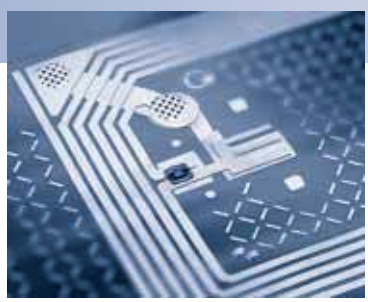
Federal Office
for Information Security

Annual Report 2005



Federal Office
for Information
Security (BSI)
www.bsi.bund.de

Information
- Internet security for all target groups
- Special issues of information technology
- Web portal for citizens, commerce and administration
- Hotline and service centre for citizens
- Publications of specialised topics and security instructions
- Presentation of work results on specialised fairs and conferences

Consultancy
- Risks concerning internet and certain IT technologies
- Secure IT platforms and infrastructures for Federal Agencies
- Penetration tests
- IT-Grundschutz as methodology and tool for secure IT infrastructures
- Risk analysis and protection of Critical Infrastructures

Development
- Encryption methods, biometrical methods
- IT security solutions (e.g. crypto devices for classified governmental material)
- Testing tools and measuring equipment for conformity tests and for protection against eavesdropping

Central services and operation
- Production and distribution of key material and Root-CA (Bund)
- Warning and alerting services, CERT-Bund
- Technical coordination of IVBB

Validation rules
- Protection Profiles for IT components and products
- Technical guidelines for components of the Federal Agencies' IT projects
- Protection profiles and guidelines of general importance

Testing, evaluation, certification and authorisation
- Evaluation and certification of IT components' and products' security
- Approval of systems for electronic processing of classified material
- Acceptance inspection and specimen testing of IT security components

Accreditation
- Recognition and quality assurance for testing authorities and auditors

Special technical measurements and acceptance tests
- Emission tests for communications systems
- Inspection and acceptance tests for telecommunications systems
- Tests for the protection against eavesdropping
- Tests of material security

Secure Information Technology for our Society

Society is increasingly dependent on information technology (IT) and therefore its protection is gaining importance. In Germany, this task is taken over by the Federal Office for Information Security (BSI). Founded in 1991, BSI is a division of the Federal Ministry of the Interior. Its work is operative for the Federal Administration, co-operative for the economy and informative for the citizen. BSI's ultimate ambition is the protection of information and communication. In this context, BSI has three strategic targets:

- **Prevention:** *to adequately protect information infrastructures*
- **Reaction:** *to act efficiently in case of IT incidents*
- **Sustainability:** *to advance German IT security technology and competence*

Who are we?
The Federal Office for Information Security (BSI) is the central IT security service provider for the Federal Government. We are responsible for IT security in Germany. The basis for our work are competence and neutrality.

What do we want?
Our goal is the secure use of information and communication technology in our society. With our help, IT security is to be put into focus as an important issue and independently translated into action. We want security aspects to be taken into account in the early development stages of IT systems and applications.

Who are our customers?
Our services address users as well as manufacturers of information technology. Today, this mainly means public administrations in the Federal Government, the Federal States and local authorities, but also business enterprises and private users.

What are our tasks?

We make it our responsibility to tackle all questions that concern IT security. We examine and evaluate existing security risks and anticipate the consequences of new developments. Based on this knowledge, we offer our customers services in the four central areas of information, consultancy, development and certification.

- **Information:** We provide information about all important IT security issues.
- **Consultancy:** We give advice in questions of IT security and offer support for appropriate action.
- **Development:** We conceive and develop IT security applications and products.
- **Certification:** We test, value and certify IT systems with regard to their security qualities. Approving of IT systems for the processing of classified information is also among our tasks.

How do we work?

The co-operation of our specialists and generalists is largely team-oriented, with great transparency of the respective competences. Our co-operative style of management is carried by trust and mutual respect. Our work stands out due to its quality, independence and service orientation.

Our technical competence is steadily increased through continuous education. Using the latest communication technology we mutually exchange the knowledge gained. Hence we can react quickly and purposefully to the constantly increasing challenges of IT security.

What lies ahead of us?

The maintenance and the furthering of our work's high quality standard is a permanent challenge to us. Through ongoing national and international exchange we quickly pick up new developments and thereby consistently increase IT security in Germany. We are going to improve co-operation on all levels even further and make our own work more efficient.

We intend to make our services known to a wider public and to address our customers more directly.

15 Years of IT Security for Our Society

My fellow citizens,

The Federal Office for Information Security (BSI) began its work on 1 January 1991. By founding an expert agency to deal with all issues related to IT security, the Federal Government took early action to realize the goal of promoting information technology by making sure it could be used safely in all areas of society.

At that time, there were few signs that information technology would assume the importance it has today, when almost every area of daily life relies on functioning information technology. The economy, public administration and private users – issues of IT security affect everyone.

Our society, with its almost insatiable demand for information and communication, currently faces enormous challenges: Networking and mobile communication not only facilitate the sharing of information, they also entail risks for government and society. The critical infrastructures on which our society depends are also vulnerable to malicious attacks using information technology.

This is why protecting information technology is a central task of domestic policy, though one that can be managed only in close cooperation with the private sector. In its coalition agreement, the Federal Government agreed to implement a National Plan for the Protection of Information Infrastructures.

Our country's internal security increasingly depends on the security of our IT systems. The areas emphasized by the BSI are therefore determined above all by the overall security situation, because the BSI must be able to respond to changes quickly and appropriately.

Since its founding, the BSI has become more than a federal security agency. It also offers services for the private sector and is taking on an increasing role as a resource for society as a whole.

I am pleased to be able to congratulate the Federal Office for Information Security on 15 years of outstanding achievement and would like to thank all the BSI staff for contributing to its success.

Bonn, April 2006

Dr. Wolfgang Schäuble, MP
Federal Minister of the Interior

BSI: an Operational Security Authority

Dear readers,

in the past year, newly emerging hazards such as phishing and bot nets have caused a tremendous stir. They have shown that inadequately protected IT systems and insufficient knowledge can lead to unpleasant consequences. And this trend will continue. At first there were computer viruses, dialers followed, today we have phishing and tomorrow internet telephony will be affected. No one can really foretell what dangers lie ahead of us in the coming years. But one thing is certain: the risks are on the rise. This was also demonstrated by BSI's report on "The IT Security Situation in Germany in 2005", published midyear. We all have to be prepared for these circumstances.

Politics is taking this task very seriously and in 2005 has set a signal. In August, the Federal Government has passed the National Plan for the Protection of Information Infrastructures. This establishes how to protect those IT infrastructures that sustain public life.

Extending co-operations and strengthening the German IT security industry – this is the way toward secure IT infrastructures and increased IT security in Germany. Connected to this is a notable extension of the responsibilities BSI will take over in the future. Not only technical expertise and BSI's recommendations will be sought after in the future, but also practical technical support – informing the public, co-operating with the economy, and supporting administration. BSI is thus shaping into an operative security authority.

BSI meanwhile employs a total of around 450 members of staff. More than 60 IT security experts were newly engaged in the past year. With this know-how and the dedication of everyone involved BSI has faced its specific responsibilities in 2005 and will successfully continue to do so in the future.

Bonn, April 2006

Dr. Udo Helmbrecht
President of the Federal Office for Information Security (BSI)

1 BSI in dialogue with citizens and experts

1.1 Internet security for everyone
1.2 The BSI – status quo and perspective
1.3 Trade fairs and conventions
1.4 Communication and co-operation
1.5 The alliance for electronic signatures

1.1 Internet security for everyone

The issue of IT security does not only concern workspaces in front of computer screens, but increasingly finds its way into everybody's daily live, be it in the car, at the doctor's or during passport inspection at the airport.

Maintaining IT security also means sensitising people to the subject matter and offering thorough counselling for the respective target groups. Among other means, BSI takes up this responsibility by providing a multitude of offers of information.

BSI's homepage www.bsi.bund.de is principally targeted towards IT experts. Like all of BSI's websites, it was designed corresponding to the German Ordinance on IT Accessibility (BITV – Barrierefreie Informationstechnik-Verordnung) from July 17th, 2002, under the German Disability Discrimination Act. Apart from current warning announcements and general information about BSI, its comprehensive pool of topics is of special interest to IT experts. In the section "Publications", most of BSI's documents are available for download in a full version.

One special feature is the Office's neutral perspective on all the topics. As a representative example for 2005 we might mention the VoIPSEC (Voice over IP) study which deals with security aspects of a technology that has matured into a valid alternative for conventional telephony in recent years. *(q.v. chapter "New challenges: Spam, phishing, bot-nets, VoIP")*

From biometrics to certification – the Internet offer of www.bsi.bund.de opens the path towards a multitude of specialized information, documents, event dates and publications. One special offer is the BSI newsletter that is published five times a year and contains information concerning publications, events and up-to-date certificates.

Central topic: electronic passport

Central topics of BSI such as IT-Grundschutz, certification/accreditation, internet security and protection of Critical Infrastructures have been supplemented in 2005 with the focal points E-passport and Biometrics. There are extensive presentations of the technical foundations of biometrical procedures and of BSI's projects in this area. *(q.v. chapter "Biometrics Technology")*

Information, clarification, sensitisation

BSI's citizens' portal (www.bsi-fuerbuerger.de) is tailor-made for the needs of private users. Here, beginners as well as advanced learners can find information and useful hints regarding the internet and PCs. The complex subject of IT security is explained to the technical layperson in a coherent manner.

Thematic key issues such as child protection or browser security are dealt with in the monthly "Focus". Practical help is offered through protection applications in the Tool Box which can be downloaded freely.

If you want to receive regular information on current security hints, you should also subscribe to the bi-weekly newsletter SICHER INFORMIERT (SAFELY INFORMED). Simply register under www.bsi-fuer-buerger.de. More than 28.000 users already take advantage of this, and their number increases daily.

In 2005 there has been huge praise for BSI's citizens' portal. TV channel WDR declared BSI's www.bsi-fuer-buerger.de website "recommended" which is the second best grade on their scale, after an evaluation of several web pages concerning IT security. "Computerbild" magazine marked it as "excellent" in its March issue.

Prepared especially for the many private PC and Internet users' questions: the website www.bsi-fuer-buerger.de (left). "Argus", a dog with a thousand eyes from Greek mythology, serves as icon for this Internet platform. The CD (right) that is available, for instance, at the numerous occasions when BSI participates in exhibitions and trade fairs, gives fundamental information regarding security on the World Wide Web.

It is therefore not surprising that BSI's Citizens' CD which mirrors the contents of the Citizens' Portal was also very popular at the family gathering day of the employees of Airbus Germany GmbH in Hamburg. Hans Werner, IT Security Officer for Airbus Deutschland, about the IT Security booth's give-away highlight: "We want to make use of BSI's offer for citizens in order to sensitise our employees and their families to the important issue of IT security." BSI staff experienced similar demand during the Federal Government's Open Day at the Federal Office of the Interior. The most urging questions of visitors at BSI's booth concerned malware and data security.

Besieged – BSI's booth during the Federal Government's Open Day at the Federal Ministry of the Interior (BMI) attracted great interest in the visitors.

Girls' Day

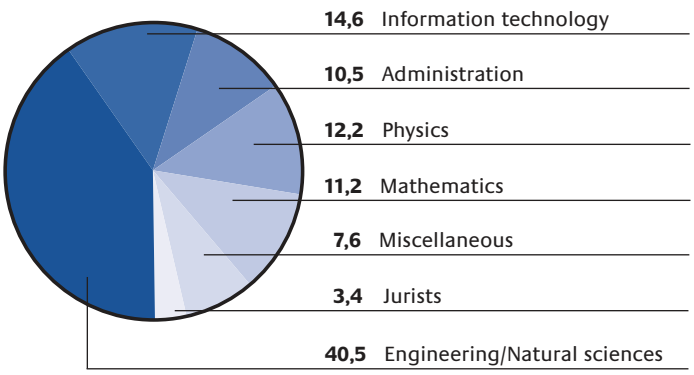
At the nation-wide future project day for girls, the so-called "Girls' Day" (April 28, 2005), schoolgirls from the Bonn area had the opportunity to get to know BSI. Numerous girls grabbed the chance to see a security office from inside.

Dialogue with BSI

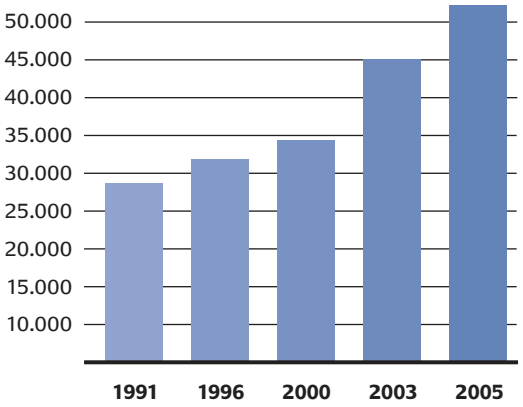
One of the offers addressed at decision makers from the business world, administration and science, is the "Dialogue with BSI" ("BSI im Gespräch"). In Berlin, participants of the event discussed the subject of "IT security in vehicles" in a small group. It is the aim of the "Dialogue with BSI" event to initiate an opinion forming dialogue with high-ranking representatives of particular technology areas, covering conceivable future issues.

Three examples for volumes containing competent specialised information from BSI: The publications reproduced here are available from Bundesanzeiger Verlag (P.O. Box 10 05 34, D-50445 Cologne, fax: +49221-97 66 82 78, e-mail: vertrieb@bundesanzeiger.de). The "E-Government-Handbuch" compilation costs 98 euros, "IT-Sicherheitsmanagement und IT-Grundschutz" is available at a price of 39,80 euros, and the standard work on IT security, "IT-Grundschutzkataloge" (formerly "IT-Grundschutzhandbuch"), costs 152 euros.

Fields of specialisation at BSI
senior and executive grades only, in percent



Budget 1991 - 2005
in thousands of euros



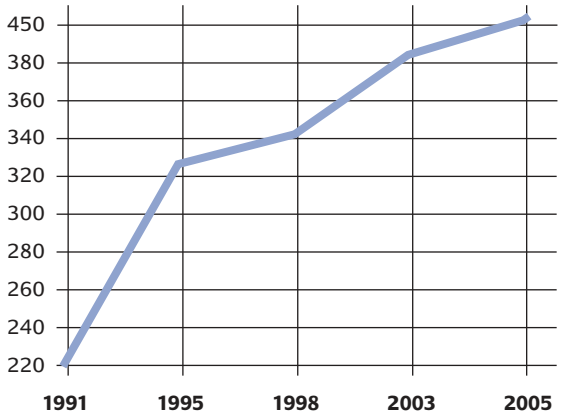
1.2 The BSI – Status quo and perspective

For 15 years, BSI has strongly committed itself to secure information technology in Germany. During this time, the office – which is a division of the Federal Ministry of the Interior based in Bonn – has been continuously evolving. In 2005, the green light was given for a new functional orientation. BSI is to take on further duties.

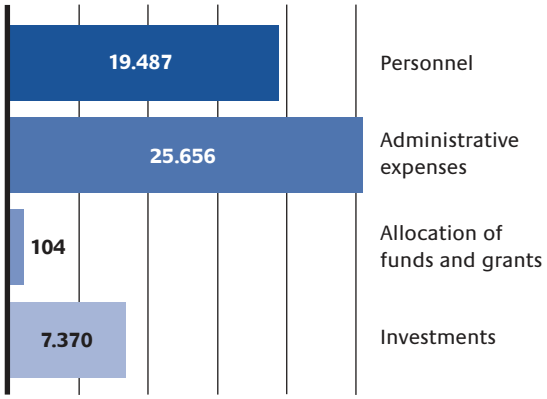
BSI in numbers

In the year 2005 BSI's overall budget reached 52.62 million euros. Compared to the previous year's period, that meant an increase of 2.9 percent. Expenses for personnel accounted for 19.49 million euros. Investment expenses added up to 7.37 million euros. Including the newly created positions in 2005, BSI now employs a total of 450 members of staff. Apart from natural scientists – who still form the largest group – the work of jurisprudence as well as administrative, economic and social scientists is also indispensable for BSI's wide range of tasks, since an issue as multifaceted as IT security needs to be viewed from many different technical perspectives. This is a development which continues along with technical progress and the admission of IT security issues into everyday life. BSI staff were not surprised when their office was rated TOP employer in the study "Absolventenbarometer 2005 – IT Edition" by the management consultancy firm trendence. BSI reached rank 8 among a total of 105 enterprises. This makes the office one of the most favoured employers among pre-graduate students in the IT sector, on a level with companies like Siemens, IBM or Microsoft.

Number of staff 1991 - 2005



Breakdown of expenditure by category
in thousands of euros



The new functional orientation

With his opening speech at the 9th German IT Security Congress on May 10th, 2005 *(q.v. chapter "Trade fairs and conventions")* former Minister of the Interior Otto Schily gave the green light for the new orientation where the Office takes on additional responsibilities within the Federal Administration. In his speech Schily emphasised that the awareness of the importance of IT security has to increase at the same pace as the growing number of sectors of economy and society relying upon IT. The primary aim of BSI's stronger commitment is to adequately protect information infrastructures and to act effectively in cases of IT security occurrences: co-operating with economy, informing the citizen and supporting public administration. Especially at federal level, BSI's efforts are directed towards setting a good example and enforcing an increased awareness for IT security.

With its "National Plan for Information Infrastructure Protection" (NPSI – Nationaler Plan zum Schutz der Informationsinfrastrukturen) in July 2005, the Federal Government has decided on a comprehensive IT security strategy. *(q.v. chapter "Report 'The IT Security Situation in Germany in 2005'")* In its function as national agency for IT security and as the central IT security provider, BSI is of crucial importance for the implementation of the NPSI.

Central contact point: CERT-Bund

In case of security relevant occurrences within the Federal administration the Federal computer emergency response team (CERT-Bund – www.bsi.bund.de/certbund) is already the central contact point. Its duties include – among others – preventive hints regarding vulnerabilities in hardware and software products, warning and alerting in case of particular threats and recommendation for reactive measures to limit damage or repair. CERT-Bund is primarily available for Federal administration. Its services also include 24-hour on-call duty which takes effect in acute IT security threats within Federal administration. Queries by other authorities as well as individuals or private institutions are dealt with according to the capacities available.

1.3 Trade fairs and conventions

For BSI, trade fairs and specialised conventions are always an opportunity to initiate contact with IT professionals, but also with private users. Placing informational offers, presenting its own products and, finally, teaching and sensitising in the realm of IT security issues – these are the goals of BSI.

In 2005 the "who's who" in the German IT security scene came together during the 9th German IT Security Congress which took place on May 10-12 in Bonn-Bad Godesberg. Under the heading "IT security concerns everyone", around 500 experts from economy, science and administration went into dialogue for three days and discussed current issues of IT security.

In his opening speech Otto Schily, then Minister of the Interior, stressed the importance of stronger public awareness for IT security issues and emphasised the effective contribution already performed by BSIto date. Among others, biometrical systems, the new EU passports and the electronic health card were focal points of the more than 30 subjects on the agenda.

As usual the congress was accompanied by an exhibition presented in the lobby. This year, cryptographic solutions came to the fore among the products and services on show. In the closing panel discussion titled "Biometrics – a new citizens' technology" the participants had the opportunity for constructive exchange of their positions.

A presence at CeBIT

At CeBIT 2005 (March 10 - 16, Hanover) the BSI's booth was located for the first time in hall 7 (the IT security area). The Golden Reader Tool (GRT), Secure Inter-Network Architecture (SINA), IT-Grundschutz and IT security certification according to Common Criteria (CC) were of particular interest for the visitors. There was also a strong demand for the CD-ROM containing the entire information from BSI's web pages. In the Public-Sector-Parc in hall 9 BSI presented itself with information concerning CERT-Bund and the virtual post office. Several series of lectures held by BSI experts in the Convention Centre and on the E-Government forum also aroused great interest.

At the world's biggest computer trade show – the CeBIT in Hanover – BSI is present with a representative exhibition booth every year.

Well-attended – BSI's 9th German Security Congress in May 2005 was met with great interest by the specialists. Right: View inside the main hall of the Bad Godesberg town hall. A conference transcript (left) is available from SecuMedia publishers for 49,10 euros plus s&h (ISBN 3-922746-95-3, 368 pages), or via http://buchshop.secumedia.de

The "German IT security award" at the "Systems" fair

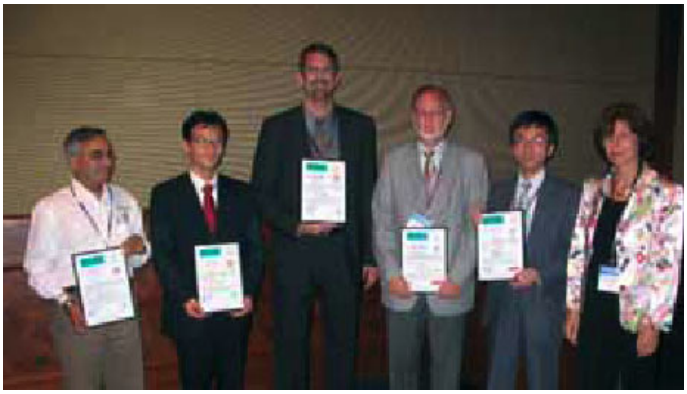
In its function as the IT security area's host institution BSI has been supporting the "Systems" trade fair (October 24 - 28, Munich) for several years. Apart from its exhibition booth, BSI was also present with a substantial programme of lectures. SINA, the Golden Reader Tool – which is the basis for electronic passports –, and the Computer Emergency Response Team are just a few examples of the subjects covered.

A novelty at this fair: In the "Blue Forum" (Forum Blau) the "German IT Security Award" was advertised. This lucrative prize under the patronage of Dr. Udo Helmbrecht is awarded by the Horst-Görtz-Foundation and will be awarded for the first time in 2006. It aims to reward contributions which the strengthen innovative forces in German economy.

BSI president Dr. Udo Helmbrecht together with Horst Görtz, initiator of the Horst-Görtz-Foundation.

Modern state

Current activities of BSI played a primary role at the “Modern State” congress which took place on November 29 - 30 in Berlin. BSI was represented as “IT security partner” with an exhibition booth and a 90-minute presentation of lectures. Interested listeners were informed by BSI employees on the subjects of virtual post office (VPS – Virtuelle Poststelle), IT-Grundschutz, and certification, as well as officially attested IT security.



ICCC Conference, September 2005 in Tokyo. Sony, Sharp, Infineon, Philips, Microsoft and Novell were, among others, presented with BSI certificates.

Internationally present, as well

On the international stage, BSI was able in 2005 to place its topics notably at the International Common Criteria Conference (ICCC) on September 28 - 29 in Tokyo, as well as at the Information Security Solutions Europe (ISSE, September 28/29) in Budapest. At the 6th ICCC, BSI was represented with an information booth in order to present facts on its certification office to over 500 visitors. Again, BSI made use of the ICCC to officially hand out certificates to several manufacturers, among them Sony Corporation, Sharp Corporation, Infineon Technologies Incorporated, Philips Semicon ductors Ltd, Microsoft Corporation and Novell-SUSE LINUX Products Ltd (sponsored by IBM).

1.4 Communication and co-operation

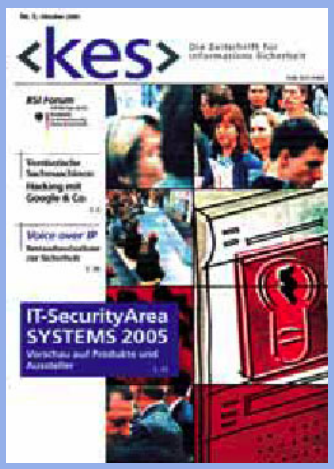
BSI makes its security advice and special topics known to the public in many different ways. Its ongoing commitment as competent and commercially independent entity is an important contribution in the fortification of a security culture in information technology.

Its first "IT security report", which brings together BSI's knowledge and experience and points out the main threats of today, is outstanding proof for this work. *(q.v. chapter "The IT Security Situation in Germany in 2005")* An equally substantial contribution toward a "culture of security" is made by BSI's co-operation partners. Besides existing co-operations, e.g. with heise security portal, the internet portal freenet or Fujitsu Siemens Computers, the "webzine" tecCHANNEL since 2005 offers an communication channel for up-to-date information from BSI.

The partnership is agreed and sealed. BSI president Dr. Udo Helmbrecht (right) with York von Heimburg, chairman of IDG Communications Publishers Inc.

BSI president Dr. Udo Helmbrecht affirmed this co-operation at the 9th German IT security congress during a meeting with York von Heimburg, chairman of IDG Communications Publishers Inc.

Through co-operation with the German partner of EU's "Safer Internet" programme – the internet portal "klicksafe" (www.klicksafe.de) – BSI supports a national campaign for sensitisation towards an advancement of media competence on the internet. BSI provides the project's operators with up-to-date information on questions regarding internet security.



<kes>: IT security at a high standard

The BSI forum <kes> is BSI's official bulletin (and also available digitally through www.bsi.bund.de). The forum is published as part of the bi-monthly <kes>, the leading magazine in information security. Its topical articles cover all aspects of IT security and are primarily directed towards IT experts. If you want to take a deeper look at current subjects such as E-government or IT-Grundschutz you will find them published in sophisticated format in the BSI's series of publications that appear in the Bundesanzeiger Verlag. (q.v. chapter "Internet security for everyone")

1.5 The alliance for electronic signatures

Already in 1997, when legislature passed the signature law, it created a basis for the use of legally binding electronic signatures for the first time. On the Federal Government's initiative, the Signature Alliance was founded in Berlin on April 3, 2003 with the goal of giving new impulses concerning a subject that is of great importance to economy and state.

From the beginning, BSI was an integral part of all task forces of the Signature Alliance. The aim was to create a stable foundation for interoperable infrastructures on the basis of mutually agreed-to standards. The resulting Signature Alliance Specifications are followed, for example, in the implementation of the Federal Government's chip card projects (eCard strategy). Private industry, which is also represented in the Signature Alliance, has also agreed to adhere to its specifications. In 2005, BSI took up additional tasks as a branch office of the Signature Alliance.

Partners from economy

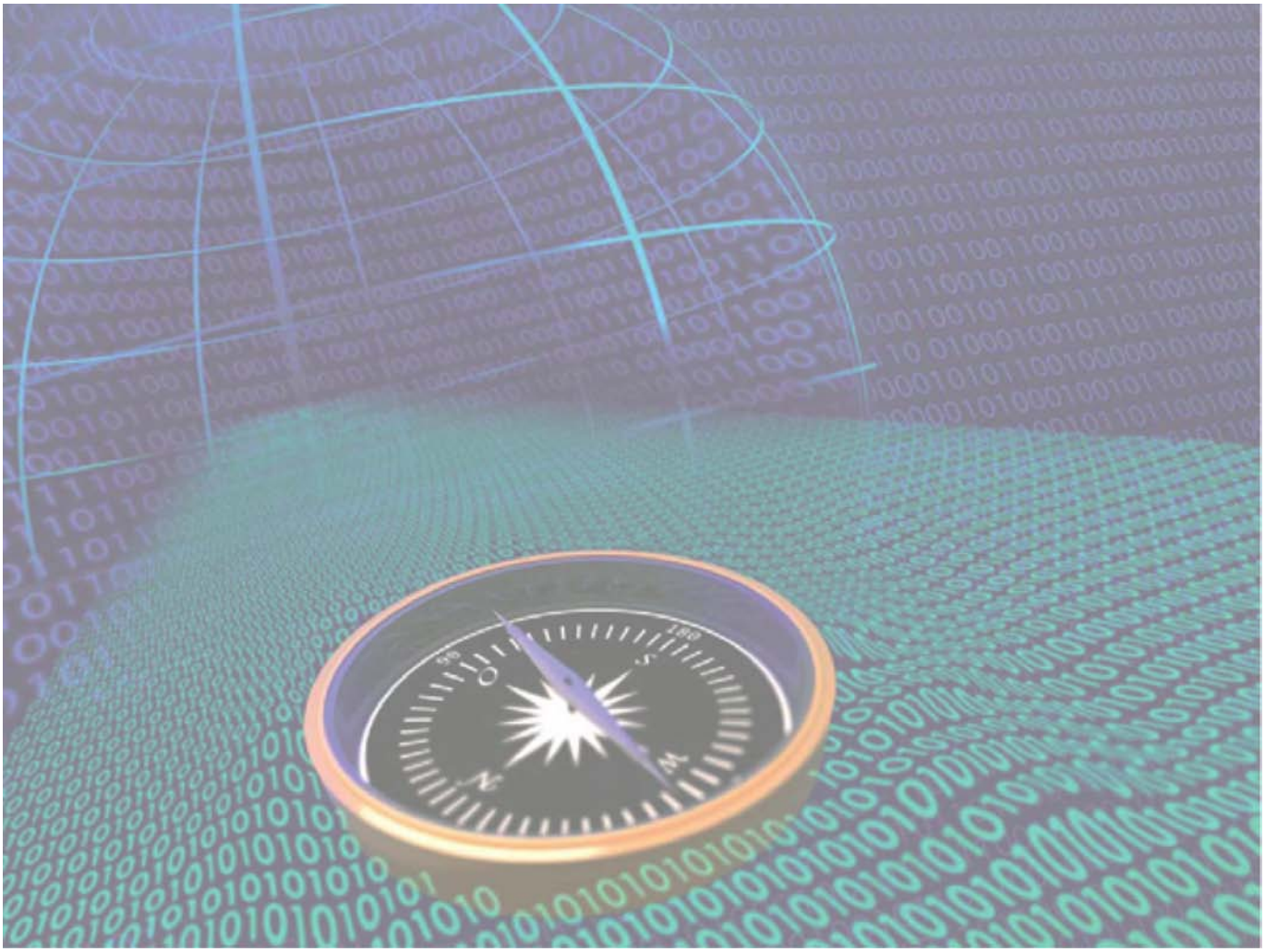
By the end of 2005 further 35 members had joined the Signature Alliance, whose founding members include, among others, the Federal Ministry of the Interior (BMI), the Federal Ministry of Economics and Labour (BMWA), the Federal Ministry of Finance (BMF) along with well-known partners from economy and industry. All in all, around 50 members are represented in the Signature Alliance at the end of 2005.

International standards

The Alliance's vision is a simple one: Citizens shall be able to use any chip card and any card reader with a wide range of – ideally all – available applications for E-commerce and E-government.

To make this vision a reality, the Alliance relies on network effects by incorporating existing card infrastructures, proven E-commerce / E-government applications, as well as an intense dialogue between state and economy. It was BSI's main objective to reach the convergent goals agreed upon by all members in 2003 by the end of 2005; apart from a few questions regarding details, this has been realised.

In order to safeguard their collective work and optimise the technical, legal and commercial framework, in 2005 Signature Alliance members dealt with the question of a re-orientation for the Signature Alliance regarding content and organisation. From BSI's point of view, main upcoming focuses will be the creation of rules for certification of products conforming with the Alliance, international standardisation, and BSI's function as Signature Alliance branch office.



2 Active shaping of security – services for businesses and administration

2.1 Report "The IT Security Situation in Germany in 2005"
2.2 Crisis management: Identify, react, protect
2.3 New challenges: Spam, phishing, Bot-Nets, VoIP
2.4 VPS – Secure Communication between citizens and public agencies

2.1 Report "The IT Security Situation in Germany in 2005"

Information technology not only allows new and more efficient services but unfortunately it also carries unknown risks. BSI's report "The IT Security Situation in Germany in 2005" gives a vivid demonstration of this. Efficient security measures have to be duly taken to make sure that information technology will remain a reliable working tool.

The report by BSI "The IT Security Situation in Germany in 2005" reveals the seriousness of matters: In the second half of 2004 more than 1,400 new flaws in IT were discovered – compared to the year's first half this means an increase of 13 per cent. Looking at IT malware, the situation is even more drastic. In the same period, more than 7.300 new variants of worms and viruses were registered. This is an increase of about two-thirds compared to the first half of the year. Trojan horses amounted to a third of the 50 most common internet threats in the second half of 2004. Spam mail meanwhile adds up to 60 - 90 percent of overall e-mail traffic. Increasing numbers of phishing attacks are also a threat to internet security.

BSI's report "The IT Security Situation in Germany in 2005" describes the current state of affairs regarding IT security in Germany and presents an overview of the challenges to come. The report can be downloaded as PDF file in German or English language from BSI's website.

Germany 2005: How safe is information technology?

During presentation of the situation report on August 8, 2005 in Berlin, BSI president Dr. Udo Helmbrecht called for increased vigilance: "Even if protection of our IT systems may be guaranteed today, we have to be armed for the future." For example, only about half of all the IT executives in businesses have a written strategy for protection of their information technologies. Despite enormous amounts of spam mails, anti-spam measures have not been realised over the whole of Germany. At least nine per cent of organisations are unprotected against this flooding with spam.
(q.v. chapter "New challenges: Spam, phishing, bot-nets, VoIP")

The attackers are acting faster and faster. The time span between the detection of a vulnerability and its actual exploit currently averages at 6.4 days, and it is going to be shorter and shorter – to the point of zero-dayexploits. Furthermore, there is an emerging trend towards professionalisation and commercialisation of cyber-crime. Targeted attacks are more and more conducted by organised crime instead of isolated computer hackers. Hackers and authors of viruses co-operate with criminals. Here, the driving force are purely financial interests.

IT security needs more significance

But there is hardly any distinct IT security competence in the different groups of society. Despite the fact that citizens are increasingly dependent on information technology – be it at work, in digital payment transactions or in the field of communications – only a few put the necessary practical value on secure information technology. The same applies to commerce and administration.

This view on the current situation shows that there are valid reasons for placing high significance on IT security. But it will also in the future be necessary to keep an eye on accumulating threats. Targeted exploits of weak points in IT systems is a central problem here. What may be the crucial motivations for such attacks?

In a world of increasing interconnectedness of global markets the security of IT systems of commercial businesses is gaining great importance. The spying on tendering, contracts or market prices for the gain of competitive advantage is going to increase. In the past year attacks on IT systems had increasingly economical backgrounds. Their aim was mainly to eavesdrop credit card information and other sensitive financial data. It is to be expected that this development will be aggravated in the future.

Up to now, programmers of malicious software mainly used e-mails in English for the spreading of computer viruses, but meanwhile more and more German texts are to be found. This regionalisation results in a growing circulation of such malicious applications also in Germany.

BSI's situation report points out vulnerabilities and threats, it shows trends and evaluates developments. But BSI does not merely want to describe the status quo. It is also important to show the possibilities of effectively advancing IT security. For this reason the report describes adequate actions to prevent flaws and threats in IT systems from becoming even more problematic in the future than they are even today. Only through a new culture of security carried together by all groups concerned will it be possible to enhance the basic conditions for a safe and reliable information technology. For this reason the Federal Government has initiated its National Plan for the Protection of Information Infrastructures. BSI in its function as the central German IT security agency will strongly contribute to this.

National Plan for Information Infrastructure Protection

An adequate degree of IT security can only be achieved through elaborate and comprehensive concepts, not through isolated action. And if this is true for businesses and public authorities, it can also be applied to the entire nation. Thus the Federal Government has decided on an IT security strategy for Germany – the National Plan for Information Infrastructure Protection (NPSI). This was drawn up under the auspices of the Federal Ministry of the Interior, in close collaboration with BSI.

Security begins with everyday life – on its website, BSI offers advice concerning the protection from fraud or manipulation at the cash dispenser: www.bsi-fuer-buerger.de/geld/10_04.htm

The NPSI is aimed at three strategic goals:

1. Prevention: Protecting information infrastructures adequately
How to adequately protect information infrastructures from threats and attacks? Here, the range of activities includes sensitisation of employees, application of secure products and cryptographic safeguarding of IT networks.

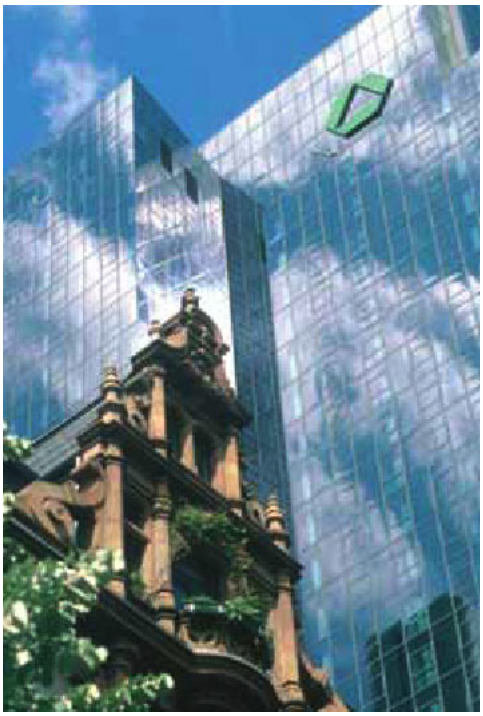
2. Preparedness: Responding effectively to IT security incidents
Two things are necessary for an efficient reaction: An accurate and up-to-date status report as well as elaborate and well practised crisis response concepts and emergency plans. This applies to businesses and authorities, but also on national level.

3. Sustainability: Enhancing German competence in IT security / Setting international standards
What Germany needs apart from the political will and readiness of all those responsible to strengthen IT security, are professional competence and trustworthy services and IT security products. This also includes teaching of IT security competence in schools and vocational training as well as the advancement of research and developments in these areas. Trustworthy IT security solutions are drawn up in collaboration with international partners. BSI, being the national IT security agency, will play an active role in the furtherment of IT security.

These broad strategic goals are substantiated through 15 individual targets for the different groups in society, ranging from public administration and commerce, science and media to the individual citizens, and are brought to life, initially for Federal administration and users of Critical Infrastructures in the private sector, through precise implementation plans.

BSI plays an active role in the implementation of the NPSI. It will further extend its consultancy services for public agencies and take an active part in the creation of IT security for the authorities and Federal big-scale projects. BSI's operations centre will be expanded into the Federal IT crisis response centre; an earlywarning system for IT security threats is being developed. *(q.v. chapter "Crisis management: Identify, react, protect")*

In order to prevent or control IT crisis situations, BSI will intensify its collaboration with the users of Critical Infrastructures.



Critical Infrastructures: Financial institutes are also among them. Guidelines and other informational material on the IT security of banks are available from BSI.

Direct help for users of Critical Infrastructures

In the context of protection of information infrastructures, in 2005 BSI has published concrete tools for businesses counting under Critical Infrastructures. Two of these tools are the sample guideline "IT security at a Critical Infrastructure – a practical example" and "IT security audit materials for the site quickcheck in Critical Infrastructures". The sample guideline is the result of a collaboration with an international company in petroleum industry. The IT security guideline used by this company was revised by BSI and matched to BSI's IT–Grundschutz manual. Now every enterprise has the possibility to check its own IT security measures and, if necessary, make the adaptions that will bring improvement. Based on the positive experience of the company that helped in creating the sample guideline, BSI offers audit materials for a so-called site quick-check according to the sample guideline's rules. These are meant to help examining the sample guideline's implementation and to give a transparent picture of the enterprise's IT security status. By making these tools also available in English, BSI meets the special needs of internationally operating companies that use Critical Infrastructures.

2.2 Crisis management: Identify, react, protect

Even with efficient protection measures IT security incidents cannot always be avoided. If a great number of institutions are affected, or if locally confined causes result in far-reaching consequential damages, there are specific rules of action for an IT crisis response centre.

In case of a "national crisis" in the area of information security or a similarly far-reaching dysfunction, an IT crisis response centre will have to

- identify the crisis early in advance,
- give out early warnings or even alarm messages to users not yet affected,
- minimise damages as far as possible through co-ordinated and well-practised reactions
- rapidly switch back to safe routine business procedures.

In case of IT security incidents of national importance, the Federal Government's decision-making ability and capacity of action has to be secured through well-processed information and competent analyses. Those responsible for IT in administration and commerce have to be supported in this.

This is the responsibility of the Federal National Crisis Response Centre at the BMI. It analyses incoming messages about IT security incidents, provides information and warnings for several target groups (Federal administration, commerce, citizens) and co-ordinates the technical measures necessary to deal with the incident.
Should more severe IT crisis situations arise, the operation centre is expanded into the Federal IT crisis response centre and its size of staff is promptly increased. BSI will then also alert its superior, the "Co-ordination Committee IT security" in the BMI and supply it with professionally competent and target-orientated information. This committee implements actions that are outside BSI's actual responsibilities.

The operations centre

The first step towards an IT crisis response centre was the creation of the operations and analysis centre at BSI which operates 8 hours per day, seven days per week. This is one prerequisite to be sure that signs of IT attacks or other incidents can be recognised early, also on weekends and holidays.
The development of special technical sensors for identification of anomalies in internet data traffic and further projects to integrate commerce and administration into a national early-warning system are the basis for the national IT crisis response centre. It is being further expanded as speedily as possible.

BSI itself has developed a number of projects for the acquisition of information, early warning and alarming, and supported the preparation of tools. These are integral parts of crisis response. With its experience and the tools developed, BSI is very well prepared for the tasks of a Federal national IT crisis response centre.

In particular worth mentioning are:

- **SIRIOS, a trouble-ticket system for handling incidents within the CERT network**

This Open Source Software (OSS) system allows for structured filing of data concerning security incidents, vulnerabilities and contact information. These are the basis for fast, high-quality processing of requests. Accessing these data is made possible on a user level by a flexible access rule model in a clientserver architecture. Workflows supported by the system can be individually organised. The system's standard-ised formats facilitate information exchange and co-operation among IT security teams. SIRIOS is used as the basis for shared documentation and statistics.

- **WID portal, portal for the warning and information service**

IT users as well as persons in charge require information and fast warnings regarding newly registered security gaps in IT systems. WID portal makes it possible to individually arrange information in personalised newsletters focusing on the technical systems involved and the evaluation of the risks of the respective security gaps. WID portal holds an archive of all registered vulnerabilities including references to applications capable of closing those gaps.

- **CBAS – CERT-Bund alarm system**

In critical situations, particularly during ongoing attacks on information technologies, or during the implementation of urgently necessary IT security measures, reliable a vailability of technical staff and decisionmakers is essential. A multi-client capable alarm system developed by BSI effects the alerting.

- **Citizens' CERT**

The citizens are also in need of information, especially warnings about new risks and recognised threats. In collaboration with Mcert, the computer emergency team for small and medium-sized businesses, BSI in 2005 prepared the establishment of a "citizens' CERT" providing private internet users with relevant information. The green light for the citizens' CERT will be given in spring of 2006.

Protection from malware – Viruses, worms and trojan horses

BSI has been in contact with leading manufacturers of anti-virus applications in order to be able to collaborate even closer in the area of IT early warnings. The aim is the creation of an information network that allows quick exchange of safe information among trustworthy partners upon appearance of new malware.

If one can obtain detailed information about malicious software as fast as possible (e.g. subject line or name or size of e-mail attachments), the time span between a detailed analysis of a malicious program and the development of signatures that allow for automatic detection and defence on the PC can be shortened considerably.

Guardians on the net

BSI – within the requirements of data protection – concerns itself with the possibility of obtaining and statistically analysing protocol data relating to internet traffic to be able to warn before anomalies as early as possible. The sensors required for this can be divided into two categories:

- sensors capable of reading data traffic in portions of the internet,
- sensors that can provide, for example, the operators of public web sites with information about communication details and response times.

Technical sensors are developed that are placed at chosen points in the internet to enable statistical analysis and to automatically alert the early-warning system as soon as any change in the internet's "background noise" is seen as anomalous and an in-depth analysis seems necessary.

The Berlin-Bonn information network (IVBB)

The IVBB is permanently monitored by an early-warning system (NAGIOS). Users are directly involved at strategic nodes via a measuring computer. Thus it can be immediately decided whether the disturbance has to do with a service or a particular user's connection.

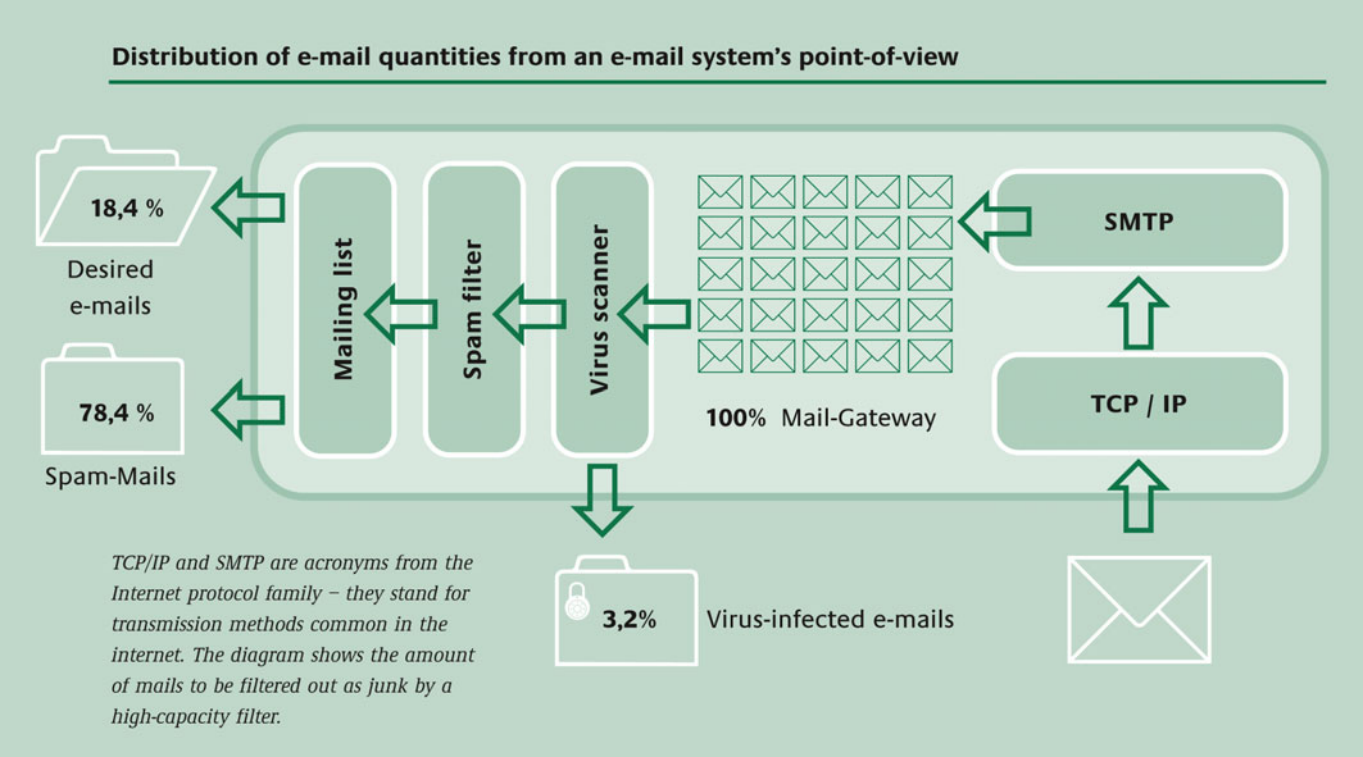
The measuring computer takes samples of IVBB services in regular intervals and from the measured data determines response times and the availability of the applications under surveillance. The actual status report of processes and connections can be retrieved online from BSI's operations and analysis centre via a web interface.

The Berlin-Bonn Information Network (IVBB) in action: Video teleconference of the Federal Ministry of Education and Research (BMBF) amongst the locations Bonn and Berlin.

2.3 New challenges: Spam, phishing, bot-nets, VoIP

The internet facilitates uncomplicated global exchange of information. But easy accessibility and the freedom afforded by the world-wide net take their toll: Internet services are increasingly misused.

It is a proven fact that spam mails add up to more than 60 percent of the ordinary world-wide mail traffic. To some this might lead to the serious question whether it would not be more effective to abolish e-mails altogether. But even today many business transactions are entirely conducted via mail. Abandoning e-mails can therefore not be practical. What is needed are reliable services and an efficient defence against more and more sophisticated spamming techniques.



BSI's anti-spam activities

In 2005 BSI focused itself mainly on determining the precise threat situation in Germany. The significance of international studies for the German market went under scrutiny. BSI could act under the assumption that German users have the same problems that occur on an international level. But there were no known details. Neither were there any data available about what amounts of spam are being processed in Germany, nor was it evident which counter measures were employed all over the country.

The answers to these questions came through intense discussions with experts and an internet survey. Among the experts were national providers, major international enterprises and a selection of interested organisations. International approaches towards defence against spam were discussed as well. This survey was conducted by BSI in collaboration at the university of applied sciences in Gelsenkirchen.

- On the basis of data return it was possible to make statistical statements concerning about 40 million e-mail accounts and around 2.3 billion e-mails per month.
- Assuming that all e-mails are being accepted,
  - approx. 18 per cent have been recognised as desired and
  - approx. 82 per cent as undesired or faulty,
- anti-spam mechanisms are used extensively.
- 30 per cents of the participants have already been subject to DDoS attacks.
- Critical business transactions are carried out via e-mail by 45 per cent of all those interviewed.
- Most respondents assume that the threat posed by spam and viruses will further increase.

Detailed results of the survey are available for download at the institute for internet security (www.internet-sicherheit.de).

The talks with experts and the survey showed that users choose different approaches at spam defence. This has technical as well as organisational reasons. Most users employ a combination of various anti-spam measures. Newer methods are also implemented, with varying success. One further result: The current methods for authentification of senders are regarded as hardly reliable by those interviewed (which might be due to these methods not being very wide-spread).

The dynamic internet accesses that are mainly used by inexperienced private users are agreed to be the main source for spam mails. This applies on national and international levels.

Those approaches at spam defence that are designed for international collaboration of organisations were most appreciated by those interviewed. Among others, collective efforts are being made to synchronise and standardise the processing of complaints. This process of abuse management serves to identify spam mails as early and as close to the sender as possible.

There are many forms of undesired e-mails. These may include commercial or non-commercial advertising, malware, phishing, chain letters or slander. Jurists and technicians view the term “spam” differently. BSI’s study **“Anti-spam strategies – detection and defence of undesired e-mails”**, published March 2005, gives detailed descriptions of ways of effective spam defense on more than 140 pages. It covers all technical, legal, economical and organisational aspects.
(Download: www.bsi.bund.de/literat/studien/antispam/antispam.pdf)

One of its conclusions is that it is more profitable to employ anti-spam measures than not to do it, even if e-mail traffic is slowed down in the process. Safely configured systems are part of a successful anti-spam strategy, and they diminish the overall amount of spam.

Spam mails are a complex international phenomenon which cannot be simply cut off through technical measures. There will always be new ways of transmission. This is a threat to IT security. This potential threat can only be minimised through international and flexible anti-spam strategies. The technical possibilities currently available are a good basis for this.

"Spam" mails are a waste of time and money for every enterprise. E-mail traffic would often be impossible without protective measures. Solutions are pointed out in the "Anti-spam Strategies" handbook available from Bundesanzeiger Verlag, Cologne (32 euros)

Phishing

In the year 2005 the phishing wave reached Germany. Phishing means that the sender with criminal intent tries to obtain confidential access data of online accounts (name, account number, PIN, TAN) with which he then can plunder these accounts. This may happen either through faked e-mails which allure the customer to access counterfeit web appearances of financial institutes, or through so-called Trojan horses which secretly record all input during online banking and transmit it to a server via ordinary e-mail traffic.

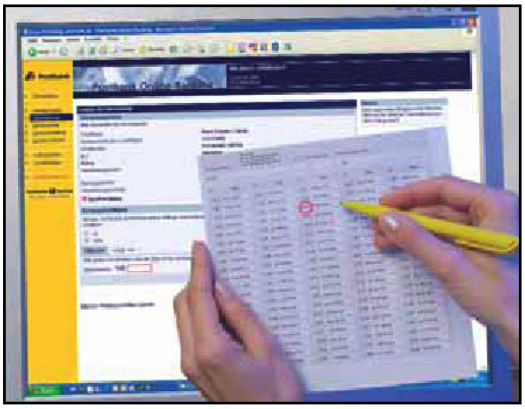
Initially these mails were written in English, or in very bad German. They could easily be recognised as falsifications. But criminal "phishers" have meanwhile improved the quality of these mails and of the fake web sites which often makes them difficult to distinguish from the originals.

BSI's task in the fight against phishing is mainly a preventive one. The main focus is the education of the public. New counterfeit bank domains have to be cut off as quickly as possible. BSI successfully collaborates with the law enforcement agencies in this.

Due to the PIN / TAN method utilised by German financial institutes the damage done in Germany is currently rather limited. In 2005 it is estimated to be still in the single-digit million range. In other countries, where a simple password is suffi-

cient for online banking, damages amount to triple-digit million figures. In order to prevent the amount of loss rising to sums of that order, banks have been developing improved methods such as iTAN (indexed TAN) or mTAN (mobile TAN via SMS).

But all these methods can only be successful if every single citizen carries out his online transactions with a focus on security, checking e-mails in particular as to their validity.



Two examples for the new security strategies used by financial institutes: TAN numbers for electronic money transactions are only valid if the number assigned on the internet corresponds to the one on the TAN list (iTAN). Alternatively, every TAN is individually transferred onto mobile phone by SMS.

Only with a secure payment system goods may be conveniently ordered from home or bills paid via the Internet.

Bot-nets

Bot-nets have in the recent past become a serious threat to internet security. “Bot” stems from the term “robot” and is used for an application that can process orders independently. It is fed onto an unsuspecting user’s computer, being controlled and misused by a third party for their own purposes. A bot-net is a remotecontrolled network of PCs connected via the internet which in the hand of cyber criminals may be used for their own intentions.

Malicious programs infect an individual computer, put it under their control and integrate it into the bot-net. It shows no detectable damage but waits for orders from outside which activate it to the ends of the cyber pirates. Criminals use other people’s computers for their felonies; the computer’s owner becomes a collaborator without even knowing it.

Bot-nets are mostly used for the distribution of spam mails or so-called Denial of Service attacks. Current bot-nets mainly utilise the Internet Relay Chat Protocol (IRC) for centralised remote control.

Bot-nets may contain thousands of individual computers whose combined capacities exceed the bandwidth of most conventional internet accesses by far. A bot-net of adequate size can easily paralyse an internet server by flooding it with huge masses of data. And what is more: Bot-nets mostly are composed of "captured" private PCs. Thus the spectrum of IP addresses will be so wide that servers under attack can only insufficiently protect themselves.

With the help of its own infrastructure and software BSI has in 2005 begun to register bot-nets and to examine their modus operandi. To this end technicians utilise, among other things, systems that simulate the existence of a complete internet environment in order to be able to analyse the malicious programs' procedures and functionalities.

IT security from the start – grown-ups should practise this with their children from an early stage.

Voice over IP

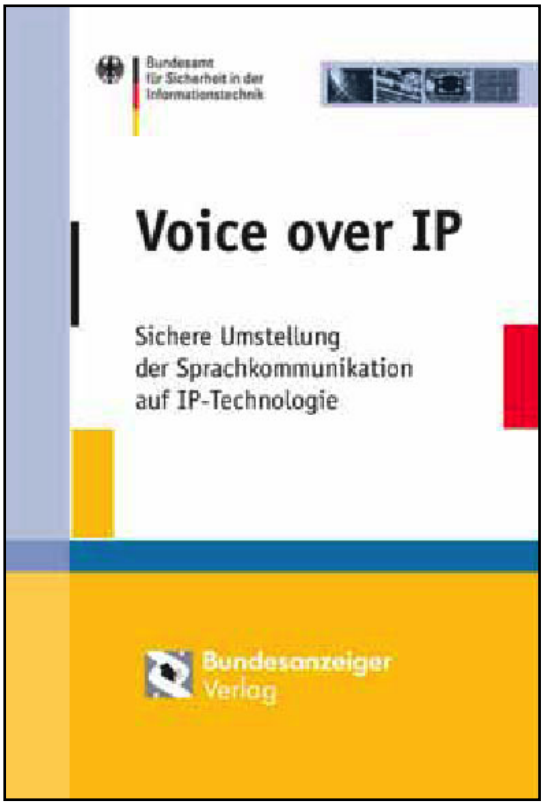
VoIP is out of its technical "teething troubles" and is steadily growing into very serious competition for conventional telecommunications systems. Unlike grid-bound dialswitching, VoIP systems transmit conversations via packet-oriented switching known from the digital world.

This results in the fact that the risks of traditional telecommunications are carried on and added to the ones inherited from the IP world. The savings potentials (due to the convergence of both systems) propagated by the manufacturers hardly bear up to adequate technical scrutiny. VoIP systems can only be made as safely available as telecommunications systems through substantial additional work and expense. The same is true for integrity and confidentiality.

Both these factors belonging into the framework of security also require detailed examination for the safe use of VoIP systems. Cost savings due to the convergence of both systems will only be possible in the medium or long term. The biggest challenge does not lie in the technology for voice transmission via networks originally designed for data flow, but in aspects of security.

This means that a security concept defining the demand for protection and analysing the risks is indispensable. It is the only way to generate a level of security appropriate to the institution in question. What is the use of huge savings having been made if the institution cannot phone any more (loss of availability), is being eavesdropped (loss of confidentiality) or ruined (loss of integrity)? Security is not for free, and in the end there is only one thing that counts: the customer's security and satisfaction!

In order to assist users, manufacturers and operators with the implementation of VoIP, BSI in 2005 has issued a study. This study highlights all technical security aspects of VoIP. In the end it always pays having considered all technical security concerns in good time! (www.bsi.bund.de/literat/studien/VoIP/)



Voice transmission via IP networks ("Voice-over-IP") is one of the most rapidly growing areas in telecommunication. Sectors of telecommunication and IT network infrastructures that previously were operated separately may now be combined, which results in substantial savings. But every new technology carries its risks along with the advantages. This handbook offers advice and illustrates security measures. Available from Bundesanzeiger Verlag (32 euros).

2.4 VPS – Secure communication between citizens and public agencies

The "Virtual Post Office" (VPS – Virtuelle Poststelle), which is a basic component of BundOnline and was developed under BSI's auspices, facilitates user-friendly and safe exchange of electronic data between citizens and authorities. It can either be integrated into existing processes – or ones newly developed for E-government – as central encryption component or it can be operated in the form of an independent mail gateway. Currently the VPS is already being used in both operating modes by numerous public agencies.

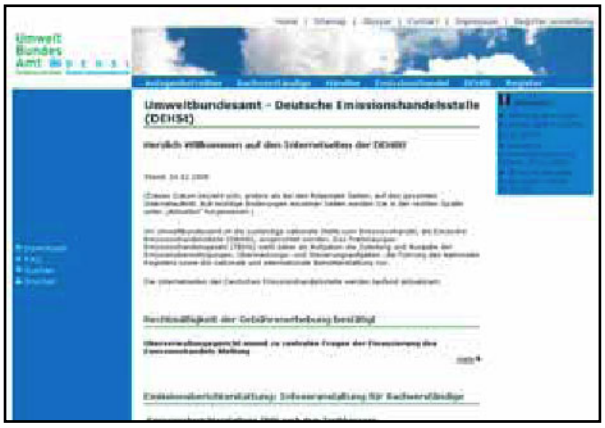
Confidentiality of data exchange via the internet can only be warranted if the information transmitted is first encoded by a cryptographic process of adequate strength. If in addition this information exchange is to be legally binding, as in E-business, E-government or internet banking, both sender and recipient of messages always have to be perfectly sure about each other's identity. Furthermore it has to be guaranteed that messages cannot be secretly modified. Encryption and confidentiality thus are indispensable prerequisites for secure E-government. The aforementioned tasks are performed centrally and largely automatic, which is an effective relief for the end user.

There is a wide range of possible formats of data exchanged in E-government: from unstructured e-mail texts with any type of attachments to well formatted data sequences, e.g. when online forms are filled in, and these sequences can immediately be integrated into the workflow of a given technical process. Due to these varying requirements the VPS is divided into two components which can either VPS be operated individually and independently or together in a network. The first component which is based on the open standard OSCI (Online Service Computer Interface) is particularly suitable for safe transmission of data entered through a web interface – e.g. an HTML form. Hence this component is casually referred to as "web VPS".

The VPS's other component uses the e-mail transfer protocol SMTP and is therefore suited mainly for transmission of heterogeneously structured data (e-mails with attachments). But what is common to both is that they – whether in individual use or in combination – fulfill the above mentioned requirements.

Be it a "Red" (as you see here in Berlin) or a "Black Town Hall" – citizens have to be able to rely on the confidentiality of their data in the electronic exchange with authorities.

Right: From the beginning, the German Emissions Trading Authority (DEHSt) has counted on electronic means of communication. The sale and purchase of certificates for CO2 emission are managed by e-mail.



VPS in electronic legal relations

As mentioned before, the web VPS is especially suited for integration into already existing technical processes. VPS users are also free to develop new client applications which transfer or retrieve data for encryption and authentication to or from the VPS's open interfaces. One such client application developed "around" the web VPS is the "electronic law and administration mailbox" (EGVP – Elektronisches Gerichts- und Verwaltungspostfach). This enables lawyers and other persons involved in legal proceedings to file legally binding written submissions (which have to conform to certain standards) with the courts, e.g. to file a lawsuit.

A statutory ordinance passed on December 03, 2004 makes it possible to electronically communicate with the Federal Administration Court and the Federal Court of Finance, equal to conventional written form. In the course of 2005 other courts joined in this, or are planning the implementation of electronic legal communication for the near future. Additional information regarding the EGVP plus the link for download of the client can be found under the URL: www.egvp.de.

The "electronic law and administration mailbox" software helps jurists in the exchange of their written submissions – but secure encryption is of highest priority especially in this context.

The Berlin Mitte power and heat supply station at night. This is also a case of the German Emissions Trading Authority awarding certificates for carbon dioxide emission by e-mail – secure communication is guaranteed by BSI.

VPS in emissions trading

Another system that went into action in the year 2005 and that makes use of the VPS is the trading of emissions certificates according to the Kyoto protocol. First of all, the participating enterprises – mainly energy suppliers and energy-intensive industrial facilities – had to register with the German Emissions Trading Authority (DEHSt – Deutsche Emissionshandelsstelle).

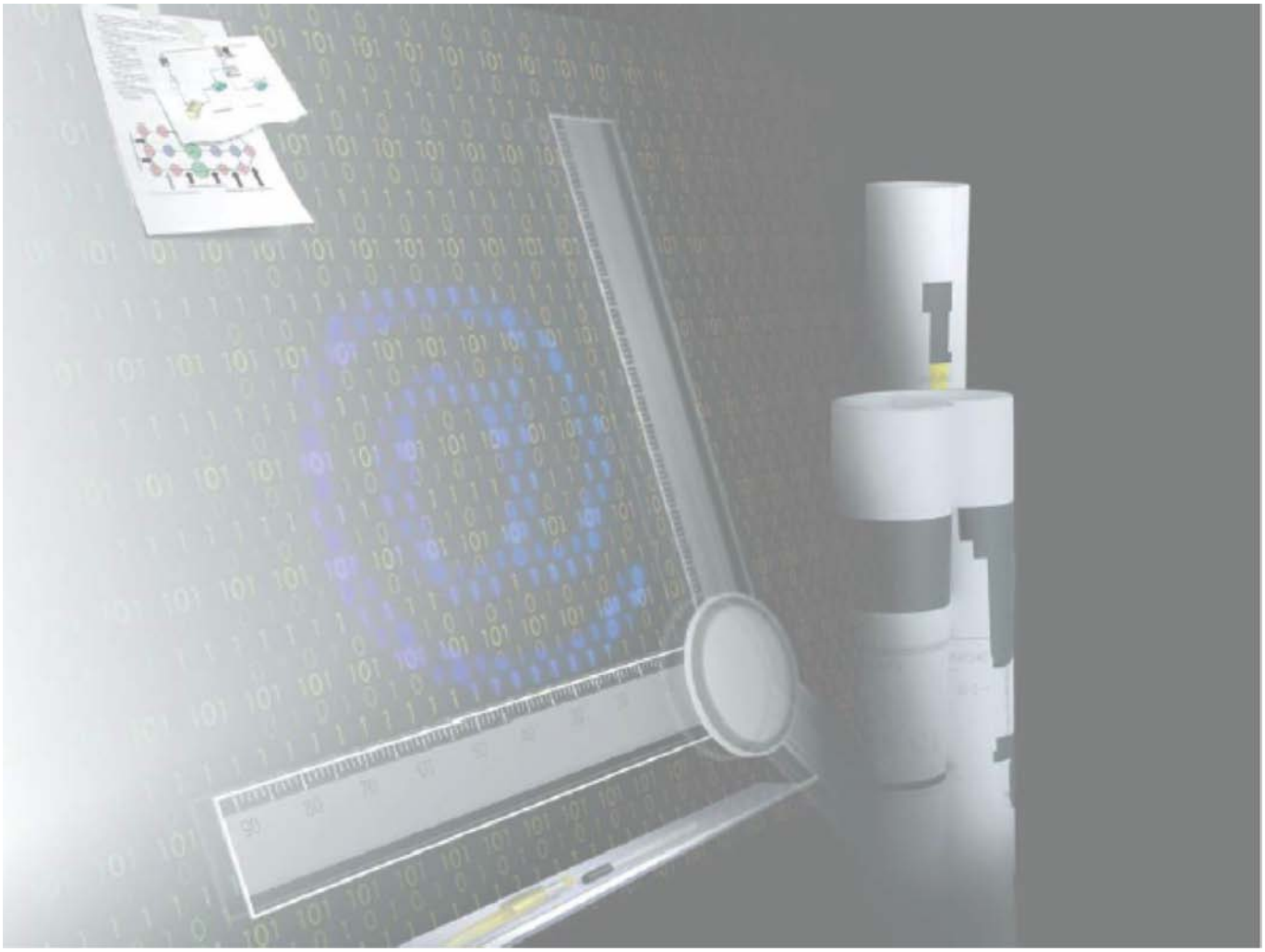
The documents that had to be filed electronically were sometimes up to 30-50 MB in size, which meant that even the registering procedure was a real challenge to performance and capacity of the VPS, or more precisely: the Web VPS. During the month-long registration period alone, about 2,500 incoming encrypted and qualified e-mails were processed by the VPS. It is a remarkable fact that the number of registration documents handed in as unencrypted e-mails, on CD or in written form was less than 2 per cent of all the applications.

Apart from the systems "electronic legal relations" and "emission certificate trading" which were already mentioned, the VPS's web component is currently also used (among other things) by airlines for transmission of data about their flying staffs' radiation exposure as well as by the Federal Nature Conservation Agency for the filing of applications for import and export of protected plant and animal species.

The SMTP component "Julia"

While the integration of the Web VPS into an already existing system generally requires certain adaptations, the SMTP component can at most times be effortlessly "threaded into" the e-mail traffic of a public agency or other organisation. According to the rules that can be freely defined by the operator, "Julia" processes incoming and outgoing e-mails in a manner fully transparent to the end user; that is to say that the latter often does not even realise he is communicating in encrypted form, since "Julia" automatically handles all encryption processes in the background.

Numerous public agencies already make use of the VPS's SMTP component, among them the Federal Foreign Office, the financial authorities, the German Pension Ensurance Federal Institution, the Federal Statistical Office, and so forth. In addition, the introduction of the VPS is planned for 2006 by many other public agencies. Link: www.bsi.bund.de/fachthem/egov/vps.htm



3 Technical solutions for secure data transmission

3.1 NEWS FROM THE WORLD OF SINA
3.2 ELCRODAT 6-2, GALILEO, SAR-LUPE
3.3 BOS – THE DIGITAL RADIO NETWORK
3.4 BIOMETRICS TECHNOLOGY

3.1 News from the world of SINA

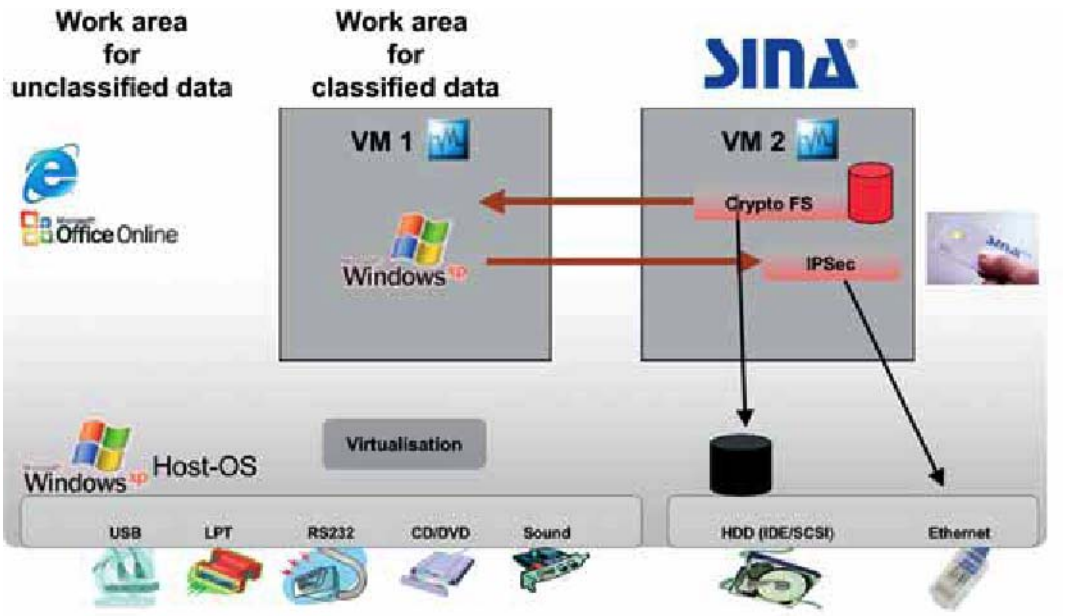
With the "Secure Inter-Network Architecture" SINA, BSI provides a technology which allows for highly secure connections via the ordinary internet. In 2005, BSI also has developed further components all around SINA in collaboration with the company secunet Security Networks AG.

Besides the elements SINA Box and SINA Thin Client which have been available for a while, the SINA Virtual Workstation (VW) is now gaining importance. This Virtual Workstation is a component of the SINA architecture which enables local processing and storage of governmental classified documents. Additionally it permits IPSec-encrypted data communication via any given network (e.g. GPRS, UMTS, WLAN or DSL). VoIP in SINA networks will be also possible in the future. In the SINA VW, operating systems that are potentially unsafe or cannot be evaluated are encapsulated in a virtual environment. This environment is provided by a virtual machine which itself is run on the evaluated host operating system SINA-Linux. The virtual machine simulates a standard hardware environment in which the guest operating system is run with its applications. Access to the physical hardware is only possible under control of SINA-Linux.

One first version, which has already proven its value to several customers, above all the Federal Foreign Office, has been thoroughly updated by BSI in 2005. Apart from a new operating system core which allows the deployment of current hardware, the previous virtual machine was exchanged for a new version by a German manufacturer. Since the source code was made available by the manufacturer, BSI could conduct an intense evaluation. Additional adaptation necessary for actual operation were made in collaboration with the manufacturer. These innovations in combination with an expansion of methods for hard disk encryption now also permit its use in the area of high security.

Sharp attention: View inside the Federal Foreign Office's operations centre

SINA Virtual Desktop



Two virtual machines (VM) are running in the hosting operating system (in this case, Windows XP). One of them (VM 1) serves as working environment for classified material (VS data). This environment is launched from an encrypted file system (Crypto FS) on the second VM, i.e. the crypto container has to be unlocked with the matching key and only then is it possible to boot this system. The Crypto FS is situated on the physical hard disk (HDD). Any communication of VM 1 happens through VM 2 via the system's ethernet interface. In this process data transmission is IPSec-encrypted. Unclassified data are processed in the host OS; which makes direct use of the necessary hardware resources (USB, sound, etc.). The guest OS in VM 1 uses these resources via a virtualisation layer.

Definitions of terms

VM	Virtual Machine (there are two of these)
Crypto FS	Crypto file system
IPSec	Term for the encryption of data transmissions. If data are transmitted from the Virtual Desktop via the net ("Ethernet"), this happens through an IPSec-protected connection. IPSec itself is a standard used by BSI in SINA.
Host OS	Host Operating System – the operating system which is the "host" for the guest operating systems.

In the foreground: The Federal Foreign Office premises in Berlin – one of BSI's "customers".

Virtual Desktop

Due to the SINA VW's architecture, the host operating system can only be provided with a limited range of virtual hardware. Specialised hardware (e.g. processors for graphics acceleration) cannot always be put to optimum use.

This is why the additional development project SINA Virtual Desktop was launched for handling of classified documents of VS-NfD status (classified material – for official use only). Here, a commercial operating system (Windows XP, for example) acts as host operating system where, apart from the usual standard applications, virtual machines ensure that additional work environments are provided for the processing of critical data.

Thus a SINA compatible IPSec component (SINA-Box) can work in one virtual environment and in addition provide the cryptographic file system for encrypted data storage, while a trustworthy environment for processing classified data is created in the other. When processing unclassified data, the host operating system can be used natively without the restrictions described above. This variant addresses cases of applications with low protection requirements.

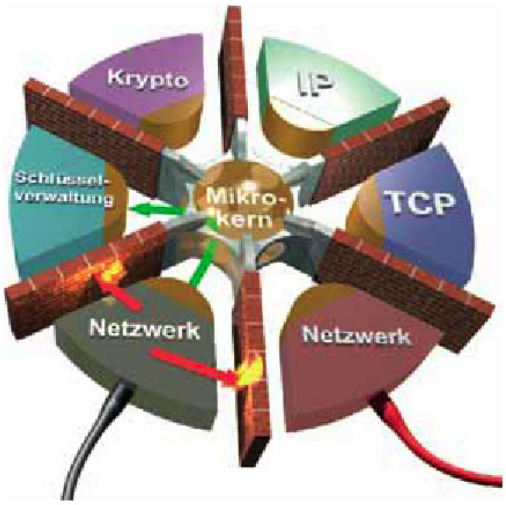
By the principle of virtualisation, which is also used in this variant, and the different logical address spaces for host and guest operating system that come with it, an adequate protection for the addressed applications can be obtained in connection with the usual security measures for commercial operating systems.

The product SINA Virtual Desktop is to be licensed in the course of 2006 for applications with VS-NfD.

Micro kernel

The architects of information technology who are responsible for safe data processing will in the future resort more and more to a micro kernel-based platform. This meets the increasing complex requirements for applications and security guidelines. A micro kernel is an extremely small operating system core that is housed as security layer between one or more of the actual operating systems and the hardware. This platform – along with the hardware available – is capable of implementing security mechanisms for memory protection and access control. Apart from an efficient communication infrastructure, it also has to provide a virtualisation layer so that so-called legacy operating systems are available for the user. A virtualisation layer provides the operating systems with virtual devices and routes the systems' virtual accesses to the existing physical software.

With the project "L4VM", BSI has developed a prototypical micro kernel-based platform which in the coming years is to replace the monolithic security platform of SINA components. A short technical description of the basic features of micro kernel technology and hardware virtualisation is necessary for the evaluation of the additional gain of security.



The micro kernel's architecture is based on firewalls sealing off the program segments from each other. Incoming information is solely processed by the kernel.

Micro kernel replaces conventional security platform

The micro kernel is the only privileged system component that is run with priority 0, i.e. the highest possible priority, on the widespread Intel architecture IA32. Every further system component or application runs in user space under complete control of the micro kernel. In a monolithic operating system kernel all system calls have unlimited access to the core memory which under certain circumstances may lead to a compromise of the entire system through unnoticed programming errors or malicious kernel modules.

Such scenarios may not be completely impossible under a micro kernel, but they cannot create immediate damage anymore. Loadable kernel modules can preferentially be loaded and implemented into separate address areas, which is known as encapsulation of the component. By displaying memory pages, the memory kernel can facilitate access to selected memory kernel areas. Besides, Inter-Process Communication (IPC) offers the possibility to record system calls and to realise a comprehensive system audit at the lowest system level.

The Virtual Machine Subsystem (VMS) is responsible for the virtualisation of hardware. The VMS enables the implementation of socalled legacy operating systems, e.g. Windows XP, for which porting to the micro kernel interface is not easily achieved or even undesirable. The principle of hardware virtualisation for the encapsulation of a guest operating system which is not generally trustworthy or cannot be evaluated provides additional protection for the host operating system. In the case of a micro kernel-based system this protection mechanism is greatly enhanced due to the VMS's fundamental encapsulation by the micro kernel. Access by the guest operating system is exclusively organised by the VMS via the communication infrastructure provided by the micro kernel.

With a high-performance hardware and/or hardware support, additional security mechanisms such as micro kernel technologies and virtualisation for the implementation of legacy operating systems can be transparently integrated into the security architecture. The existing prototypical generic solution developed by BSI is not only suited for use in the maximum security scenarios within the Federal Government, but is also of public interest when it comes to the requirements for a reliable IT system's environment.

3.2 ElcroDat 6-2, GALILEO, SAR-Lupe

The ISDN crypto system ElcroDat 6-2 is approved for transmission of data of the highest degrees of classification. It prevents eavesdropping or secret manipulation of the transmitted data by unauthorised persons.

There is an increasing exchange of sensible data between the Federal administration, industrial enterprises commissioned with the protection of secrecy, or security authorities. There is thus a need for encryption systems that meet the highest demands for security and offer sufficient bandwidth for modern applications.

Project ElcroDat 6-2

The maximum security solution ElcroDat 6-2, developed by BSI and the company Rohde & Schwarz SIT GmbH, covers a multitude of scenarios. Telephone and data connections as well as faxes and video conferences – even via satellite – are possible. Idea, concept and numerous technical details of this system originate at BSI.

The system is authorised by EU and also by NATO, and is suited for all national degrees of classification including TOP SECRET. It consists of the following components:

- the encryption devices ElcroDat 6-2 S and ElcroDat 6-2 M
- a management station for cryptographic management
- a service station for remote administration of the encryption devices
- a logging station for remote observation of the encryption devices

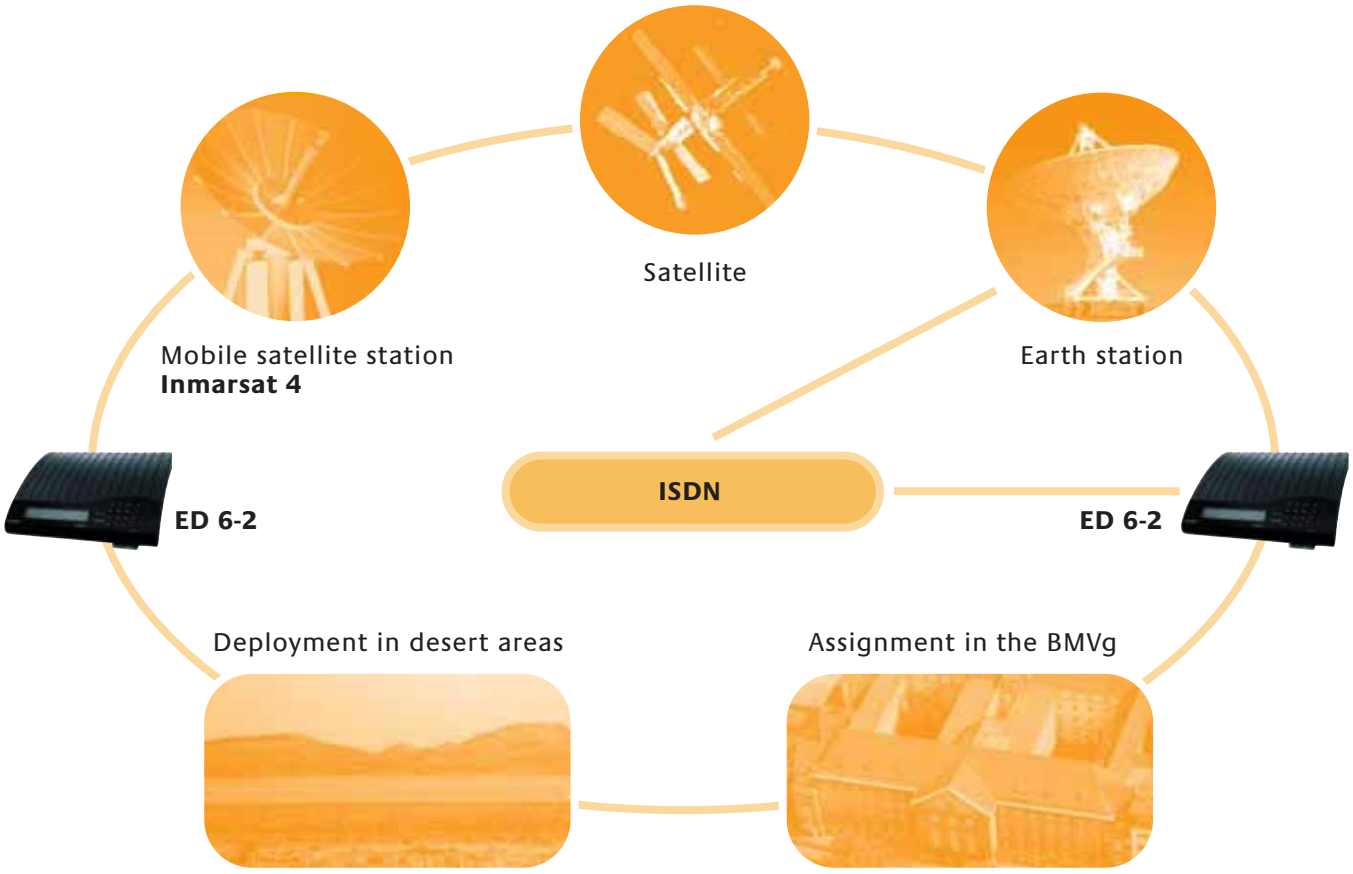
There are two types of devices: the ElcroDat 6-2 S for basic ISDN access on two information channels, and the ElcroDat 6-2 M primary rate interface with 30 information channels. The public key infrastructure relieves the user entirely from having to feed key information to the system. Cryptographic maintenance of the devices is taken over by the management station.

A “Gateway” – completed in 2005 – as connector enables communication between digital ISDN and already existing cryptosystems based on analogue networks.

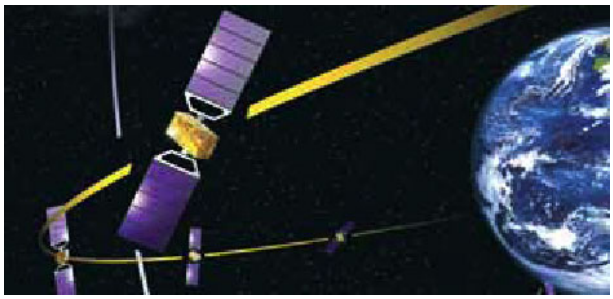
The ElcroDat 6-2 meanwhile is being used by security authorities all over the world. Among the users are the EU and a number of European governments. NATO has chosen Elcro-Dat 6-2 for its standard ISDN encryption system, and some of them have been installed since 2005. There is a steadily rising demand for ElcroDat 6-2 devices and system components.

The system is continuously brought up to date, tested, and put into action. An additional module is currently being conceived which will – in combination with the Secure Communication Interoperability Protocol (SCIP) – also facilitate encrypted connections across network borders. Thus in the future a communication between ElcroDat 6-2 and analogue ways of application. A further product and connections, mobile phones or non-ISDN-system innovation will be the possibility to compatible terminals will also be possible. update the software in a secure procedure. This opens an enormous range of possible ways of application. A further product and system innovation will be the possibility to update the software in a secure procedure.

From the desert straight to the Ministry of Defence:
Secure ISDN connection due to ElcroDat.



The codification of ISDN connections via satellite links is another feature of the ElcroDat 6-2 encryption system. An example: The daily status report of a Federal Armed Forces Command abroad, e.g. in Afghanistan, is transmitted via video teleconference to the Federal Armed Forces' operations centre (BMVg). Since there is no fixed-line ISDN connection available here, satellite terminals are put into use. The connection with the receiving earth station is made via the Inmarsat network. In order to obtain the necessary bandwidth, several transmission channels are multiplexed. The connection is encoded with the ISDN encryption device ElcroDat 6-2.



One of the 30 satellites that together will form the European navigation system GALILEO (diagram).

Satellite projects

In 2005 BSI made essential contributions to the design and development of up-todate satellite systems. Here, we must mention the Global Navigation Satellite System (GNSS) GALILEO and the national observation system SAR-Lupe.

GALILEO

GALILEO is a next-generation navigation system. It has ground stations spread all over the world and is monitored and operated by two control centres. There are four different services on offer: an open service (OS), a commercial service (CS), an air service (SoL) and a governmental service (PRS). GALILEO also supports the maritime rescue system (S&R).

All these services have their individual requirements concerning security, quality and availability:

- The OS is to be free of charge for all users. Thus, guaranteed security and availability are not to the fore here.
- Commercial providers through the CS have the possibility to offer their services (e.g., fleet management or route tracking) to logistics enterprises, for example. The design of the CS allows for an increased degree of security, quality and precision.
- The SoL serves for the navigation of aircraft.
- For governmental users, the PRS offers a maximum of security, availability and quality.

A system of such complexity is exposed to a multitude of risks. The aim of BSI's co-operation is therefore to repel these threats with appropriate security measures in the system.

The emphasis of its support lies on the specification of satellites, of the ground components and of the respective security relations including management, and of the different services especially of the PRS. GALILEO as an international project in particular requires arrangements with foreign national security authorities, participating industries and the project management (ESA). Support covers all aspects of security; among others, cryptographic and IT security.

BSI's involvement is of special importance in the protection of the governmental Public Regulated Service (PRS). Because the PRS was developed exclusively for public agencies or similar national and international institutions, this service is exposed to potential threats from outside, for example Denial-of-Service or unauthorised use. Therefore it makes extremely high demands not only concerning confidentiality but also with regard to the quality of the signal transmitted, the source's confirmability and the integrity of the information, also in those situations where other services are not available.

After completion of the specifications – estimated for 2006 – BSI, within the framework of the team of national experts (NETeam) which consists of staff members from the different nations, will be involved in the evaluation process accompanying development. On national level, BSI in co-operation with other Federal authorities is going to develop a management for national use of the PRS and the system's interfaces according to the GALILEO specifications. The evaluation of Cryptography by BSI has already been completed to a greatest extent in 2005.

In the GALILEO satellite surveillance system, the different control segments, the key management and the generation of mission data are combined in two control centres (GALILEO Control Centre – GCC). These are also responsible for the linking with external partners or centres. The GALILEO system possesses 30 sensor stations for the monitoring of satellites and uplink stations spread all over the world which control the satellites and provide the users with the necessary data and information. All in all, the GCC have to monitor, navigate and administer 30 satellites in three separate orbits. All communication relations are protected – in some cases on multiple levels – from external and internal attacks by the appropriate IT or cryptographic measures. Right: View inside the German space control centre in Oberpfaffenhofen, one of the two future GALILEO control centers.

SAR-Lupe

The global surveillance system SAR-Lupe consists of several satellites which can take pictures of the earth's surface. It is divided into one purely national and one international part. Cryptographic security is the sole responsibility of BSI which closely co-operates with the Federal Office for Defence Technology and Procurement (BWB – Bundesamt für Wehrtechnik und Beschaffung) in Koblenz, with industrial firms and further Federal authorities. In 2005, the focus of BSI's activities with regard to the national part was on the evaluation of the crypto-components. In addition, BSI supported SAR-Lupe in the preparation and updating of the IT security documentation. In the international area the crypto-concept was a focal point in 2005. Here, BSI also co-operated with the BWB in the design of IT security documents.

The Federal Ministry of Defence uses SAR-Lupe, the first German satellite-supported reconnaissance system for early detection of crises and crisis management.

3.3 BOS – the digital radio network

The first parts of the new digital radio network BOS are due to be established in the course of 2006. This network is meant for communication between public agencies and organisations with security tasks (BOS-Digital).

There are several ways of implementing such a digital BOS radio network. On international level, the ETSI standard "TETRA" (Terrestrial Trunked Radio) and the industrial standard developed by the company EADS have been established.

In the future there is also to be a system variant suitable for BOS-digital based on the GMS standard. A multitude of different systems are already in use Europe-wide.

BSI is in charge of supplying the emerging radio network – independent of the actual choice of radio system – with a so-called end-to-end encryption. This will ensure a particularly high level of security.

In order to achieve this, BSI has in recent years been working intensely on the development of an innovative encryption technology based on chip cards. Nearly every portable communication terminal today has an interface for the insertion of a SIM card.

Chip cards with highest security standards

Due to the integration of encryption onto a chip card, radio terminal devices that are already commercially available hardly need any technical modifications. At the same time chip cards are mainstream products that meet the highest security demands and have proven their worth millions of times in various security systems.

According to plan all of the about 450.000 terminal devices in the network will be equipped with the new "BOS chip card". This comprises all the security relevant functions. A BOS chip card can be produced at very little cost; nevertheless it is a fully-fledged encryption tool with all the necessary features.

BSI's BOS cryptosystem has an autonomous Public Key Infrastructure which in the future is to be operated by BSI. This allows for very efficient rollout and parametrisation of the systems. In the context of the system's development and adaptation the experts have taken into account all conceivable BOS-specific scenarios.

In this way all security demands of institutions such as the German disaster relief organisation (THW – Technisches Hilfswerk), fire brigades and special task forces (SEK – Sondereinsatzkommandos) could be considered. Special care was taken for the system's integration into control centre systems.

The modular nature of this approach greatly simplifies the development of terminals for the new digital BOS network and by this allows for reduction of costs and choice between a wide range of products. Principally the BOS radio set of the future will hardly differ from conventional mobile phones. The modification of industrial series products that use the BOS chip card as security anchor will take the place instead of the construction of new appliances.

Mobile phone users are familiar with the main principle: For BOS users, logging into the radio network follows the SIM card principle. The security card's functions are only available after putting in the correct PIN data on the key pad.

Data base connection

The high security level of the end-to-end encryption should also be maintained when individual terminals are communcating with central points of the BOS network. For example, connecting a database to the BOS network requires simultaneous managing of numerous encrypted connections which may connect to various BOS members all over Germany. In the future it would be possible, for instance, to retrieve biometrical data (fingerprints, facial image, etc.). A police officer could in this way make a complete personal identification on site. For these cases of application a multichannel complement for the BOS chip card is to be developed at BSI's commission.

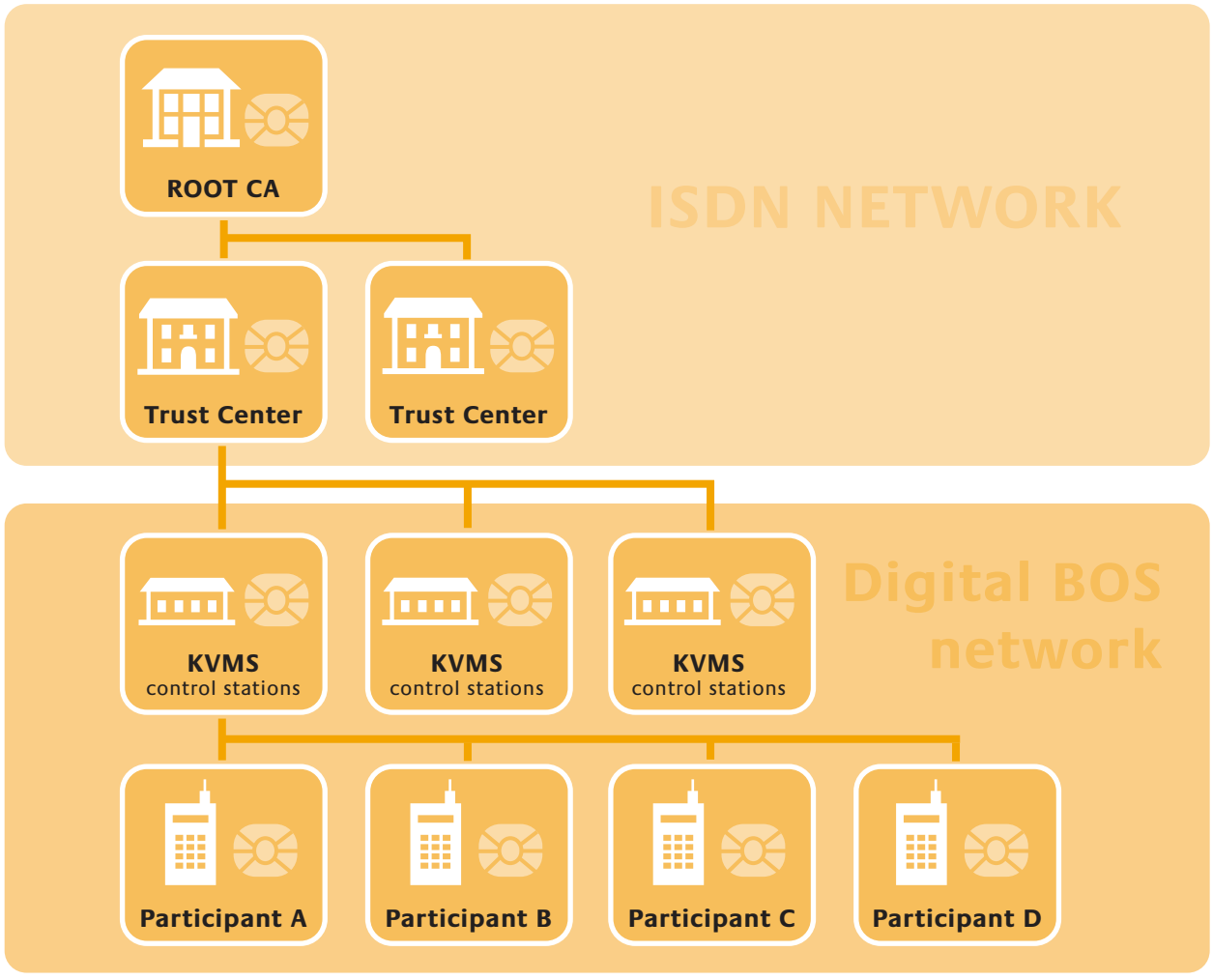
Chip card technology and cryptography are highly dynamic research areas subject to constant innovation and cannot be assesed independently from all possible scenarios of application. Radio networks are becoming increasingly powerful and will probably allow for much faster transmission rates in the future. Radio terminals will also have to meet increasing demands on their performance.

The speed of this development is largely dictated by the rapid advancements in the sector of mobile communication. BSI for this reason pursues long-ranging strategies for the BOS cryptosystem's maintenance and further development. These include the porting of the BOS chip card onto newer, more powerful types of cards and the card's integration into alternative forms such as the SD memory card.

Fireworks display at the Berlin Olympic stadium: Such big events are particular challenges for the security forces.

The German disaster relief organisation (Technisches Hilfswerk, THW), fire brigades and police all need a secure radio network that forbids misapplication and is of multifunctional use.

System architecture digital network Public agencies and organisations with security tasks (BOS)



Inside the BOS radio devices, a chip card (security card) serves as a module which packages cryptographic algorithms and the necessary cryptographic keys. In addition, the security card provides the network access function (SIM function) and the transmission of the BOS's operational tactical address. For the BOS's special concerns, the key management system was optimised with regard to availability and flexibility. It is based on an infrastructure consisting of the levels KVMS (Crypto-Variable Management System) and TC (Trust Center) and Root CA (Root Crypto Authority). Security cards are scheduled as crypto modules and authentication modules also for KVMS and TC. Following a resolution by the German Federation and the Federal States, BSI is going to manage the components Root CA and Trust Center in the digital network's future operation.

3.4 Biometrics technology

BSI in 2005 has consistently pursued its biometrical projects. Laboratory experiments were followed by field tests, practical application was put to the fore. BSI experts addressed new biometrical technologies such as 3D facial recognition and with its investigations on multi-modality pointed out methods which may multiply the capacities of biometrical systems.

BioFace

The BioFace project series begun in 2002 was continued in 2005 with further studies concerning the potential of facial recognition systems. BioFace III, a study of the limitations of such systems already completed in 2004, was analysed in 2005 and prepared for publication. At the same time, with Bio-Face V BSI stayed abreast of the current technological trend towards three-dimensional face recognition.

Using the data obtained in a field test, the functionality and recognition performance of two systems available on the market and one specially developed for the project were examined. The study's results went into a BSI article for the standardisation approaches of ISO.

BioP

The examination of biometrical verification methods in the context of the BioP II project had the goal of assessing the capacity of face, fingerprint and iris recognition systems available on the market at the time. From this, conclusions as to the successful use of biometrical methods in connection with id documents could be drawn. The results of this study can be viewed at BSI's homepage under www.bsi.de/literat/studien/ biop/biop_2.htm.

BioP II comprised a practical testing of the three mentioned biometrical methods based on scientific criteria in a comparative system test. The focus was on examining technical feasibility. The vital questions were:

- What degrees of performance do systems for face, finger and iris recognition have?
- Can these methods yield satisfying results using image files according to ICAO reference?
- What is the three methods' practical efficiency in a large-scale test? What about usability and acceptance?
- Which of the methods is best suited for use in id documents, and under what circumstances?

The overall project was led by BSI in close co-operation with BKA (Germany's Federal Criminal Police Office) and the two companies Fraport AG and Deutsche Lufthansa AG. Also present: The company secunet Security Networks AG as contractor.

In the year 2005 BSI also had these biometrical scanning screens for face and gesture recognition tested.

BioFinger II

Several methods of increasing recognition performance of fingerprints were at the centre of the BioFinger II test series. The idea was to use several fingerprints instead of only one. This provided answers to the questions as to what increase of performance could be obtained if

- two pictures of the same finger are taken and stored during enrolment,
- two pictures of the same finger are taken and compared during verification,
- two different fingers are used during enrolment and verification, or if
- two different algorithms were used for finger recognition.

In the most favourable scenario – two fingers instead of only one – error rates could be reduced to about one-tenth of the original results.

BioMulti

BioMulti combines several biometrical methods and is based on BioP II data. BSI in 2005 has refined the BioFinger II methods and used them for the coupling of

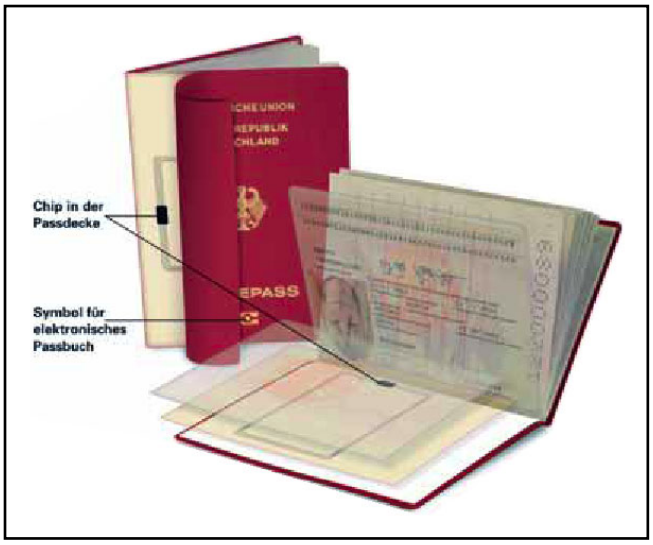
- iris and face recognition,
- face and finger recognition,
- iris and finger recognition, as well as
- double finger recognition.

These couplings, according to the studies, allow for error rates of around one-tenth compared to the methods using only single samples.

Passport with biometrical features – ePassport

The introduction of the new electronic passport (ePassport) on November 1, 2005 set the priorities in the debate about biometrical features in official travel documents.

Germany is among the first EU member states to introduce the ePass. Stored on the chip are biometrical data: initially the digital passport photo, and in addition fingerprints shall be digitally recorded from March 2007 onwards.



Presentation at the "Moderner Staat (Modern State) 2005" fair: The electronic passport's chip cannot be read out without appropriate authorisation – BSI supplies the necessary software application, the "Golden Reader Tool".

EU heads of states and governments had basically agreed in mid-2003 to include biometrical features in the ePassports. A resolution concerning this was passed in December 2004. According to this, all EU member states will have to integrate digital facial images into their passports within 18 months. BSI made significant contributions to the technical design of the security specifications in committees of the International Civil Aviation Organisation (ICAO) and of the EU.

The main focus of the "Official Documents Task Force" ("Projektgruppe Hoheitliche Dokumente") in BSI was on the realisation of the IT security concept in the new ePassport. To keep public discussion of the new passport's security impartial, the Federal Office has provided all technical details concerning the ePassport for interested citizens on an individual homepage (including e-mail- and telephone hotline).

Information concerning the electronic passport

Project department – Governmental documents and electronic ID cards

P. O. Box 20 03 63, D-53133 Bonn

Internet: www.bsi.bund.de/fachthem/epass

E-Mail: ePass@bsi.bund.de

Hotline: +49-1805-274 300

(12 ct/min. from the german fixed network. Costs from abroad dependent on provider.)

Country Signing Certification Authority (CSCA)

In time with the start of the new ePassports' production, BSI in its function of Country Signing Certification Authority (the major authority in the ePassport context) (CSCA) has issued Document Signer Signature Key Certificates (DS) to the German Federal Printing Office. Thus the passport producer is able to protect integrity and authenticity of the data stored on the ePassport's RF-chip against falsifications or manipulations.

During border controls, for instance, it is possible to check whether the signed data on the ePassport were created by an authorized office and whether they have not been modified since its production. The integration of this digital signature defines new quality levels concerning anti-counterfeit passports.

Not a "magical eye" – this person is approaching an iris scanning device

Digital security features in the ePassport

- **Extended Access Control – BSI's security concept**

From 2007 onwards, fingerprints shall be stored on the EU passport's RF-chip in addition to the facial image. Such highly sensitive data has to be especially protected against unauthorised readout. For this, BSI has developed the Extended Access Control (EAC) Protocol for extended access protection and presented it to the responsible EU working team.

The EAC protocol provides an authentication mechanism for the validity check of an RF-chip in the ePassport and of the reading device. The reading device is equipped with its own pair of keys and a certificate that can be verified by the RF-chip and defines the data that may be accessed. This ensures that reading devices can only access those data for which they are authorised.

- **The "Golden Reader Tool" – basis for inter-operable electronic passports.**

The "Golden Reader Tool" (GRT) developed at the commission of BSI is a software application for the readout of ICAO-conforming passports with RF-chips (eMRTD: electronic Machine Readable Travel Documents). With the GRT, BSI pursues the aim of creating the foundations for world-wide inter-operabilty of eMRTDs based on the ICAO's specifications. Tests in Singapore, Japan and the USA have proven that GRT can be applied world-wide. With this, BSI has created the possibility to read ePassports according to a unified standard world-wide and under observance of the high security requirements.

- **Protection profiles for eMRTD**

In the so-called Protection Profiles, BSI has defined all the security criteria that have to be met by RF-chips. The RF-chips designated for German passports have already been tested and certified according to the security criteria of BSI-PP. Meanwhile, the security criteria of BSI-PP are being used Europe-wide in the testing of ICAO-conforming chips.

The sample photograph gallery of the Federal Printing Office (Bundesdruckerei) shows the important features of passport photos. They have to meet the requirements of the International Civil Aviation Organization (ICAO), a subsidiary of the United Nations. The old-fashioned photo machine at central station may soon be obsolete.

4 Testing, evaluation, certification

4.1 Technical security guidelines
4.2 Growing significance of certificates
4.3 Profiled protection

4.1 Technical security guidelines

With the publication of technical guidelines, BSI pursues the aim of determining requirements and recommended ways of action for the development and implementation of secure and interoperable IT security solutions.

By help of the defined criteria it is possible to choose suitable products and test their conformity to the respective guideline. These technical guidelines are recommendations. They can become binding if the specifications given in the TR are applied during tendering procedures.

Technical guideline SmartCards

SmartCard solutions often are characterized by the discrepancy between their widespread and cost-effective use and the lack of interoperability of different card types and hardware components. The BSI's guideline aims at an increase in IT security as well as a usage of existing card infrastructure that corresponds to the standards and is multifunctional, interoperable and future-proof. The technical guideline for SmartCard solutions consists of three parts:

- **Part 1: Chip cards**

This part describes the properties of an interoperable and multifunctional chip card in consideration of international standards and restricted degrees of freedom for reasons of interoperability and compatibility. From the operational goals arise the functional and technical security requirements. Together with the requirements of practical use these form the basis for quality assurance tests.

- **Part 2: Chip card readers**

Part two describes the requirements for interoperable and multifunctional chip card readers. These have to be suited for the following applications:

- Access control,
- Time & attendance,
- Computer/network access,
- Interoffice communication,
- Internal company accounting systems.

The multifunctional Dual-Interface chip card specified in part 1 serves as the basis for this. This part contains recommendations for both inexpensive standard readers and professional multifunctional chip card readers suited for a multitude of present and future chip card applications.

- **Part 3: Chip card-specific requirements for applications**

The third part describes the chip card-specific requirements for background systems that make use of the capacities of the multifunctional chip card specified in part 1 of the Technical Guidelines. The guideline defines actual implementations that safeguard functional and safe coaction between chip card and background system. At the same time the harmonization of methods creates the foundations for a consistent authorization management system open to further system applications.

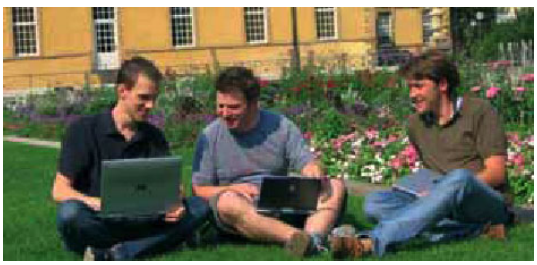
Secure verification of electronic signatures is made possible by special SmartCards. They are connected to the computer via a reading device.

Technical Guideline Secure Wireless LAN (TR-S-WLAN)

The TR-S-WLAN is meant to advance the development and implementation of secure, interoperable and standard-conforming wireless LAN systems and infrastructures according to the IEEE 801.11 standard. To this end, the Technical Guideline (TR) provides concrete recommendations for planning, procurement, installation, configuration, certification, administration and shutdown of secure wireless LANs in the fields of commerce and public authorities.

The TR targets all those concerned with the safeguarding of WLAN installations, be it as planners, suppliers, operators or users. They will be assisted in the choice and procurement of secure, interoperable and future-proof WLAN systems. Manufacturers and those entities responsible for validation will find the necessary security functionalities of WLAN products and test methods in the TR.

Wireless internet access – this router has several outlets for DSL, network and radio connections.



The blessing of wireless connections: Students in the palace garden of the University of Osnabrück using their laptops to communicate with fellow students.

The Technical Guideline Secure WLAN comprises several parts:

- **Part 1: Presentation and assessment of security mechanisms**

This part describes and evaluates the essential marketable methods and mechanisms for WLAN protection that are emerging through standardisation. Further topics are architectures, implementation alternatives and fields of application.

- **Part 2: Specifications of a WLAN security concept**

Here the threat situation is analysed and from this general as well as specific security measures are deduced. The composition of this is orientated along the IT-Grundschutz manual's structure and methodology. A model concept illustrates the application of the specifications.

- **Part 3: Selection and testing of WLAN systems**

The third part of this guideline is divided into two documents. Part 3a defines the criteria for the selection of WLAN systems, i.e. verifiable product features of a WLAN system's various components. This document principally addresses suppliers and manufacturers. The test criteria in Part 3b define the methods for testing whether the demands made in the selection criteria are being met. Depending on the required for test result, three test categories are defined, ranging from manufacturer's instructions to functional laboratory tests to evaluation and certification according to Common Criteria.

On the basis of the TR-S-WLAN it will in the future be possible to create special protection profiles that follow the Common Criteria.

This Technical Guideline is addressed at all those concerned with the safeguarding of WLAN installations, be it as planners, suppliers, operators or users. It facilitates the selection and procurement of secure and interoperable WLAN systems. Available in printed form including a CD from SecuMedia Verlag (www.secumedia.de) at a price of 75 euros.

Surfing on the tramway: this is also possible by radio if there is a so called Hotspot around – a router with network connection.

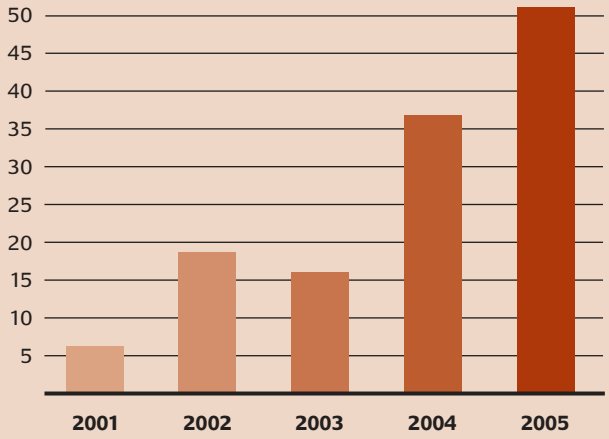
4.2 Growing significance of certificates

Certification of IT products based on internationally acknowledged IT security criteria is of growing importance to BSI. The purpose of certification – to make IT products and systems transparent and comparable as to their security qualities – in the past year caused a strongly rising demand particularly for internationally agreed certificates on the basis of the Common Criteria (ISO/IEC 15408:1999).

Due to this, BSI in the year 2005 was able to issue more than 50 certificates for a wide range of different product types from the areas of both hardware and software.

In the software area this is exemplified by z/OS – a mainframe operation system of the company IBM. This system received a certificate for use on IBM zSeries computers.
In the hardware area BSI has issued numerous certificates, mainly in the field of SmartCard development. One concern among others was their use in electronic passports.

More and more certificates



A new all-time high in the awarding of certificates was reached in the year 2005: BSI certificates went to software manufacturers such as IBM, for instance. But the internationally approved attestations were also handed out in the field of SmartCard development relating to the electronic passport.

As in the previous year, several certificates and reports for “Assurance Continuity” could also be presented in 2005. This procedure is to authenticate whether a certificate remains valid in spite of modifications made on the product. “Assurance Continuity” offers a significant increase of efficiency particularly for hardware manufacturers in the certification of their products.

All international tests passed: View of the premises of the Federal Office for Information Security in Godesberger Allee in Bonn.

BSI certification authority had itself tested

This year in May the BSI certification centre has successfully undergone an inspection by the CCRA. The CCRA (Common Criteria Recognition Arrangement), an international agreement for the approval of certificates, requires this mutual review. Currently there are 21 nations combined in the CCRA. Representatives from the USA, Canada and Sweden have tested the BSI certification centre with positive results.

Regular examination ensure that all nations maintain equally high quality standards in certification. The requirements of the CCRA largely conform with the international standards DIN/EN 45011, or ISO-Guide 65 respectively. The certification and accreditation body's quality management handbook served as the basis for the tests.

International co-operation

As it is true for the development of protection profiles *(q.v. chapter "Profiled protection")* BSI is also involved in various different international certification projects. These include, for example, the further development of the Common Criteria on the basis of version 2.1.

The new version 3.0 will bring fundamental changes that respond to current trends in information technology. It is the aim to make evaluations and certifications more efficient and economical. Version 3.0 has already been presented to the respective ISO committees.

BSI's task is the annotation of new or modified sections. The revision of individual sections is also BSI's responsibility. This is to adapt security requirements to the life cycle of the products that are to be certified, and to have the necessary revisions of user guides.

As with the last Common Criteria update, trial evaluations in the areas of both hardware and software are already being conducted on the basis of the new CC version 3.0. BSI uses these projects to be able at early stages of development to gather practical experience that can be applied in later certification procedures.
Furthermore, BSI is involved in international projects such as the certification of different system components of the A400M airplane. Cockpit systems are the main subject here.

As of January 1, 2005 BSI presides the "Joint Certification" panel. Germany, Spain, France, Belgium, England and Turkey are associated in this panel.

The Airbus A400M (simulation) – a tactical long-range military transporter, ready for operation from 2007.

New test centres licensed

In 2005, the twelve test centres already accredited and licensed have been joined by two more that have successfully completed the licensing procedure. Since mid-2005 the companies "media transfer AG" and "Secunet SwissIT AG" are entitled to test the security qualities of IT products according to the international security criteria (Common Criteria) in the context of BSI certification procedures.

IT-Grundschutz: Future development

IT security is not only dependent on technology and the products in use. Organisation and personnel parameters are of equal importance. Apart from product certification according to the Common Criteria, firms have the possibility to have their business units or transactions certified.

The IT-Grundschutz manual, which has been constantly revised for years, offers the necessary fundamentals for this. The standard security measures defined in it allow for an adequate level of security for typical IT systems. Adhering to the IT-Grundschutz manual is a prerequisite for the issue of a certificate. In 2005, development of the new ISO 27001 certificates on the basis of IT-Grundschutz was completed. They will be available from the beginning of 2006.

BSI president Dr. Udo Helmbrecht with department chief Bernd Kowalski and head of division Jürgen Schwemmer of the Federal Network Agency presenting an IT security certificate to Dr. Rüdiger Mock-Hecker, manager for the card systems branch of the German Savings Bank's publishing house, for its electronic signature software "S-TRUST Sign-it", at the Systems trade fair.

4.3 Profiled protection

So-called Protection Profiles map out the requirements for product classes (e.g. firewalls, cash cards or operating systems), without having to refer to a particular product.

With Protection Profiles it is possible to define the IT security requirements of a whole category of IT products or IT systems without referring to the actual implementation of one IT product or system.
With the aid of the requirements from the Common Criteria a model solution is detailed on an adequately abstract level. Thus the authors of Protection Profiles can set the standards which are then nationally and internationally accepted.

The concept of Protection Profiles substantially increases the comparability of product evaluations according to the CC. Due to the general security concept of a Protection Profile there is a guarantee for good comparability of different products that have been developed and evaluated on the basis of one and the same Protection Profile.

Suppliers of IT can take advantage of these possibilities. During tendering procedures they can demand for conformity with a certain Protection Profile in the performance specification. In some areas this is already common practice, for example in waste disposal or the digital signature.

Certified Protection Profiles are published on the official „Common Criteria“ web site and the respective national web sites of certification bodies. They can be used as the basis for the evaluation and certification of IT products.

Protection profiles for various product categories

In 2005 several Protection Profiles for various product classes were developed at the commission of BSI and were certified by it. Some examples follow below:

- **Protection Profile for biometrical verification systems**

A biometrical verification system conforming to this Protection Profile serves to verify a user’s stated identity by unique features of his body in order to control access to a portal.

- **Protection Profiles for electronic health cards**

These Protection Profiles specify the requirements for the use of an electronic health card based on the regulations of the German health care system.

• **Two Protection Profiles for IT-supported processing of personal data**
These Protection Profiles describe the logical functional components of video surveillance systems (recording and devices for operation, administration and revision).

• **Protection Profile passport/card reader**
This is used in data transmission between an electronic passport and the card reading device, based on the ICAO standard (International Civil Aviation Organisation). In its variant “Basic Access Control”, the ICAO Protection Profile serves for authentication between card and reader. This Protection Profile - after international agreements concerning electronic travel documents - was developed and certified by order of the Federal Ministry of the Interior. It describes the purposes and requirements of the contactfree chip.

The new electronic health card also has a protection profile. The Federal Office for Information Security (BSI) is involved in all steps of the technical development.

Especially at the airport during check-in, there is data transmission, input and printout. Protection profiles guarantee that data transmission paths can neither be wiretapped nor spied on.

Systems with low protection needs

In the context of projects for the evaluation of Protection Profiles with requirements from version 2.4 of the Common Criteria, several Low Assurance Protection Profiles were developed which describe the requirements for systems with low protection needs. The aim of these Low Assurance Profiles is to facilitate the introduction into a Common Criteria Certification. Short descriptions of certified Low Assurance Protection Profiles are given below:

• **Low Assurance Protection Profile for an Office Based Photocopier Device**
This Protection Profile defines the functional requirements and criteria of the trustworthiness of a photocopier in a common office environment. A photocopier conforming to this Protection Profile is an independent device that needs no additional hardware, firmware or software.

• **Low Assurance Protection Profile for a Software Based Personal Firewall for home Internet use**
This Protection Profile defines functional requirements and the demands on the reliability of a Personal Firewall. A Firewall conforming to this Protection Profile is to be implemented as software exclusively and is meant for the connection of a private PC to the internet.

• **Low Assurance Protection Profile for a VPN Gateway**
This Protection Profile specifies functional as well as reliability requirements for Virtual Private Network (VPN) Gateways. It defines the security demands for VPN Gateways regarding identification and authentication of users, management of the Gateways, trustable channels and the Gateways' self-protection.

• **Low Assurance Protection Profile for a Voice over IP Infrastructure**
This Protection Profile specifies functional as well as assurance requirements for "Voice over IP"-infrastructures (VoIP). This Protection Profile defines the security requirements of VoIP-infrastructures for identification and authentication of users, management of the infrastructure, logging and the system's self-protection.

Another BSI project connected to the preparation of Protection Profiles is the conversion of already existing Protection Profiles towards the requirements made in the new version 3.0 of the "Common Criteria". The "Smartcard IC Platform Protection Profile", in which prominent hardware manufacturers define the security requirements for the Integrated Circuit (IC), is to the fore here.

This Protection Profile, which describes the latest approaches towards modularity and re-use of evaluation procedures, is adapted to the current standard with support from BSI. Here, BSI attends both the editorial work and the Protection Profile's evaluation. A certification on the grounds of the "Common Criteria" in version 3.1 is planned for mid-2006.

Further projects for the development of various Protection Profiles are planned in co-operation with the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway. BSI provides technical assistance in the development of Protection Profiles for secure signature creation devices (SSEE – sichere Signaturerstellungseinheiten), signature application components (SAK – Signaturanwendungskomponenten) and technical components for time stamping services (TSS).

The purpose of the Protection Profiles is to create unified IT security standards as target specifications for SSEE, SAK and TSS which serve as development specifications for the needed functionality of security for the manufacturers.

Health card with reading device. Access is always made following the double-key principle: data are readable only if doctor and patient simultaneously use their keys.

5 Precise measurement – secure operations: IT and protection of secrecy

5.1 Emission-proof hardware
5.2 Testmethods for eavesdropping prevention
5.3 Attenuation testing of real estate and buildings

5.1 Emission-proof hardware

Every electronic apparatus emits more or less intense electromagnetic waves. This emission is called interference radiation. If this concerns equipment that processes data – such as a PC – it might also carry the information that has just been processed. This case is known as "Temporary Emission and Spurious Transmission" (TEMPEST).

If this radiation is received at a distance, for example in a neighbouring house or a vehicle parked in the vicinity, the original information can be restored. The confidentiality of the data is put into question. Emission protection means diminishment of so-called Temporary Emission and Spurious Transmission to levels that present acceptable risks.

NATO has created a set of regulations for the control of Spurious Transmission. This describes methods for the determination of the radiation's information content and establishes threshold values. These measuring specifications have been adopted for national use. BSI also employs them during its authorisation examinations. The NATO regulations provide three categories of threshold values from which result three classes of devices with different degrees of interference suppression. They describe emission security using the electronic device itself.

The zone model

BSI has gone one step further and has developed a so-called zone model. It proceeds from the assumption that electromagnetic fields become weaker in the distance and are measurably absorbed by the structure of a building (bunker, wooden house). From this BSI has devised three categories grading a given location into "Zone 1" (weak attenuation), "Zone 2" (medium) or "Zone 3" (strong attenuation). If the attenuation detected using this classification is insufficient, the zone model cannot be applied to the location. The location is not emission-proof and falls into category "Zone 0". As in the testing of Electro-Magnetic Compability (EMC) (EMV – Elektro-Magnetische Verträglichkeit) prescribed by law, the emission level is also measured in the zone model under conditions as close to reality as possible, but with individual threshold values and bandwidths. The signal's content is not analysed. This allows for quick testing; with the automated measuring method developed by BSI it is possible to test up to two devices per day. On a weekly average, six to eight IT devices (PC, printer, server or other system components) that electronically process classified documents receive authorisation for use within the framework of the zone model (published on the BSI's web site under "German Zoned Products List" – TL 03305)

View inside a measuring cabin. This can determine the intensity of spurious transmission emitted by an IT device.

Every PC emits a certain amount of radiation during information processing which may be intercepted and decoded using the appropriate equipment.

Increased legal requirements

Due to the legal requirements for EMC protection having increased in recent years, many IT devices nowadays pass the "Zone 2" examination without or with very few additional measures of interference suppression. The devices are so safe that they can be put to use in buildings offering medium attenuation of radiation. But for "Zone 1" (weak attenuation) additional steps to suppress interference are necessary. "Zone 3" implies strong attenuation and from the device itself requires the lowest level of emission protection. The upper limit of permissible radiation is established in the Law on Electromagnetic Compatibility (EMVG – Gesetz über die elektromagnetische Verträglichkeit von Gerüsten).
But whoever wants to work safely in a "Zone 0" environment has to put such strong demands on the equipment that the classical methods of interference suppression cannot succeed. It is impossible to diminish radiation to such a degree that "Zone 0" threshold values are not exceeded. Therefore individual methods of signal analysis are used which ensure that the portion of the interference that carries the information does not exceed the threshold levels. To this end, the signals have to be identified and systematically minimized – a task that may take weeks or even months and accordingly causes substantial costs for the development of adequate suppression. "Zone 0" devices are for this reason only utilized where it is unavoidable.

In contrast to the IT devices treated above, systematic analyses are obligatory for crypto-devices for the protection of secrecy. Among others, the key device ElcroDat 4-2, a system for the connection of analogue and digitally encrypted telephone systems (Red Gateway), and the key input device DTD were approved in the year 2005. A crypto radio set for the fighter plane "Jagdflugzeug 2000" and a key distribution device for helicopters are under way, among others.

The "Jagdflugzeug 2000" is a 4th-generation fighter aircraft and equipped with state-of-the-art technology. German Armed Forces pilots performed the first test flights at the end of 2005.

Co-operation with the German Armed Forces

For such IT devices approved according to the zone model, BSI has developed a shortened testing procedure that verifies the quality of individual devices and is carried out by “accredited laboratories”. But this procedure is too unspecific for devices that are emissionproof enough for use in “Zone 0”. It cannot comprehend the special methods of interference protection. Here so-called Short Test Procedures are put to use which BSI explicitly draws up for the device in question.

The primary measuring of mobile systems of the German Armed Forces also falls under BSI’s responsibility – from the off-road vehicle with IT and communication equipment to the large transport aircraft. These primary measurings are carried out in close co-operation with the German Armed Forces’ emission testing service which then also conducts the individual testing of other similar systems. For the year 2005 special mention must be made of an Armed Forces reconnaissance system (KWS-RMB).

Further systems have been tested on location by BSI experts together with the Ger-man Armed Forces’ emission testing service. The Armed Forces received counselling in those cases that were caused by system modifications during the modernisation of Armed Forces networks.

BSI also brings its competence to international co-operations. The primary measuring of a Norwegian frigate was planned for 2005 as a joint project of the Norwegian authority, the German Armed Forces’ emission testing service and BSI, but it had to be postponed until 2006. BSI is active as technical authority in the working teams of international projects such as “Jagdflugzeug 2000”, “Nato Helicopter NH 90” and “Transport Aircraft A 400 M”.

With its studies on emission security in information technology used for classified documents, BSI makes an important contribution to IT security in the protection of secrecy.

BSI, in collaboration with the Federal Armed Forces, has for instance conducted emission tests on off-road vehicles with IT and communications equipment (above) or on the NATO helicopter NH 90 (left).

5.2 Testmethods for eavesdropping prevention

In the year 2005 BSI has further developed its measuring systems and test methods to ensure the confidentiality of personal and telephone conversations, for its tasks also include the protection of the spoken word in the area of governmental nondisclosure – the protection against eavesdropping. Some selected testing methods are presented below.

Every layperson knows “bugs” from spy movies. These miniature listening devices for illegal eavesdropping on conversations transmit the overheard content via radio frequencies. In this context it is easy to forget that even a badly soundproofed door or a single-glazed window make it possible to listen in on conversations from the corridor or from out on the street – be it with the naked ear or using a technical aid such as a directional microphone.

So if one wants to prevent being spied upon, one has to take great care for the sufficient soundproofing of windows and doors, walls, ceilings and floors. For the metrological assessment of soundproofing BSI uses a so called building acoustics measurement system. With the standardized measurement results obtained in this way, deficiencies can be specifically targeted and eliminated.

“Bugs”, or more precisely: radio tapping devices, transmit on certain frequencies which can be identified by help of special measuring receivers, for example spectrum analysers. But it is very difficult to precisely locate such a signal because one needs to scan the frequencies of a multitude of legal transmitters such as radio and television stations, mobile phones or radio data transmissions. The “bug” turns out to be the needle in the haystack.

Endoscopic examination of a cable conduit in the context of bugging protection: The monitor displays the images captured inside the cable ducts by the camera with the flexible tube.

Voice privacy must also be provided for the most up-to-date devices. Today’s mobile video phones are not bigger than a laptop.

With torch light and mirror

But what happens if the radio tapping device was simply switched off? The current makes can be remote-controlled, and if they are deactivated prior to the inspection the measuring instrument cannot detect anything. Apart from that there are tapping devices on the market that use electric lines or infra red light instead of radio waves as their medium for transmission.

Therefore the most important test method still is the so-called visual examination. Furniture and fixtures, hollow spaces in walls and ceilings, but also electric equipment are checked for unwanted installations using a variety of tools – from simple ones like electric torches or mirrors to high-quality fibrescopes.

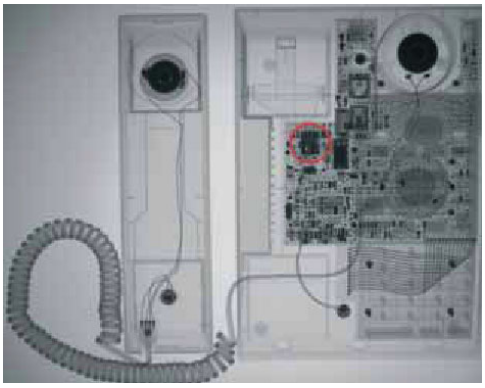
But what about objects that cannot be dismantled? Or high-grade technical appliances that might suffer damage when taken apart? In these cases a modern x-ray system is put to use. By the use of a highly sensitive sensor the radiation level can be kept so low that any risk to the testing personnel is excluded.

Regarding electric lines – and this also includes those for telecommunication and information technology – there is not only the danger of them being abused as transmission medium for tapped conversations. They may also serve as power supply for the "bugs". Testing the lines with specialised equipment is therefore also essential for eavesdropping prevention.

The detection of listening devices built into the building fabric, i.e. walls, ceilings and floors, is particularly difficult. The so-called nonlinearity detector has proved of value as standard measuring instrument for the non-destructive examination of a building structure. This device reacts to any kind of electronic circuitry, including tapping devices. Nevertheless, due to the high sensitivity of this measuring method false alarms are a frequent issue. Combination of several testing methods is the remedy here. For example with a thermographic camera: Listening devices spend electricity which means they slightly warm up compared to the surroundings. The thermographic camera indicates the differences in temperature.

Left: Examining a wall with the non-linearity detector. This responds to anomalies in electric oscillations.

The radiograph (right) shows a telephone set with an integrated bug marked by a circle for illustration.



Protection for digital telephone systems

The use of modern digital telephone systems may bring a particularly high risk of eavesdropping. These systems are always equipped with features such as the "babyphone" function for acoustic room surveillance, direct speech to the telephone set or overplugging of phone conversations or teleconferences, which do make sense and are convenient in many cases of application. But an illegal eavesdropper can easily misuse these functions.

Many systems even give the possibility to disable critical warning signals or messages on the display. Whoever is capable of manipulating the telephone system accordingly can remain undetected. The settings do not even have to be changed directly. In many cases this can be done via a remote maintenance line if it is not adequately secured.

In its security tests concerning eavesdropping BSI examines whether a telephone system is configured for possible wiretapping functions. For the types of equipment that are most used by the Federal administration, BSI has developed software tools that to a large extent perform this task automatically. At this opportunity it also checks whether the remote maintenance line, if there is one, is adequately protected.

This representation of possible testprocedures for eavesdropping prevention cannot, for understandable reasons, be exhaustive. But it should have become clear that one has to react to increasingly sophisticated methods of illegal eavesdropping with equally differentiated test procedures. Eavesdropping prevention tests that do not meet a certain minimum standard are unsound.

Also, these prevention tests can always merely present momentary glimpses. They cannot substitute the necessary personal and material safeguarding measures. Only in this manner the installation of listening devices in imperilled rooms can effectively be prevented.

This conference, for instance, could easily be monitored and recorded using a phone set up for acoustic room surveillance.

5.3 Attenuation testing of real estate and buildings

One way for unauthorised persons to get hold of confidential information is to record the spurious emissions of IT devices (q.v. chapter "Emission-proof hardware"). If this is to be avoided, special security measures are necessary.

For example, protection may consist in shielding the IT equipment itself so it cannot emit any compromising radiation. But such devices, so-called "TEMPEST" equipment, are extremely expensive. They are therefore only put to use in situations that place particularly high demands on emission protection.

Another method is the creation of a security zone around the IT equipment. But here it has to be proven that the spurious emission has indeed faded to an unusable level on reaching the security zone's boundaries. The detection limits for spurious emissions are defined by appropriate NATO regulations wherever governmental classified documents are to be protected.

It depends on many factors how strongly the spurious emission is dampened on its way from the IT device to the receiver (the potential attacker). Apart from the spacial distance, the building fabric and infrastructure play a crucial role. Since these influences are difficult to sum up on the basis of the building plans alone, there is only the possibility to determine the degree of attenuation by measurement on site.

Measurement of the estate

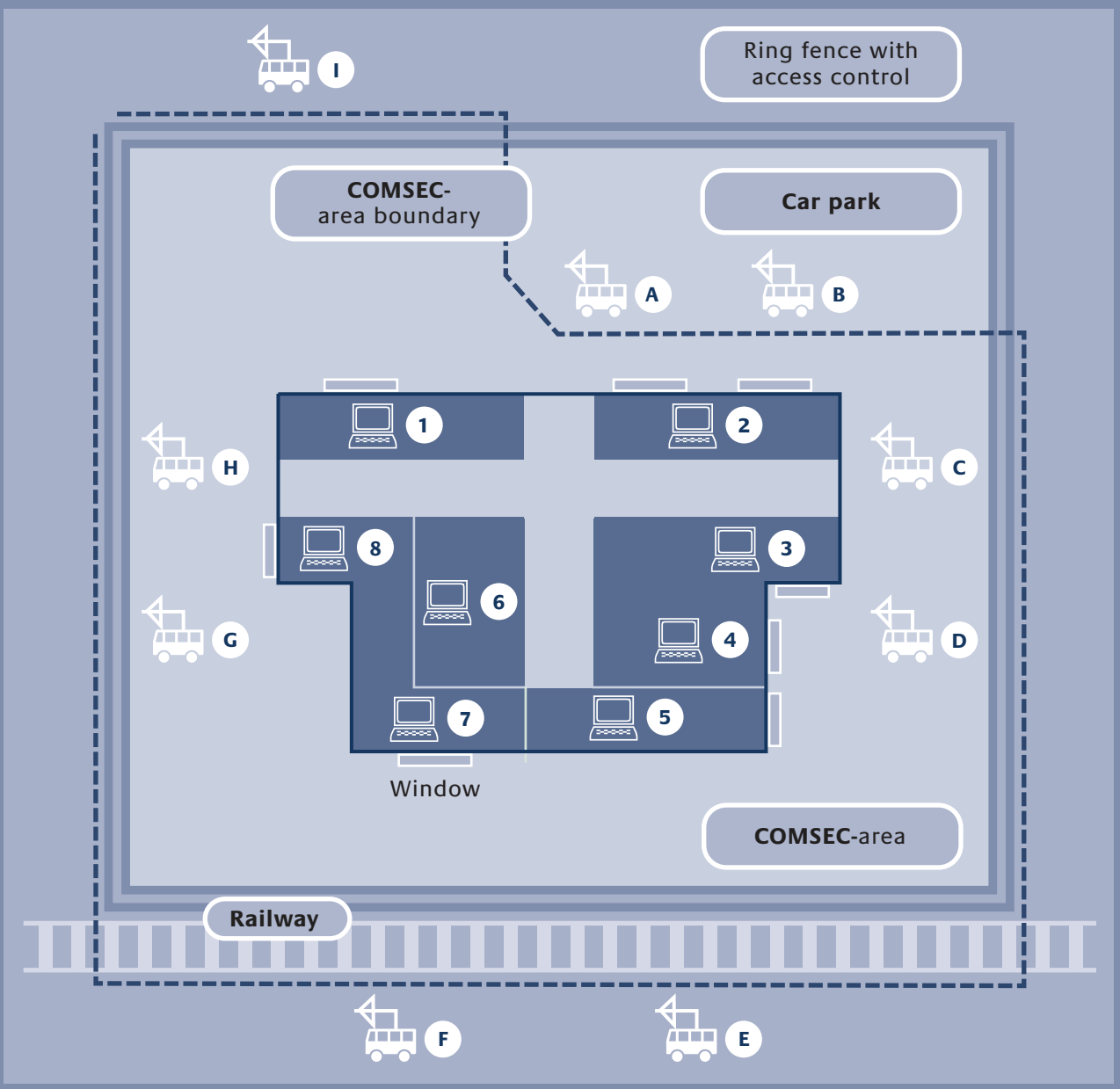
A first step will be to determine the boundaries of the security zone. This zone has to be controllable by security measures such that attempted attacks from there can be excluded. This area does not necessarily have to coincide with the premise boundary. On the one hand, areas of the estate that are difficult to control, such as a publicly accessible car park, can be taken out. But on the other hand the security zone can be expanded by external areas where no one can stay for longer periods of time without being noticed. This may apply, for example, for a neighbouring railroad property or a road with heavy traffic.

After the area boundaries have been established it is necessary to determine the exact attenuation of spurious emissions on their way from the source to the border line. To achieve this, a transmitter is placed in the room that is to be examined which emits a signal that is received at the security zone's border.

According to the actual degree of absorption of the radiation on its way from transmitter to receiver, the room is assigned to a certain zone. Depending on the location or the type of the room under scrutiny, several measurements with different receiver positions may become necessary.

The "zone" for the respective room is determined from the readings following fixed criteria. The grading is set by the results with the smallest values.

Experimental measuring system to define emission security



The figures 1 to 8 correspond to the room numbers and simultaneously to the transmitter locations, whereas the letters A to I symbolise the receiving locations without and within the enclosure at the area boundary. The measurement concerns the different degrees of attenuation of IT equipment being used in different rooms and the degree of the interference's decrease outside the area boundary. From the combination of the measured emission security of the device itself and the degree of attenuation, it can be determined which equipment can safely be used in which location.

The receiving unit – as part of a measuring system capable of classifying zones.

Zone rating

Relating to a reference reading with 20 metres of free space between transmitter and receiver, there are the following classifications:

- Zone 1 corresponds to attenuation equivalent to 20 metres of free space
- Zone 2 corresponds to attenuation equivalent to 100 metres of free space and
- Zone 3 results from Zone 2 plus 20 dB.

Zone 1 is the area with the weakest, Zone 3 the one with the strongest attenuation. Zone 0 is assigned to rooms that do not meet the minimum absorption requirements. In these cases specially shielded (TEMPEST) devices have to be used.

Limitations

The zone model can only be applied to such buildings, estates and mobile equipment in stationary use for which a clearly definable boundary outside the building can be established. Individual floors or rooms inside a building cannot be "zoned" or classified in comparison with other floors or rooms.

This is due to the fact that the IT equipment's spurious emission may also interfere with various metallic conductors which will then scatter it uncontrollably over longer distances inside the building. Since this scattering cannot be avoided by justifiable time and effort, the zone boundary must be outside the building itself.

Activities

The measurement of real estates according to the zone model is one of BSI's tasks. The Federal Office is active for both Federal agencies and, through the Federal Ministry of Economics, those branches of economy that receive support in the protection of secrecy. In all cases this concerns objects where confidential data are processed that are subject to special protection. BSI offers its customers comprehensive counselling in questions of emission security, also at early planning stages.

By the independent assessment of a building's attenuation levels and the equipment's interference radiation, the zone model facilitates the user's choice and the implementation of electronic equipment for processing of confidential data. The zone model is applicable for buildings and estates that fulfil the criteria for establishment of a security area. If this is not the case, the use of authorised emission-free IT equipment for processing of confidential data is necessary.

To the right: the transmitting unit belonging to a classified measuring system.

Dr. Udo Helmbrecht,

President of the Federal Office for Information Security

Michael Hange,

Vice President of the Federal Office for Information Security

Dr. Hartmut Isselhorst,

Head of Department 1 – Security of Applications, Critical Infrastructures and Internet

Dr. Gerhard Schabhüser,

Head of Department 2 – Cryptology and Counter-Eavesdropping

Bernd Kowalski,

Head of Department 3 – Certification, Accreditation and Conformity Tests

Horst Samsel,

Head of Department Z – Central Tasks

Anja Hartmann,

Head of Information, Communication and Public Relations Division
e-mail: anja.hartmann@bsi.bund.de

Matthias Gärtner,

Press Officer
e-mail: matthias.gaertner@bsi.bund.de

Milestones in BSI history

1990 The Act for Establishment of BSI, which stresses the importance of information technology, is passed.

1991 The Federal Office for Information Security commences operation on January 1, 1991. The founding president of BSI is Dr. Otto Leiberich. The European IT Security Criteria are developed under direction of BSI.

1992 Start up of certification and accreditation proceedings according to ITSEC/ITSEM. IT Grundschutz concept developed. Training system for the Federal Administration for more than 1,000 delegates starts its work.

1993 Following the retirement of Dr. Otto Leiberich at the end of 1992, Dr. Dirk Henze is appointed new president of BSI on January 1, 1993. BSI starts to be involved in the Common Criteria certification standard.

1994 A broadly designed crypto innovation strategy starts to be implemented in BSI. This has resulted to date in the development of important cryptographic systems such as ElcroDat 6-2, cryptosystem for the BOS digital radio, PLUTO high-performance crypto module, ElcroDat 4-2 radio system, SINA and numerous innovations in the area of public key cryptography.

1996 Version 1.0 of the Common Criteria published.

1998 The new “Internet Security” department addresses the growing importance of the World Wide Web.

1999 BSI provides extensive services and information relating to the “Year 2000 problem”, e.g. a special brochure for the public. Set-up of and support for the public key infrastructure. With the launch of the Governmental Berlin-Bonn Information Network (IVBB), BSI takes over technical co-ordination.

2001 Federal Minister of the Interior Otto Schily puts in force new organisational, personnel related and technical framework conditions for the further development of BSI into the central IT security provider of the German government. As part of the anti-terrorism package, the IT Penetration Centre department and the Biometrics project team are set up. The department for Critical Infrastructure protection initiates extensive sector analyses in response to the terrorist attacks.

2002 Launch of the Citizens’ CD which has since then been expanded into an online portal. More than 1.6 million copies of it have been distributed.

2003 Following the retirement of Dr. Dirk Henze in November 2002, Dr. Udo Helmbrecht becomes new president of BSI in March 2003.

2004 BSI’s new strategic master plan brings the customers’ demands more into focus by the implementation of modern control instruments. One highlight in the events of 2004 is the ICCC/ISSE congress organised by BSI.

2005 The Federal Government introduces its National Plan for the Protection of Information Infrastructures. Related to this is the expansion of BSI into an operative security authority. With the development of a Protection Profile for the electronic health card BSI contributes to one of the largest and most innovative IT projects world-wide.

B

BKA – Federal Criminal Police Office (Bundeskriminalamt)

BMF – Federal Ministry of Finance (Bundesministerium der Finanzen)

BMI – Federal Ministry of the Interior (Bundesministerium des Innern)

BMWA – Federal Ministry for Economics and Labour (Bundesministerium für Wirtschaft und Arbeit)

BOS – German authorities and organisations with security-related tasks (Behörden und Organisationen mit Sicherheitsaufgaben)

BWB – Federal Office of Defense Technology and Procurement (Bundesamt für Wehrtechnik und Beschaffung)

C

CBAS – CERT-Bund Alarming System

CC – Common Criteria

CCRA – Common Criteria Recognition Arrangement

CERT – Computer Emergency Response Team

COMSEC – Communication Security (NATO standard for telecommunication security)

CS – Commercial Service

CSCA – Country Signing Certification Authority

D

DDoS-Angriffe – Distributed Denial of Service attacks

DEHSt – German Emissions Trading Authority (Deutsche Emissionshandelsstelle)

DS-Zertifikat – Document permitting the creation of signature keys (Document Signer-Signature Key-Certificate)

DTD – Document Type Definition

E

EAC – Extended Access Control

EADS – European Aeronautic Defence and Space Company

EEMA – European Electronic Messaging Association

EGVP – Electronic law and administration mailbox (Elektronisches Gerichts- und Verwaltungspostfach)

ElcroDat 6-2 – Crypto system for secure communication and data transmission via Euro-ISDN

eMRTD – electronic Machine Readable Travel Document

EMVG – Electro-magnetic compatibillity law (Gesetz über die Elektro-Magnetische Verträglichkeit)

EMVP – Electro-magnetic compability test (Elektro-Magnetische Verträglichkeitsprüfung)

ePass – Electronic passport

ESA – European Space Agency

ETSI – European Telecommunications Standards Institute (Institut Européen des Normes de Télé-communication)

G

GNSS – Global Navigation Satellite System

GPRS – General Packet Radio Service

GRT – Golden Reader Tool (Software for the readout of electronic documents)

H

HTML – Hypertext Markup Language

I

ICAO – International Civil Aviation Organization

ICCC – International Common Criteria Conference

IEC – International Electrotechnical Commission

IEEE – Institute of Electrical and Electronics Engineers

IP – Internet Protocol

IPC – Inter-Process Communication

IRC – Internet Relay Chat

ISDN – Integrated Services Digital Network

ISO – International Organization for Standardization

ISO Guide 65 – Audit for certification authorities

ISSE – Information Security Solutions Europe

IT – Information technology

iTAN – Indexed transaction number (TAN) in Electronic Banking

IVBB – Information network (Informationsverbund) Berlin-Bonn

K

KRITIS – Critical Infrastructures (Kritische Infrastrukturen)

L

L4VM – Prototypal micro kernel-based platform

LAN – Local Area Network

M

MCert – Cert for small and medium businesses (q.v. CERT)

mTAN – Mobile TAN (via SMS)

N

NAGIOS – from “Network” and “Hagios” (Greek for “sacred”) – software that allows the mapping and monitoring of complex IT structures

NETeam – National Experts Team

NPSI – National Plan for the Protection of Information Infrastructures (Nationaler Plan zum Schutz der Informationsinfrastrukturen)

O

OS – Open Service

OSCI – Online Service Computer Interface

OSS – Open Source Software

P

PIN – Personal Identification Number

PKI – Public Key Infrastructure

PRS – Public Regulated Service

R

RFChip – Radio Frequency Chip, digital data storage chip for contactfree radio transmission readout

S

SAK – Signature application components (Signaturanwendungskomponenten)

SAR-Lupe – Reconnaissance satellite equipped with Synthetic Aperture Radar

SCIP – Secure Communication Interoperability Protocol

SEK – Special police task force (Sondereinsatzkommando)

SIM-Karte – Subscriber Identity Module (chip card for mobile phones)

SINA – Secure Inter-Network Architecture

SIRIOS – A system for dealing with security incidents for Computer Emergency Teams

SmartCard – Chip card with integrated circuit (Mikrochip)

SMTP – Simple Mail Transfer Protocol (E-mailtransmission system)

SoL – Safety-of-Life: Air service (Luftverkehrsdienst)

SSEE – Protection profiles for secure signature creation devices (sichere Signaturerstellungseinheiten)

T

TAN – Transaction number in Electronic Banking

TCP/IP – Transmission Control Protocol/Internet Protocol

TETRA – Terrestrial Trunked Radio (digital trunking standard for public authorities and private mobile radio)

TETRAPOL – Digital trunking system for the French Police Nationale

TK – Telecommunications

TR – Technical Guideline (Technische Richtlinie)

TR S-WLAN – Technical Guideline Secure Wireless LAN

TSS – Timestamping Server

U

UMTS – Universal Mobile Telecommunications System

URL – Uniform Resource Locator

V

VMS – Virtual Machine Subsystem

VoIP – Voice over Internet Protocol

VPN – Virtual Private Network

VPS – Virtual Post Office (Virtuelle Poststelle)

VS-NfD – Classified document – for official use only (Verschlusssache – nur für den Dienstgebrauch)

VW – Virtual Workstation

W

WDR – German television station (Westdeutscher Rundfunk)

WID – Warning and information service (Warn- und Informationsdienst)

WLAN – Wireless Local Area Network

Z

z/OS – An operating system for IBM mainframe computers

Imprint

Published by
Federal Office for Information Security – BSI
D-53175 Bonn, GERMANY

Reference office
Federal Office for Information Security – BSI
Section 321 – Information and Communication, Public Relations
Godesberger Allee 185-189, D-53175 Bonn
Phone: +49 (0)3018 9582-0, e-mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

Text and editorial staff
Felix Fortelka, BSI; Volker Thomas, Thomas Presse & PR

Translation
Ralf Östereich, Berlin

Layout & design
Thomas Presse & PR, Berlin/Bonn
Graphics: Annette Conradt, Pierre Boom
Screen version: Ludwig Lang
Internet: www.thomas-ppr.de

Picture Credits
1&1 Internet AG, Alcatel Deutschland, AOK-Bundesverband/Presseservice, AVM Computersysteme Vertriebs GmbH, Berliner Flughäfen/Pressestelle, Berlin Partner/FTB-Werbefotografie, Bildstelle im Bundesministerium der Verteidigung (BMVg), Pierre Boom, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesanstalt Technisches Hilfswerk (THW), Bundesbildstelle, Bundesdruckerei, Bundesministerium des Innern (BMI), Deutsche Postbank, Deutsche Telekom, Deutsches Zentrum für Luft- und Raumfahrt (DLR), Dresdner Bank/Presse-Center, Andreas Ernst, Fraunhofer-Gesellschaft/Volker Steger, Intel Pressroom, OHB-System, Rohde & Schwarz, Siemens, Volker Thomas, Vattenfall Europe, virtUOS/Universität Osnabrück
Photo Composings: r.e.m./Hans-Georg Gaul

Date
August 2006