act 2.0 adds a new target group, „companies of particular public interest", to the BSIG. The new rules on companies of particular public interest in Section 8(f) BSIG cover companies in three different categories. As defined by the BSIG, companies of particular public interest are:

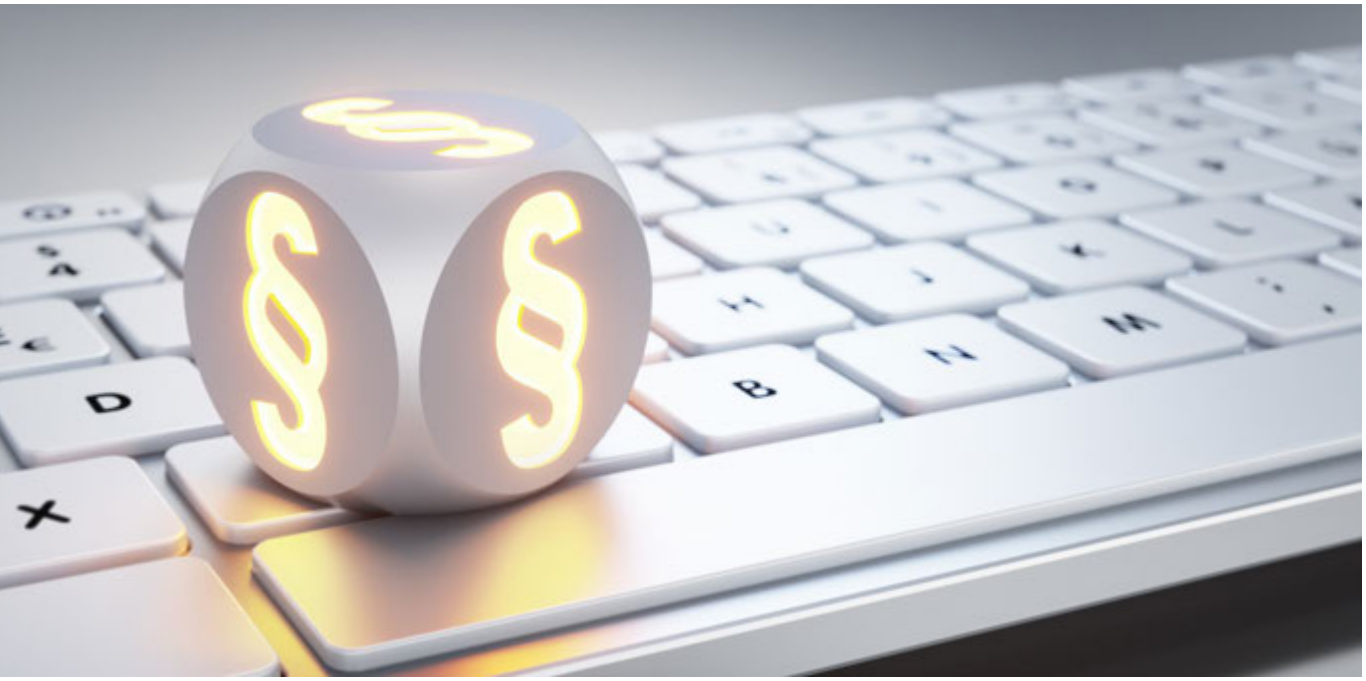
1. Companies covered in the scope of Section 60(1) Sent. 1 and 3 of the Foreign Trade and Payments Ordinance (AWV) (e.g. defence contractors, producers of IT products for processing classified material)
2. Companies that are among the largest in Germany on the basis of the value they generate domestically, as well as suppliers that are particularly important to such companies due to their unique characteristics
3. Operators of a higher class of operating area as defined in the Hazardous Incidents Ordinance (Störfall-VO) or an equivalent operating area

Due to the type of goods and products manufactured (armaments), the handling of materials with particular hazard potential or the economic damage that could be caused by cyber attacks or other IT faults, there is a particular public interest in protecting these companies. While classification in categories 1 and 3 is clearly defined by the scope of the AWV or Störfall-VO, further specification is required for category 2 with regard to which companies should be considered to be of particular public interest. This specification will be implemented through a corresponding ordinance comparable to the BSI CI Ordinance (BSI-KritisV).

Companies have different responsibilities depending on how they are classified in the categories. Companies in categories 1 and 2 must submit a self-declaration to the BSI every two years regarding their IT security. On this basis, different tasks arise relating to certification in the area of IT security and other security audits or inspections, as well as special protective measures for IT systems, components and processes requiring particular protection. At the same time, these companies must register with the BSI and designate a point of contact when submitting their first self-declaration. For companies in category 3, registration is voluntary. However, all these companies have a reporting obligation in relation to disruptions in the availability, integrity, authenticity and confidentiality of their IT systems, though in a category-specific form.

Milestone on the road to digitalisation in Germany

The German IT Security Act 2.0 is an important milestone on the road to successful digitalisation in Germany, but it is not the final destination. The Bundestag has already provided initial impetus for the continued development of IT security legislation in the form of a motion for a resolution for this law. Meanwhile, the highly charged debate involving industry associations and other organisations in civil society regarding this law has offered some important starting points for the further development of the BSIG. In addition, there is already a regulation at the European level that is currently being agreed in the form of the NIS 2 Directive. This will also have a major impact on German IT security legislation, particularly the BSIG.



In addition to the introduction of new rules for companies of particular public interest, the competencies of the BSI in relation to critical infrastructure have been expanded. The municipal waste disposal industry has been added to the BSIG as a CI sector, and the BSI has been given the ability to request submission of all documents required to assess a company's CI status. If the BSI finds that a business meets the critical infrastructure criteria, it can be registered by the BSI as CI. These measures significantly strengthen the BSI in its supervisory role in the area of critical infrastructure.

Just as digitalisation continues to change our everyday lives, it is necessary to continuously develop IT security law and adapt it to the new tasks and challenges at hand. The BSI is ready to join partners from business and society in contributing its expertise to the task of shaping the ongoing change process brought about by digitalisation. ■

IT SECURITY IN PRACTICE

The IT Security Label

Shaping Information Security for Manufacturers and Establishing Transparency for Consumers

By Joshu Wiebe, Head of Section Granting of IT Security Labels

When the German IT Security Act 2.0 came into force on 28 May 2021, it gave the BSI a mandate to introduce a voluntary IT Security Label. It is intended to improve consumer transparency by making the security properties promised by manufacturers of digital products and services transparent to customers and by providing up-to-date security information on aspects like updates and vulnerabilities.

Why does the IT consumer market need greater transparency?
Products that are connected to the Internet – such as "smart" vacuum cleaners, watches or virtual language assistants – are intended to make life easier and have now become little helpers for our everyday lives. They are part of the "Internet of Things" (IoT). As these devices become accepted members of many citizens' households, more and more areas of daily life are becoming digitalised.

Meanwhile, data is also being collected and sensors are making it possible to gain in-depth insights into our private lives. Normally, such devices only use the collected data for the purposes to which users have consented. To ensure there is no unwanted access to the data and functions of devices, their manufacturers need to protect them with suitable security functions and regularly apply security updates.

When purchasing IT products, it is often difficult for customers to determine which security functions they have and how long security updates will be available. Consumers want more information about how these devices are protected. In a representative online survey conducted by the Federal Ministry of the Interior and the BSI on Safer Internet Day 2020, 77.3% of the participants cited a need for such details.

The BSI Digital Consumer Protection Report provides information on the findings of a company that specialises in the security of IoT devices. In December 2020, this company reported there were a total of 7,339 vulnerabilities in just six consumer products: a smart speaker, a messenger for children, a drone, a smart home camera system, a pet monitoring camera and a streaming device for children. Due to insecure remote maintenance features, a lack of encryption, and out-of-date software with known vulnerabilities, these products fulfilled "not even basic security characteristics".

Another finding that fits this picture is the fact that one in four people in Germany has been a victim of cybercrime, according to a survey of citizens conducted by the BSI for the Digital Barometer 2020. Here, it comes as little surprise that people who own more devices are more frequent victims of cybercrime.

The BSI is confronting the problem with the IT Security Label in order to improve transparency in the market for consumer IT products. This enables citizens to easily identify the basic IT security characteristics of products and take them into consideration when making a purchase decision.

How does the IT Security Label work?
This voluntary approach gives manufacturers a way to declare that their products conform to IT security specifications issued or acknowledged by the BSI for the IT Security Label. This declaration includes the manufacturers' assurance that its products have been tested in accordance with the underlying standard and meet its requirements.

When granting the IT Security Label, the BSI conducts a plausibility check of the manufacturers' application and declaration. This gives the BSI an idea of whether the information provided by the manufacturer and the testing methods and safeguards it implements seem transparent and plausible. If applicable, the BSI can also take account of known problems (e.g. vulnerabilities) with the product in question or any prior incorrect behaviour on the part of the manufacturer (e.g. product warnings) in the approval process. The BSI can also withhold approval of the IT Security Label, if there are serious doubts about the manufacturers' declaration, regardless of the documents submitted.

It is important to note that unlike in a certification process, the BSI does not initially check whether a given product meets the relevant requirements as promised when conducting the approval process for the IT Security Label. This is done after approval in a process referred to as market surveillance.

Market surveillance may be conducted with or without a relevant reason. In cases that do not involve a relevant reason, the BSI follows a systematic inspection concept (e.g. random sampling) to determine whether the requirements of the IT Security Label have actually been met.

In other cases, a relevant reason to conduct market surveillance might involve information the BSI receives about vulnerabilities or other circumstances suggesting that a product no longer meets the requirements of the IT Security Label. However, the BSI can also carry out its own technical checks or request more detailed evidence from the manufacturer.

Given that IT products can become more susceptible to attacks over time as new vulnerabilities become known, it makes sense to apply continuous market surveillance after issuing the IT Security Label.

Based on its findings in these efforts, the BSI provides relevant security information. Such security information is a main component of the IT Security Label and is integrated into BSI information pages on the respective products. The link to the security information for each product is displayed as text and QR code on the product-specific IT Security Label. This makes it easy for consumers to take this information into account when making a purchase decision. It is a centralised and easily accessible way of showing identified corresponding vulnerabilities or available security updates, that should be installed. This content is updated depending on the findings of the BSI.

The BSI thus provides convenient information on the security of specific products and the related functions guaranteed by their manufacturers. Current and security-relevant information, such as on vulnerabilities and security updates, is also provided. In this way, the IT Security Label helps make the security of consumer IT products more transparent. ■

Further information:

www.bsi.bund.de/IT-SIK.

Digital Consumer Protection Report

A Close Examination of Cyber Security in the Digital Consumer Market

By Stephanie Hartmann, Section Safe Consumerproducts and -services and Market Monitoring and Jörg Hübner, Section Basic Issues of Digital Consumer Protection and Cooperations

The Federal Office for Information Security (BSI) is shining a new spotlight on key issues with the "Digital Consumer Protection Report". It is the first publication in Germany that methodically and from now on annually provides an assessment of information security in the consumer market, takes a closer look at key focus areas and current developments, and outlines action areas to better protect consumers in everyday digital life. For the 2020 reporting year and in view of the ongoing pandemic, the topic of cyber security in the healthcare sector was selected as focus area and examined in greater depth.

In the middle of this year, the "Digital Consumer Protection Report 2020" was published with the intention of addressing institutional information multipliers in consumer protection, among others. These include consumer advice centres, associations and organisations, but also public authorities that need to be made aware of the challenges of digital consumer protection and with whom shared action areas should be actively developed.

A systematic literature review, media research and further empirical analyses were conducted to take a close look at digital consumer protection in 2020. As part of this process, experts reviewed and assessed IT security incidents related to consumer protection and other trend developments. In addition to this – and forming the main focus of the report – was an in-depth investigation of health apps.

"Only minimal research is required to find indicators of consumer threat in the digital sphere in 2020." This statement from the report highlights both how frequent and how diverse the IT security risks are that consumers are exposed to in their everyday digital lives. What are the key findings of the report?

Focus topic: health

The past year was characterised by challenges for society as a whole, which have influenced the digital world with huge momentum and had a lasting effect. Whether dealing with intelligent information or interaction in the health sector, focusing on e-learning in education or the networked home office as a new priority in everyday working life – the global coronavirus pandemic has undoubtedly accelerated development that is constantly opening up new targets for attack as digitalisation progresses. Many consumers had a greater need for information, particularly at the start of the pandemic – and cyber criminals used this to their advantage. In North Rhine-Westphalia alone, more than 1,200 reports of crime related to the pandemic were received by mid-September 2020. For example, criminals pretended to be medical experts, virologists or service providers and circulated fake websites and e-mails. If you opened certain e-mail attachments or websites, your connected device was infected with hidden malware.

Setting aside the coronavirus pandemic, the health sector itself represents a large application area for digital products and services. For example, mobile health applications in particular have become a trending topic in the digital consumer market in recent years. The increasing popularity of wearables, such as fitness trackers and smartwatches, has promoted this development. As personal health and body data have increased protection needs it is particularly important to maintain high IT security standards to ensure the confidentiality, availability and integrity of the data and the system.

Through its market monitoring in digital consumer protection and as part of a study that is presented in more detail in the report, the BSI has conducted an in-depth examination of selected consumer apps in the health sector that are neither medical devices nor listed in the "Directory of Digital Health Applications (DiGA)". The health apps market is highly dynamic and lacks transparency. However, a survey of service providers made it clear that essential IT security principles such as security by design, mandatory update regulations and processes for dealing with vulnerabilities are not given sufficient consideration during the development and marketing of such apps. Technical analyses of selected apps showed that it was possible to intercept, read or manipulate communication – for example, through a lack of certificate pinning or the transmission of passwords that are not hashed.

Action areas

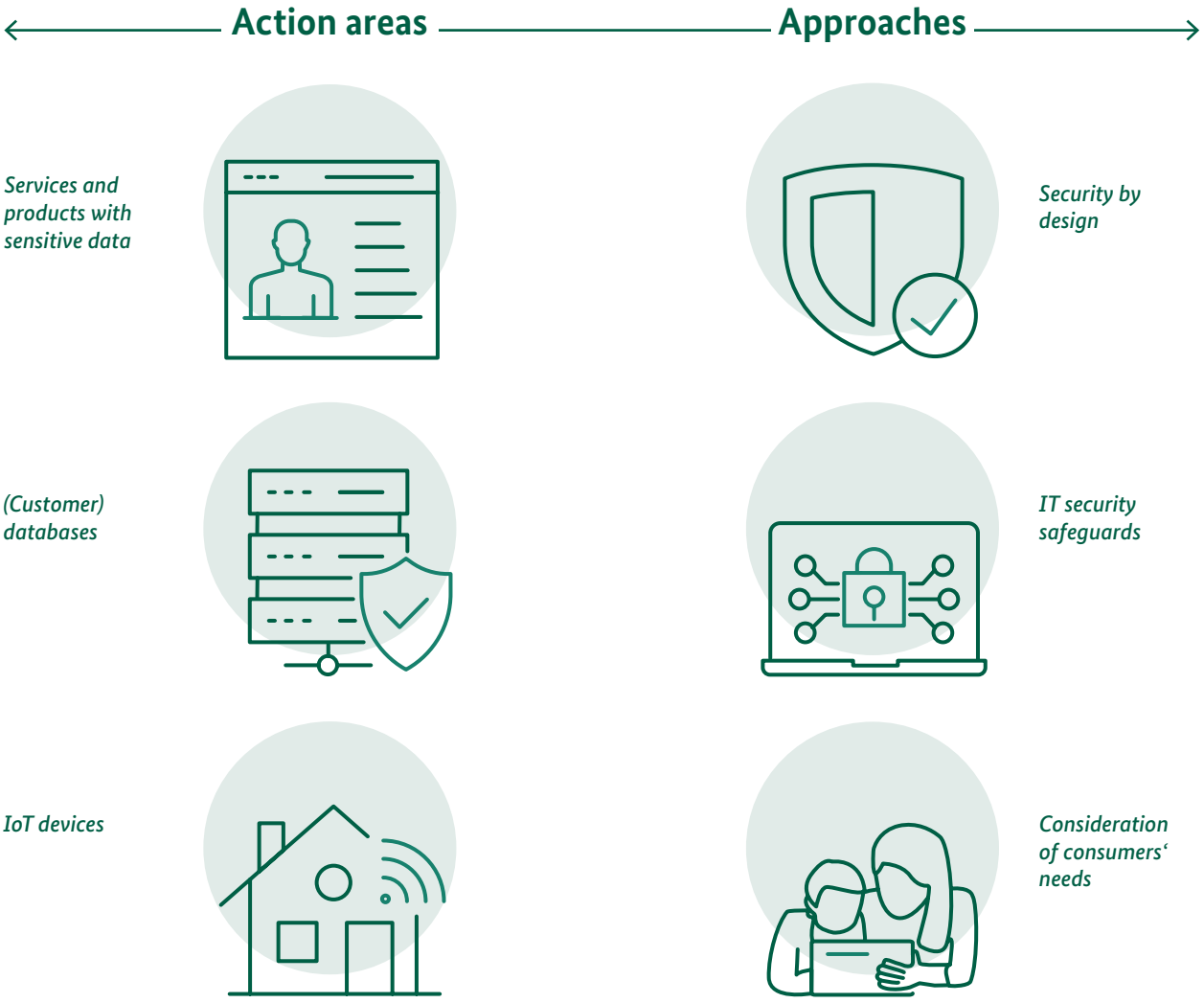
In addition to health apps, the current report outlines that a large number of products and services that handle sensitive data generally do not have adequate IT security precautions in place. In the period in question, several incidents were reported in which consumers were exposed to considerable security risks: Internet of Things (IoT) devices, particularly smart home technologies, play a major role in this regard. While these products are popular with users because of their 'smart' features, they frequently contain known open vulnerabilities and exhibit insufficient security features in their product design. For example, an analysis performed by a company specialising in IoT security found over 7,000 vulnerabilities in six selected products alone.

Unsecure (customer) databases are a further source of danger, as consumers are defenselessly exposed to potential data leaks. Such data leaks are made public on an almost daily basis. In this respect, we urge providers to take appropriate technical and organisational precautions to achieve better information security and to minimise the risk of customer data falling into the hands of criminals.

Approaches

In many cases, even the simplest safeguards are sufficient to minimise security risks. The BSI continuously advises companies and manufacturers on the fundamentals of IT security safeguards and how to implement them. Manufacturers are urged to focus on the concept of security by design right from the design stage of products and services to establish secure consumer products and services on the market. In addition, proper IT security management and implementing the IT-Grundschutz helps protect the data of both companies and their customers. A large number of other safeguards, such as implementing technical guidelines and standards, which establish important security features and protection mechanisms as standard, provide the basis for information security that is "built in" right from the product development stage. The analysis and target-group-appropriate preparation of consumer needs by providers and manufacturers themselves as well as by other stakeholders such as associations, societies and government institutions cannot be ignored, as the findings produced can pave the way for the secure use of digital products and services through holistic approaches.

A first in Germany: From now on, the "Digital Consumer Protection Report" will examine information security in your personal everyday digital life on an annual basis. (cover image)



Action areas and approaches for better digital consumer protection

Outlook

Digitalisation offers consumers tremendous opportunities to make everyday life easier and more convenient. Digitalisation and information security are two sides of the same coin. This means that information technology and the associated security risks in the digital consumer market and consumer environment must be considered at every point of development, marketing and consumption processes. Consumers as well as economic, governmental and societal stakeholders have shared responsibility in this respect.

The "Digital Consumer Protection Report" for the upcoming 2021 reporting year will once again address recent IT security incidents and continue to monitor the development of IT security risks for consumers in order to derive among other aspects actions for the BSI. Similarly, there will be a focus on new security issues and trends in the digital consumer market. In addition, the BSI investigates the needs, competencies and expectations of digital consumers on an ongoing basis to obtain and share insights for holistic digital consumer protection. ■

Download the "Digital Consumer Protection Report 2020" or find out how to order a printed copy at:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/lageberichte_node.html

Well Prepared for the Next Emergency

IT-Grundschutz Adds Many Auxiliary Resources to BSI Standard 200-4

By Cäcilia Jung and Daniel Gilles, Section BSI Standards and IT-Grundschutz

From cyber attacks to the coronavirus pandemic or natural disasters, companies and public authorities are always exposed to risks that could interrupt their business operations. Time-critical business processes are suddenly brought to a standstill and no one knows what to do. In BSI Standard 200-4 and various new auxiliary resources, the BSI provides practical and advanced guidance on establishing a business continuity management system (BCMS). This article offers a brief overview of the auxiliary BCM resources available from the BSI.

When an emergency strikes, it is often hard to know what to do. It is also usually impossible to dismiss the possibility that an interruption of time-critical business processes could cause substantial damage, or even cause a business to fold. Business continuity management systems (BCMS) have become established as a way of protecting against this risk. A BCMS is partly a preventive measure to reduce the risk of such an emergency happening in the first place. However, it also ensures that an institution is prepared to respond to potentially damaging events and remain operational in a crisis or emergency.

One major challenge in this context is the question of how many resources should be expended on a BCMS. Particularly in companies, this often involves making some tough cost/benefit calculations; after all, even the best possible protection is useless if the costs involved make it impossible to operate economically. Meanwhile, public authorities also have limited resources. This means implementing a BCMS in the most economical way possible is essential.

A simple entry point into BCM

In view of the above, one of the main goals in updating BSI Standard 100-4 to BSI-Standard 200-4 was to formulate practical implementation instructions. The new standard is aimed at less experienced users and intended to provide a simple entry point into the field of BCM. However, it also addresses BCM professionals, who will soon be able to access a requirements catalogue in the auxiliary resources that enables quick and effective conformity checks to the requirements from BSI Standard 200-4.

The auxiliary BCM resources make it much easier to work with BSI Standard 200-4. They are a continuation of the auxiliary resources from the implementation framework (UMRA) for BSI Standard 100-4 and can be classified in the following three categories:

- Normative annex (requirements catalogue and glossary)
- Document templates for key documents required in BSI Standard 200-4
- Additional information

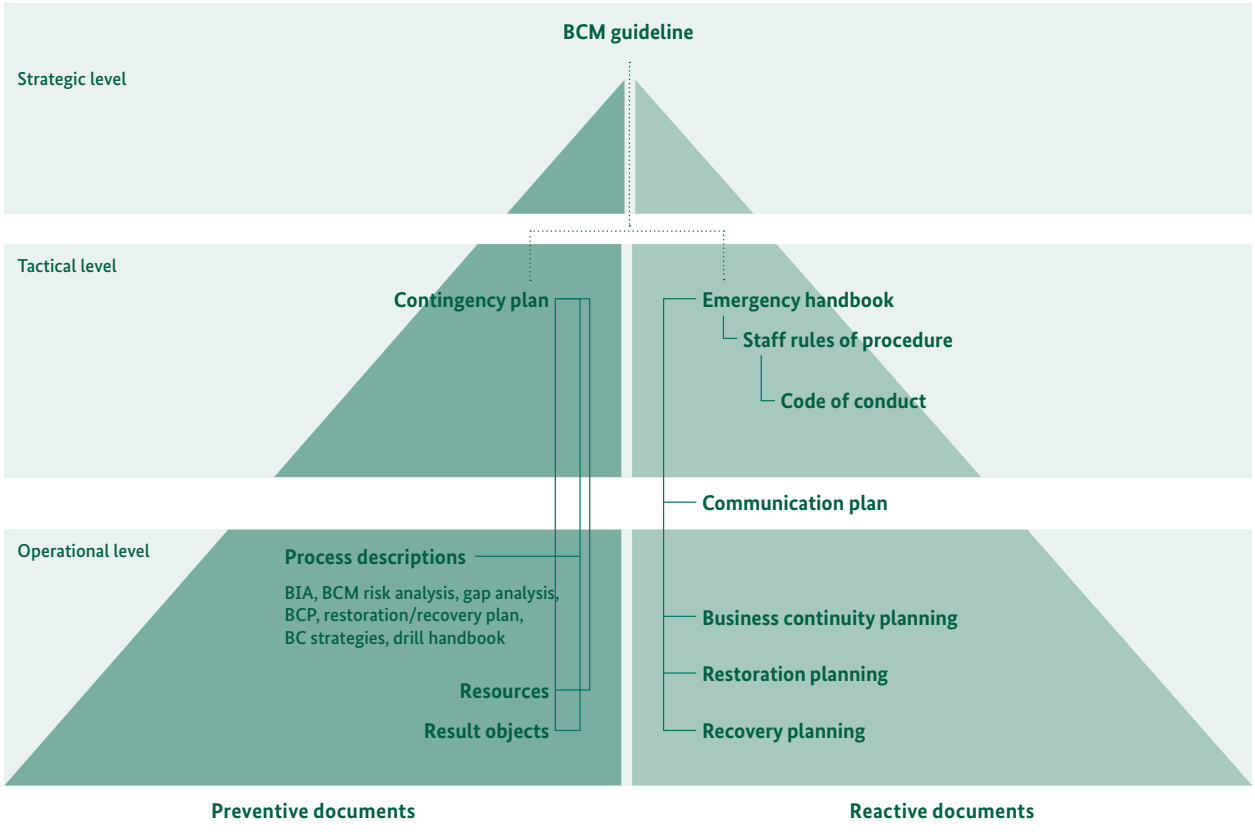


Figure 1: Document pyramid for BSI Standard 200-4

Document templates for guidance and structure

BSI Standard 200-4 puts the requirements from ISO 22301:2019 in concrete terms and recommends a specific document structure (see Fig. 1) that serves as a practical guide for users. For many of these documents the BSI also offers support in the form of document templates that include example texts. Users can adapt the templates and example texts to match their own institution and thus automatically meet numerous requirements of BSI Standard 200-4. The benefit of this approach is that it significantly reduces the amount of work involved in handling documents.

Feedback for the IT-Grundschutz team

The auxiliary resources for BSI Standard 200-4 are published as community drafts and are supplemented and updated on an ongoing basis. Comments and suggestions on the auxiliary resources and BSI Standard 200-4 itself can be sent to grundschutz@bsi.bund.de.

Additional information

Since the scope of a standard reference work is limited, the BSI has published additional aspects of the treated topics in the auxiliary resources for Standard 200-4. These provide further information on BCM tools, proposed BC strategies, further aspects of incident or crisis response (see "Side note on crisis management: analogue crises vs. IT crises") and many other useful publications. For example, the document "Suggestions for BC-Strategies" explains some specific ideas for how users can develop successful strategies and solutions. ■

Side note on crisis management: analogue crises vs. IT crises

Crisis management is a complex and extensive topic that cannot be covered completely in BSI Standard 200-4, since a separate crisis management system is required for this purpose. However, BSI Standard 200-4 fundamentally enables institutions to manage crises caused by an interruption of time-critical business processes through an appropriate incident crises response structure.

Further information on crisis management can be found in the auxiliary resource "Further Aspects of Incident and Crisis Response". Along with example proposals on the structure of incident and crisis committees, it looks at the particular features of IT crises. Such crises, and in particular cyber attacks, are very different from conventional analogue crises (see Fig. 2). Generally, they are not restricted to a particular location and develop and spread much faster and more dynamically. Furthermore, they are not always immediately recognised, and they are characterised by attack scenarios (e.g. targeted cyber attacks) that are much less common in a comparable form in analogue environments.

Key differences between non-digital and IT-related crises

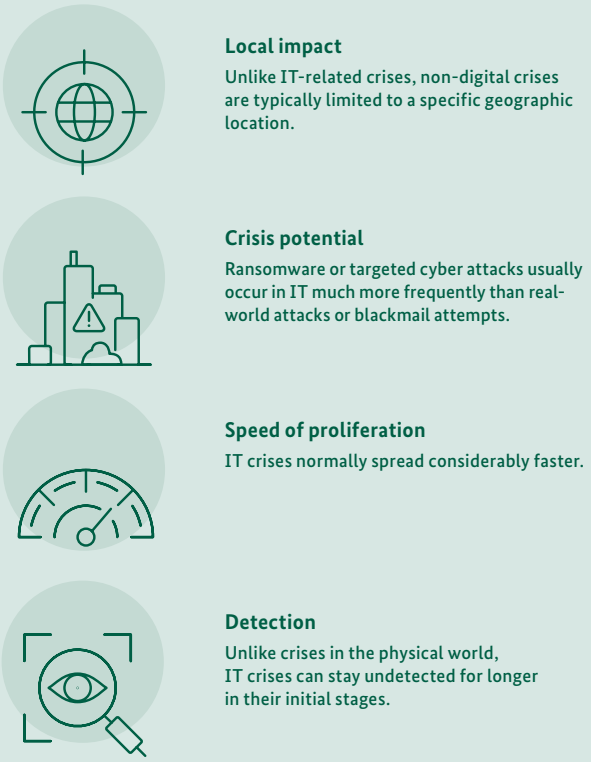


Figure 2: IT crises versus non-digital crises

BSI INTERNATIONAL

Strengthening Europe's Digital Sovereignty

The European Competence Centre, the National Coordination Centres and the Cyber Security Community

By Sirko Höer and Heiko Siebel, Section Technology and Research Strategy

As people's everyday lives and the business processes in organisations become more and more connected with digital technologies, it becomes even more important to enhance the skills needed to protect against cyber security incidents. The European Union is aiming to take a leading role in this regard by strengthening its own digital sovereignty.

When it comes to research, technologies and industrial development in the field of cyber security, the activities currently under way in the EU are extensive. However, these activities are often restricted to certain regions, industries and business areas, or to companies of a certain size. The EU is set to enable closer coordination across these areas in the future to combine resources, leverage synergies and achieve a consistent and competitive cyber security level.

The European Cybersecurity Competence Centre

Through Regulation 2021/887, the European Commission resolved to set up a European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC, referred to as the "Competence Centre" below). It is also establishing a Network of National Coordination Centres (NCC) in the EU Member States. The Competence Centre is based in Bucharest and will become the EU's most important instrument for combining investments in research, technology and industrial development in the field of cyber security. This includes implementing cyber security products, services and processes. In particular, there will be better coordination between the plans for the European funding programmes Horizon Europe and Digital Europe in the area of cyber security. In all these activities, there needs to be a particular focus on the concerns of small and medium-sized enterprises (SMEs), as well as start-ups.

The Competence Centre will be administered by the Member States and the European Commission. A governing board made up of members of the Commission and representatives of the Member States has been set up for this purpose. The BSI is Germany's representative on the governing board. The board is responsible for controlling the strategic direction of the Competence Centre's activities and ensuring that its tasks are in line with the aforementioned Regulation.

Unlike Computer Security Incident Response Teams (CSIRTs) and CSIRT networks, the Competence Centre will not undertake any operational cyber security tasks

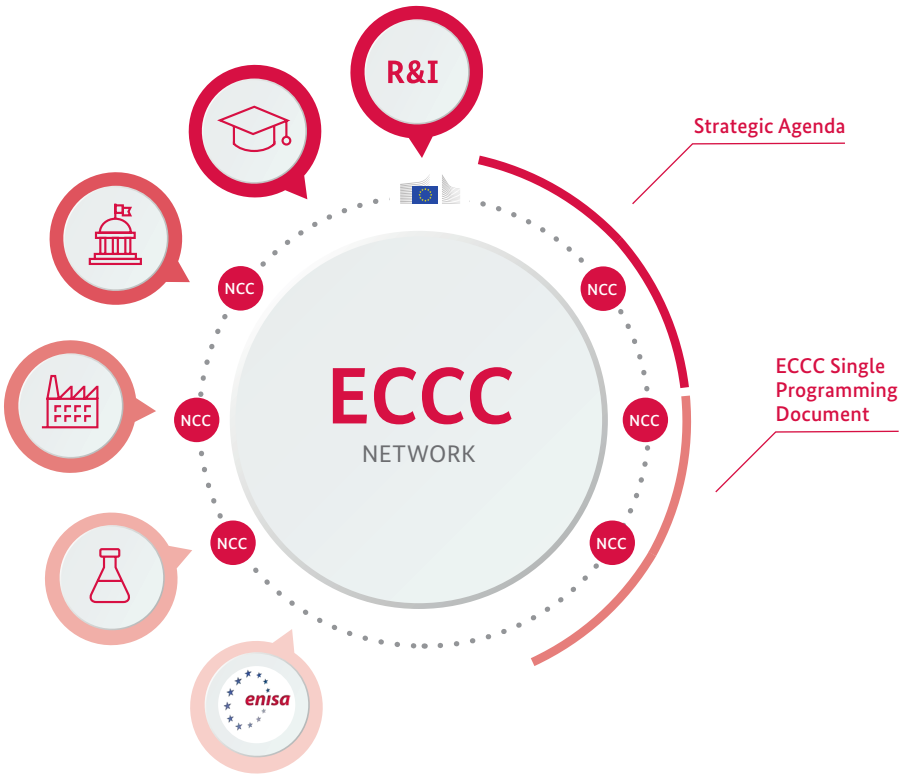


Figure: ECCC

such as detection and management of incidents. However, the Competence Centre needs to be capable of facilitating the development of digital infrastructure in the service of business – particularly SMEs, the research community, civil society and the public sector – based on the mandate and goals of the Regulation.

Goals and vision

The Competence Centre's primary goals include strengthening the EU's leading role and strategic autonomy. It will do so by preserving and developing capacities and capabilities in the field of cyber security. In addition, the Competence Centre focuses on increasing the global competitiveness of the cyber security industry and guaranteeing high cyber security standards.

The European Network of National Coordination Centres (NCCs) will ramp up the sharing of information among the Member States so that the identification and agreement of potential international project partnerships can be accelerated. The National Coordination Centres will promote such exchanges among relevant national bodies in research and business in the areas of cyber security and cyber defence within the Member States. This will consolidate the flow of information to the Competence Centre so that the best possible support can be offered to the relevant national cyber security communities. Another goal of the National Coordination Centres is to promote and spread educational programmes in the area of cyber security.

The European Union Agency for Cybersecurity (ENISA) is also involved as an advisory partner to the Competence Centre and the National Coordination Centres.

The National Coordination Centre for Germany

The German National Coordination Centre for Cyber Security in industry, technology and research (NKCS, the German NCC) is a joint virtual institution involving the Federal Ministry of the Interior, the Federal Ministry of Education and Research, the Federal Ministry for Economic Affairs and the Federal Ministry of Defence, as well as certain subordinate departments. The role of the BSI will be to act as the lead body and single point of contact.

The goal of the NKCS is to provide a national information platform for all interested parties, to promote networking in the German cyber security community and to offer initial advice on issues relating to cyber security research and development, including projects with a European perspective. ■

Further information:

EU Regulation 2021/887
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32021R0887&qid=1623142941122

Horizon Europe
https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

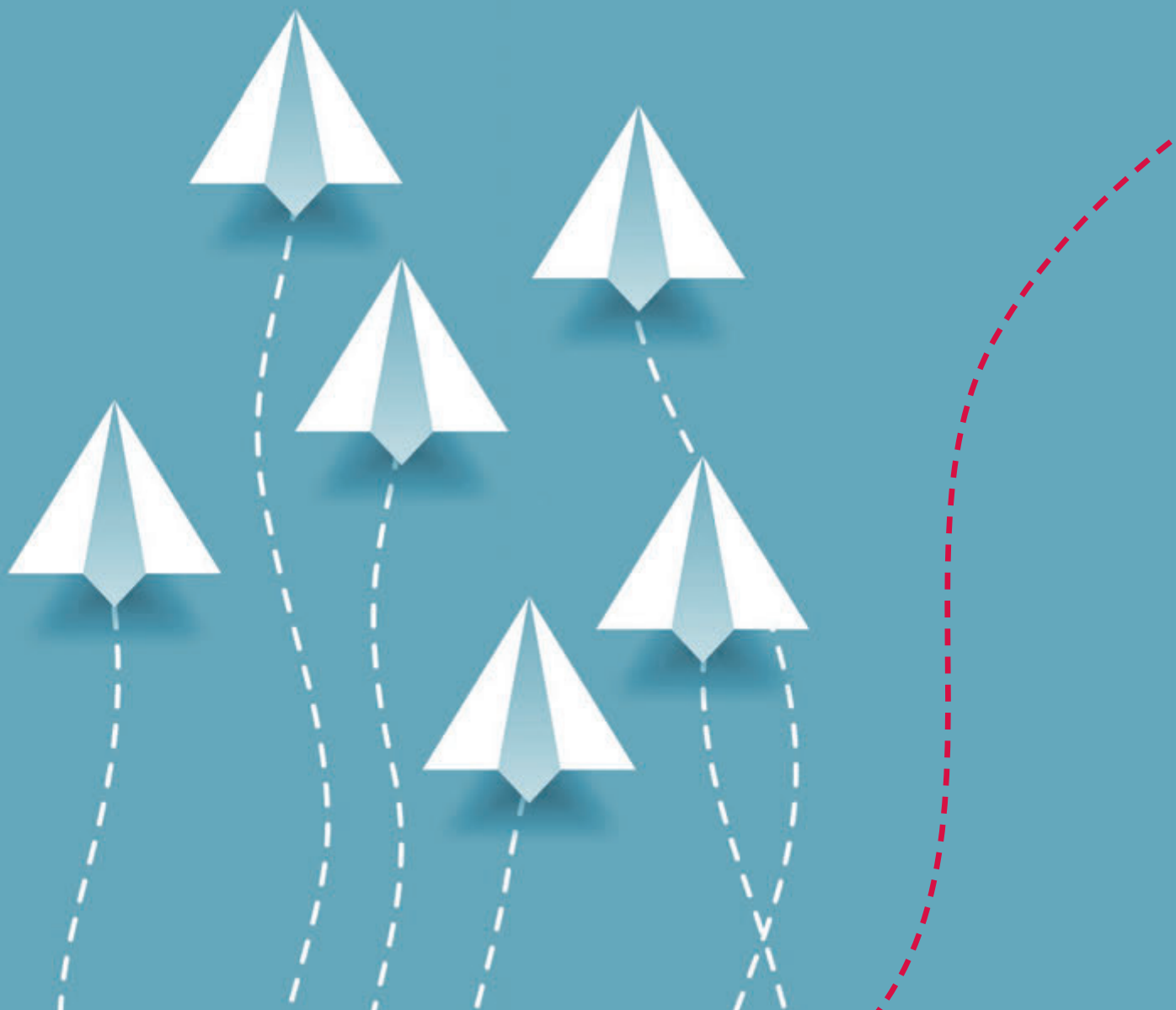
Digital Europe
https://digital-strategy.ec.europa.eu/en/activities/digital-programme

The European Citizens' Initiative

Online Collection Systems for European Citizens' Statements of Support

By Yona Raekow, Head of Section Certification according to Technical Guidelines

Since 1 April 2012, the European Citizens' Initiative (ECI) has been an essential instrument for participatory democracy in the EU. One million EU citizens living in a quarter (at least seven) of the Member States contribute by using this instrument to make their voices heard in Brussels: EU citizens can call on the European Commission to propose new laws. In general, the right to submit an ECI is similar to the right of initiative of the Parliament and the Council. In order to undertake an ECI, you must go through the following stages:



1 Citizens' committee
The first step of launching an ECI is establishing a group of organisers, the "citizens' committee". This committee must be made up of at least seven people living in at least seven different Member States. The committee serves as the Commission's point of contact for the ECI.

2 Registration
First, the ECI must be registered with the Commission. The Commission decides if the initiative will be registered within two months. Registration is refused if the procedural requirements are not fulfilled or if the initiative is not within the scope of the Commission's power to bring forward a proposal for a legislative act. It will also be refused if the initiative is manifestly frivolous, abusive or vexatious, or is contrary to the values of the EU. Registered initiatives are published on the Commission's online portal.

3 Collection of statements of support
Once the ECI has been registered, organisers can start collecting statements of support. They have 12 months to collect the minimum number required. Statements of support can be collected on paper or online.

Since 2020, the Commission has provided a central online collection system (OCS), which European Citizens' Initiative organisers can use free of charge. As an alternative to the central OCS, organisers also have the option to collect statements of support online via individual self-developed online collection systems. However, these individual OCS must be certified by the responsible authority of the member state in which the system is operated before they can be used. In Germany, the responsible authority for certifying this type of OCS is the BSI.

4 Verification of signatures
Once the organisers have collected the minimum number of statements of support required (more than 1 million in at least seven different Member States), they must submit them to the responsible national authorities. In Germany, this is the Federal Office of Administration. The authority is responsible for validating the statements of support and certifying the number of valid statements.

5 Submission and examination
At this stage, organisers must submit the relevant certificates from the national authorities.

6 Receive response
If sufficient signatures are successfully collected for the initiative, the Commission must immediately publish it in a register and meet with the organisers at the appropriate level so that they can explain the details of

Figure: Phases of the EBI

their application. After an exchange of views with the Commission, the organisers are given the opportunity to present the initiative at a public hearing held by Parliament. The hearing is organised by the committee responsible for the subject matter of the citizens' initiative. In the ideal case, the Commission will follow on from this with a legislative initiative.

Remit of the BSI

The BSI is responsible for certifying the conformity of individual OCS. An individual OCS is made up of

- the technical platform (hardware, software, host environment),
- business processes,
- employees and
- infrastructure

both at the ECI organisers and at the hosting provider and commissioned data processor. The applicant must provide the required documentation of compliance of an individual OCS with the ECI Regulation for all elements of the system.

The BSI first checks that the submitted evidence is complete, i.e. whether all requirements have been substantiated by suitable evidence. It then performs a substantive check based on EU Commission specifications.

If necessary, the BSI is authorised to request additional documents, amendments or corrections. In addition, the BSI can arrange on-site audits at the applicant's or the hosting provider's sites and perform practical tests with the OCS (e.g. vulnerability/penetration tests). If the process is completed successfully, the BSI issues the certificate.

Pending initiatives

To date, six initiatives have achieved the required number of signatures ("Right2Water", "One of Us", "Stop Vivisection", "Ban Glyphosate", "Minority SafePack – One Million Signatures for Diversity in Europe" and "End the Cage Age") and have been submitted to the Commission. Since the ECI was launched, 107 applications for registration have been submitted as of August 2021, of which the Commission has registered a total of 82 initiatives. From these 82 initiatives, the BSI certified the conformity of the OCS used on 20 occasions. ■

Further information:

https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Leistungen-und-Kooperationen/Europaeische-Buergerinitiative/Europaeische_Buergerinitiative/europaeische_buergerinitiative_node.html

https://europa.eu/citizens-initiative/_de

New Impetus to Strengthen the Digital Single Market

Current Developments in European Cyber Security Certification

By Diana-Victoria Menzel and Patrick Seidel, Section Expert Committee Work and Quality Management for Evaluation and Certification Processes

Since 2019, work has been ongoing to establish a common European framework for cyber security certification to strengthen the Digital Single Market. The BSI has been playing a major role in this, but also needs to accomplish some organisational developments.

Cyber security certification has always been a subject area in which different interests are represented. On the one hand, certification is used to consider the interests of manufacturers to enable them to remain competitive on the market with their products. On the other hand, the interests of legislators who created the necessary framework conditions are specified in detail. And last but not least, the interests of consumers are considered, as independent certification enables them to better assess products available on the market.

The European Commission has taken these different interests into account to prepare the EU Digital Single Market for the challenges of the coming decades. By implementing the EU Regulation 2019/881 also known as Cybersecurity Act (CSA) which came into force in summer 2019 a solid foundation for the joint development and recognition of the European cyber security certification framework is provided. The CSA also strengthens both trust among each other and in the Digital Single Market.

Division of responsibilities as specified by the CSA

The CSA specifies that all European Member States must appoint a National Cybersecurity Certification Authority (NCCA). The IT Security Act 2.0 (German: IT Sicherheitsgesetz 2.0), which passed the German Bundestag in May 2021, appoints the BSI according to Paragraph 9a as the German NCCA . Based on that, the NCCA is divided into two areas of responsibility within the BSI: certification and supervision.

In its role as the certifying NCCA, the BSI is the only certification body in Germany according to the German IT-Security Act 2.0 that issues cyber security certificates for the assurance level “high” of the CSA, provided that this assurance level has been defined within a European certification scheme. To fulfil this task, the BSI benefits from its long-standing and internationally recognised certification experience. The first common European cybersecurity scheme is expected to be EUCC which is based on the Common Criteria certification. Over the past decades the BSI has used Common Criteria successfully to build up trust in the quality and independence of its certificates outside of Germany. The BSI also took a leading role in shaping the new European requirements.

Control through supervision

The other important area of responsibility of the NCCA involves supervision, which in the future will ensure compliance with the specific requirements of a European cybersecurity certification scheme. This covers the manufacturer’s self-declaration (assurance

level: “basic”), the private certification bodies (assurance level: “substantial”) and the certifying NCCA of the BSI (assurance level: “high”).

In the future, complaints can be directed to the supervising NCCA if it is suspected that the CSA or the rules specified in the respective European cybersecurity certification scheme have been infringed. If the supervising NCCA determines that such a violation has taken place, it has the power to impose appropriate sanctions, e.g. in the form of financial penalties. Another aspect that has also been enshrined in law is the authorisation of conformity assessment bodies by the BSI as necessary precondition to act in accordance to the European cybersecurity certification.

Since the beginning of 2021 work has been ongoing to establish the NCCA. The new BSI office in Freital is playing a key role, as a large proportion of the tasks indicated in the CSA are located here. This requires both organisational developments and personnel increase.

Collaboration in Europe

The close collaboration at a European level is another important task of the NCCA due to its membership of the European Cybersecurity Certification Group (ECCG). This mainly involves shaping the further development of the European certification framework and facilitating communication between the NCCAs. Moreover, the conformity assessment bodies for each European cybersecurity certification scheme have to be reported to the European Commission and the European Union Agency for Cybersecurity (ENISA). In addition to the permission to issue certificates, any certificates that are withdrawn by the supervisory NCCA are also reported and published in this way. This ensures that certifying bodies of the Member States comply with the demanding requirements of the European certification framework. ■

Further information:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/NCCA/ncca_node.html

https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

DIGITAL SOCIETY

Crash Test for Cyber Security

How IT security Is Driving the Shift Towards more Eco Friendly Transport and Supporting the Growth of Germany‘s Key Industries

The automotive sector is the largest branch of Germany‘s manufacturing industry. In terms of turnover, it is also the most important industrial sector in the country by some margin. Faced with the challenges of climate change and the need to shift towards more eco-friendly modes of transport, the sector is currently in a period of rapid change. This is being driven not only by the transition to alternative powertrains and electromobility, but also by the increased use of information technology.

Today‘s cars are much more than just mechanical objects; they are becoming fully connected platforms in their own right. Manufacturers are developing their own cloud infrastructures, and technologies like vehicle-to-vehicle communication and 5G are being deployed to make driving a safer and more comfortable experience. Digitalisation is opening the door to a whole new world of services and functions in vehicles. Self-driving cars are just one aspect of this developing trend; in the future, artificial intelligence (AI) will control of a wide range of functions to create an eco-friendly, connected transport system that conserves resources.

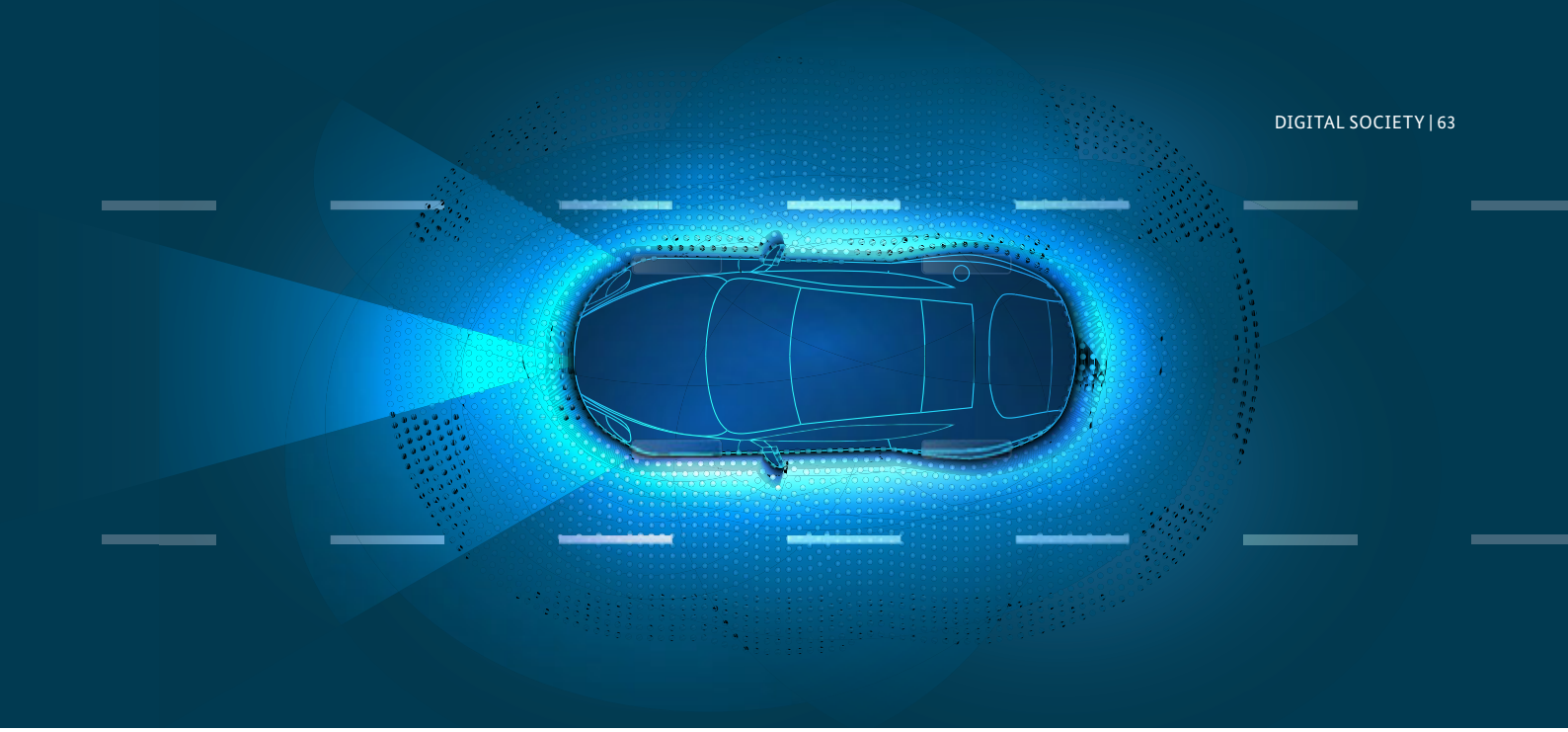
New challenges for cyber security

As the extent to which our vehicles are connected to the outside world increases, so too does their vulnerability to attack. In turn, the topic of IT security has moved up the agenda in the automotive sector. The double-edged sword of connectivity affects the entire value chain as well as the vehicle itself. With cyber attacks becoming increasingly sophisticated, it is all the more important that cyber security be made a priority and implemented from the outset in all areas and across all digitalisation concepts.

Recent cases in which car manufacturers and their suppliers have been specifically targeted by attackers have proven just how serious the consequences can be. In 2017, a French automotive manufacturer’s production process was brought to a complete standstill by the malware “WannaCry”. Its suppliers were also affected, rendering them unable to provide parts. In 2020, cyber criminals encrypted the systems of a German company that supplies and provides services to the automotive sector, stealing many gigabytes of data in the process. In 2021, two other suppliers were affected by a ransomware attack.

New technologies: an opportunity and a risk

As the importance of IT in vehicles grows, IT security is becoming an increasingly critical aspect of the overall safety of our cars – and creating a completely new set of challenges in terms of approvals, as well. This is particularly true of systems that rely on artificial intelligence. AI systems are complex, and it is difficult to understand and interpret exactly how they work. The high level of connectivity among the IT components within a vehicle and external IT systems significantly increases the intricacy of the overall landscape even further. To further complicate matters, the IT installed in a vehicle changes over the course of its life cycle – through software updates or replacement parts, for example. To evaluate system security effectively, the industry must constantly develop new methods and tools.



Making AI systems more robust not only helps prevent attacks by hackers, but also reduces the system's susceptibility to errors in normal operation. In so-called adversarial attacks, for example, AI systems can be confused by optical perturbations (such as stickers on road signs). Methods that increase the robustness of AI systems against this kind of manipulation also help reduce the effect of other sources of optical perturbation, like dirt or snow on signs.

Improving cyber security together: the work of the BSI

The BSI actively seeks to connect and engage with the relevant stakeholders to improve IT security in the automotive industry. It collaborates with manufacturers and suppliers on security-related topics under the umbrella of the German Association of the Automotive Industry (VDA), for instance, which has resulted in joint research projects both in Germany and around the world.

Working with partners in Germany and other European countries, the BSI also develops standards used to test the security of AI systems in the automotive sector. It is working with the German Federal Motor Transport Authority (KBA) to implement the new UNECE (United Nations Economic Commission for Europe) rules on cyber security in type approvals and market surveillance. In addition, the BSI is currently supporting the first manufacturers to certify their cyber security management systems (CSMS) and software update management systems (SUMS) under UNECE rules R155 and R156.

It is also working with TÜV-Verband e. V. to develop concepts for evaluating and assessing AI-based components and functions. At the European level, the BSI is part of a team that is hard at work developing and co-ordinating joint standards that will apply across the continent. At IAA Mobility 2021, the BSI presented an automotive industry security report for the first time, highlighting the cyber security aspects of IT both in vehicles themselves and throughout the supply chain during the manufacturing process. The BSI published two Technical Guidelines (TR-03164-1 and -2) on IT security in co-operative intelligent transport systems (C-ITS). Meanwhile, the BSI is currently developing a set of penetration test guidelines for connected vehicles as part of a project on hardware and software analysis. The guidelines – which are intended for public authorities, testing bodies and companies – set out the organisational and technical requirements for conducting the tests and describe the typical wireless and wired interfaces in connected vehicles.

IT security as the key to trust in new technologies

Improved IT security creates an essential factor for the acceptance and use of new technologies. This is particularly true of the transport sector: after all, no one wants to risk their life travelling by plane, train, ferry or car. In the aforementioned industry snapshot, BSI President Arne Schönbohm summed up the challenge at hand: "Computers are the brain of every modern vehicle and have been in charge of central control functions for some time now. If vehicles are connected to other vehicles or to transportation infrastructure, we need to be certain that we are protected against attempts at manipulation by third parties. Cyber security is just as important as having a working set of brakes. We need a crash test for cyber security!" As the Federal Government's cyber security authority, this is the challenge the BSI aims to tackle – to ensure secure and connected transportation for us all. ■

Further information:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Branchenlagebild/branchen-lagebild-automotive.html

Next Stage for the Smart Meter Gateway

How the Digitalisation of the Energy Transition is Making Steady Progress

By Michael Brehm and Thomas Joachim, Section Cyber Security for Digitization of the Energy Sector

The roll-out of smart meter gateways (SMGW) is under way, laying the foundation for the secure smart grid of the future. The task now is to build on this by working with the Federal Ministry for Economic Affairs (BMWi) and market players to develop standards for energy-sector application scenarios in the context of intelligent metering systems. This will help ensure that the digitalisation of the energy transition succeeds.

The rapid development of technology, in particular the digitalisation of many areas of society, presents major challenges for government, business and society. In the future, the smart grid will be required to integrate a large number of decentralised power-generating systems (e.g. photovoltaic plants) rather than a small number of large power stations. On the consumer side, the growing number of consumption points, such as electronic vehicle chargers and heat pumps, requires secure and intelligent load management. The smart grid of the future will need to offer flexibility so that power generation and consumption can be coordinated to ensure grid stability.

The use of intelligent metering systems (iMSys), combined with the resulting deployment of certified SMGWs, will ensure that critical systems in the energy grid are interconnected by a secure communications infrastructure. Thus, grid status data can be obtained using iMSys, creating greater transparency regarding the power flows in the distribution network. Moreover, it will then be possible to control flexible consumption points and decentralised power generation plants via iMSys so that they can be utilised to the advantage of the grid and market.

Stages of digitalisation – the roll-out since 2020

The potential of the secure gateway communication platform has already been extensively utilised since the start of the roll-out in 2020. Valuable experience has been gained that will help in the further development of the technical standards. The BSI and the BMWi prepared and published a joint standardisation strategy (the “BMWi-BSI Roadmap”) for the sector-wide digitalisation of the energy transition. This strategy now forms the common basis for working with partner authorities, industry associations and companies in the energy sector to specify the technical key points and the resulting requirements for establishing the secure smart grid of the future.

Potential low-voltage installation scenarios/use cases*	Status 2021	Prognosis (2030)
Consumers using 6,000–100,000 kWh per year	3.7 Mil.	4.1 Mil.
Consumers using 4,000–6,000 kWh per year (dynamic pricing)	-	0.4 Mil.
Consumers in property model and sub-metering system	-	> 1.8 Mil.
Flexible consumers	1.0 Mil.	> 5.2 Mil.
Generators based on German renewables/CHP legislation, 7–100 kW	1.2 Mil.	2.2 Mio.
Prosumers with PV 1 to 7 kW and an adjustable consumption system	0.6 Mil.	1.2 Mil.
Public charging infrastructure for electric vehicles	0.1 Mil.	> 0.5 Mil.
Total	**6.6 Mil.**	**> 15.4 Mil.**

*Figure: Application and sales potential for the iMSys – now and in the future (*source: Technische Eckpunkte)*

The technical key points published in May 2021 contain guidance on the next steps in the development of the standards for the digitalisation of the energy transition. The description of the corresponding development stages for the iMSys was released with the publication of the stage model (version 2.0) in June.

While Stage 2 has already been reached, the development stages that build upon it contain further functional and technical system enhancements for the iMSys, particularly for the SMGW. Stage 3 focuses on extending the monitoring options in the smart grid for customers and operators (e.g. voluntary high-frequency capturing of measurement data, network status data transmission), as well as on secure control of flexible consumption systems and power-generation plants. In addition, uniform standards on connecting further system units are being established to enable a gradual roll-out for additional installation scenarios on the basis of available certified technology.

Further development of the BSI technical standards

The description of the technical standards is provided in Protection Profiles and Technical Guidelines of the BSI. In early 2021, the BSI joined partner authorities and key stakeholders in the energy sector in revising Technical Guideline BSI-TR-03109-1 for the SMGW. The the updated version reflects the Stage 2 requirements in full and provides a basis for the conformity assessment procedure for proving interoperability as required by the Metering Point Operation Act (Messstellenbetriebsgesetz). To further expedite the certification process, the synergy effects between the necessary legal metrological certification, functional certification (Technical Guideline) and IT security-related certification (Common Criteria) will need to be utilised in the future.

The re-certification of a third SMGW manufacturer on the basis of Common Criteria, whose devices therefore fulfil the functionality of Stage 2, demonstrates that the planned expansion path can be achieved with functional software updates on existing SMGWs, and that the technology is in line with expectations.

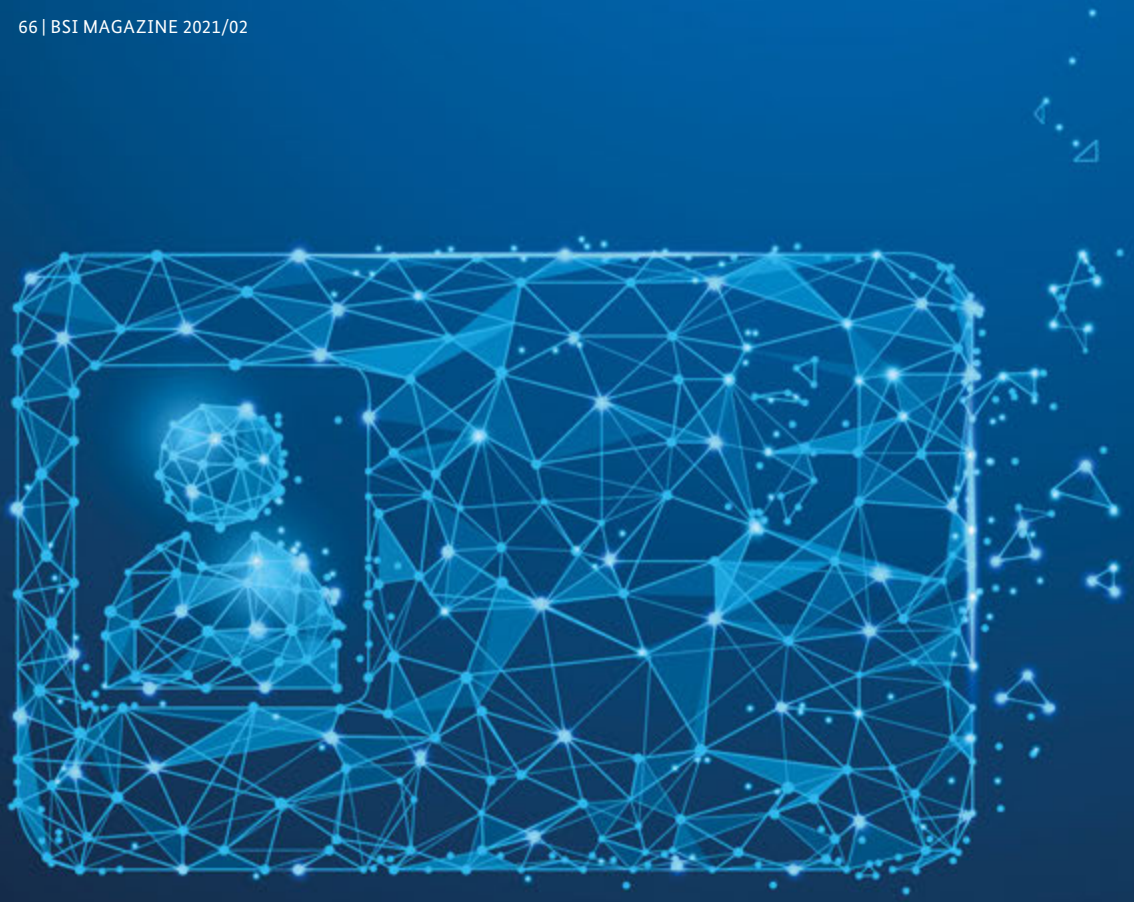
Development prospects of the intelligent metering system

The application potential of the iMSys as a key technology in the digitalisation of the energy transition is huge and continues to develop dynamically (cf. Fig. 1). The bodies driving this ongoing development are the dialogue forums of the BMWi and BSI within the roadmap process, which include task forces on individual topics such as metering, grid or e-mobility, as well as the working group on gateway standardisation.

Further benefit is set to be created in the future for a diverse range of applications related to the energy transition on the basis of the iMSys. The technical standards for additional system units in Stage 3 (for control, integration of sub-metering and the simplified connection of additional systems) are scheduled to be described by the end of 2021, i.e. corresponding certifications will then be possible for these components. ■

Further information:

https://bsi.bund.de/SmartMeter



Smart eID

The Future of Mobile Identity

By Philipp Zimmermann and Christopher Boysen, Section Technical Requirements for eID Components and Official Documents

The use of mobile identities (Smart eID) is an important step in supporting the ongoing process of digitalisation. This enables secure storage of a digital identity on your smartphone, making it possible to use the online ID function without a physical ID document.

The introduction of Germany's new ID card and a residence permit with the online ID function, along with the eID card for EU citizens, has made it possible to implement mutual authentication of ID card holders and service providers within e-business and e-government applications. This procedure is now set to be simplified as part of the digital transformation of business processes. In the future, it should be possible for users to take advantage of the online identification function solely with their smartphones, without the need for a physical ID document.

Dr. Markus Richter, Commissioner of the Federal Government for Information Technology and State Secretary at the Federal Ministry of the Interior, Building and Community (now: Federal Ministry of the Interior and Community), launched the project as part of his nine-point plan for a digital Germany. The implementation of the project is now being driven through a collaboration between the Federal Ministry of the Interior, Building and Community and the Federal Office for Information Security. The BSI, which is in charge of the technical management and coordination of the project with various private contractors, is integrating the Smart eID into the existing eID infrastructure.

Introduction of the Smart eID

The introduction of the Smart eID enables a smartphone to obtain identity data from an ID card, an electronic residence permit or the new ID card for EU citizens, which was introduced in January 2021. Using AusweisApp2, Germany's federal eID client, the user's identity data is read out once from one of these documents via the NFC interface and stored securely on the smartphone through a personalisation service. Access to the stored identity data is protected by a six-digit user PIN. If the smartphone has an integrated Secure Element, it provides further access protection and data security. This hardware security chip provides cryptographic functions and enables secure storage and use of key material in the hardware on the mobile device. Access to these functions can be encapsulated by a cryptographic service provider (CSP), which represents a standardised interface.

As of the introduction of the Smart eID, smartphones with a Secure Element and a CSP (such as the Samsung S20) are initially supported. Other devices with a Secure Element and a CSP, a Secure Element but no CSP, no Secure Element, or no means of accessing a Secure Element will be added soon so that as many users as possible can gain access to the Smart eID.

Control over your own identity data

Users retain complete control at all times of their own identity data, as it is only saved locally on their own smartphone. The Smart eID can be deleted at any time using AusweisApp2. If a smartphone is lost, the Smart eID can either be deleted using the remote deletion function of the mobile operating system or blocked by calling the blocking hotline (tel.: 116 116) and providing the blocking password. The blocking password is displayed to the user once during the Smart eID setup process and sent by letter to the address saved on their ID card.

If the user owns several smartphones, a Smart eID can be derived and set up for each smartphone. An overview of all Smart eIDs can be requested via the ID card producer's information service. The creation date, expiry date and blocking password for each Smart eID are shown together with the model and manufacturer of the smartphone. None of the user's identity data is processed or captured by this service.

The user can obtain information on the identity data saved in their Smart eID using the online ID function and AusweisApp2. As is the case for self-disclosure with other ID documents, the saved data is securely decrypted and displayed to the user.

The user has the freedom to decide whether to use the conventional online ID function with a physical ID document or the Smart eID. A service provider may only require a physical ID if it needs to guarantee a special assurance level.

The Smart eID represents a milestone on the road to a digital Germany. The BSI has contributed significantly towards guaranteeing the security and reliability of the Smart eID for citizens. ■

Highly Secure: Germany's 2021 Parliamentary Elections

An Interview with Dr. Georg Thiel, President of Germany's Federal Statistical Office and Federal Returning Officer

Under the watchful eye of Federal Returning Officer Dr Georg Thiel and his team, Germany's recent election was completed without any major incidents – thanks in no small measure to a package of advance measures and other steps to ensure information security during the voting process. At six o'clock on the morning of 27 September 2021, Dr. Thiel was able to announce the preliminary official result of the election for the 20th German Parliament.

Dr. Thiel, how would you describe your role on the evening of the election? And how do you think about the course of the evening?

I spent the election day with my team at the Reichstag in Berlin, monitoring how the voting was going. At six o'clock in the evening, the process of counting the votes at each polling station commenced. The results were quickly passed through to me by the district and state teams, and my team checked them for plausibility. Once we had all the district results, we calculated the preliminary official result and announced it at six o'clock on Monday morning.

"We were well prepared, thanks in part to the support provided by the BSI."

Overall, the parliamentary elections went well. Of course, we followed up on the problems we encountered in a number of Berlin's polling stations and made sure that we dealt with these issues in a transparent way, but apart from that, there were no major incidents. We didn't have any serious problems neither with regard to information technology nor to security. We were well prepared, thanks in part to the support provided by the BSI. All the hard work we did together paid off!

In the run-up to the election, the BSI consulted with various security authorities and concluded that cyber-stalking/harassment, information operations and untargeted attacks such as ransomware were all potential threats. What do you think was the most severe threat to the parliamentary election?

In advance of the election and on the election day itself, there was some incorrect and misleading information in circulation that was intended to influence voters and provoke a sense of distrust in the election and its results. To combat this, we monitored the reporting by traditional media outlets and what was being said on social media channels and provided comprehensive, reliable information from the Office of the Federal Returning Officer.

We also worked with the BSI to secure the information technology we used to transmit the preliminary results on election night. This included organising IT security trainings for the municipalities and drawing up a guide for election officials. The security arrangements were continually monitored and modified as needed. Our ability to quickly identify some attempted attacks in advance of the election showed, that these security systems were effective.

Before the election, media reports repeatedly questioned the security of postal voting, claiming that it was not as secure as traditional ballot box voting. Can you explain why these kinds of doubts arise so frequently?

Postal voting differs from in-person voting at the ballot box because it is impossible to be certain that the voter has filled out their own ballot without any interference from others. Postal voting is therefore directly linked to the principles of a free and secret election. In this case, it is the voter's own responsibility to ensure that these principles are upheld.

On the other side of the coin, postal voting helps uphold another principle: namely that all eligible voters should have the opportunity to participate in an election, particularly during a pandemic. The Federal Constitutional Court has ruled on a number of occasions that the postal vote, which was introduced in 1957, is constitutional.

How do you think digitalisation will affect the voting process in the future? What kinds of software do you envisage to support future elections?

An important part of our work in preparing for the next election is expanding our digital options to simplify them, and to speed up our processes. In many areas, voters can already request postal voting papers using a QR code printed on their polling card. I'm also working to ensure that German citizens living abroad will be able to submit digital applications to be added to the electoral register, which should help prevent problems caused by postal delays.

When it comes to the process of voting itself, I don't think digitalisation is realistic in the near future. The Federal Constitutional Court has set stringent requirements for the use of electronic voting devices: The voting process itself must be secret, but the counting process must be public and repeatable. The process used to arrive at the result must be transparent and accessible to everyone. There is no voting computer or online voting system that can meet these requirements.

Meanwhile, there's no need for software support at polling stations, especially since the validity of each ballot paper would still need to be checked individually. We do, of course, use software to collate the results from all 299 voting districts and to determine the distribution of seats. Our website provides a step-by-step guide to how performing the calculations and working out the distribution. It's important that this phase of the election is transparent even without the use of software; the ability to verify and explain the result is an important cornerstone of our voting system.

On election day, the team comprising the Federal Returning Officer's staff and members of the BSI was joined by the Federal Office for Civil Protection and Disaster Assistance, the Federal Information Technology Centre and IT service provider elect-IT. Which partnerships would you like to build on to ensure the security of future elections?

No public authority or voting body could achieve this on its own. In addition to the partners already mentioned, we work with organisations such as the Federal Agency for Civic Education and the Federal Press Office to share information on the voting process and prevent the spread of inaccurate information. The Federal Ministry of the Interior and Community and other security authorities are constantly monitoring and analysing the security situation to ensure that elections are secure for all citizens.

In the future, we want to continue making advancements in the cooperation of all these experts working on the various necessary tasks. ■

The Federal Returning Officer is the independent election official responsible for conducting parliamentary and European elections in Germany. In accordance with established government practice, the Office of the Federal Returning Officer is assigned to the President of the Federal Statistical Office. Dr. Georg Thiel has held both roles since 1 November 2017.

BSI Basic Tip

Access Your Data from Anywhere

The cloud is increasingly being used to store photos, videos, documents, applications and even health data. The “cloud” in this case is actually a term for data centres that are connected to the Internet. A cloud service is an online service that users can access via the Internet at any time and from any end device, such as a PC, smartphone or Internet-enabled television. Data and applications are not stored on the device, but on remote servers. The benefits are obvious: documents can be edited by different people, photos can be shared with friends and family and videos can be streamed from anywhere.

Examples of cloud services

- Online data storage
- Webmail
- Smartwatches and fitness trackers
- Streaming platforms
- Online programs for text and image editing

More information and the “Using Cloud Services Securely” guide:

https://www.bsi.bund.de/cloud-sicherheit

Using cloud services securely
Cloud services are useful, but there are risks involved in using them. Whenever you use a cloud service, you are handing over private and sensitive data to the cloud service provider. You are also giving up control and responsibility, and thus trusting the provider to protect your data adequately.

Here, we have put together five important tips to help you protect your data in the cloud:

- Make sure that your access device has adequate basic protection, such as a screen lock and an automatic update function.
- Protect cloud services with a secure password and a second factor, if possible.
- Check the provider’s privacy policy and terms and conditions to find out whether your data will be stored in the EU, where the Europe-wide General Data Protection Regulation applies. The risk of using a particular cloud service must be assessed in each individual case.
- When choosing a provider, make sure that your data will be transferred via a secure connection (identifiable by “https”) and encrypt your personal data before uploading it to the cloud.
- If you wish to share data with other people, share as little information as possible and make sure it is only shared for a limited period.

Federal Office
for Information Security

BSI

Save the Date

The 18th German IT Security Congress

1-2 February 2022 (virtual format)

Register now! The event is free to attend.

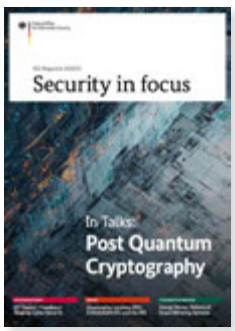
www.bsi.bund.de

Order Your BSI Magazine!

Federal Office
for Information Security

Federal Office for Information Security (BSI)
Section Public Relations

P.O. Box 20063
53133 Bonn, Germany
Phone: +49 (0) 228 99 9582 0
Fax: 0228 99 9582-5455
email: bsi-magazin@bsi.bund.de



Twice a year, the BSI Magazine "Security in focus" offers insight into national and international cyber security, digital society and IT security in practice. You can receive the latest issues by mail by subscribing to the distribution list with the form below.

I would like to subscribe to the following BSI publication:

☐ BSI Magazine "Security in focus" (2/year, print)
☐ The State of IT Security in Germany (1/year, print)

Last name, first name

Organisation

Street

Postal code, City

Email

Data protection consent:
I consent to my aforementioned personal data being used, electronically stored and processed by the BSI as the responsible body for the dispatch or transmission of the aforementioned publications. No data will be given to third parties without consent.

Date/Signature:

The Federal Office for Information Security, PO Box 200363, 53133 Bonn, Germany, is responsible for processing your aforementioned personal data. The information you provide will only be used to manage the sending or transmission of the information you have consented to above. You may revoke this consent at any time. Simply send an email to bsi-magazin@bsi.bund.de. Revoking consent does not affect the legality of prior processing before revocation. For more information on how we process your personal data and what rights you are entitled to, please refer to the "Data Protection Information" attached for ordering BSI publications.

Simply send in the form by fax or email:
Fax: 0228 99 9582-5455 | email: bsi-magazin@bsi.bund.de

Or you can register directly online: https://www.bsi.bund.de/EN/BSI-Magazine

If you no longer wish to receive BSI publications, simply send us an email at **bsi-magazin@bsi.bund.de.**

Data protection information: https://www.bsi.bund.de/datenschutzrechtliche-hinweise

LEGAL NOTICE

Published by:	Bundesamt für Sicherheit in der Informationstechnik (BSI) 53175 Bonn
Source:	Federal Office for Information Security (BSI) Section WG 24 – Public Relations Godesberger Allee 185–189 53175 Bonn Phone: +49 (0) 228 999582-0 email: bsi-magazin@bsi.bund.de Internet: www.bsi.bund.de
Last updated:	December 2021
Content and editing:	Nora Basting and Mark Schulz, Federal Office for Information Security (BSI); FAKTOR 3 AG
Concept and design:	FAKTOR 3 AG Kattunbleiche 35 22041 Hamburg www.faktor3.de
Printed by:	Appel und Klinger Druck & Medien GmbH Bahnhofstraße 3 96277 Schneckenlohe Internet: www.ak-druck-medien.de
Item number:	BSI-Mag21/714-1e
Image credits:	Title: GettyImages © C.J. Burton; p. 4-5: © Secunet Security Networks AG; AdobeStock © only kim; p. 6: AdobeStock © your123; p. 9: AdobeStock © Graphic in Motion; p. 10-11: AdobeStock © Olga, © BMBF/Hans-Joachim Rickel, AdobeStock © AKS; p. 14-15: AdobeStock © Sikov, AdobeStock © Olena; p. 16: AdobeStock © phive2015; p. 18: AdobeStock © vpanteon; p. 23: AdobeStock © putilov denis; p. 24-25: AdobeStock © rh2010, © BSI; p. 26-27: © BSI; p. 30-31: GettyImages © gremlin, AdobeStock © Halfpoint, AdobeStock ©Jacob Lund; p. 32-33: AdobeStock ©TTstudio, © BSI, © BSI; p.36: © BSI; p.41: AdobeStock © Robert Kneschke; p.42: AdobeStock © TIMDAVIDCOLLECTION; p.44-45: AdobeStock © peterschreiber.media, AdobeStock © Olive; p. 47: AdobeStock © egor; p.49: © BSI; p.51: AdobeStock © Feodora; p. 54: AdobeStock © Inna; p. 56-57: AdobeStock © Grecaud Paul, GettyImages © merovingian; p.61: AdobeStock © Max Brosza; S .63: AdobeStock © ZinetroN; p.64: AdobeStock © rh2010; p.66-67: AdobeStock © pickup, AdobeStock © tippapatt; p. 68: AdobeStock © Ronny Behnert, © Bundeswahlleiter; p. 70-71: AdobeStock © AVTG, AdobeStock © katie martynova

The BSI Magazine is published bi-annually. It is part of the Federal Office for Information Security's public relations work.
It is provided free of charge and is not intended for sale.

Scan the QR code for the digital version of the BSI Magazine

https://www.bsi.bund de/EN/BSI-Magazine

www.bsi.bund.de