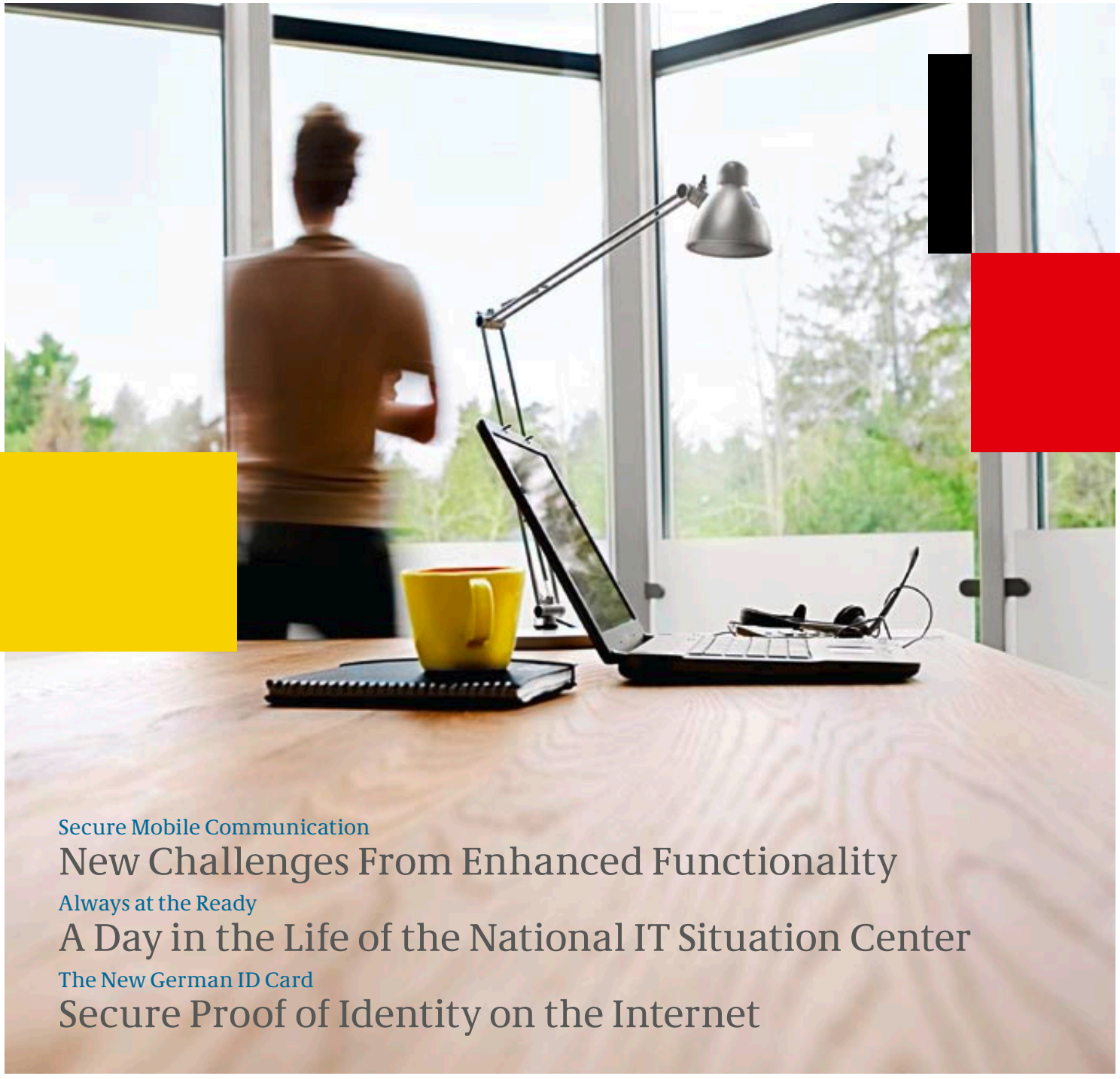
Federal Office
for Information Security

Improving IT Security

BSI Annual Report 2008/2009



Secure Mobile Communication

New Challenges From Enhanced Functionality

Always at the Ready

A Day in the Life of the National IT Situation Center

The New German ID Card

Secure Proof of Identity on the Internet

Improving IT Security

BSI Annual Report 2008/2009

IT Security

This refers to the security of information technology, a generic term for a state of affairs in which IT systems are free from risk or harm. Security can be achieved if dangers are identified and eliminated in advance. The main task is therefore to counter threats with appropriate protective measures and thus forestall any possible damage.

Adapted from an definition in Brockhaus

Dr. Thomas de Maizière,
Member of the Bundestag
Federal Minister of the Interior

Responding Rapidly to Technological Changes

Dear Readers,

Information technology opens up many new opportunities. It is changing our world faster than any previous industrial or technological revolution. The internet, "cyberspace", is a place of innovation and the creation of value. Germany's well-being and participation in the global economy depend critically on our ability to make use of the possibilities presented by IT and the internet. Being able to trust the security of information technology is a key part of this.

The Federal Office for Information Security (BSI) is an important partner to the business community, public authorities and society in IT security matters. Founded 19 years ago, the BSI already has some major accomplishments under its belt. Today the BSI is a center of competence that is much in demand in Germany and Europe. Following its successful model, similar institutions have been set up in our European neighbor countries.

The BSI will continue to play an important role in shaping IT systems in the future. It has to respond rapidly and flexibly to changing conditions and come up with innovative solutions for IT security. Adequate IT security is not a state but a continuous process for which all interested parties – whether users, suppliers or IT security agencies – are equally responsible.

I hope that reading this report will give you plenty of insights and food for thought on the subject of IT security.

Berlin, May 2010

Dr. Thomas de Maizière

Strengthening and Intensifying IT Security With Strategy and Know-How

Michael Hange
President of the Federal Office for Information Security (BSI)

Dear Readers,

Nowadays almost 70% of Germans are online and most German households possess more than one PC or laptop. Shopping on the internet, online banking, e-government, keeping in touch via the internet – most private and social interactions have made their way into the virtual world. And with ever increasing popularity. As users shift their activities onto the internet, the incentive for cyber crime is experiencing exponential growth. Attacks on systems are assuming professional dimensions. Whereas in the past the perpetrators were driven by the desire for publicity, today financial incentives are the main source of their motivation. As a result they try to ensure that their attacks go unnoticed, which makes countering them very difficult.

For the BSI and its approximately 500 staff, this challenge is our motivation. Establishing possible solutions for greater IT security, bearing in mind the data and consumer protection provisions, requires a wealth of ideas, flexibility and, last but not least, a courageous gaze into the future. The new BSI Act, which entered into force in August 2009 and confers our organization with further powers, provides us with additional scope for action. The BSI sees itself as a shaper of IT security and an IT security partner and works closely with institutions in both the private and public sectors – with the aim of achieving greater IT security and safeguarding the interests of all internet users in the Federal Republic of Germany. But we also promote IT security concepts and standards in the international arena, as the virtual world knows no borders.

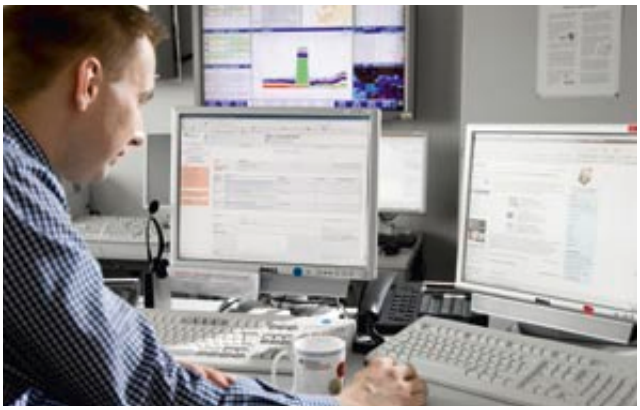
My personal links with the BSI as an employee go back many years, and in my new role as President of the BSI it gives me great pleasure to be able to offer an insight into our work and selected projects in this publication. This report primarily covers the years 2008 and 2009, but we have also allowed ourselves to gaze into the future. For one thing is certain: we will all come to depend even more heavily on reliable information technology in the future. My colleagues and I will continue to champion the cause of making processes and applications safe and trusted so that users can benefit unreservedly from the opportunities presented by information technology.

Bonn, May 2010

Michael Hange

Page 8
Turning Points for Information Security

Page 18
Holistic Information Security as a Model for Success – Benchmarks for Information Security Management



Page 24
Always at the Ready: A Day in the Life of the National IT Situation Center

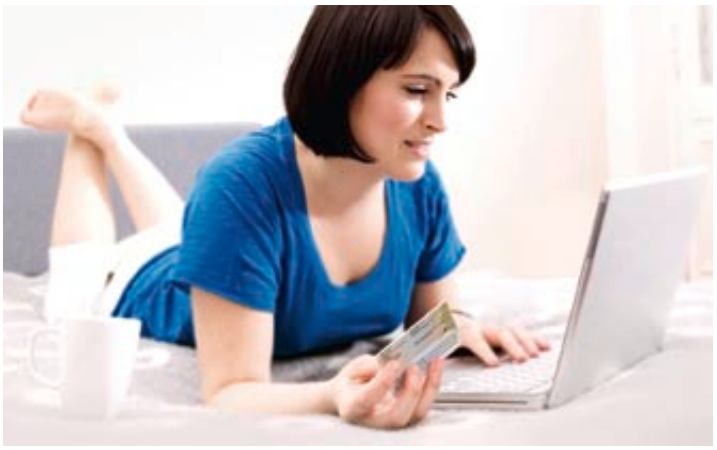
Setting the Course – Planning the Future

Shaping IT Security

Security for the Cyber World

Page 37

Guaranteed Interception-Proof! Counter-Eavesdropping at the NATO Summit in Baden-Baden and During President Obama's Visit to Dresden



Page 44

Secure Identification on the Internet With the New ID card – a BSI Project That is Unique in the World

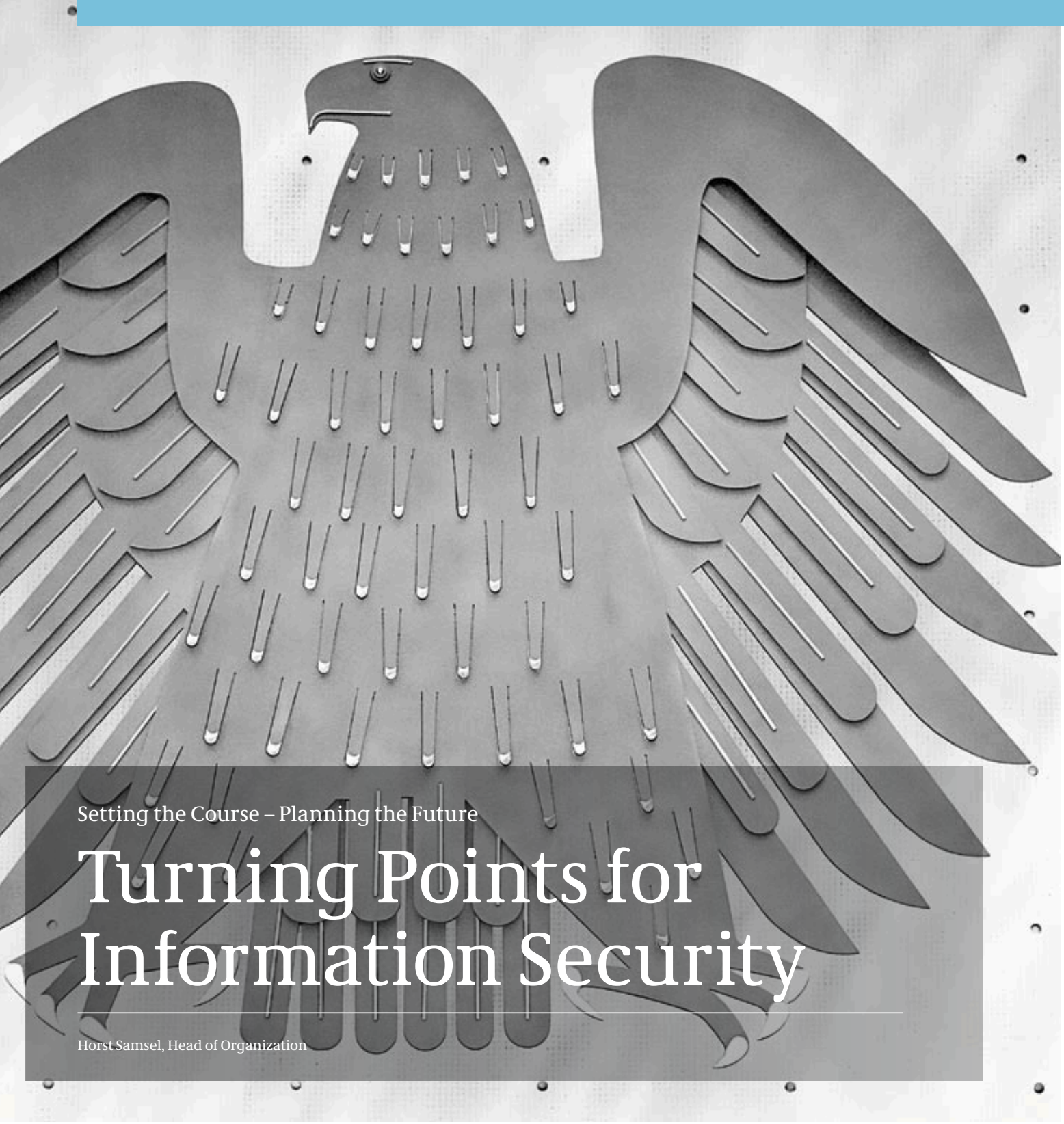
Page 54

The Heart and Brains of the BSI: Our Staff

Communication – Mobile and Protected

Secure Electronic Identity

Tackling the Challenges Together



Setting the Course – Planning the Future

Turning Points for Information Security

Horst Samsel, Head of Organization

These days countless processes and tasks in the public and private sectors are supported by IT. Businesses, public authorities and the public are thus highly dependent on properly functioning information technology and secure information infrastructures. However, our growing dependence on technology presents a number of risks which are at odds with the opportunities that result from the use of information and communications technology. These risks stem from the ever greater threat posed by cyber crime. Today foreign intelligence services and organized crime carry out highly professional IT attacks which are directed at the information and IT structures of the administration, businesses and also private users. It is therefore no surprise that IT security is becoming more and more important at business, social, political and legal levels.

SAFEGUARDING DATA SECURITY AS AN ELEMENT OF THE GERMAN BASIC LAW

In the Population Census Judgment of December 15, 1983, the Federal Constitutional Court recognized for the first time the right of individuals to decide how much information is disclosed about themselves ("the right to informational self determination"). This right is derived from the general right to privacy and the guarantee of human dignity enshrined in the German Basic Law. In its judgment of February 27, 2008 concerning the "basic right to confidentiality and integrity of information technology systems", the Federal Constitutional Court set a further milestone toward establishing the protection of data. The basic right is intended to protect personal data that are stored or handled in IT systems; this basic right can only be encroached upon within narrow limits.

At the same time IT security has also indirectly entered into the German Basic Law by way of the new version of Article 91c. This article codifies cooperation between the federal government and the Länder in the information technology used by public authorities. Under the amended article, the federal government and Länder may work together on the planning, establishment and operation of the IT systems they need to fulfill their functions and enter into agreements to determine the standards and security requirements for communication between their IT systems.

In a statement issued on March 27, 2008, the then Federal Minister of the Interior, Dr. Wolfgang Schäuble, said:

"There is agreement in the Commission that we need a new constitutional basis for the central infrastructure of the 21st century. IT has the same monumental importance for our century as the railways had for the 19th century and aviation for the 20th century. It is revolutionizing the way we work, live and communicate. The railways and aviation already fall within the ambit of the German Basic Law. It is high time that IT is also included and that clear responsibilities are set out for the use of information technology in public administration."
(http://www.cio.bund.de)

"The BSI Act makes our agency better equipped to deal with present and future challenges in IT security."

Horst Samsel

THE AMENDMENT OF THE BSI ACT (BSIG)

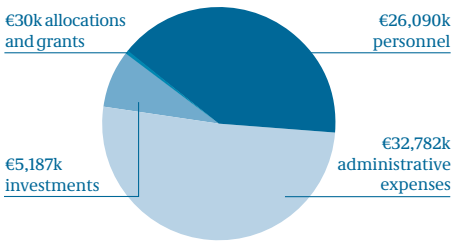
The Act to Strengthen the Security of Federal Information Technology *(Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes)*, which was passed by the Bundestag on June 19, 2009, strengthens the role of the BSI as the German government's IT security agency, and at the same time introduces changes in the way IT security is anchored in law that have enormous implications for the BSI. The new Act significantly widens the spectrum of the functions and powers of the BSI and puts the agency in a better position to meet current and future challenges in IT security.

INFORMATION ON SECURITY VULNERABILITIES AND MALICIOUS CODE

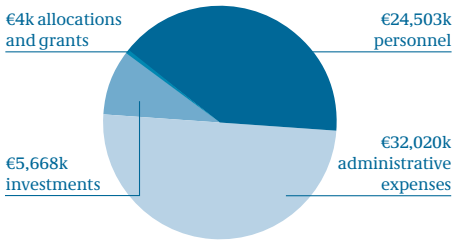
In order to be able to effectively counter the present threats and take account of the increasing importance of information and communications technology in present-day society, the BSI was given additional functions and powers in the amendment of the BSI Act (BSIG). Under Section 4 of the BSIG, in its role as central liaison point for cooperation between federal agencies in the area of IT security, the BSI will in future collect and analyze information about security vulnerabilities and new types of attack. This will make it possible to draw

The BSI In Figures

Budget total 2009: €64,089k



Budget total 2008: €60,195k



up a reliable picture of the situation, detect attacks early on and take countermeasures. In this connection data protection issues must naturally be taken into account. The definition of information that has to be reported and the reporting procedure were decreed at the end of 2009 in the form of an administrative regulation issued by the Federal Ministry of the Interior after consulting with the Federal Commissioner for Information Technology (Federal CIO).

Section 4 of the BSIG is primarily directed at public authorities. However, under Section 7 of the BSIG the BSI is also responsible for warning the business community and the public about security risks. Under this Section, the BSI will be able to pass on information and warnings about security vulnerabilities in information technology products and services and on malicious code to the agencies affected or to the public. Its initial duty is to inform the manufacturer in advance, giving it the opportunity to develop security updates and make them available to its customers. Only after this, or if the purpose of the measure cannot be achieved with advance information, will the BSI make a public announcement. **The information is available to all**

interested parties via www.buerger-cert.de and can also be obtained by subscribing to a newsletter.

PROTECTING THE INFORMATION TECHNOLOGY OF THE FEDERAL GOVERNMENT

In addition to the tasks of gathering information and issuing warnings, the BSI also plays an active role in protecting federal communications technology. Section 5 of the BSIG confers on the BSI the power to collect, evaluate, store, use and process logged data and data generated through operation of the federal government's communications technology. This will ensure that indications of IT attacks can be detected and combated.

To address the special sensitivity of these data, Section 5 of the BSIG imposes detailed requirements on the collection and evaluation of data. This provision only gives the BSI powers to collect and evaluate by automated means the data generated through operation of the federal government's technology. In the exceptional cases where further processing is permitted, the data must be deleted immediately and without trace after evaluation. In particular, the use of personal data for unrelated purposes, for example to create communication profiles or to check the behavior and performance of employees, is not permitted. The data may only be evaluated on an individual basis if there are concrete suspicions that they could be needed to avert dangers posed by malicious code. Only data generated through operation of the federal government's communications technology assets are to be collected – not data that originate from uninvolved third parties engaged in internet activities. The use of data that are attributable to the core area of citizens' private lives is likewise prohibited.

SECURITY CERTIFICATES AS PROOF OF QUALITY

The BSI is also empowered to define standard and stringent security standards for the federal administration and, if required, to commission, put out to tender and supply suitable products (Section 8 of the BSIG). It will thus be possible to prevent unsuitable products with security vulnerabilities or IT components that have been tampered with from being used in the federal administration and government networks.

Under Section 9 of the BSIG, as the federal administration's national certification body for IT security the BSI is able to certify the quality of security-relevant offerings by establishing certification criteria and issuing quality certificates (cf. p. 14ff).

The Coalition Agreement: Spheres of Activity for the BSI

The expanded legal requirements enable the BSI to effectively counter the increasingly taxing challenges of IT security. But given the rapid technical developments and constant changes in the underlying conditions, it is already clear that the BSI will continue to acquire even more new spheres of activity. Thus the Coalition Agreement concluded by the CDU/CSU and the FDP in October 2009 after the 2009 Bundestag elections includes the following words:

"We [ed.: the coalition parties] are committed to strengthening IT security in the public and non-public domains, above all to protect critical IT systems from attack. To this end, we want to encourage people to protect themselves better and to use secure IT products through education and awareness raising among the public. This objective will give the Federal Office for Information Security a major boost."

"Trusted, high-performance and secure information and communications technology is essential for our high-tech country and for Germany as a business location. We will protect IT assets against internal and external threats so as to preserve our economic capability and administrative capacity to act. We will therefore direct special attention to countering IT attacks, and to this end we are bundling together competencies in the federal administration in the hands of the federal government's Information Technology Officer. To support him, we will continue to expand the Federal Office for Information Security as the central cyber-security agency so that it is specifically in a position to coordinate countermeasures against IT attacks."

Investing in IT Security

Frank Koob, Research Coordinator at the BSI

IT Security Research: Investing in the Future

A forward-looking national IT security policy needs to keep up with developments in technology, as the innovation potential in the information and communications technology arena is increasing dramatically. Hand in hand with this is an ever-increasing danger from IT security risks. In recognition of this, it is clear that in addition to actual technology research, increasing emphasis needs to be placed on IT security research if the growing threat situation is to be countered on a lasting basis in the future. Whereas up to now IT security research has been viewed and dealt with as something that is incidental to general technology research, the interdisciplinary nature and the special importance of IT security increasingly justify the need for this research to be conducted independently. Such independence has and will increasingly make it possible to promote ongoing IT security research with partners in Germany, integrate IT security as an integral element of technology development at an early stage and, based on new developments, develop innovative IT security procedures and methods and convert them into marketable products. A massive gain in security can be achieved as a result.

Innovative Research Programs

Application-oriented innovations in the fields of internet early warning systems, trusted computing and biometric and identification systems are being developed in the BSI's in-house IT security research program, Zukunftsfonds. For this purpose, between 2006 and 2009 funding of EUR 36.5 million was made available from the German government's EUR 6 billion innovation program. The projects are due to be completed in 2010.

In addition, in October 2008 the Federal Ministry of the Interior (BMI) and the Federal Ministry of Education and Research (BMBF) agreed in a joint declaration to establish IT security as a new focus of research funding in ICT. The then Federal Minister of the Interior, Dr. Wolfgang Schäuble, and the Federal Minister of Education and Research, Professor Annette Schavan, agreed in September 2009 to launch an extensive joint program of IT security research. Funding to the tune of EUR 30 million is to be provided over a period of five years for this purpose. This funding is intended to create the basis for the development of verifiable and totally secure IT systems and for research into new approaches in the analysis and protection of ICT systems. The BSI had a significant influence on determining the subject areas to be covered under the work program. In addition, the agency is involved in the assessment of proposals and the selection of the projects to be funded. Eligible to participate in the program are universities, research institutions and other R&D institutes, public authorities and companies that are based in Germany and whose results will predominantly be exploited there.

Research Cooperations for IT Security

However, the increasingly more complex demands imposed on IT security research also call for equally long-term and continuous interdisciplinary collaboration between research institutions, industry and the BSI. One way of organizing this collaboration is to form research clusters and cooperations. The aim of the BSI's involvement in these clusters is to exercise a strategic influence on the orientation of the research content and hence, in particular, to ensure that BSI-specific IT security aspects are included in this IT research and development. At the same time, funding innovations and improving education will also give indirect impetus to the German IT security industry. Cooperative agreements in the area of IT security already exist with the Center for Advanced Security Research Darmstadt (CASED) and, based on a memorandum of understanding, between the BMI/BSI and the Fraunhofer Gesellschaft.

EUR 220 Million for IT Security – the German Government's IT Investment Program

As well as the amendment of the BSI Act, IT security is also a focus of political attention in another area: in the Protection of Employment and Stability Act *(Gesetz zur Sicherung von Beschäftigung und Stabilität)* passed in 2009, the Bundestag resolved to invest about EUR 500 million in information and communications technology. Almost half of the budget, about EUR 220 million, is to be invested in IT security measures, including encryption-capable cell phones, encryption technologies, measures to increase network security, IT Grundschutz certification, security training and measures relating to the new German ID card.

The BSI Creates Solutions

More specifically, the BSI implements projects providing secure mobile voice and SMS communication – up to RESTRICTED level – for the federal administration. The aim of this measure is to make existing solutions interoperable and to procure appropriate devices known as encryption-capable cell phones (see p. 34ff). Another project is the joint procurement of equipment for secure, mobile e-mail communication with PDAs that satisfy the IT security requirements of the federal government as specified by the BSI. The BSI is also in charge of the initial introduction of a secure, approved solution for the processing of local data on mobile workstations (laptops) and a secure network connection over public networks to the intranets of government agencies that require a higher level of protection.

But the measures implemented by the BSI are not confined to advances in secure mobile communications. Other projects forming part of the investment program are concerned with the nationwide protection of government networks from malicious code (malware). In particular, these include improving internet security and the security of government websites, but also the procurement of specialized IT security products to protect networks against malware for use by local authorities.

Key Focal Points of Research Funding

- Security in insecure environments: In practice, it is no longer possible to protect large ICT environments (for example, on the internet) due to their complexity. The security of ICT systems, especially mobile systems, therefore needs to be assured in insecure environments as well.
- Protection of internet infrastructures: It is not possible to totally protect ICT systems against attacks, but they can be protected against "epidemics". This requires attacks to be detected, malware isolated and prevented from spreading and third parties to be informed promptly.
- Built-in security: Subsequent protection of ICT Systems is extremely costly and in many cases is simply not feasible. ICT systems should therefore be designed and developed with a demonstrable, defined level of IT security right from the start.
- New challenges to protect IT systems and identify vulnerabilities: In order to be able to counter specific attacks – and ones that might arise in the future – novel techniques, methods and approaches need to be developed to protect ICT systems.

Source: BMBF/BMI Arbeitsprogramm IT-Sicherheitsforschung

Shaping IT Security

Benchmarks for Product Security

Gereon Killian, Head of Certification Section, BSI

"The demand for trusted IT products is rising."

Gereon Killian

With the aim of integrating IT security into products, the BSI provides a series of appropriate IT security standards and test specifications. These are developed, adapted and made available to the business community in accordance with ever more stringent requirements.

The IT security standards, especially the Protection Profiles (PP) defined under the internationally recognized Common Criteria (CC) and the Technical Guidelines (TR), serve as the basis for the development of IT security products and also define systematically developed test specifications for IT security evaluations. On top of this, the Technical Guidelines provide criteria and methods for conformity testing – both for the interoperability of IT security components and for functional IT security requirements that have already been implemented. In addition to the certification of Protection Profiles and IT security products that comply with the Common Criteria, confirmations are also issued in accordance with the German Digital Signature Act (*Signaturgesetz*).

As in previous years, the number of certification processes carried out in 2008 and 2009 increased. The demand for trusted IT products has continued to rise despite the economic crisis. The BSI is therefore setting new benchmarks for the security of IT products.

A Practical Example: the Technical Guideline on Trustworthy Electronic Long-Term Storage

Growing mountains of files and documents are making it imperative for government agencies to use more efficient processes to interact with the public, businesses and other institutions. The use of appropriate electronic communication and information technology not only simplifies and speeds up the exchange of data, but in many cases it also brings savings.

New challenges arise as digitization progresses at an ever-increasing rate:

- Electronic documents do not themselves provide any indication as to their integrity and authenticity. In electronic legal and business correspondence there is no guarantee that the legal rights of the originator or third parties will be protected or upheld or that legitimacy can be proven; this can only be achieved and permanently maintained with additional technical and organizational measures.
- Independently of individual products and manufacturers, the readability and availability of storage media and data formats must be guaranteed throughout the long retention periods required and hence throughout IT innovation cycles that are becoming ever shorter.
- Access to electronic data and documents must satisfy data protection and data security requirements, including over long periods of time and across changes of systems.

BSI Technical Guideline 03125 is concerned with the definition of requirements for protecting the evidentiary value of cryptographically signed documents that have to be complied with in connection with the retention of electronic documents until the end of the relevant terms, on the basis of existing statutory and technical standards and national and international experience.

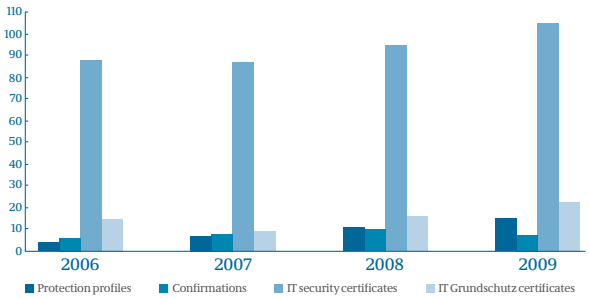
Given that cryptographic procedures used in connection with digital signatures can be subject to "technical decay" with the passage of time, a legally prescribed procedure exists as to how to avert the threatened loss of security suitability of the key and hash procedures used in digital signatures without any loss of evidentiary value occurring. BSI-TR 03125 is a set of guidelines drawn up by the BSI which specify how digitally signed data and documents can be stored in a trustworthy fashion over long periods of time and retain their evidentiary value, in particular without every individual archived document having to be completely re-signed after a few years. In so doing, TR 03125 does not aim to replace well-known and established requirements and definitions. Rather, the requirements for proper retention must also be observed for digitally signed documents; this is presumed by TR 03125. The reference architecture of TR 03125 is not therefore intended to be a substitute for an archive system but rather a concept for middleware which specifies how to implement the requirements for preserving evidentiary value in a legally valid manner during the retention period.

The TRs are directed first and foremost at federal agencies which have to comply with certain legal retention obligations. In addition, the Technical Guidelines are essentially a set of recommendations, as in virtually every area of business the need to preserve evidentiary value of cryptographically signed documents in a legally valid manner is becoming more and more pressing. Electronic documents in the healthcare sector, registers of births, deaths and marriages and many other documents call for effective solutions as the digitization of business transactions gathers pace. These examples illustrate how important the preservation of cryptographically signed documents in a manner that retains the evidentiary value is for trusted, long-term electronic storage.

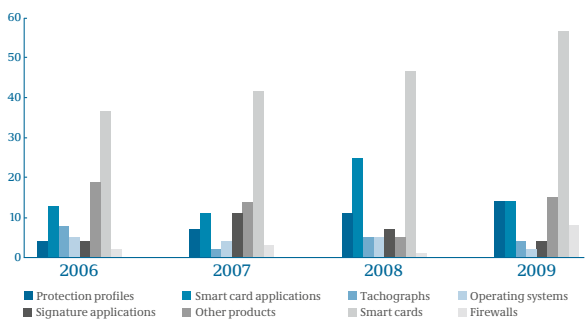
BSI TR 03125 certification provides the manufacturers of relevant solutions with evidence from an independent, neutral party that their products meet these requirements.

Overview of Certificates Issued

Certificates Issued



Certificates Issued by Product Group



The Importance of Certification for Industry

Guest Contribution from Dr. Peter Laackmann and Marcus Janke, Infineon Technologies AG

In many areas, present-day society needs a high level of security that is optimized to the requirements of the application. A clear example of this is in relation to the storage or processing of trusted data, for example, which can range from personal data to contractual or payment data. Among other things, such data must be protected against unauthorized access and alteration.

Modern security solutions that incorporate appropriate countermeasures, especially smart cards, are issued by manufacturers to protect against the many different kinds of attacks. However, given the wide range of forms that attacks can take, it is very difficult for customers to obtain a truly objective picture of a product and thus to compare the security of different products. Trust in the data provided by the manufacturer can, however, be strengthened by an independent test. The preferred choice in terms of security is the internationally accepted and used Common Criteria certification.

The vulnerability analysis required for the purposes of Common Criteria certification entails extensive investigation and testing, in the course of which practical attacks are carried out, and the amount of effort expended is evaluated using a points system. For each attack carried out, the expertise required, the complexity of the equipment, the time taken and the number of chips needed are considered.

A product is only assigned a HIGH[1] security level if it fends off all attacks corresponding to a high attack potential.

The BSI has already set many important milestones in Common Criteria certification. For example, the BSI's work resulted in alpha radiation for fault induction attacks being used for the first time in connection with product certification. This enabled the continuing development of attacks to be taken into account in security certification. Another example that has been adopted internationally is the definition of quality criteria for generators of genuine, physical random numbers which were specified in directive AIS-31. This directive has developed into a de facto standard for security products.

Independent testing and certification of products for the security market, taking into account the latest developments, are crucial in today's industry. Not only can manufacturers use Common Criteria certification as a confidence-building instrument, the level of security certified is also an effective advertising tool. For industrial customers, certification confers a more objective picture of the available suppliers and makes it easier to compare them, and they are able to achieve the appropriate level of security for their systems by asking for a particular security level in their specifications or supplier conditions. Finally, end customers and users benefit from the quality inherent in the level of security certified, as they can trust the security of the resulting complex system. **By publishing certifications and associated details on the BSI website, we are facilitating transparent security for all partners. Making it possible to meet the high security requirements of today's society.**

[1] Highest possible security level in CC certification

Greater Acceptance of Products

Guest Contribution by Armin Lunkeit, Chief Development Officer and Member of the Management Board, OpenLimit Group

Our company made the decision to offer certified components at an early stage. A primary consideration in this was our focus on the requirements of the Digital Signature Act and the Digital Signature Ordinance.

Common Criteria evaluation and certification have had a very positive impact on our company's development and QA processes. Thus, taking into account the requirements of the Common Criteria, we were able to set up a development and quality model which actively supports the robustness and security of OpenLimit software and minimizes risks in the form of damage in faulty software, for example.

Since then, OpenLimit has seen interest in its products grow steadily. **Common Criteria certification leads to greater acceptance and demand for products among customers, as the Common Criteria are recognized as an international testing standard in many countries.** One criterion that is regularly cited is that the audit scheme used should guarantee the independence of the test and certification body, thus providing maximum transparency as regards fulfillment of the product's promised functional and technical security performance.

Holistic Information Security as a Model for Success – Benchmarks for Information Security Management

Isabel Münch, Head of IT Grundschutz Section, BSI

IT Grundschutz:
IT Grundschutz provides a structure to the complex subject of IT security and makes it manageable.

In 2009 IT Grundschutz celebrated its 15th year. The IT Grundschutz methodology was introduced by the BSI in 1994 with the aim of helping government agencies and businesses to build up and operate a secure IT landscape. Since then business processes, information technology and many other framework conditions have repeatedly undergone massive change. As the BSI's present IT Security Situation Report 2009 confirms, the level of threat remains high. At the same time, however, IT users are constantly confronted with new forms of malware. These days, threats from the real world are also to be found on the internet. A DDoS attack, which paralyzes the availability of an entire IT system, is nothing more than vandalism using the resources of information technology. Despite this, users are often unaware of the dangers, as the threats are usually intangible and attacks are virtually invisible. Government agencies and businesses therefore need to be made more aware of how to protect themselves properly.

Making the Increasing Complexity of IT Manageable with IT Grundschutz

The ever greater complexity of IT systems makes it difficult for businesses and government agencies to take appropriate measures to increase information security. IT Grundschutz helps to make the complexity of this area more manageable by introducing systematic and permanent procedures. This approach has proved its worth over the last 15 years and the IT Grundschutz methodology has become a recognized standard for information security. IT Grundschutz provides a structure to the complex subject of IT security and makes it manageable. In 1994 we published the first edition of the IT Grundschutz Manual, a volume with just under 150 pages. Today the IT Grundschutz website offers information and resources for the various target groups. The offering now comprises four BSI standards, the IT Grundschutz catalogs and numerous implementation tools. In this way the BSI offers a sound methodology and supporting materials for assessing the information security of an institution and identifying which measures are necessary and how they can be implemented. Numerous government agencies and businesses use IT Grundschutz to efficiently implement their security policies, and many popular management strategies such as Governance, Risk, and Compliance (GRC) can also be covered.

Over time, the scope of IT Grundschutz has been expanded to include new professions, e.g. auditors for ISO 27001 certification on the basis of IT Grundschutz, IT Grundschutz consultants, IT Grundschutz auditors or federal government IT security officers, for whom IT Grundschutz is part of the basic training. IT Grundschutz is also used as a best practice model in many other European countries, for example Estonia and Sweden. A large number of materials are now available for this in English and other languages.

The IT world has changed radically over the last 15 years, but the concept of IT Grundschutz continues to work. The reason for the success of this model is the fact that it takes a comprehensive view of information security, but also that it constantly adapts to new challenges and changes in business models and IT environments. For this reason new subject areas have been and will continue to be tackled and integrated into the existing corpus of works on an ongoing basis. Thus BSI standard 100-4 on the subject of business continuity management was published at the beginning of 2009. The 11th update to the IT Grundschutz catalogs, which includes a number of new texts and revisions intended to deal with the constantly changing threat situation, appeared in December 2009. The eleventh update also contains new modules on Deletion and Destruction of Data, Microsoft Vista and the free Samba software, along with revisions of existing modules such as module B 1.3 on Business Continuity Management and module B 1.6 on Protection against Malware.

Support with the IT Grundschutz Tool

With the IT Grundschutz Tool (GSTOOL) introduced in 1998, the BSI provides a regularly updated and easy-to-use software package that efficiently helps the user create, manage and update security policies in accordance with IT Grundschutz. Following developments in IT Grundschutz and in response to user requests, version 4.7 of GSTOOL is now available.

Roland Schubert, Member of the IT Security Team, SIGNAL IDUNA Group

"In our Group we have had our first practical experience of using this BSI IT Grundschutz tool, and I must say I am full of admiration. All aspects of the user interface are intuitive, it is easy to understand, and it takes account of modeling and report generation requirements. The basic concept of object orientation with its inheritance mechanisms is reflected intelligently in this tool. Once you have understood the system, it is easy and efficient to use. You get the feeling that not only is this a visually appealing tool, but that the developers have also got to grips with the target functionality from the point of view of the end user."

To improve the ease of use of the GSTOOL and optimize the benefit to the user, it is constantly revised and updated in line with the latest technical developments. The BSI will soon be launching a modern application with an improved user interface that can be used over a web front-end. The GSTOOL is also being made platform-independent. In addition to various functional enhancements, the following new features have been added, primarily with larger institutions in mind: a grouping manager, an interface to directory services and an open interface for access from external applications.

ISO 27001 Certification on the Basis of IT Grundschutz
Following the model of the ISO 2700x series, a manageable and technically sound description and operating guide have been produced. As a result, IT Grundschutz complies with international requirements and can be used internationally.

For BSI certification, both the information security management system (ISMS) and the specific safeguards are tested on the basis of IT Grundschutz. It should be emphasized that the certificate always includes official ISO certification to ISO 27001, but due to the additional technical aspects tested it is a lot more informative than ISO certification on its own. Auditors licensed by the BSI satisfy all ISO requirements for ISMS auditors.

Additional Resources for IT Grundschutz
The BSI regularly publishes additional resources such as the IT Grundschutz profiles. In these profiles, case studies are used to explain the process of planning, implementing and maintaining a security policy. At the beginning of 2009 the IT Grundschutz profile for the manufacturing industry was published; this explains how IT Grundschutz can also be applied to a small manufacturing company. Resources are developed in response to questions and suggestions from IT Grundschutz users. Questions about the tasks and role of the IT security officer are frequently asked. Every government agency and every company should have an IT security officer. For German federal agencies this is a mandatory requirement. Therefore, the Model For Appointing an IT Security Officer describes the role defined in BSI standard 100-2 in concrete terms.

Special themes such as the security of routing procedures – for example, data transmission using Dense Wavelength Division Multiplexing (DWDM) and with Multiprotocol Label Switching (MPLS) – are also to be found among the IT Grundschutz resources. In the summer of 2009 short studies were published on the subjects of DWDM and MPLS. These studies offer an overview of the specific dangers and safeguards to be taken where these technologies are used.

Dr. Günter Steinau,
Managing Director, BEIT Systemhaus GmbH

"The requirements of the international standard ISO 27001 are for the most part formulated in general terms. It describes what needs to be done but says comparatively little about how to meet the requirements. So we soon recognized the value of the BSI IT Grundschutz model as a means of infusing life into our ongoing ISMS process. We use its extensive stock of tools, concepts, guidelines and sample solutions to structure our ISMS process and as a benchmark for the ongoing maintenance and improvement of our information security."

Dr. Johann Bizer, Director Solutions, Dataport

"Data security calls for structured IT operations. But you can only structure them when you have designed the underlying IT concept and set up the necessary processes. Over the last five years we have integrated four different local cultures with their various preconceptions into a single security culture. That is a considerable achievement. We have succeeded in this because IT Grundschutz has enabled us to orient ourselves toward a recognized security standard and integrate the security processes into our ITIL process culture. This is an ongoing requirement and achievement which would not be possible without the highly motivated staff at Dataport."

Standard on the High Availability of Critical Business Processes

With the High Availability Compendium (HA Compendium), which the BSI presented for the first time at CeBIT 2009, the BSI unveiled a new standard for the specification and guarantee of high availability for critical business processes. To help with the design of high availability architectures, a series of revised catalogs of measures, in which the section on availability has been expanded to include IT operations and IT organization, are now available on our website. In this way the BSI is addressing IT system operators that offer IT services for critical business processes. The HA Compendium provides extensive recommendations for safeguarding availability in system and network architectures. Going beyond purely technical aspects, it makes recommendations on securing the availability of applications and services from a holistic point of view. These descriptions of measures are presented in compact, summary form in the measures catalogs of the HA Compendium. The intention is to include assessment and control instruments in future updates of the Compendium. The main focus of the content is on the process orientation of the IT organization and tools for assessing the architecture potential and control of IT processes. The Compendium so far extends to three volumes, and the latest version is available as a download on the BSI website.

De-Mail – as Simple as E-Mail and as Secure as Conventional Mail

Dr. Astrid Schumacher,
De-Mail Project Manager, BSI

De-Mail – an Infrastructure for Secure Communication

Developed out of the Citizens' Portal project, the De-Mail project aims to set up a secure communication infrastructure for the public, businesses and public authorities and is designed to be easy for everyone to use. It is an important element of the German government's E-Government 2.0 program and is one of the four spheres in which the federal government is actively pushing e-government as a means of modernizing public authorities and Germany as a business location. The BSI is playing a major role in the conceptual design of the system.

Trust Through Security and Certification

Critical to the success of De-Mail is that the providers of the services should actually guarantee the security they promise. The primary basis for this is a suitable IT framework security concept covering everything that is relevant to the infrastructure. To be accredited as a De-Mail service provider, companies need to produce security certificates covering the themes of security, interoperability and functionality which they can obtain by following the BSI's tried and tested certification process. The aim is to enable potential suppliers to achieve a reasonable level of security, while at the same time allowing them sufficient leeway to design their own application environment. The BSI is responsible for the security and certification concept and is thus contributing its core competencies to the project. In doing so it is making an important contribution to implementing the vision of a secure and reliable infrastructure for trusted and binding electronic communication.

State and Business Community Together Define the Framework – Business Implements De-Mail

The basic security, functionality and interoperability requirements were drawn up jointly by the federal government and the future De-Mail providers and defined in BSI Technical Guidelines. Adherence to these guidelines by the De-Mail providers is verified in a legally regulated accreditation and certification process.

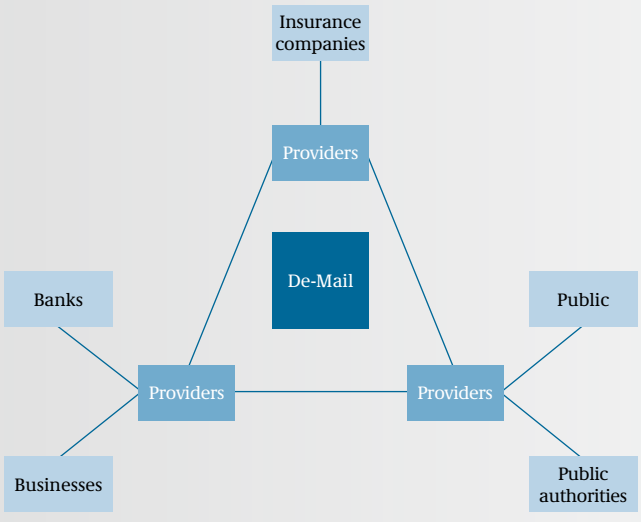
De-Mail services are thus offered by competing companies that are able to differentiate themselves from each other on the basis of the standard framework by offering additional products and services. De-Mail therefore forms the basis for a nationwide, competition-friendly infrastructure – in the interests of secure electronic communication.

Kick-off in Friedrichshafen

With the first De-Mail pilot providers, GMX, T-Home, T-Systems and WEB.DE, De-Mail reached the point where it was possible to launch a pilot in Friedrichshafen by Lake Constance on October 9, 2009 (www.fn.de-mail.de). Among the companies taking part in the tests are AWD, Citibank, CosmosDirekt, EADS, Gothaer, HUK24, LVM, Sparkasse Bodensee, Volksbank Friedrichshafen, ZF and the city of Friedrichshafen, the Ulm Chamber of Handicrafts and the Lake Constance/Upper Swabia Chamber of Industry and Commerce – along with many members of the public who are able to use De-Mail free of charge during the pilot phase. The pilot phase kicked off with the first De-Mail being sent by BITKOM to Professor Werner Zorn who, as one of the founding fathers of the German internet 25 years ago, had also received the first e-mail in Germany.

The main aim of the pilot phase, which was scheduled to last for six months, is to monitor user acceptance of De-Mail between businesses, the public and public authorities in different areas of application. The idea is that any acceptance problems or difficulties in the user interface should be detected and eliminated early on, so that by the time it actually becomes operational, the public, businesses and public authorities can be presented with a mature and recognized platform.

The Structure of De-Mail



What the Providers and Users Say:

"There is a great need for secure and trusted electronic communication between businesses, public authorities and private individuals on the internet. With De-Mail we see an opportunity to at last create a widespread standard in Germany that meets these needs. For this reason, Deutsche Telekom and T-Systems are fully committed to supporting the Federal Ministry of the Interior and the BSI in designing the functions and architecture of De-Mail and making the solution user-friendly. In this connection, the BSI was and is a strict yet cooperative and therefore ideal sparring partner. Besides this, our aim is to be one of the first providers of De-Mail."

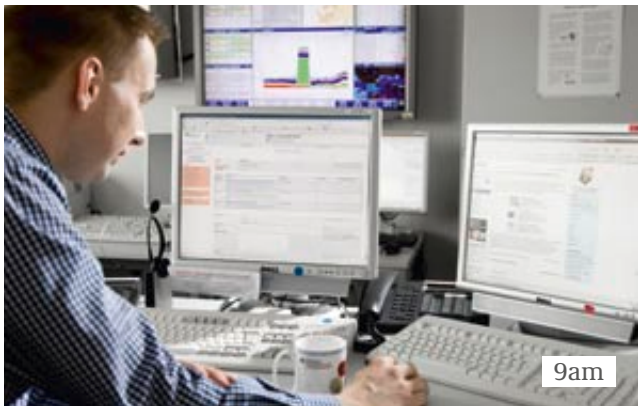
Gert Metternich, T-Systems International

"As the biggest e-mail providers in Germany, GMX, WEB.DE and 1&1 welcome the De-Mail project. Communication that currently takes place in paper form because of the requirement for a high, standardized level of legal certainty and legal force needs an equivalent digital service. GMX, WEB.DE and 1&1 have taken an active part in the project since the beginning. We have participated in the De-Mail pilot phase in Friedrichshafen and plan – assuming that the pilot is a success – to become De-Mail providers to the public, business and public authorities. To become a De-Mail provider, we will need to prove that we have implemented a series of technical and organizational measures and also prove the interoperability of the De-Mail services as part of a BSI accreditation process. We are pleased that the processes to be implemented have been closely coordinated with the business community so as to guarantee a highly secure, fast and cost-effective accreditation process."

Michael d'Aguiar, 1&1 Internet Portale (GMX and WEB.DE)

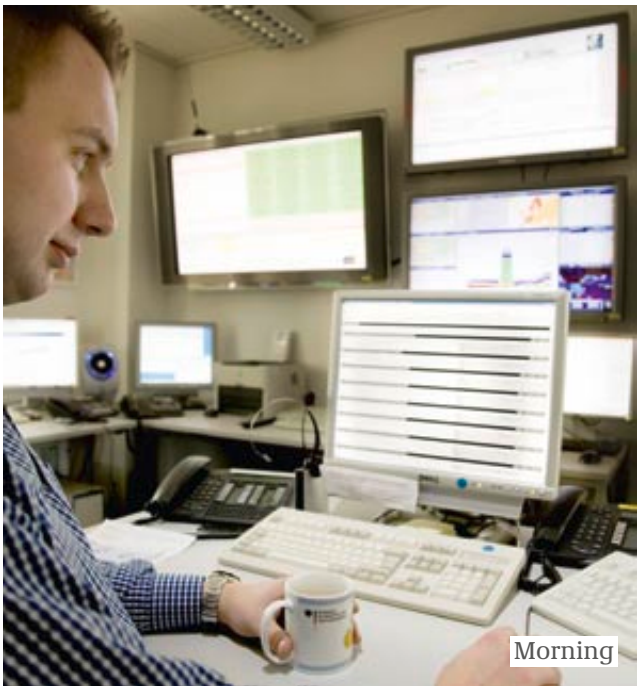
"The insurance industry offers its customers and business partners wide-ranging information services and facilities for exchanging data in electronic form. However, if a business process is to stand as legally binding today, the electronic documents have to be printed, sent out and then completed, signed and sent back by the customer or partner. With the planned De-Mail, the standardized framework conditions and IT infrastructures – which we in the insurance industry are in urgent need of – will be defined so that IT service providers can offer secure and binding e-mail services based on them. Being able to communicate by e-mail with customers, business partners and public authorities in a secure and legally binding manner is of central importance to insurance companies. We will then be able to send information to our communication partners and process it electronically quickly and without any discontinuity of media. In this connection it is critical that these infrastructures are based on verifiable standards and are overseen by the BSI as the responsible institution."

Gesamtverband der deutschen Versicherungswirtschaft e.V.


9am


10am


11am


Morning

"The trend toward the commercialization of criminal attacks that threaten the existence of the victims is becoming ever more pronounced."

Stefan Ritter, Head of the IT Situation Center, BSI


Noon

Security for the Cyber World

Always at the Ready: A Day in the Life of the National IT Situation Center

The BSI's National IT Situation Center is contactable 365 days a year. Its function is to be able to provide a reliable picture of the latest IT security situation in Germany at any time. As a result of its work, when IT security incidents strike the need for action and the options available can be rapidly and competently assessed both at state and business level.

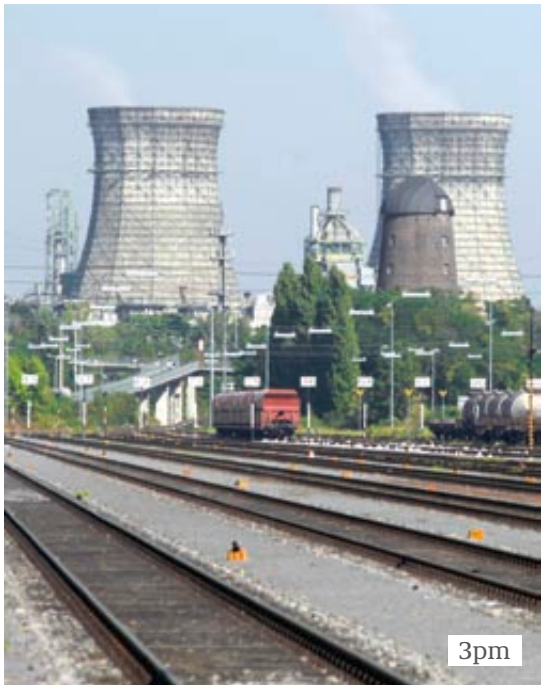
Morning: Start of Work at the Situation Center
The duty officer checks the computers and various monitoring systems in the Situation Center and consults with his colleague who was on standby during the night. He then evaluates any non-critical alarms that have occurred during the night. Intently he examines the media situation.

9am: Situation Monitoring
Point by point, the duty officer screens over 60 national and international information sources during his shift, using an extensive, web-based checklist with standard instructions. This entails going through a wide variety of specialist sources and portals and filtering all the relevant messages. Content that he judges to be of particular interest is researched further, documented and immediately forwarded to the relevant colleagues.

10am: Monitoring of Technical Sensors
While he is screening the sources, the duty officer always has his eye on the displays of the various technical sensors within and outside the government networks. These include counts of the volumes of e-mail and viruses, flow data and a wide assortment of measurement data. Should he become aware of any abnormalities, especially if threshold values have been exceeded, he alerts the relevant experts, who then immediately research the circumstances and take appropriate measures.

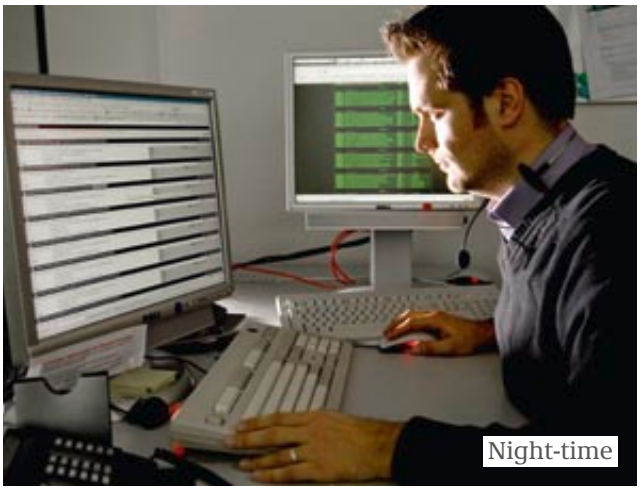
11am: Editorial Session on the IT Security Situation Report
Every quarter the Situation Center publishes a summary of the IT security situation. This entails describing, explaining and commenting on attacks and security incidents, threats and dangers, trends and statistics for the interested public. This report is based largely on the daily situation assessments, along with findings from other BSI sources that are not in the public domain.

Noon: Midday Situation Report
The duty officer presents the results of his situation assessment to the representatives of the specialist sections at the midday meeting, in the course of which the situation reports are supplemented, scrutinized and analyzed by the specialists. Additional subjects covered include the latest contributions from the specialist sections and news from meetings, events and congresses.



"Our Situation Center monitors and analyses the daily security situation and issues warnings in the event of a critical incident."

Stefan Ritter, Head of the IT Situation Center, BSI



1.30pm: Special Meeting Called to Deal With an IT Security Incident
A government agency has reported a serious IT security incident. The incident is systematically recorded and more information is requested from the office concerned. As the duty officer judges the event critical, an ad hoc meeting is called to assess the case. The duty officer presents all the known facts. The various experts called in from the specialist sections discuss and assess the situation. The next step is to ascertain possible solutions and measures and propose them to the agency.

2.30pm: Warning Message
The IT security incident has been further investigated – and a systematic vulnerability in a product used by the federal administration has been brought to light. It is now a matter of providing information and taking quick preventive action: the Situation Center and the CERT-Bund (Federal Computer Emergency Response Team) together compose a technical warning message which is immediately distributed over the warning and information service (https://www.cert-bund.de) and over BürgerCERT (www.buerger-cert.de) in a special issue of the newsletter.

3pm: Operators of Critical Infrastructures Warned
The security incident continues to keep the Situation Center busy. The vulnerability discovered clearly also affects systems that are used by operators of Critical Infrastructures (KRITIS). After consulting briefly with the BSI colleagues responsible for Critical Infrastructures, the Situation Center therefore decides to send a vulnerability warning to the partners. Over the last few years an appropriate alert procedure has been established jointly with the public and private operators of Critical Infrastructures in Germany. Using emergency contacts specially set up by the operator companies, the appropriate parties are informed promptly of the vulnerability.

KRITIS

Critical Infrastructures are organizational and physical structures and facilities that are of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences.

4pm: Exercise Preparation
The warnings that were necessary today have shown how important it is in a crisis to have an established set of contacts and well coordinated mechanisms in place. The BSI Situation Center therefore practices the response to minor and major crises in the federal administration and Critical Infrastructures with the National IT Crisis Response Center. The staff work and situation handling are run through, and vulnerabilities are identified and rectified for the next time. In this way everyone knows what they have to do in a crisis. Exercises are resource-intensive and good preparation is necessary to achieve the exercise goals.

Night-time: Constantly at the Ready
The situation is monitored on an ongoing basis. Even outside regular office hours, the Situation Center can be contacted at any time and is always ready to respond. A member of staff on standby and a manager from the Operations Team can be contacted by the federal administration and the partners of the BSI around the clock. Depending on the situation, they can escalate emergencies via various alarm chains – and in this way ensure a prompt response capability to particular IT security incidents in Germany and abroad.

Security for the Cyber World:
Analysis and Measures

Measures to Increase Security on the Internet

Dr. Lothar Esser, Head of
Internet Security Division, BSI

Botnets – No Thanks!

The problem posed by botnets has massively increased over the last few years. More and more users have a broadband internet connection. Many computers are connected to the internet around the clock. PCs can become infected with bots which exploit known security holes in services and applications, for example. Another effective method of infecting PCs is the use of social engineering, whereby the user is induced to take some action without thinking through the consequences, such as clicking on malicious e-mail links or instant messaging messages or executing e-mail attachments. There have also been recent instances of legitimate and heavily frequented websites being tampered with for the purposes of disseminating malicious code.

Botnets are the biggest threats currently to be found on the internet, and manifest themselves in the form of spam, phishing, identity or data theft (e.g. theft of passwords, PINs or TANs), blackmail, espionage and distributed denial of service attacks (DDoS). Germany is one of the top five countries in terms of computers infected with bot software. Most users are not in a position to adequately protect their computer and will often fail to notice that it is part of a botnet.

The BSI therefore provides technical expertise to support the anti-botnet initiative of eco-Verband der deutschen

Internetwirtschaft e.V. (eco: Association of the German Internet Industry), the federation of German online businesses, to cut the number of computers infected. This initiative, which was unveiled at the federal government's 4th National IT Summit at the end of 2009 in Stuttgart, is intended to make life more secure for the end user and to effectively knock the bottom out of botnets based in Germany wherever possible. The BSI is involved in the development and coordination of technical concepts for the implementation of the initiative.

As a first step, the initiative entails using honeypots and spamtraps to identify infected computers in a manner that conforms with data protection legislation. The honeypot systems are in the network area of the provider and are attacked by the infected computer. The providers' spamtraps receive the spam e-mails sent from there. In the second step, infected users are informed that their computer has been infected and at the same time receive help with eradicating the infection. Additional help is available in the form of information on a central website and a telephone help line.

"With the Botnet Initiative our medium-term aim is to remove Germany from the top 10 countries that host malicious online activities."

Sven Karge, Section Head Content, eco

Improving the Security of the Domain Name System (DNS)

In 2008 a vulnerability was discovered in a key internet service, the Domain Name System (DNS), which enabled attackers to potentially divert users' internet traffic, read their data and manipulate content. To eliminate this vulnerability, internet providers had to install software updates. But as hackers were now exploiting this vulnerability, the BSI warned all internet users and recommended that they monitor their own internet connection for susceptibility to the DNS vulnerability using a tool provided by the BSI. In this way, users could find out whether their existing internet connection was adequately protected or whether further action was needed on the part of the provider. Since then the BSI has warned a number of times of vulnerabilities in the DNS. So far it has only been possible to close security vulnerabilities temporarily.

In order to permanently improve the Domain Name System, the BSI is recommending the introduction of Domain Name Security Extensions (DNSSEC) which enable the validity of DNS entries to be checked using cryptographic procedures. DNSSEC enables known security vulnerabilities to be closed and tampering to be made more difficult.

Initiative for Greater Security

Working with eco and DENIC, the German Network Information Center, the BSI has therefore launched an initiative aimed at introducing DNSSEC in Germany. Operational and technical experience will be collected and examined within a test environment provided by DENIC. In this way the potential impacts on security and reliability will be evaluated before a possible introduction. For example, the BSI has tested home routers for DNSSEC suitability. The results suggest that many manufacturers need to perform further remedial work: out of 36 devices tested, only nine of the DNS proxies installed in the devices are compatible with use of the security enhancements introduced by DNSSEC. On the other machines, it is only possible to use DNSSEC if the installed DNS proxies are circumvented. The aim of the initiative is therefore to make the design of the products and product characteristics more secure from the start in terms of the security features to be implemented.

The BSI study on DNSSEC suitability of internet access routers can be downloaded from www.bsi.bund.de (in German only).

The Domain Name System (DNS) protocol is responsible for the translation of domain names, such as "www.buerger-cert.de", into the corresponding internet address (IP address), in this case: 62.50.36.75. The DNS is a hierarchically organized directory. If a name server cannot answer a query itself, it receives the reply from the responsible system and thereafter normally keeps it in the cache to enable future queries to be rapidly processed.

Secure Internet Access in Federal Agencies

“Aggressors Typically Exhibit a High Degree of Professionalism”

Within the federal administration, internet access is particularly sensitive and is subject to extremely high security requirements. After all, whereas the availability of the internet and online accessibility are very important for a modern administration, the latter is also a decidedly attractive target for attackers. Protecting it therefore poses high demands on the technology to be used and those responsible for it.

An interview on the subject with Dr. Dirk Häger – Head of IT Penetration Center / Defense against Internet Attacks Section, BSI

How important are networks to the German administration's ability to function?

From power cuts to floods or even terrorist attacks – the ability of federal agencies to communicate with each other has to be beyond question in every situation. Only if this is the case can remedial action be effectively coordinated. But even normal administrative activities can be threatened by disruptions or malfunctions in the information technology used, for example, if procedures for controlling the federal budget do not work properly or confidential information relating to procurement operations is leaked.

What are the special challenges that you face in protecting these networks?

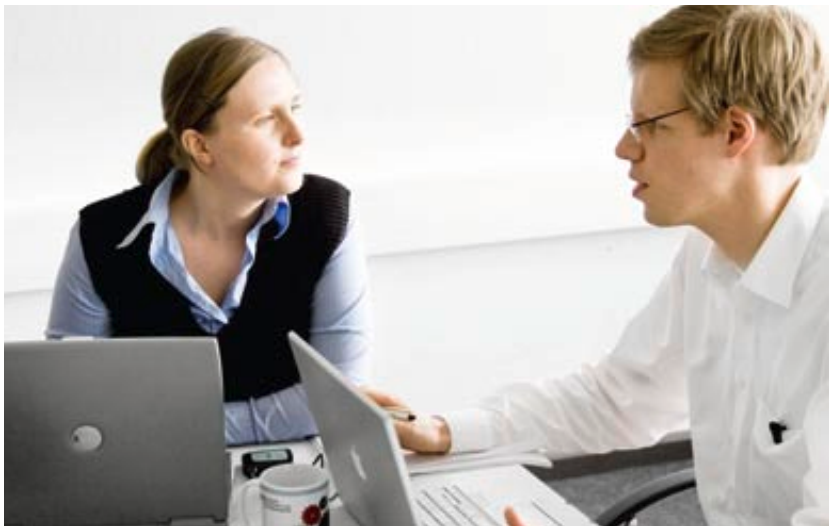
It is not just single PCs or servers like those we are familiar with in the home environment that are used by aggressors as targets. The special IT systems used by public authorities, some of which are unique to them, are also analyzed by professional criminals and their weakest points identified by stealth. Vulnerabilities in operating systems and application programs are exploited, spam e-mails are sent and attempts are made to render these services unavailable using botnets. The widespread sending of e-mails that contain backdoor Trojans and the manipulation of mobile end systems are also scenarios which, sadly, are observed every day. The information technology equipment used by public authorities is so diverse and so complex that it is not possible to protect the technology and data using the kind of simple measures that could be used for a private PC, for example. Protection of the communication infrastructures and especially the two nationwide administrative networks, the Berlin-Bonn Information Network (IVBB) and the Federal Administration Information Network (IVBV), is therefore one of the primary functions of the BSI. Under the Federal Networks project, for which the BSI is responsible, the transformation of these two central cross-departmental government networks into a powerful and secure common network infrastructure has been planned and implemented since 2008. This also takes into account the recently increased threat to entire states, as illustrated, for example, by the cyber attacks on Estonia.

Why is a federal agency's e-mail access so sensitive? And what does that mean in practice?

Anyone seeking openness also has to circumvent the problems that go hand-in-hand with it. Our situation is this: many government websites provide e-mail addresses so that the public can communicate directly with the office concerned as easily and quickly as possible. The other side of the coin is that unfortunately these addresses are also collected and exploited by senders of spam. The result is that the volume of spam e-mail received by federal agencies is vast, accounting for up to 99% of all incoming e-mails. Since 2006 the volume has increased 20-fold. However, using special techniques, the BSI is able – except in a few cases – to fend off these e-mails. In this way it is possible to reduce the burden on individual members of staff emanating from spam to a minimum. That is a genuine success. Without these protective measures, every government employee would have to deal with an average of 20,000 e-mails per month. Again, this means it is possible to effectively contain the harmful potential of spam e-mails in the form of malicious attachments and links.

What are the salient features of the attacks?

Typically the attackers exhibit a high degree of professionalism, while the attacks are increasingly directed at quite specific groups of people. Malware is often embedded in an innocent-looking document with content that is relevant to the recipient and only addressed to one



or a small number of recipients. Usually the documents in question look official and even attentive staff do not notice their malicious nature. Malicious code that is targeted at a few individuals in this way is also often missed by virus scanners.

What other objectives have been pursued in the protection of the German government's networks?

As was also the case in planning the Federal Networks project, the main design goal in setting up the IVBB/IVBV is to guarantee a high degree of protection even in special situations. To this end the following essential measures have been planned and/or implemented by the BSI:

- Redundancy: All the essential components of the networks have been designed with in-built redundancy, and not just at one location but at all the important node locations in different towns within Germany.
- Encryption: The information is transmitted encrypted. This makes it impossible for it to be read by unauthorized persons or altered.
- Central hubs: Although the different agencies are situated in many places throughout Germany, the common, shared network means that only a few central hubs need to be used. This means that the necessary safeguards can be offered in a professional manner, centrally and cost-effectively.

Standard security management is also very important. As the central IT security service provider of the federal government, the BSI has defined key principles for the security of the networks and has been involved in their implementation. The BSI Act offers an improved foundation for this. Last but not least, we offer all federal agencies security software and services for different purposes. This includes virus protection programs for workstations, for mobile devices such as cell phones and PDAs and also for mail servers. Most of the programs are free of charge to the federal government, while other products and services can be obtained under a master agreement. Authorised users can find full details in the protected area for IT security officers on the BSI website.

How would you sum all of this up?

More than ten years of successful defense against attacks proves that the measures being taken are effective and necessary. However, the changing IT landscape and the professionalization of the attacks call for a continuing improvement process, which in the medium term – bearing in mind the increasing threat potential – requires that protective measures are constantly improved.

IVBB/IVBV

The Berlin-Bonn Information Network (IVBB) entered into service as the communication platform of the ministries and other constitutional bodies following a resolution by the Federal Cabinet in 1998 and was an enhanced version of the Bonn Government Agency Network. Deutsche Telekom was involved in the development work. Services such as telephony, e-mail and video conferencing were integrated into this broadband network. The IP service platform has developed into an extremely important module both for the use of the internet and also for the shared intranet of the federal government. In 2003 a further milestone toward a shared administrative network for the federal administration followed in the form of the Federal Administration Information Network (IVBV). This gives federal agencies that do not have their own administrative network access to the cross-departmental government agency procedures and services.

Trust in the Cyber World: Education and Awareness Raising

In our society there is an increasingly great need for information about potential threats and protection options that is provided by a competent, independent party. At the same time, the information and services offered must be specifically geared to the needs of the target groups in public authorities, business and society. This includes not "overloading" them, but helping to raise the level of knowledge through the specific preparation of materials. This is essential if a corresponding media competence is to be achieved and trust in the cyber world boosted.

The German Government's coalition agreement promises to strengthen IT security in both the public and non-public domains. Greater self-protection and the use of secure IT products are important goals in this regard. The BSI is also being strengthened in this connection.

The BSI has already been active in Awareness Raising for many years. It provides information for the public, among other things through the internet portal www.bsi-fuer-buerger.de, the *Sicher Informiert* newsletter and the service center from which users can obtain telephone help and information. By attending trade fairs and information events, the BSI promotes regular exchanges of information with the various target groups, enabling it to tailor its information offerings even more effectively to their current needs.

Establishing a broad IT security culture is a demanding objective which cannot be met by a single government agency operating alone. In its public communications, the BSI therefore relies increasingly on exchanges and cooperation with partners and disseminators who are equally concerned with the subject of IT security. This enables this issue, along with its diverse technical, educational and psychological aspects, to be handled competently and exhaustively.

What the BSI's Cooperation Partners Say

AIRBUS Operations GmbH

"Airbus has been using the BSI's materials to inform and support its staff with information and security tools for many years."

Peter Behrens, Coordinator klicksafe, State Media Authority of Rhineland-Palatinate, Ludwigshafen

"The klicksafe initiative is a partner in the German Safer Internet Center of the European Union. klicksafe's mission is to run a broad media campaign and to promote media competence on every aspect of the internet among parents, teachers, educators, children and adolescents. The initiative extends across Germany and across Europe and works with players from the worlds of politics and business, NGOs and consumer protection organizations. On the basis of its technical expertise in the area of internet security and its role as a cyber security agency, the BSI is an important partner to klicksafe, and we plan to continue cooperating with it in the future in the interests of our mutual aspirations for a secure internet."

Professor Dieter Kempf, Chairman of Deutschland sicher im Netz e.V. and Chairman of DATEV eG

"In the Federal Office for Information Security, Deutschland sicher im Netz e.V. (DsiN) has a competent cooperation partner with outstanding expertise at its side. Internet security has been a central focus of the work of the BSI for years. As a result of this working relationship, both partners have already succeeded in making an important contribution toward improving IT and internet security. DsiN looks forward to continuing to work with the BSI on important activities to improve IT security in the future."

Communication – Mobile and Protected

Secure Mobile Communication – New Challenges From Enhanced Functionality

Joachim Opfer, Head of Counter-Eavesdropping Division, BSI

Today's world of work is characterized by an ever more pronounced trend toward technology-assisted mobile working. "Mobile office" is the buzzword: modern information and communications technology enables us to access corporate data, diaries and e-mail mailboxes remotely on business trips or from home. Working on the move or from home represents a genuine alternative, not least as a precaution against a possible pandemic. This has only been made possible with the development of the cell phone into the intelligent smartphone which can be used as a "mobile office in your pocket". Mobile terminal devices have long ceased to be used simply for phoning and sending text messages; these days they offer mobile internet with all the key applications and communication functions of a fully-fledged mobile office. On top of this, most of them can also be used as a digital camera, GPS navigation system or handheld computer.

"The increasing popularity of mobile working is making smartphones particularly attractive as targets for attack."

Joachim Opfer

Keeping Mobile Workstations Protected and Available

The wide range of services available on smartphones and the incontestable advantages of working on the move mean that in many places working processes are changing so much that we can no longer imagine performing our job effectively without a smartphone. As a result, society is becoming more and more dependent – dependent on protecting data against the unauthorized eyes of third parties and dependent on the constant availability and reliable operation of the mobile office.

The trend toward increased mobile working is making smartphones particularly attractive as the target of attacks. It is not just the terminal devices themselves that are tempting targets; the network infrastructures can also be the subject of an attack. Thus the potential for damage is enormous: high costs on the part of the user, loss of data, services, functions and accessibility, and, as a result, a negative impact on business productivity.

The modern information society is therefore highly dependent on the security and availability of mobile workstations. Wide-scale attacks can even have a negative impact on an entire national economy.

No End to the Threats and Malicious Functions Directed at Cell Phones

To ensure that the data stored on the PDA are protected in the event of loss or theft of the device, it should only be possible to use the device after the user has been authenticated, e.g. by entering a PIN. In addition, the data on the device should always be stored in encrypted form. If these protective mechanisms are absent or are easy to overcome, the thief or unscrupulous finder will have full access to the stored data – and may even gain access to the company's fixed-installation network or computer. Even without an attack on the terminal device, the transmitted data and conversations can be listened to by unauthorized parties if there is inadequate end-to-end encryption on the radio link. It has long been known that the standard encryption used on the GSM network can theoretically be overcome. Despite this, until recently the encryption used on cell phones was viewed as sufficiently secure for everyday applications, as highly specialized supercomputers would be needed to crack the encryption. In the meantime, however, decryption procedures have been perfected to the extent that these days even skilled hackers on modest budgets can intercept GSM mobile connections.

If an attacker has physical access or remote access via an insecure wireless interface such as Bluetooth, he can infect the terminal device with malware. As is the case with fixed-installation IT, infection over the internet is possible. One particularly malicious function

is the ability to transform mobile terminal devices into pocket bugging devices which enable hackers to eavesdrop on conversations in the vicinity unnoticed. Again, cell phones can be remotely controlled over the cell phone network. The company IT administrator, the manufacturer of the terminal device or even the network operator can easily arrange regular software updates or install new programs. But these capabilities can also be abused with the aim of "breaking in" to the terminal device and infecting it with malware. These examples illustrate how mobile terminal devices are exposed to a variety of threats that have to be countered with effective protective mechanisms.

The BSI Offers Solutions

The BSI plays an important role in making mobile communication secure. It is responsible for equipping the federal administration with secure devices and making appropriate recommendations. To this end, developments in cell phone standards, network technology and mobile terminal devices are carefully followed and investigated. The BSI regularly carries out studies on cell phone security and publishes the results in the form of brochures on its website, www.bsi.bund.de. In these studies threat scenarios are systematically investigated and concepts for protective mechanisms developed.

In addition, the agency produces criteria and security policies for mobile working for which the Mobile Synchronization Services protection profile serves as a template (specification) for developers of secure mobile solutions.

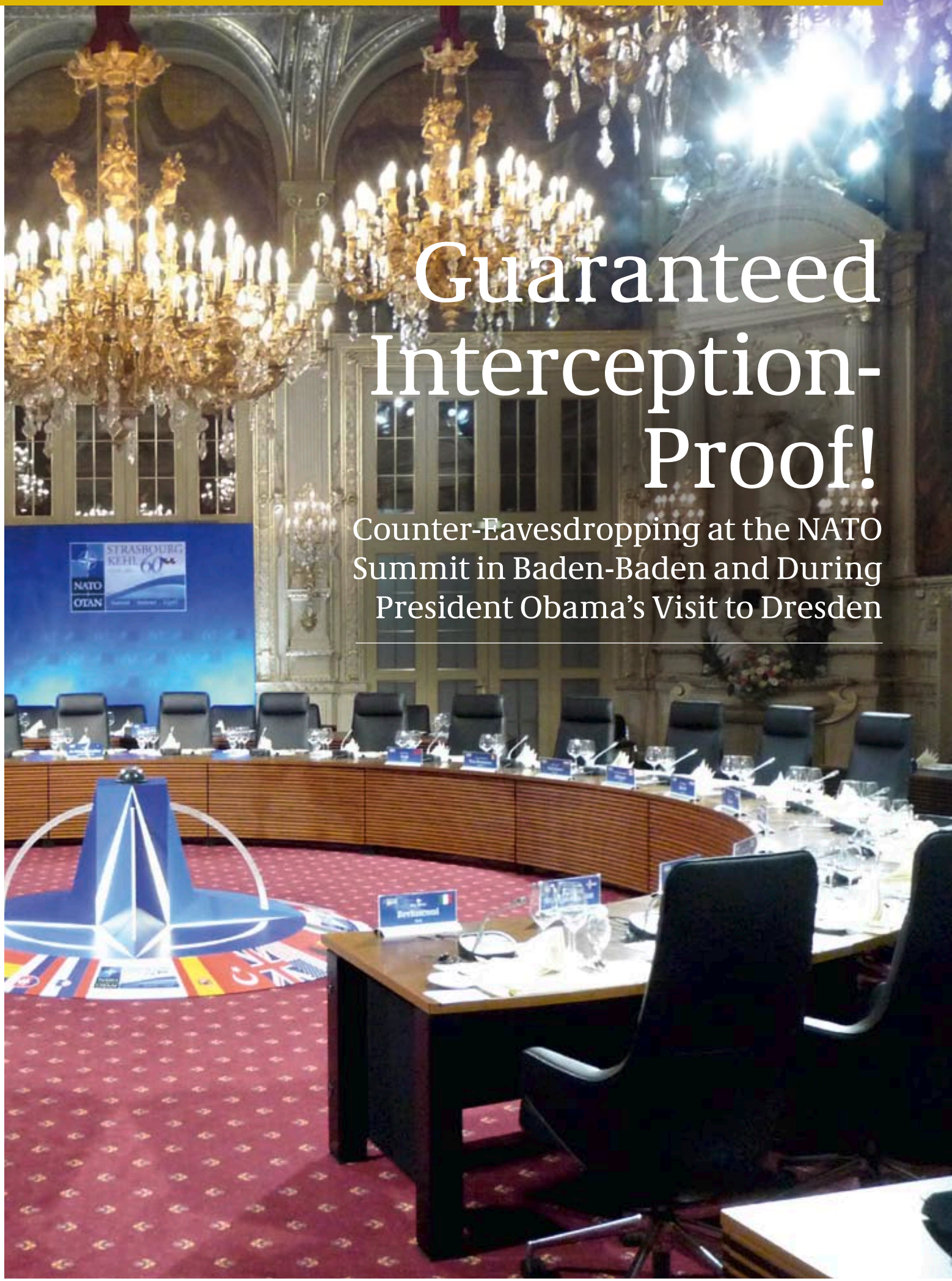
The BSI supports the development of security products for security-critical applications with the aim of approving them for use in secure applications. The core tasks entailed here are performing security evaluations and issuing approvals, recommendations for use and security certificates. Recent examples include the approval of interception-proof cell phones (Topsec Mobile from Rohde & Schwarz and Secuvoice from Secusmart) and recommendations for the use of a secure mobile PDA (SiMKo2 from T-Systems).

Interception-Proof Communication

At the beginning of 2009, the federal government approved the IT investment program as part of the Pact for Employment and Stability in Germany. This would include the introduction of 5,000 secure cell phones and a minimum of 4,000 secure smartphones in the federal administration. The BSI is in charge of this measure and is coordinating its implementation.

SiMKo2, a secure smartphone for the federal administration, was first unveiled to the public at CeBIT 2009. The BSI has approved this product as suitable for use with material classified as RESTRICTED. All the user's data are stored encrypted on the device and data are also encrypted during transmission. The software is protected in such a way that it is not possible for an attacker to tamper with the device either remotely or with direct access to it or to read data handled with the device without authorization.

With Topsec Mobile and Secuvoice, two different cell phones suitable for encrypted, interception-proof telephony up to RESTRICTED category are now available.



Guaranteed Interception-Proof!

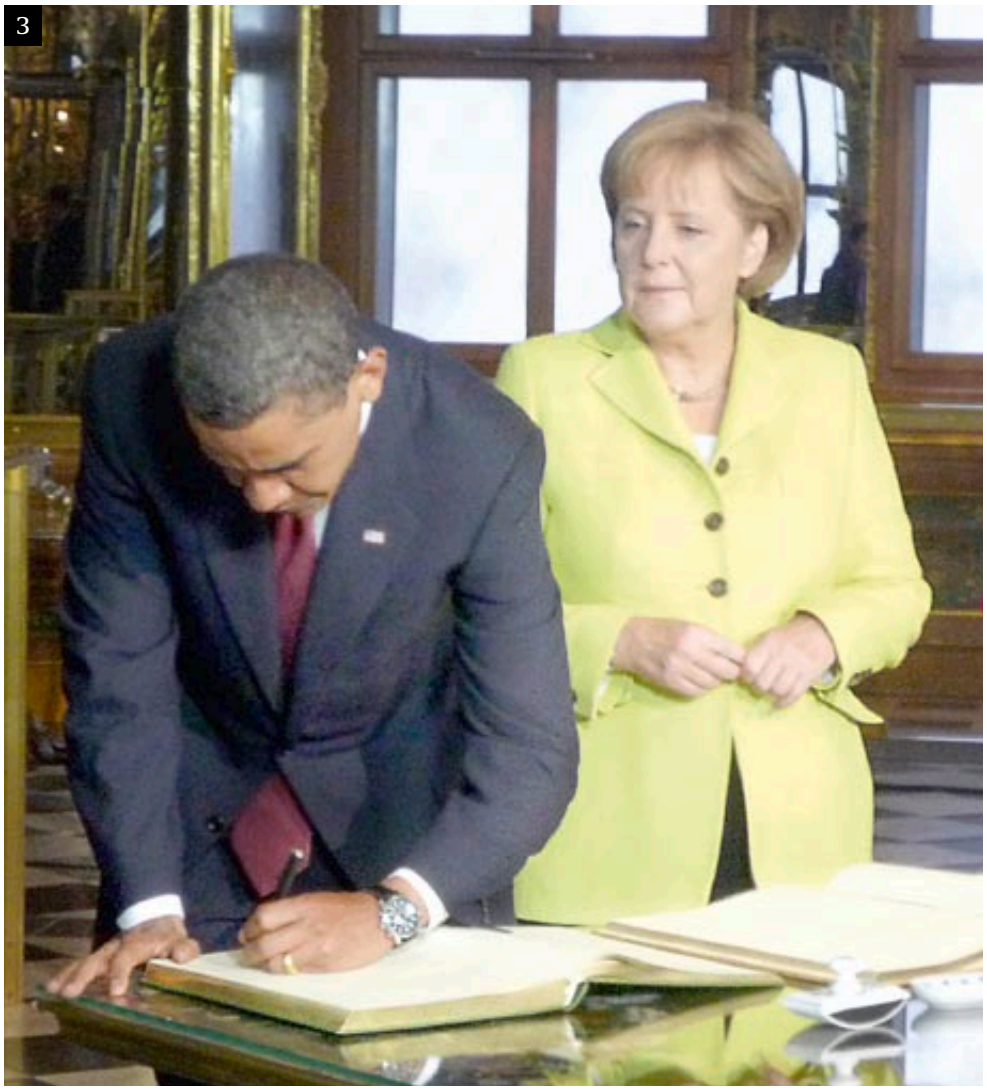
Counter-Eavesdropping at the NATO Summit in Baden-Baden and During President Obama's Visit to Dresden

The BSI offers eavesdropping countermeasures in government agencies as a service. It also provides support services for high-level conferences and bilateral meetings at which it is essential that conversations should remain totally confidential. The job of the Eavesdropping Countermeasures section is to ensure that no bugging devices are present and that it is not possible for information relating to meetings to fall into the hands of unauthorized persons by other routes, for example via cell phones that have been tampered with or accidentally activated. The most prominent events in 2009 for which the BSI provided this service were the NATO summit in Baden-Baden and the visit of US President Barack Obama to Dresden.

From Major Conferences to One-To-One Discussions – the BSI Keeps it Confidential.

Just as the occasions themselves can be very different, so too are the measures that need to be taken. This becomes clear when one considers the different rooms and orders of magnitude involved in high-powered meetings. While Baden-Baden was the venue for a large-scale gathering of NATO heads of state and government, in Dresden the job was to protect a tête-à-tête that took place in the historic Grünes Gewölbe (Green Vault) located on the ground floor of the Residenzschloss (Royal Palace) behind barred windows. The Bronzenzimmer (Bronze Room), which was earmarked for the meeting, had been open to the general public just a few days earlier. The entire Residenzschloss was therefore closed to the public during the preparatory phase so that the BSI staff could start their eavesdropping countermeasures.

3

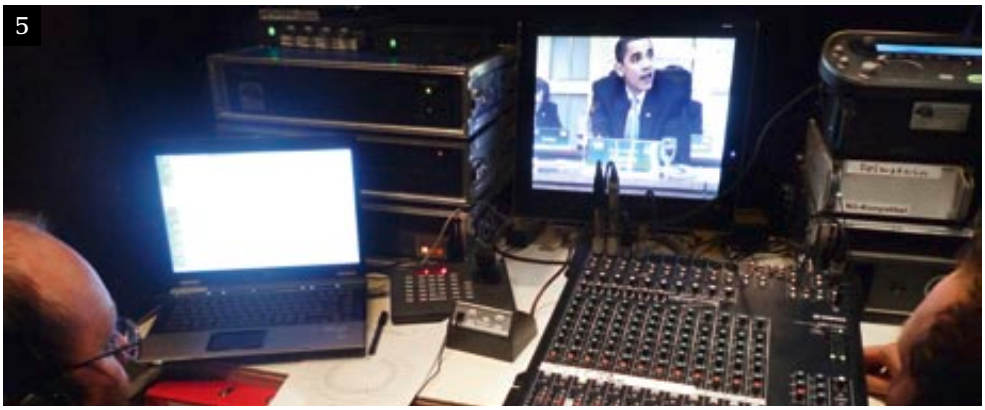


4

1

2

5



1. *The chairs on which the Federal Chancellor and the US President sat during the one-to-one conversation were X-rayed.* **2.** *In the adjoining Wappenzimmer (Coat-of-Arms Room), which was also earmarked for a confidential discussion with a larger number of participants, the measures taken included examining the numerous wall cabinets for illegal bugging devices.* **3.** *Immediately before the meeting, the Federal Chancellor and the US President signed the Golden Books of the Free State of Saxony and the City of Dresden.* **4.** *While the confidential meeting was going on, a BSI monitoring vehicle outside the building was monitoring the high frequency spectrum for illegal bugging transmitters and active cell phones in the conference room.* **5.** *Over to the NATO summit in Baden-Baden – at events with international participants, elaborate conference technology is often used for translation and sound recordings. Depending on the type of event or meeting it is important to ensure that no confidential information imparted at the meeting can be intercepted or recorded by unauthorized persons.*

“The EasyPASS pilot project is intended to provide detailed information about the security, efficiency and practicability of biometrics-based border controls.”

Markus Nuppeney

Secure Electronic Identity

EasyPASS – Fast and Easy Border Control With the Electronic Passport

Markus Nuppeney, Project Manager, Official Electronic ID Systems, BSI

In 2006 the technical specification for electronic passports (ePassports) was finalized by the International Civil Aviation Organization (ICAO). As part of its work on international standards, the BSI made significant contributions to this specification, in particular the electronic security mechanisms for ePassports.

Today over 60 countries in the world issue ePassports that comply with the ICAO standards. These passports have an integrated, contactless readable chip (RF chip) on which the electronic security features are held, along with the personal data and a digital photograph of the passport holder.

Secure, Efficient and Convenient
The increasing use of ePassports is opening up new possibilities for the implementation of official identity checking processes. Thus, for example, the use of ePassports promises a number of advantages and optimization opportunities in the context of border control:

- **Increased Document Security**
  Thanks to the electronic data and security features that are additionally incorporated into the ePassport, document forgeries and misuse can be easily and reliably detected and prevented.
- **Efficient Document Verification**
  The RF chip integrated in the ePassport enables rapid and automated checking procedures that are useful for coping with an increased flow of passengers at border checkpoints.
- **Convenient Use Cases**
  Thanks to the ePassport and the automation potential that goes hand-in-hand with it, new potential use cases such as self-service border control processes for ePassport holders become feasible.

EasyPASS Pilot Project for Faster Border Controls
To exploit this optimization potential in practice and open it up for actual border control processes, the BSI is running the EasyPASS pilot project at Frankfurt airport in collaboration with the German Federal Police. The design phase of the project began at the end of 2007. The main aim was to examine the use of biometric facial recognition based on the ePassport in the context of a (partly) automated border control process. One core element of the design is the BioMiddle biometrics framework, which was developed jointly by the BSI and secunet Security Networks AG specifically for use in governmental biometric applications. BioMiddle is already used successfully in various official scenarios, and in the context of EasyPASS it also constitutes the central integration platform. The modular architecture of the middleware – which is based on international standards – ensures vendor-independent interoperability, so that hardware and software components from different suppliers can be used simultaneously and individual subcomponents can be easily exchanged.

The design phase was followed immediately by the development and integration of the individual system components (hardware and software), with the result that the EasyPASS passenger system (four eGates, each equipped with a

EasyPASS consists of the following four process steps:

1. **Optical Document Check**
   During the optical check, the data that are visible on the data page of the passport are scanned and the optical security features of the passport are checked.
2. **Electronic Document Checking**
   The electronic check is carried out based on the data stored on the RF chip of the ePassport. The data from the chip are read after appropriate authentication and the entire set of electronic security features of the ePassport is checked.
3. **Biometric Comparison**
   For the biometric check, the photograph electronically stored on the ePassport chip is compared with a live image of the person taken inside the eGate.
4. **Police Search Warrant Check**
   In the police search warrant check, a query is sent to the central police information system about the person being checked.

In addition to the checks necessary for the actual border control process, further biometric tests with algorithms from different suppliers are also carried out for the purpose of system evaluation.

The following aspects are of prime interest for the technical evaluation of EasyPASS:

- **Biometric Performance**
  For the purposes of assessing biometric performance, the main focus is on recognition accuracy, that is, how well passengers can be authenticated on the basis of their picture. The quality of the pictures used in the process and the number of verification attempts are also determined.
- **Time Required**
  One important goal in this context is to determine how long the entire automated control process takes. To enable detailed analysis of the time required and ascertain the potential for improvement, the time required for each individual step in the process is recorded during the pilot phase.
- **Sources and Frequency of Errors**
  To ascertain the sources and frequency of errors, an error protocol is maintained for all the process steps during the pilot phase.
- **Usage and Document Statistics**
  The usage and document statistics are intended to provide information on how frequently the EasyPASS systems are used and on the demographics of the user group (age, sex, etc).
- **Ease of Use and User Acceptance**
  In addition to the technical evaluation aspects, the pilot study will include an assessment of the system usability, and data on user acceptance will also be collected.

document reader and an intelligent camera system) was installed at Frankfurt airport ready for intensive testing in summer 2009. The official opening by the Federal Minister of the Interior took place in October 2009.

Less Waiting Time for Passengers

Citizens of the European Union (EU), the European Economic Area (EEA) and Switzerland who have an ePassport and are at least 18 years old may take part in EasyPASS on a voluntary basis and without prior registration. Under the EasyPASS procedure, the passenger places his ePassport on a document reader and then enters an eGate. Inside the eGate, a facial picture is taken by a height-adjustable camera and, using appropriate facial recognition software, this is compared with the picture stored in the RF chip of the ePassport. Meanwhile the authenticity of the document is verified and police search warrant checks are carried out in the background. If these checks do not throw up any irregularities, the eGate opens and the passenger is allowed to cross the border. Officials from the Federal Police oversee the process and can intervene as required. They also decide on the basis of the verification results whether and what control follow-up measures are necessary.

The EasyPASS pilot project is intended to provide detailed information about the security, efficiency and practicability of biometrics-based border controls. At the same time it is intended to significantly reduce the workload of conventional border checkpoints and the amount of time that passengers have to spend waiting.

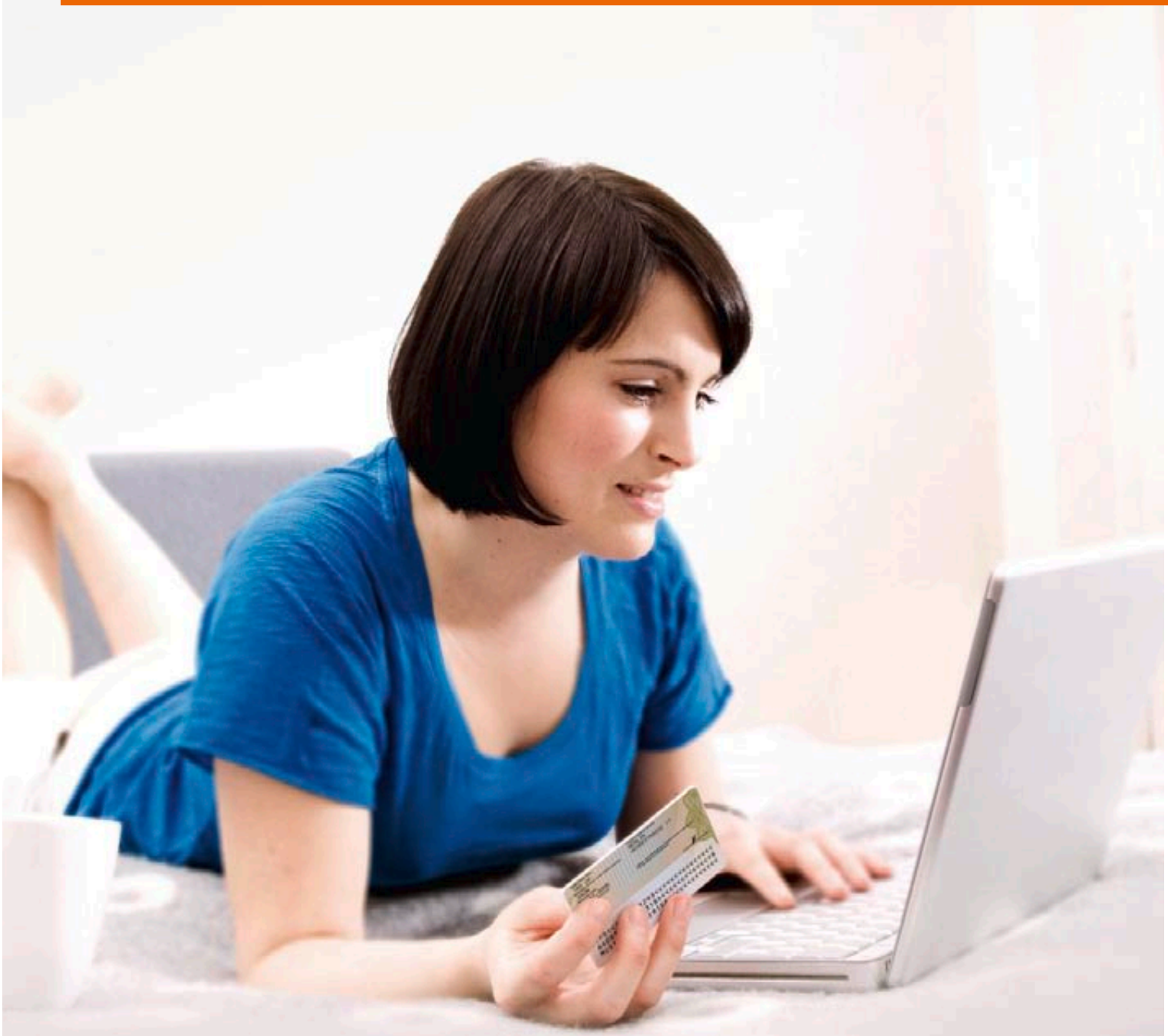
“Our Aim is to Raise the Level of Security.”

Three questions for Wolfgang Wurm, President of the Federal Police Directorate, Frankfurt Airport

What form does the collaboration between the Federal Police (BPOL) and BSI take?
EasyPASS is a joint project between the Federal Police and the BSI on behalf of the Federal Ministry of the Interior. In the context of electronic checking of official documents and the use of biometric systems, the BSI has once again proved a competent and reliable partner to the Federal Police. This constructive cooperation contributed significantly to the successful start of the project.

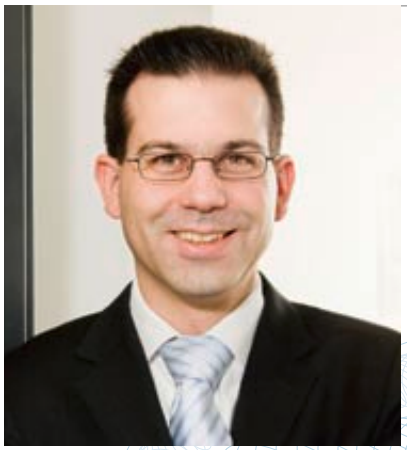
What benefit does EasyPASS bring to border police in practice? Has EasyPASS already proved its worth?
With the introduction of ePassports, additional security features were incorporated into the travel document in the embedded chip. As a (partly) automated border control system, EasyPASS is able to check these security features quickly and reliably and thus to verify the authenticity of the travel document. In addition, the system performs automated identity checks and police search warrant checks. Due to the rising number of passengers arriving at German airports, we need to upgrade the conventional border control procedures used up to now with the use of secure, reliable, user-friendly and cost-effective technologies. With an average check time of about 15 seconds per passenger, EasyPASS is already ensuring a gratifyingly high passenger throughput rate in the pilot run. Moreover, the check procedures implemented also have the effect of raising the level of security. Through this functionality, and also the fact that the system takes up less space, the number of border control officers required can be reduced and selectively deployed to other areas, for example, to cross-border traffic and search duties. Meanwhile travelers benefit from noticeably shorter waiting times at the border checkpoints. The stable functionality and the very low rejection rate suggest even now that the test run will have a positive outcome.

What are the next steps beyond the pilot phase?
Once the EasyPASS pilot phase is over, the system will be evaluated in terms of functionality, security, ease of use and cost effectiveness on the basis of the findings to date. Only then can the requirements for a future rollout be defined and included in plans to implement (partly) automated border control systems. However, on the basis of the positive preliminary results I have outlined, we expect to be able to roll it out quite soon.



Secure Identification on the Internet With the New German ID Card – a BSI Project That is Unique in the World

Manuel Bach, Technical Project Manager, Bürgerclient, BSI



"A fine balance has been achieved between data protection and user convenience."

Manuel Bach

Working on behalf of the Federal Ministry of the Interior, in 2008 and 2009 the BSI worked intensively on a major project that will become relevant for large sections of the German population from November 2010 onwards: the introduction of the new German ID card. As well as some other innovations over the old ID card (credit card format, contactless RFID interface, biometric picture and optional storage of two fingerprints), the new ID card offers functions that will open up completely new possibilities for members of the public using the internet, thanks to an integrated computer chip.

RELIABLE PROOF OF IDENTITY

Just as in the offline world, in which German citizens can prove their identity by presenting their ID card (e.g. when they collect a parcel from the post office), in the future they will be able to do this online as well. This possibility has enormous advantages for both the users and providers of services or goods on the internet. An internet supplier can be sure that no-one can create a user account with false identity data. As a result, dispatching goods on account will become a lot less risky for an internet retailer. There will also be many advantages for individuals. Take someone who wants to invest money in an online bank, for example. They can open an account online and even transfer their initial deposit online, but they will usually have to go to a post office and prove their identity with their ID card using the Postident procedure. This is annoying for the customer – and expensive for the bank. In future, people will be able to use the new ID card to transmit their personal data securely over the internet.

LESS INFORMATION WHEN APPROPRIATE – WITH ELECTRONIC PROOF OF AGE AND PASSWORD SUBSTITUTE FUNCTIONS

For many transactions on the internet, all you have to do is prove that you are of the minimum age required

The new German ID card (nPA) guarantees secure transmission of personal data over the internet

Holders of the new ID card have complete control over their data

for the transaction. The provider does not need to know your name and address, but for youth protection reasons they must make sure that people below the minimum age do not have access to their goods and services. The new ID card has a function for this situation too: electronic proof of age. In principle the exact date of birth can be transmitted, but often all that is needed is proof that the person is at least 16 or 18. Again, such data protection-friendly yes/no information can be transmitted with the new ID card.

Finally, the new ID card can also be used as a substitute for a username and password – even where the user does not want to reveal their personal data to the internet provider. For example, on web forums it is usual to make up a username. The person behind that name is not even known to the operator of the forum. With the new ID card it will be possible to register and log on in a forum completely anonymously. For this purpose a sector-specific ID will be generated by the ID card chip – in combination with a key sent by the service provider along with its certificate of authenticity. Then the service provider will recognize the ID card holder the next time they log on. This ID does not contain any other information on the person such as their name or address. The ID card generates different sector-specific IDs for different service providers. If, for example, the user has one anonymous account with a web discussion forum and another with an online games portal, the two operators of these web services have no way of finding out that they are dealing with the same person – not even if they were to compare their databases – either legally or illegally.

SECURE DATA TRANSFER WITH THE BÜRGERCLIENT

For all these applications there are two more things people will need besides the new ID card and a computer with an internet connection: a contactless card reader and some special software, the Bürgerclient (Citizen's Client). The card reader will be available for purchase for a small sum and will probably even be routinely installed in computers, while the Bürgerclient will be provided free of charge to people by the federal government in versions for the Windows, Mac OS and Linux operating systems. Once the necessary

components are on hand and installed, the procedure will always be the same. For example, if you want to log in to a web portal – that of your e-mail provider, say - you will open the relevant website in your browser and click on the "Log in with ID card" option. A Bürgerclient window will open, in which you will be able to see not only what data the service provider is asking for (you are free to decide what authorizations you want to grant), but also exactly which provider you are dealing with, as the service provider also identifies themselves to you. The authenticity of these data is also confirmed by the state: the service provider receives an electronic certificate of authorization from the Federal Administration Office. You then place your ID card on the card reader, enter your six digit ID card PIN (which you can change at any time) and the login process is over within just a few seconds.

Another function of the new ID card is the ability to create qualified digital signatures. With the aid of the Bürgerclient and a suitable card reader, a person will be able to append a legally binding digital signature to any data (e.g. e-mails or PDF forms). Unlike the electronic proof of identity, however, this function will not be included in the ID card fee, but will only be pre-enabled on the card. They will be able to acquire a suitable signature certificate online from a provider of their choice. Alternatively, instead of the ID card, they will also be able to use any of the other signature cards commonly available on the German market with the Bürgerclient.

SUCCESSFUL BALANCE BETWEEN DATA PROTECTION AND USER CONVENIENCE

In the course of the ID card project, the BSI not only provided the technical specification of the ID card's security properties; the software infrastructure ("eCard API framework"), the Bürgerclient, the card reader, the data entry terminals at the data collection points, and many other necessary components are also based on technical guidelines issued by the BSI. The overall concept is not only meeting with great interest among service providers, even leading advocates of data protection have lent it their support. In comparison with other countries' e-ID solutions, which often require the entire personal data set to be sent to the interrogator at once, holders of Germany's new ID card have full control over their data. Each time they use the card they can decide what data they want to disclose and to what extent. Moreover, the Bürgerclient will show them clearly which service provider they are dealing with. The identity of the service provider will have been previously checked by the Federal Administration Office. So the new ID card and the Bürgerclient are making an important contribution to fighting the fraud which, sadly, is a daily occurrence on the internet – and are also protecting individuals against the collection of personal data by companies that do not really need these data for the intended transaction. In short, a fine balance has been achieved between data protection and user convenience.

Application Tests

Practical tests are being used to prepare the way for, test and evaluate the use of electronic proof of identity for access to e-business and e-government services on the internet and in cash machines. The test phase has been running since October 1, 2009 and will continue until October 30, 2010. In June 2009 thirty interested parties were selected for the centrally coordinated part of this test from a large number of registered companies, institutions and authorities. This part focuses on the practicality, manageability and acceptance of the electronic proof of identity of the future ID card. The aim is to create a large number of attractive potential uses for the new ID card and then make these available in practice to members of the public from November 1, 2010 onwards.

Tackling the Challenges Together

Security in IT – It Has to Be Learnt!

As the threat level increases, the demand for qualified IT security experts in the private and public sectors is increasing. The BSI plays an active role in training and continuing education at federal administration level and makes a key contribution to making the processes of today and tomorrow more secure. It goes without saying that the BSI is also involved in knowledge transfer in the area of IT security in academia and is an established center of technical competence.

IT Security Certificate

In 2009, 46 people passed the basic course and a total of 31 certificates were awarded. Twelve people attended extension course A, with seven certificates awarded. 2009 was the first year in which a participant achieved the highest level of training. The IT Security Officer in Public Administration certificate is valid for a fixed period, but can be renewed through regular continuation training and workshop attendance.

Secure Administration with the IT Security Officer in Public Administration Certificate

The federal government implementation plan requires all government agencies to appoint IT security officers, draw up IT security policies and above all respond promptly to security recommendations. The idea is that the IT Security Officers in Public Authorities will initiate and monitor the necessary security process measures, supported by the management of the authority concerned. All activities relating to IT security must be professionally organized, and the BSI standards have become established as best practices for setting up and operating IT security management.

In collaboration with the Federal Academy of Public Administration (BAköV), the BSI offers training and further education courses with a graduated, three-stage final examination to become a Certified IT Security Officer in Public Administration. The content is constantly adapted by the BSI to reflect current knowledge about security risks and safeguards. The training is given in blocks structured by subject which can be chosen in modular fashion in line with the prior knowledge of the student. The final examination comprises project work, presentation of the project at a seminar and a written test in which candidates have to answer multiple-choice questions on IT security.

More than 100 IT Security Officers in Public Administration meet once a year to exchange ideas and information

Markus Ullmann of the BSI (right) supervises the BA dissertation of Ranbir Singh Anand, an Information Sciences student at Bonn-Rhine-Sieg University of Applied Sciences

The job profile of the certified IT Security Officer in Public Administration creates structure, competence and recognition and thus provides an optimal basis for ensuring that IT security is maintained at a high level in government agencies. Communication between security consultants and IT security managers takes place on equal footing, with both sides using the same language and having the same understanding of security. In this way, it will be possible to respond immediately in an IT crisis – without any loss of information or communication problems.

Cooperation for Mutual Benefit

Since 2001, the BSI has had a cooperative arrangement with Bonn-Rhine-Sieg University of Applied Sciences. Staff from the BSI support the university's Information Sciences faculty by running courses on information security. In 2009 the relationship was reinforced by the appointment of Markus Ullmann, Head of the New Technologies and Scientific Foundations Section at the BSI, as an honorary professor at Bonn-Rhine-Sieg University.

This cooperative arrangement brings benefits to both sides. On the one hand students profit from the practical lectures, which significantly enhance the teaching on information security at Bonn-Rhine-Sieg University. The BSI for its part benefits from an additional multiplier effect through the use of BSI public domain content in the security courses. In addition, the teaching activities make it possible to involve students in the work of the BSI through work placements and Bachelor's or Master's dissertations, to the benefit of both sides. Students can familiarize themselves with the BSI and its work and also get to know the agency as a potential employer. As the market demand for graduates in Mathematics, Information Sciences, Science and Technology increases, early contact with students is becoming more and more important for the BSI – especially at a time when the number of new graduates is decreasing.

However, the primary objectives of the collaboration are to institutionalize teaching in information security more strongly and to increasingly cooperate in applied research in the area of information security.

IT Security – an International Task

The cross-border networking of communication and information systems makes it imperative to join forces at an international level. The BSI also meets the global challenge of information security through its active involvement in committees, for example in the EU, NATO, OECD and ISO, and also through bilateral and multilateral cooperation with other states.

The international activities of the BSI are shaped by its role as the national IT security agency and as an internationally acclaimed IT security competence center. Through its technical and operational competence, its successful collaboration with industry and involvement in international collaborations, the expertise of the BSI is much in demand – in Europe, for example, for European Commission consultations and expert workshops, in the development of the IT security architecture for the Galileo satellite system, or as a partner and member of the management board of the European Network and Information Security Agency (ENISA).

On top of this, the BSI maintains a valuable dialogue at managerial and technical levels with numerous government agencies and ministries around the world.

Tackling the Challenges Effectively

Guest Contribution by Patrick Pailloux, Director General of the French Network and Information Security Agency (FNISA), France

"These days the internet is part of the daily life of all Europeans. But as innovative applications have been developed and the concept of the information society has taken shape, the malicious use of the internet has undergone exponential growth – to an extent that jeopardizes the opportunities that information technology offers us. On the other hand, a global political awareness is already germinating, and the desire to tackle the challenges factually and objectively is taking root. It is interesting and at the same time reassuring to note that the Germans and French share the same strategic vision as regards cyber security. This has led to similar conclusions, which are manifested in three areas. The first of these is the strengthening of the claim to leadership by the national structures that are responsible for the security of information systems. Secondly, we are seeing a high-level urgency in the implementation of cyber security, especially through monitoring of the most sensitive networks. And finally there is a recognition that the development of security products needs to be speeded up.

In both our countries these aspects have been expressed in concrete terms at the political level, in France through the publication of the directive to set up the French Network and Information Security Agency on July 7, 2009. This was done as part of the new French strategy on defense and national security, which attaches a high degree of urgency to the defense against IT attacks. In Germany the amendment of the BSI Act, which gives the BSI additional tasks and powers, entered into force on August 19 of the same year.

In practice there are many points of convergence in the newly defined missions of our two agencies. Our radius of action covers the totality of the information society. Going beyond the protection of classified information – which has long been anchored in our history – we are increasingly directing our attention to the general public. As part of our primary mission we are feeding our expert knowledge of IT security through to the administration, the operators of critical infrastructures, all the various business players and the wider public.

As well as providing assistance, we must use our technical expertise to actively make services and trusted security products available to government agencies and business players. And we also have a duty to develop and contribute innovative solutions and to no longer confine ourselves to the role of critical observer, as we have done in the past in France. In the face of a greater threat, our commitment and our active participation are ever more important. There is a compelling need to find pragmatic and affordable solutions to the problems that we face.

All in all, effective action presupposes an exchange of information, a sharing of experience and cooperation among allies. These are not just words – deeds are an unavoidable obligation. One aspect has to be emphasized above all: the threat today is global. The internet sets aside the notion of distance and borders. In view of this trend, it is imperative that we cooperate so as to defy this threat.

In the area of cyber security, the Franco-German relationship must be and must remain a shining example. It will be the engine for the further development of IT security in the European Union."

"We Need the BSI's Expertise in Europe"

Interview with Dr. Udo Helmbrecht

Dr. Udo Helmbrecht is Executive Director of the European Network and Information Security Agency (ENISA) in Heraklion, Crete, and was President of the BSI from 2003 to 2009.

Dr. Helmbrecht, in which areas do you think Germany should play a key role at EU level and what contribution do you expect the BSI to make toward strengthening IT security in Europe?

The BSI has already done a great deal to increase the level of security in Europe. I am reminded here of all the many cross-border contacts that have been established. But it is also extensively involved in many projects like the STORK[2] project. We need the BSI's wealth of experience and expertise in Europe. I would like to see this knowledge transfer and the involvement of the BSI in many international forums and bodies further expanded, especially its involvement in the ENISA executive board, on which the BSI represents Germany. The BSI stands as a shining example in the European Union. For example, just look at France: a similar security agency, FNISA (French Network and Information Security Agency) has been set up there in the past year.

On which areas is ENISA currently focusing?

ENISA's work program for 2010 features three major themes: the resilience of networks including critical IT

infrastructure protection, stronger forms of cooperation such as CERTs and addressing emerging and future risks. This year we have also turned our attentions to some preparatory programs: firstly, the issue of trust and the legal protection of a person's privacy, including digital identities (e-ID), and secondly, incentives and obstacles for multi-stakeholders – cooperation models in the area of network and information security.

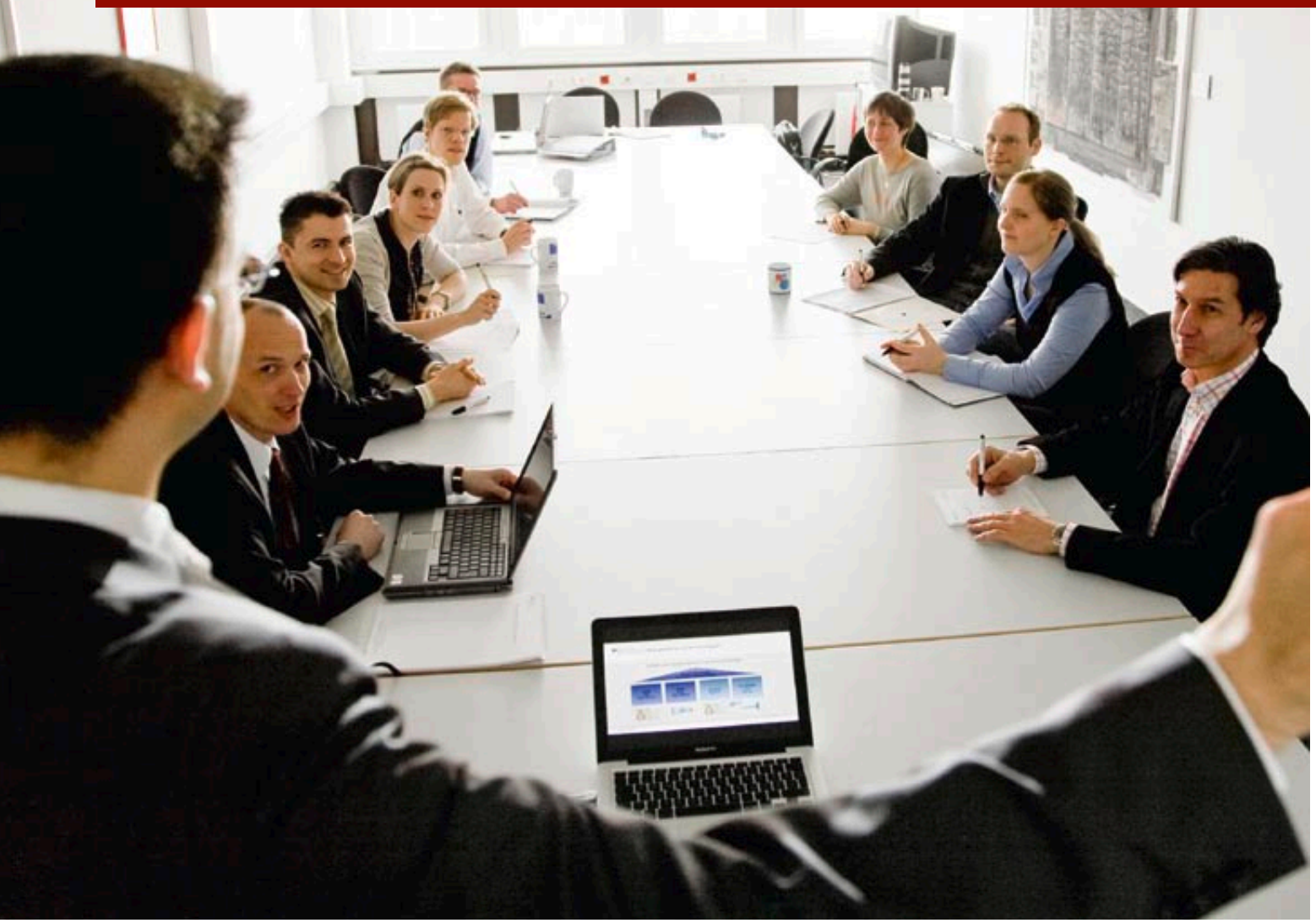
How are you finding cooperating with the member states?

As a competence center, ENISA brings together all the relevant stakeholders and boosts the exchange of experience and information. We are positioning ourselves as a pioneer of greater IT security in order to come up with European solutions in a close partnership. Indeed, some member states have already made a lot of progress in some areas. We expect them to be willing to transfer their knowledge to the new member states, for example. We are all aware that security does not stop at the border, and at the end of the day every transfer of know-how will enhance our own security. I am optimistic that this will continue, and to a greater extent as well. There are plenty of examples of this already, such as in the CERT/CSIRT[3] area. It is our aim to see a government CERT in every member state. Thus Germany will be able to benefit from cooperation with ENISA with improved IT security at European level.

What would you like to see in terms of IT security in Europe?

ENISA must take up the future technical challenges of information and communications technology in its work program by further expanding the high-quality dialogue with member states, EU institutions and all the other players in the information society. But in doing so, ENISA should not duplicate any activities of the member states or compete with them. Rather, it should provide advice and support in cases where there is added value to be gained in the European alliance, either for the individual member state or the EU as a whole. The results, which at the end of the day reflect the efforts of all the partners, must be visible in the member states. To this end I call on all parties to cooperate.

[2] STORK (Secure Identity Across Borders Linked): www.eid-stork.eu
[3] Computer Emergency Response Team/ Computer Security Incident Response Team



Tackling the Challenges Together

The Heart and Brains of the BSI: Our Staff

Actively Shaping IT Security

The critical success factor behind the work of the BSI is its employees. Many of the staff who work in the Federal Office for Information Security see their job not just as a career but also as a calling. For them, having the opportunity to actively help shape the theme of IT security going forward is both a challenge and an opportunity. At BSI, employees enjoy very good working conditions, for example a high degree of personal responsibility, state-of-the-art technology and excellent training opportunities – coupled with a positive working environment and the prospect of a secure job. On top of that there are plenty of contacts at international level and with the private sector.

Further information about working at the BSI and job vacancies can be found at www.bsi.bund.de.

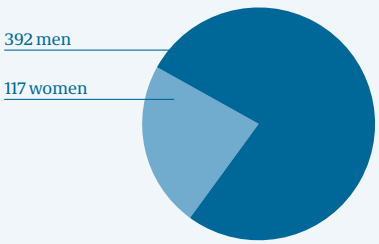
"The working environment is very friendly. Experienced and young staff cooperate very well."

Semra Agirtas

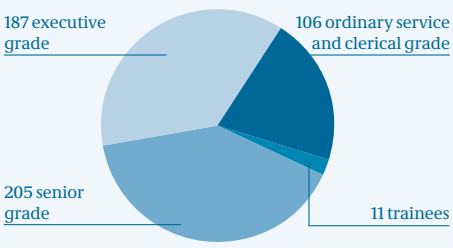
Semra Agirtas, Specialist, Accreditation and Quality Management of the Certification and Accreditation Scheme

"I find the subjects and tasks that the BSI handles fascinating. What is important here is not helping a company make more money, but offering a useful service to the public, government agencies and thus to society in the form of standards, guidelines, advice and warnings. What motivates me particularly about my work is that it is part of a bigger cause, which usually affects and interests the whole of Germany and drives it forward. It is exciting to be playing a part in shaping the future in areas such as the electronic health card, De-Mail or digital radio and to do my bit in the ever changing world of technology and society. In fact, I like everything about working at the BSI. The tasks and subjects are very varied, and I have a modern workstation that is geared towards my needs. The working environment is very friendly. Experienced and young staff cooperate very well, and there are lots of joint events that generate a team spirit. There are also plenty of opportunities to look beyond the rim of your own teacup. The continuing professional development opportunities open up new horizons and show me that I am valued as an employee. At the BSI you can plan your future, as it has policies that are designed to enable a woman to combine career and family."

Statistics – Employees (end of 2009)



Employees (Career Groups)



Focusing on the Next Generation

Since 2008 the BSI has provided Bachelor's degree students with grants coupled with the promise of a permanent job when they graduate.

"At the BSI, decision-making lines are short and the mindset is customer-oriented."

Dr. Uwe Kraus

Dr. Uwe Kraus, Head of Cryptographic Technology Division

"I enjoy being able to put my knowledge and ability as an engineer and business information graduate to good use at one of Germany's top IT employers, which I joined in 2004. After two years of working as a specialist, I was put in charge of the Evaluation of Cryptographic Systems section in November 2006, and since April 2010 I have been in charge of the Cryptographic Technology division. The technically varied and complex subject areas within IT security are particularly motivating. The tasks of evaluating and assessing IT security products, particularly in relation to handling classified material, include testing different product categories such as software-based encryption solutions for hard disks and e-mails through to highly complex tactical radio systems and satellites. Working with highly qualified and motivated experts makes for a positive working environment and really helps us achieve positive results. Another thing I like about the BSI is the unbureaucratic way of working here – so unusual for a government agency – which is manifested in short decision-making lines and a customer-oriented mindset."

"Subject-wise, we have our finger on the pulse of the times."

Matthias Intemann

Matthias Intemann, Senior Specialist, Certification

"In the course of my work in product certification at the BSI, I have the opportunity to help shape exciting areas of IT security. The large number of communication partners and products you get to deal with over time makes the work extremely varied: there are always fresh challenges to be found. It's simply not possible to feel bored. Subject-wise, we have our finger on the pulse of the times. The diversity is also reflected in the type of activities, which range from managing projects to advising or evaluating content. Working with such highly competent colleagues, including across responsibilities, and with external experts makes my work particularly exciting. The in-depth exchanges of ideas and information that take place help you develop your own skills. The good continuing professional development opportunities at the BSI are also very helpful. You are expected to maintain a high standard even when the workload is heavy, so people automatically work efficiently. Quality management and process optimization, which belong in a professional environment, are a matter of course. Especially during meetings with external contacts, you are constantly reminded that the BSI is a widely accepted and valued government agency. And the feeling that your work is instrumental to IT security in general gives you the additional satisfaction of doing something useful."

"During negotiations you get to know the viewpoints of other nations."

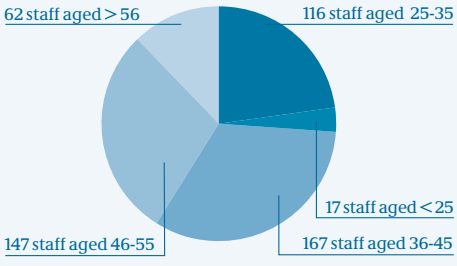
Dr. Dörte Rappe

Dr. Dörte Rappe, Senior Specialist, Executive Staff, Internal Audit

"In working at the BSI I have found my dream job, as the work is extremely varied and interesting. There are lots of nice colleagues who you can get to know socially outside of the office setting as well. By taking part in international working groups and conferences you have the opportunity to get to know the world and political perspectives and meet other scientists, talk to them and exchange ideas with them. During negotiations you learn about the viewpoints of other nations and represent German interests. In contrast to university, working at the BSI provides you with insights into real-life problems in the application of IT security, so you gain completely new perspectives.

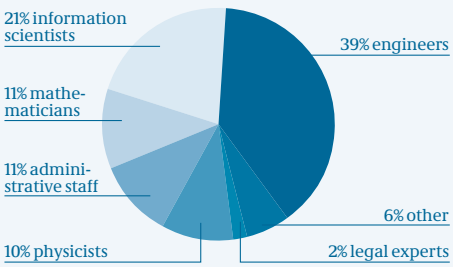
I find it particularly fascinating to explore the field of cryptography, not just theoretically but also in a practical way, and in doing so, finding out how the political and technical interests of users can be optimally reconciled with each other. Thanks to the extensive continuing professional development opportunities – both technical and general – there is an unbelievable number of fascinating areas to explore within the agency. Because you have the opportunity to rotate for a fixed period, you never stop learning and it never gets boring. What's more, this is the best way to discover which areas suit your own interests and capabilities best. Other attractions of working here are of course the flexible working hours and the possibility of combining family and career."

Age Structure of Employees



Career Background

(executive and senior grades only)



The BSI Comes Out On Top!

The BSI is once again ranked among Germany's top IT employers – as the most popular public sector agency.

... And These Were the Events of 2008/2009

A Review of 2008/2009

January

January 16-18

Omnicard

The BSI presents lectures at the leading technical congress for the smart card sector.

January 24

CAST Workshop

The BSI attends the CAST Workshop in Darmstadt on the subject of digital signatures.

January 31

Five years of www.bsi-fuer-buerger.de

The BSI has been informing the public about the dangers of the internet on its portal since January 31, 2003 (photo).

February

February 11

Workshop on Education and Awareness Raising in IT security

To mark the EU's Safer Internet Day, experts from business, academia and administration meet at the invitation of the BSI for the workshop on Education and Awareness Raising in IT Security.

February 20

Virtualization and IT Grundschutz

Virtualization and IT Grundschutz: in collaboration with Networkers AG, the BSI organizes the first IT Grundschutz Day 2008.

March

March 4-9

CeBIT 2008

BSI experts provide information about IT Grundschutz, IT early warning systems, CERT-Bund and official identity documents at CeBIT 2008.

April

April 8-10
RSA Conference

In San Francisco the BSI presents its main activities in the area of IT security at the joint German stand led by TeleTrusT.

April 9
2nd IT Grundschutz Day

At the 2nd IT Grundschutz Day 2008 some 120 participants consider the security aspects of the Microsoft Windows Vista operating system.

April 22-23
3rd Interdisciplinary Symposium

The 3rd Interdisciplinary Symposium of the BSI and the Identitätsschutz im Internet (identity protection on the internet) working party (a-i3) is attended by representatives of businesses, academia, government and specialist associations.

April 24
Girls' Day

The BSI takes part in the Germany-wide action day for vocational training with lectures and presentations.

May

May 28-31
LinuxTag in Berlin

The BSI presents its OSS solutions, which include free security solutions for Windows as well as free software for Linux.

June

June 17-18
OECD conference on the Future of the Internet Economy

At the OECD conference on The Future of the Internet Economy in Seoul, Korea, BSI President Dr. Udo Helmbrecht presents IT and internet security aspects of the planned electronic ID card and the Citizens Portals.

July

July 7

Call for Papers

Start of the call for papers for the 11th German IT Security Congress.

August

August 23-24

"Invitation to Visit the State" in Berlin

The federal government opens its doors to interested members of the public. The BSI provides information about the service portfolio for private users at the Federal Ministry of the Interior.

September

September 1-2

3rd Annual Meeting for IT Security Officers

The BSI and the Federal Academy of Public Administration (BakövV) organize the 3rd annual meeting for IT security officers of federal agencies.

September 8-13

INFORMATIK 2008

The BSI attends the 38th annual conference of the Society for Information Science with presentations and an information stand.

September 23-25

9th International Common Criteria Conference (ICCC)

The BSI presents papers at this conference in Korea.

September 23

3rd IT Grundschutz Day

The BSI and Informatikzentrum der Sparkassenorganisation GmbH (SIZ) host the 3rd IT Grundschutz Day (photo).

October

October 7-9
10th Information Security Solutions Europe (ISSE) Conference

The BSI attends the 10th Information Security Solutions Europe (ISSE) conference in Madrid.

October 7-10
Security Trade Fair

The BSI attends the Security trade fair in Essen with an exhibition stand and technical presentations.

October 21-24
Systems 2008

The BSI takes over sponsorship of the IT SecurityArea and presents a series of papers and an exhibition stand (photo).

October 24
German IT Security Prize

The Horst Görtz Foundation's German IT Security Prize, endowed with a total of €200,000, is conferred under the patronage of the BSI, which was represented on the jury.

November

November 3
4th IT Grundschutz Day

Presentations and discussions on information security and data protection are the focus of the 4th IT Grundschutz Day in Berlin.

November 4-5
Modern State

At Modern State, the most important conference and exhibition for public administration in Berlin, the BSI acts as Partner for IT security.

November 10
Cooperation Agreement

Federal Minister of the Interior Wolfgang Schäuble and Hans-Jörg Bullinger, President of the Fraunhofer-Gesellschaft, sign a cooperation agreement for collaboration in the area of IT security. The BSI and the Fraunhofer Institute for Secure Information Technology SIT will be the active partners (photo).

November 12
5th IT Grundschutz Day

Due to high demand, the BSI organizes another event with Informatikzentrum der Sparkassen-Organization GmbH (SIZ) in Bonn.

November 20
3rd National IT Summit

The new electronic ID card is one of the central themes of the 3rd National IT Summit in Darmstadt. The BSI presents its work on fingerprint sensors with live finger recognition and other biometric systems.

November 28
Auditors' Meeting

Over 200 auditors are briefed on the latest developments on every aspect of IT Grundschutz and certification at the annual Auditors' Meeting in Bonn.

December

December 2
ZertiFA 2008

The BSI delivers papers at ZertiFA 2008 in Berlin.

January

January 20-22

Omnicard 2009

The BSI unveils innovations and services in the area of card technology and applications in Berlin.

February

February 10

Safer Internet Day 2009

The BSI answers questions from members of the public on the subject of "Surf, but be safe!" in a telephone campaign.

February 12

1st IT Grundschutz Day

The BSI organizes the first IT Grundschutz Day of the year with the Fraunhofer Institute for Secure Information Technology SIT and the Center for Advanced Security Research Darmstadt (CASED).

March

March 3

Report on the IT Security Situation in Germany 2009

IT threat situation remains at a high level: the BSI publishes the report on the IT security situation in Germany 2009.

March 3-8

CeBIT 2009

The BSI attends the world's biggest computer trade show, CeBIT, with a stand, several papers and presentations.

March 23-24

Interdisciplinary Symposium

a-i3 and the BSI provide information and discuss the subject of identity protection in e-government and e-business at the Interdisciplinary Symposium.

April

April 20-24

RSA Conference in San Francisco

The BSI is represented as an exhibitor on the stand shared by the Federal Ministry of Economics and Technology (BMWi), AUMA and TeleTrusT.

April 23

Girls' Day

Once again the BSI takes part in the annual Girls' Day.

May

May 12-14

11th German IT Security Congress

"Secure paths in the networked world": some 500 participants from business, administration and academia exchange information and ideas about current trends and perspectives in IT security at the 11th German IT Security Congress.

June

June 18

3rd Berlin Meeting of the Münchner Kreis

The BSI provides a briefing on the technical implementation of the planned electronic ID card at the 3rd meeting of the Münchner Kreis communications research association in Berlin.

June 23

15 Years of IT Grundschutz

The BSI hosts an anniversary event in Bonn with distinguished IT Grundschutz experts.

June 24-27

LinuxTag 2009

In Berlin the BSI shows off its latest IT security solutions based on Open Source software, among them free software for Linux, Windows and Mac OS X.

July

July 2

Initiative for Security Enhancements in the Domain Name System

Initiative for more internet security: launch of the joint initiative for security enhancements in the Domain Name System by DENIC, eco and the BSI in Frankfurt (see p. 29).

August

August 20

BSI Act

The new BSI Act enters into force.

August 23-24

Open Day for the Federal Government

BSI for citizens: the BSI presents its services for the public at an Open Day for the federal government held at the Federal Ministry of the Interior.

August 30

Open Day in the Former Government Quarter

The BSI takes part for the first time in the Open Day in the former Government quarter and introduces itself to interested members of the public at its Bonn headquarters.

September

September 10

Company Fun Run in Bonn

BSI staff take part in the Company Fun Run in Bonn for a good cause.

September 11-12

Workshop on Factoring Large Integers

The BSI is co-organizer of the workshop on Factoring Large Integers at Ruhr University in Bochum.

September 22

2nd IT Grundschutz Day

The 2nd IT Grundschutz Day is held in Bonn, jointly hosted with Informatikzentrum der Sparkassenorganisation GmbH (SIZ).

September 22-23

Annual Meeting for IT Security Officers

The annual meeting of federal government IT security officers is held in Brühl, chaired by the BSI and BaköV.

September 22-24

10th International Common Criteria Conference

The BSI attends the 10th International Common Criteria Conference (ICCC) in Tromsø, Norway (photo).

October

October 13-15
it-sa

The BSI attends the successor trade fair to SYSTEMS, it-sa in Nuremberg, with its own stand and several presentations.

October 14
3rd IT Grundschutz Day

The 3rd IT Grundschutz Day is held as part of the it-sa trade fair in Nuremberg.

October 16
New Management at the BSI

Michael Hange becomes the new BSI President, Horst Flätgen succeeds him as Vice President.

October 23-25
IT Talent Summit

In the context of its activities to promote young talent, the BSI attends the IT Talent Summit at Burg Liebenzell.

October 27
Public IT Security

BSI President Michael Hange opens the new Public IT Security (PITS) conference and exhibition in Berlin.

November

November 19
4th IT Grundschutz Day

The BSI and the Horst Görtz Institute host the 4th IT Grundschutz Day of the year in Bochum.

November 24-25
Modern State 2009

Modern State 2009 in Berlin: the BSI is an exhibitor at the public authorities trade fair.

November 27
Auditors' Meeting

Some 200 auditors who carry out ISO 27001 audits based on IT Grundschutz gather for the BSI's annual auditors' meeting in Bonn (photo).

December

December 1
ZertiFA 2009

The BSI attends ZertiFA 2009 in Berlin, presenting various papers and also chairing the conference.

December 2
New President

Michael Hange is officially installed in his new position as President of the BSI by State Secretary Dr. Hans Bernhard Beus, who was also the Federal Commissioner for Information Technology (photo).

December 8
4th National IT Summit

At the 4th National IT Summit, the BSI and eco - Verband der deutschen Internetwirtschaft e.V. agree joint activities to combat botnets (see p. 28ff).

Organization Chart

April 2010

President Michael Hange

Vice President Horst Flätgen

Executive Staff
Internal Audit

International Relations

Press Officer

Department 1
Dr. Hartmut Isselhorst

Division 11
Security of Applications and Critical Infrastructures

Communication Security of Business Processes
Critical Infrastructures and IT Security Audit
Security Consultancy Service
IT Security Management and IT Grundschutz
High Availability of Critical Business Processes

Division 12
Security of Networks

Federal Computer Emergency Response Team (CERT-Bund)
Internet Security
IT Security in Operating Systems
IT Penetration Center
Defense against Internet Attacks
Government Networks

Department 2
Dr. Gerhard Schabhüser

Division 21
Cryptographic Technology

IT Security Architectures and Platforms
Development of Cryptographic Components
Development of Cryptographic Systems
Evaluation of Cryptographic Systems
Cryptographic and IT Security Administration

Division 22
Counter-Eavesdropping

Mobile Communication Security
Emission Security
Fundamentals of Counter-Eavesdropping
Eavesdropping Countermeasures
Physical Security

Competence Centre Cryptography

Design and Evaluation of Cryptographic Mechanisms

Department 3
Bernd Kowalski

Division 31
New Technologies and Conformity Projects

New Technologies and Scientific Foundations
Official and Electronic ID Documents
Industry Relations

Division 32
Certification, Approval and Conformity Testing

Information and Communication, Public Relations
Certification
Approval and Test Standards
Accreditation and Quality Management

Department Z
Horst Samsel

Organization, Human Resources, Financial Affairs
Internal Services, Project Management
Protection of Property and Classified Material

IT Staff

IT Organization & Planning
IT Operations

Picture Credits

adpic, ANSSI, BEIT Systemhaus, Bitkom, BMI, BSI, Frankfurt am Main Federal Police Directorate, Dataport, Deutsche Messe Hannover, Eric Lichtenscheidt, Fotolia, Girls' Day, Infineon, insafe, Linux-Day/Messe Berlin, Norbert Luckhardt (kes), OpenLimit, Secumedia Verlag, Shutterstock, SIGNAL IDUNA, T-Systems/HTC, trendence, www.omnicard.de

Publisher
Federal Office for Information Security BSI
53175 Bonn, GERMANY

Project Manager
Anke Gaul

Text and Editorial Staff
Federal Office for Information Security BSI
DauthKaun Communication Group

Layout and Design
DauthKaun Communication Group

Printed by
Das Druckhaus Bernd Brümmer, Alfter

Date
May 2010

Article Number
BSI-JB10/601e

Distribution Office
Federal Office for Information Security BSI
Section 321, Information and Communication, Public Relations
Godesberger Allee 185-189
53175 Bonn, GERMANY
Phone: +49 228 99 9582-0
E-Mail: oeffentlichkeitsarbeit@bsi.bund.de
Internet: www.bsi.bund.de