Federal Office
for Information Security

Annual Report 2006
2007

Secure Information Technology for our Society

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

Modern States Need Secure Information Technology

Dear fellow citizens,

Virtually all areas in society are linked by information and communication systems to an extent that was unthinkable 20 years ago. For their business procedures, trade, the transport sector as well as the public administration increasingly rely on IT.

At the same time the increasing network of information and communication systems constitutes an exceptional challenge, as interdependence also results in new threats. Whether it be a computer for private use or entire company networks, all IT systems are subject to hacker attacks and threats caused by malware. This threat has greatly increased recently.

Modern industrial nations depend on information technology. Due to their obligation to provide services of general interest, states have to prevent failures of critical infrastructure. We need solutions which in the long term guarantee the use of these technologies. We also need an awareness of these threats among the general public as well as in the business and scientific community and in state administration. The Federal Government is aware of the fact that nowadays our internal state security is inextricably linked to secure information technology infrastructures. The Federal Office for Information Security (BSI) therefore plays a prominent role when it comes to designing IT systems in the present and in the future.

The BSI contributes substantially to our IT security. In order for the BSI to continue to be able to assume its responsibilities in a competent and responsible manner and adequately perceive the current threats IT security legislation must be adapted. Part of this is also the current fundamental revision of BSI Legislation. BSI will only then be able to respond according to the changing framework conditions and will as the only state IT security authority, be capable of taking responsibility for our government communication and be in a position to ensure IT security in Germany.

Berlin, May 2008

Dr. Wolfgang Schäuble, MP
Federal Minister of the Interior

The BSI:
Modern, Efficient, Service Oriented

Dear readers,

Germany requires secure information technology. Challenges such as the increasing dependence on modern information technology underline this. According to the report on the IT Security Situation in Germany 2007 the number of threats has been increasing in recent years. In the meantime, 40 million people have gone online in Germany. When surfing on the internet or receiving e-mails, one third of the users have already had contact with malware such as Trojan horses and 60 per cent have already fallen foul of computer viruses and worms. The threats are also increasing for the business community. There are few security relevant companies which have not yet experienced espionage attempts via the internet. As attacks are becoming more sophisticated, the challenges for secure information technologies are constantly increasing. Especially medium sized businesses have considerable requirements in this area.

The Annual Report 2006/2007 which is now available documents impressively the BSI's work in the protection of IT and its commitment to secure information technology. The BSI is the central IT security services provider in Germany. We are a modern and efficient public authority acting in a service and customer oriented way. The year 2006 was a special year in the history of our institution: The BSI was able to celebrate its 15th anniversary. Founded in 1991, the BSI laid the foundations in the 90s for the creation of an IT-Grundschutz as well as a certification and accreditation process. In the past few years the BSI has been able to strengthen and consolidate its outstanding position in the field of IT security. In the meantime around 500 BSI employees are contributing to Germany's internal security. This concentration of expert knowledge is unique in Europe. Nevertheless, the IT security level can only be improved in the long term if all groups in society cooperate. I am hopeful that this Annual Report will contribute to informing and educating the general public.

In 2008 the BSI will be concentrating particularly on issues such as net security, protection against trojans, security of official documents, citizen portals, mobile communication security and the consolidation of technical evaluation capacity. Thus BSI is consistently implementing inter alia the objectives of the National Plan for Information Infrastructures Protection (NPSI) and is also reacting to the changes in the IT security situation.

Bonn, May 2008

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

1.1 Facts and Figures

Information Technologies (IT) permeate all areas of life: Telecommunication, stock exchanges, insurances, public authorities, production processes, entertainment industry. Where millions of information and data packages are processed, security mechanisms have to be in place, in order to ensure that systems vital for the functioning of society do not fail or are subject to external interference.

The Federal Office for Information Security (BSI) as the central German IT security authority has been contributing substantially to this for more than 15 years. As the highest level federal authority within the area of responsibility of the Federal Ministry of the Interior (BMI) BSI is operating for the Federal Government, cooperating with the business community and informing the general public on IT issues.

The foundation for its work is the legal act setting up the Federal Office for Information Security presented by the current Federal Minister of the Interior Dr. Wolfgang Schäuble also then in office. On January 1st 1991 the BSI started operating under its founding president Dr. Otto Leiberich. Thus in 2006 the authority could look back on a 15 year history.

Objectives of the BSI

The BSI's primary objective is to protect information and communication. According to the "National Plan for Information Infrastructures Protection" of the Federal Government, three strategic objectives constitute the priorities of the BSI's work:

- **Prevention:**
  To sustain adequate protection information infrastructures.
- **Reaction:**
  To react efficiently to IT security incidents.
- **Sustainability:**
  To promote German IT security technologies and competence – to set international standards.

Tasks and Self-Perception

The Federal Office for Information Security offers public administration a complex variety of services on a federal, state and municipality level as well as to companies and private users. It offers customised services to the respective target groups:

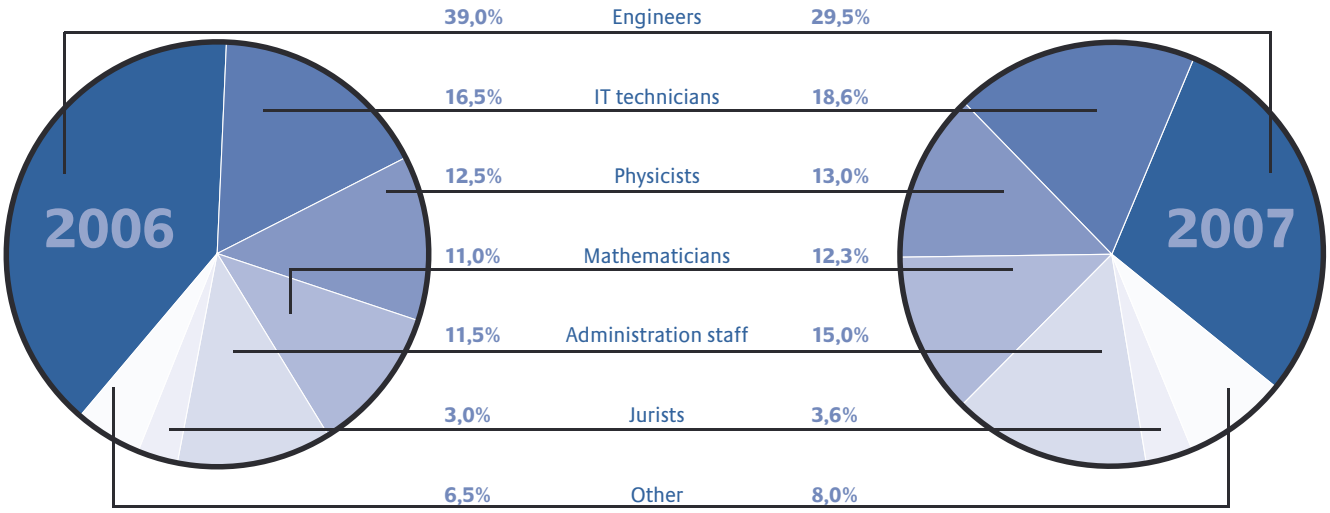
- **Information:**
  The BSI provides information regarding all important topics related to IT security.
- **Advice:**
  The BSI advises and supports clients in the implementation of adequate measures.
- **Development:**
  The BSI designs and develops IT security applications and IT security products.

A further important task is the testing, evaluation and certification of IT products and IT systems with regard to their security properties. Accrediting IT systems for the processing of confidential information is also an area of the BSI's work.

The BSI works in all important fields related to IT security and is the leading institution in this field in Germany. Its aim is to make the results available not only to state institutions but also to industry and the general public. At an international level the BSI sees itself as a representative of German security interests. Its employees prove themselves to be competent in providing the authority's services. Many components of their work are recognised as best practice models.

Fields of Specialisation at BSI – 2006 and 2007 in comparison

senior and executive grades only, in per cent



When implementing its tasks the agency works with a service and customer oriented approach. At the same time the BSI aims continuously to optimise the relationship of costs and results. To this end modern management tools such as gearing all the BSI's operational tasks towards programmes, the cost-performance-calculation and a balanced scorecard are employed.

A broad range of services: BSI's variety of offers ranges from A as accreditation up to Z as zoned products.

Figures: Personnel and Budget

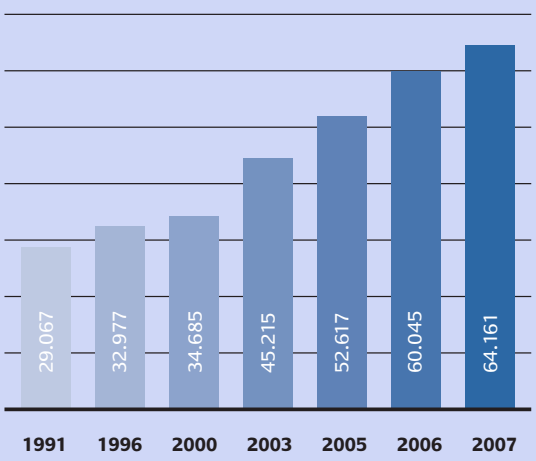
Almost 500 all-rounders and specialists work on a complex task at BSI, i.e. raising the IT security level in Germany. 50 more employees have been taken on since 2005. The BSI's tasks are diverse and so are the specialisations of the employees. Out of the 500 employees engineers represent the largest group with 29.5 per cent, followed by the specialisation information technology with 18.6 per cent. Nevertheless other specialisations such as law, political and communication sciences are also represented. Therefore the BSI is able to respond in a competent and differentiated way to the diverse challenges resulting from the rapid developments taking place in the field of information technology. Apart from the questions related to information technology, IT security also involves economic, legal and social aspects.

The continuously increasing budget of the BSI is also an indication for its growing relevance. In 1997 the budget amounted to circa 33.5 million Euros, the overall budget in 2007 had risen to about 64 million Euros. Compared to 2006 this constitutes an increase of 4 million Euros. Out of this sum the expenditure for personnel accounted for 24 million Euros and non-personnel expenditures amounted to 33 million Euros. Investment expenses added up to 6.8 million Euros.

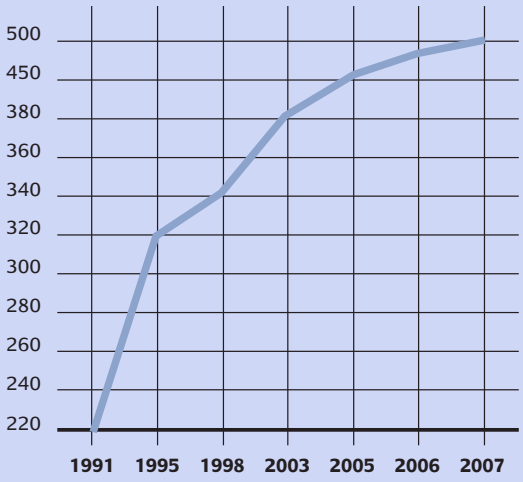
For years the BSI has been considered one of the most popular employers within the IT sector. This is an indication for its top-ranking status in the IT industry. On the ranking list developed by the company trendence Institut GmbH "Das Deutsche Absolventenbarometer – IT-Edition" the BSI is ranked 13th among 98 companies in 2007. 4.893 students were interviewed. Thus the BSI is located at the same level as international companies such as Microsoft, Google or Siemens.

Budget 1991 – 2007

in thousands of Euros

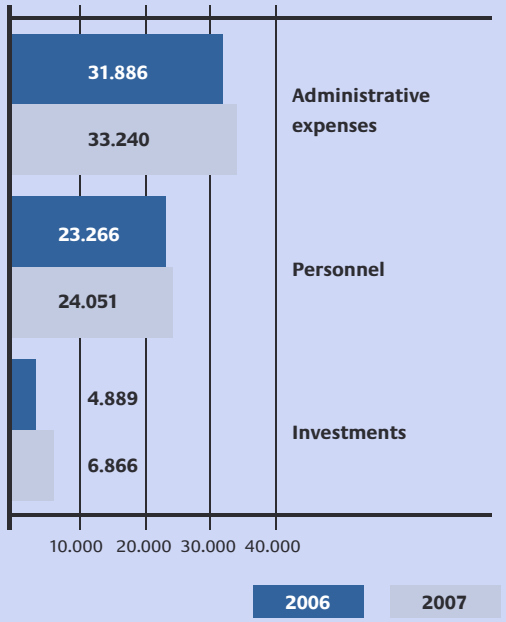


Number of Employees 1991 – 2007



Breakdown of Expenditure by category

in thousands of Euros



1.2 Information and Communication – BSI in the Public Eye

Education and awareness imply active information, communication and interaction. It is the only way of sustainably presenting the issue of IT security as an on-going topic in the conscientiousness of the general public.

Raising awareness in the general public for latest issues in IT security and building up IT security competence in concrete terms implies the following:

- raising awareness among the different target groups;
- building up expert knowledge in order to recognise current threats;
- taking adequate security measures.

The target groups are the general public, public administration (federal, state and local level), the business community, multipliers (especially the media) as well as organisations, federations and associations. The objective context presentation, independent of the products is of fundamental importance. To this end the BSI has a broad range of offers and services.

The BSI's Internet Presence

The BSI website www.bsi.bund.de is primarily directed at experts. Here the reader will find extensive information regarding issues such as IT-Grundschutz, CERT-Bund or certification and accreditation. Studies, publications, articles and technical papers can be downloaded from the website. There is also a subscription offer for the BSI newsletter. It is published five times a year and contains up to-date information on BSI's publications and events.

The Website for Beginners

On the website www.bsi-fuer-buerger.de the BSI offers information for private users on all topics related to IT security presented in a compact and understandable way. Various chapters provide basic knowledge on how users can protect themselves against viruses and worms, on how data protection works as well as on how to deal

with confidential data. A tool box with programmes, a glossary and manyssues such as Web 2.0, patch management or how to deal with file sharing networks.

In September 2007 the website was redesigned. Visually it was made more attractive. Familiar structures such as the menu navigation remained, as well as “Argus” the mascot who guides the user through the site.

All web content of this website is also available on the CD-ROM “Ins Internet – mit Sicherheit” (“Going online – but safely”). As it was possible to specifically approach multipliers at adult evening classes, consumer protection centres and in the police crime prevention at federal and federal state level, this CD was distributed widely in 2007. In cooperation with the editor Deutsche Sparkassen Verlag the information brochure “Einfach Online – Mit Sicherheit durchs Internet” (“Going online made easy – surfing safely”) was published.

A “Longseller” of BSI: This CD ROM not only offers information but also security programmes free of charge.

The Bürger-CERT (Cert for Citizens)

In March 2006, the German Federal Minister of the Interior Dr. Wolfgang Schäuble formally launched the online information service Bürger-CERT www.buerger-cert.de. In addition to “BSI für Bürger” (“BSI for citizens”) this service provides warnings on current viruses, worms and other malware which are updated on a daily basis. Behind the Bürger-CERT there is a team of specialists who deal extensively with IT security. They observe the IT infrastructures in networks, give warnings and information on security and provide support in cases of IT security incidents. The abbreviation “CERT” stands for “Computer Emergency Response Team”.

The Bürger-CERT constitutes the first neutral and free warning and information service for IT security in Germany. This service gives internet users online access to extensive and competent information and an early warning system regarding special risks and dangers resulting from current security gaps.

The Bürger-CERT also provides three different information services:

- The fortnightly **online newsletter "Sicher Informiert" ("Safely informed")** provides an overview of the most important security news.
- In case of extremely time critical security leaks and the need for immediate action **extra issues** of the online newsletter warn the readers.
- **"Technical warnings"** with detailed background information for readers interested in the technicalities and more **knowledgeable readers are also on offer.**

Furthermore the Bürger-CERT website contains an archive for research into former warnings as well as a glossary which explains technical IT terms which are easily understood.

In May 2006, the Bürger-CERT won the award "Sicherheit im Internet" ("Safety on the internet") initiated by "klicksafe" supports projects, which are particularly committed to media competence and internet security.

The high-ranking jury justified its choice as follows: "With regards to the content and in technical terms Bürger-CERT is a high quality product, which is capable of reaching the general public and familiarising it with security issues. This approach where by a public authority opens itself and shares its information understandable to the general public is to be highly commended. As a result, users are guaranteed independent and expert information for free. The Jury was also convinced by the wide ranging advice. In the first month alone, 60.000 citizens subscribed to this warning and security service."

BSI's Cooperation Partners

In order to raise the security consciousness within society the BSI cooperates with different partners from the business community. In this context the public authority cooperates with a number of partners in the field of public relations:

heise security
Under www.heise.de/security/ presentation of a selection of information from the BSI.

Freenet.de
Under the topic Computer&Technology –> Viruses & Security warnings are published as well as articles on IT security for the target group private users.

Fujitsu-Siemens
By means of BSI's pre-installed content by the above mentioned hardware producer, the user is informed about the fundamental importance of IT security immediately after buying a new PC.

Netzcheckers

BSI is present on www.netzcheckers.de with content for specific target groups such as “Computerspiele – aber sicher!” (“Computer games – but safe ones!”) or “Handy-Payment kann teuer warden” (“Mobile payment can cost you!”). Through its presence BSI is trying to raise awareness especially among young people for topics related to IT security.

Educating and raising awareness in the general public is always driving home how important IT security is.

BSI’s Presence at Trade Fairs and Conventions

The BSI presented itself at various trade fairs and conventions in 2006 and 2007 with topics such as IT-Grundschutz and IT security certification but also with new developments taking place in the field of “Official Documents”. On these occasions there was the opportunity of directly contacting IT experts and presenting BSI’s services to the private users.

The 10th German IT Security Congress

From May 22nd until May 24th 2007 the 10th German IT Security Congress of BSI convened at the City Hall in Bonn-Bad Godesberg. The anniversary congress took place under the motto of “Innovation Driver IT Security”. On the three conference days the diverse aspects of IT security were examined.

CeBIT Hannover

At the CeBIT trade fairs in March 2006 and 2007, BSI was represented in hall 7. Issues such as internet security, secure e-government or IT security certification according to Common Criteria were of special interest at the BSI stand. Furthermore there was a great demand for the CD, which contains information from the BSI website. BSI was also represented at the stand of the Federal Government, the Public-

Sector-Parc. A series of lectures at the Convention Center rounded off the comprehensive offers at the CeBIT.

Systems Munich

At the trade fairs Systems 2006 and Systems 2007 BSI took over the patronage of the IT Security Area in both years. The main topics of the technical presentation at the BSI stand were Secure Inter Network Architecure (SINA), Mobile Security as well as information related to IT security certification. On Tuesday October 23rd 2007, BSI president Dr. Udo Helmbrecht formally opened the IT Security Area at Forum Blau. All the lectures on IT-Grundschutz, official documents, IT security certification and eCard-API held by BSI experts took place here.

Security Essen

In Essen BSI presented its security solutions and advisory services. The principle topics at the BSI stand in the Common Area "IT Security Theme Park" were advisory services on material security and on IT-Grundschutz. Approaches to solutions for problems in the organisational joining of material security and IT security were also demonstrated by BSI at the congress accompanying the fair, inter alia with the lecture held by the president of the BSI Dr. Udo Helmbrecht on the topic "Information Protection – why many companies can't help themselves".

Modern State Berlin

IT security was one of the main topics in both years at the trade fair "Modern State". The IT security theme park with its 20 exhibitors approximately formed the central meeting point for the IT security industry. In its function as IT security partner of the trade organiser, BSI informed on current issues. In addition BSI organised a series of lectures on SINA architecture, communication security in e-government and risk management.

LinuxTage Wiesbaden and Berlin

At the LinuxTage 2006 in Wiesbaden and 2007 in Berlin, BSI presented up-to-date IT security solutions on the basis of open source software. One central aspect within the Federal Government's IT strategy is the promotion of software diversity. Monocultures can only then be avoided and IT security can be better guaranteed.

LinuxTag 2007 under the Berliner Funkturm – the trade fair premises of the Messeplatz in Berlin is a very popular meeting point for IT security experts several times a year.

Further Events

Open Day in Berlin

Under the heading “Invitation to a State Visit“, the Federal Government and also the Ministry of the Interior (BMI) in Berlin open their doors for interested members of the public every year. In 2006 and 2007 BSI was there and presented its services and information packages for private PC users. Main topics were the website www.bsi-fuer-buerger.de as well as the warning and information service www.buerger-cert.de with the free newsletter “Sicher • Informiert” (“Safely Informed”).

Girls’ Day

BSI participated in the nationwide future project day for girls the so called Girls’ Day in 2006 and 2007, with lectures and presentations on the topic “Security – This is for Women too!”. BSI experts from various departments showed the girls which tasks IT specialists carry out at BSI.

Dialogue with BSI

With a series of events called “Dialogue with BSI”, BSI offers a regular forum of communication between the business and the scientific communities as well as the public administration. In small groups, high-ranking experts discuss issues such as “IT Security as a Business Model” and “IT Security and the Law”. The objective of this series of events is to kick-start a sustainable dialogue on cutting edge issues.

Experts Required

Information technology has also been a consistent issue in the press, on the radio and on television. IT security particularly is discussed in this context. Papers and magazines, online media as well as radio and television programmes increasingly report on how private users can protect their PCs and their personal data against online attacks. In this context the BSI’s experts are very popular as guests and interview partners. They explain the threats and attack scenarios and give hands-on advice on secure IT for the general public. The media also frequently refer to the information and services provided by BSI (“BSI for citizens” and “Bürger-CERT”).

<kes> – The Magazine for Information Security

The BSI's official bulletin is BSI forum in the <kes> magazine. Six times a year the forum offers information with articles by BSI authors or guest authors on relevant IT security topics. IT security experts are the main target group. Among the readers of <kes> are the important IT decision makers from a variety of companies, banks and public authorities. Besides the printed version, BSI forum can also be found as an electronic version in the <kes> magazine under www.bsi.bund.de/literat/forumkes.htm.

1.3 International Cooperation

The international movement of goods and people, the closely linked financial markets, the rapid worldwide data exchange show the following: IT security is not only a national affair.

BSI tackles global challenges through international cooperation. Only if information and experience is exchanged and jointly used, important developments in the field of IT security can be recognised and security relevant gaps can be identified as early as possible.

The BSI's international cooperation involves for example:

- **developing** adequate measures for tackling IT crises through computer emergency teams or in the field of critical infrastructures;
- **safeguarding** international interoperability with biometric applications;
- **standardising** security products (Common Criteria);
- **participating** in major technical projects in the aerospace sector such as with the Airbus A400M or with the satellite project Galileo;
- **supporting** international organisations by means of approved BSI products such as SINA and the encryption device Elcrodat.

BSI represents German interests in international bodies e.g. NATO, EU, ENISA and ISO as well as in bi- and multilateral cooperation with other states. Besides the BSI's traditionally strong commitment within NATO, in 2006 and 2007 the cooperation with the EU has been intensified. BSI is the central national contact point for the European Network and Information Security Agency (ENISA). BSI has been a member of ENISA's international Management Board since the middle of 2007. Since 2006 the "Staff International Relations" has been coordinating the international activities of BSI. Externally it is the central contact point for all international affairs.

IT Security with a European Dimension

The EU Council Presidency, which was held by Germany in the first half year of 2007, was expected to initiate political processes. In the corresponding work programme of the Federal Ministry of the Interior (BMI) “Living Europe Safely” IT security played a major role.

Two major events organised by BMI and BSI together, addressed an international expert audience. The workshop “Trusted Computing from a European Perspective – The Impact on the Public Sector” brought together 70 Trusted Computing experts and persons responsible for IT from 19 EU member states as well as from the USA, Japan and New Zealand in February 2007.

In June 2007 under the heading “Innovation and Responsibility” the international IT security conference with 250 participants drew attention towards the aspect of how responsibility for IT security should be distributed between the government, the business community and the general public. The results of both events are presented on the following website www.itsecurity2007.de.

2.1 Always Cutting Edge – BSI's Operations Centre

Manufacturers inform on security updates. IT security specialists warn against recently discovered vulnerabilities. The media report on "critical" incidents and threats. Innumerous warnings on IT security make it difficult for the user to separate the wheat from the chaff.

The real significance of these warnings, as well as the context and the consequences can often only be grasped by teams of specialists who have the necessary comprehensive background knowledge. Most non specialists are out of their depth. There is broad consensus that the protection of information technology is of special importance due to the constantly increasing risks and interdependencies.

Studies conducted by BSI (see "The IT Security Situation in Germany 2007") show, that four out of five people interviewed had personally had negative experience with online threats already. Words such as viruses, worms, trojans, spam or phishing have become an integral part of every day vocabulary. In the light of the flood of information the question raised even more urgently is, how the general IT security situation can correctly and constantly be evaluated and how to adequately respond to individual items of information. An overall evaluation by varying companies and industries at a national level is a particularly complex challenge.

Whilst presenting the new IT Security Situation Report BSI-President Dr. Helmbrecht said: "Mechanisation is increasing and a growing number of private and business activities are being transferred to the virtual world. The professionalisation and commercialisation of IT threats continue to go hand in hand."

The Basic Concept

One possible solution is a structural approach with resources dedicated to one particular purpose. Specially trained IT experts are constantly working on the different phases of the operating cycle "Situation Monitoring – Situation Evaluation – Decision – Measures". Not just technical aspects but also psychological effects, economic considerations or political implications must be taken into account in this context.

The following questions show the wide range of problems which can emerge in an IT security incident:

- Is the confidence in an institution or mechanism jeopardised?
- Is the potential damage in terms of a risk calculation tolerable?
- What are the consequences of the incident for the services and products on offer?
- Will the result be of political importance?
- Is it necessary to calm down or escalate the situation?
- Is there a risk of overreacting?
- Is the problem being ignored or not even perceived?

Ideally IT security is evaluated with an interdisciplinary approach. The incident must be identified and above all evaluated. Afterwards measures for the solution of the situation and the mitigation of the effects must be taken. The operational process and decision criteria must be defined clearly, communication details must be defined and emergency plans developed. Inflexible behaviour patterns would be out of place: An operations centre must be in a position to act flexibly, in order to deal with unexpected situations as they arise. The evaluation of the political or business philosophical interdependencies to a large extent depends especially on the experience and the knowledge of the personnel deployed.

Political Mandate

In the “National Plan for Information Infrastructure Protection (NPSI)” the federal government decided inter alia to establish and operate an operations and analysis centre. In the coalition agreement it was decided to implement the NPSI in this legislative period. Apart from the other important targets set in the NPSI, especially objective 8 and 10 aim to have a reliable conception at any time about the IT threat situation in Germany. Thus, the conditions are created which enable swift and competent assessment of the need for action and the available options in cases of IT security incidents at state level but also with regards to the business community.

The operational form was defined by means of specific implementation plans for the federal administration (implementation plan Bund) and for the private sector, which is allocated to the so called “critical infrastructures” (implementation plan KRITIS). These implementation plans form the basis for exchange of information. Their objective is, in accordance to the target group, to inform, warn and alert the user groups which are affected or threatened by severe IT security incidents according to escalation needs. In general the ability to react is supposed to be improved in order to undertake counter measures in time and to avoid large scale damage.

The NPSI was developed under the auspices of the Federal Ministry of the Interior (BMI). Its implementation will lead to improving the protection of information technology in Germany against world-wide threats.

Operational Mode

The Federal Office for Information Security (BSI) as the national and competent public authority for IT security created the necessary conditions and has been operating an operations and analysis centre since the beginning of 2006. At the core of the centre lies the federal Computer Emergency Response Team (CERT-Bund).

The operations centre has proven its efficiency on a day to day basis and with exceptional events such as the FIFA World Cup 2006 and the G-8 summits in June 2007. Individual pieces of information are collected carefully and developed into situation reports, whereby each of them reflects the current IT security situation. Thus, against this backdrop, IT incident warnings can be further processed and then interpreted and evaluated. In this context it became evident on various occasions that at the moment of first sighting and the first evaluation of the situation, not all information is available. The information gathered afterwards can considerably change the initial evaluation of the situation.

Further experience reveals that every profound evaluation depends on knowing the local framework conditions. Only in the context of these details sound evaluations are possible. Differing assessments of the same situation by different bodies are often due to the local framework conditions being evaluated differently or they are not known. This highlights the challenge an analyst is confronted with when making a cross-departmental overall assessment. By concentrating primarily on the processing of information the specialised staff of BSI despite the above mentioned restrictions are nevertheless able to monitor the IT security situation in an overall view. The individual warnings are put into the respective context and evaluated from the perspective of the national operations centre responsible. The specialists face this challenge literally on a daily basis. Weekends and holidays are no exception. The staff of the operations centre systematically and regularly analyse different sources of information which are free of charge, offered on a commercial basis or which are not accessible to the general public. The conclusions are complemented by the evaluation of technical sensor data which form a central element of a future IT early warning system.

From June 6th until June 8th 2007 the G-8 summit took place in Heiligendamm. On the photo: "Kempinski Grand Hotel", where the heads of government convened for their talks. Security technology ensured that the building was protected optimally.

IT-Early Warning

New technological developments tend to have an Achilles heel. The complexity of today's networks, the available high transmission band widths as well as the powerful connected end-devices make for faults. An example of this is the mass dissemination of malware. The dissemination potential and the theoretically possible dissemination pace of such malware reaches a dimension which seemingly allows for little room for manoeuvre. Infamous malware such as CodeRed (2001), Slammer (2003) or Blaster (2003) have displayed this quite clearly in an alarming and impressive way.

Despite early detection becoming increasingly difficult in times of information superhighways and the correspondingly shorter time-frame, the following principle for BSI is even more valid: "Early detection, early warning, gain response time!" It will only be possible in a few cases to warn before the damage is done, however it can be assumed that when the corresponding malware starts to have an effect, groups not affected or only marginally so, still exist. Furthermore, countermeasures are recommended which, according to the situation, not only are pre-emptive but can also reduce the consequences or help to rapidly reassume IT operations.

Sensors

The BSI operations centre accesses various information sources and monitoring networks for the internet – so called sensors – in order to be able to identify as early as possible deviations from the normal situation. Amongst others the internal monitoring systems of the government network "Informationsverbund Berlin Bonn" (IVBB) allow for early conclusions to be drawn. Despite the significance of IVBB representative conclusions can be drawn only to a limited extend.

BSI therefore developed an own data protection-conform internet analysis system for the recording of statistically relevant protocol information and is already operating some sensors of this system. In addition, a framework for a classic, event-oriented sensor network with a central evaluation platform is under development. A common characteristic of both developments is the fact that anomalies which could be an indication for failures or attacks can be detected and analysed at an early stage. From these analyses further conclusions regarding the current level of threat can be deduced. The quality of these conclusions depends on how representative the analysed

samples are. BSI is therefore constantly looking for further cooperation partners, who could contribute to a national early warning system and operate further sensors. Only then will it be possible to compare the locally available findings with the sector specific ones or the overall evaluations. By means of this approach it can be determined whether the incident in question was an isolated one or whether it occurred regionally or on a large scale. The necessary counter-measures can be better targeted.

Cooperation and Communication

Not only good organisation and cutting-edge technology are necessary, concentrated expert knowledge must also be available. Security experts must have the opportunity of being able to cooperate smoothly on a national and international scale. One important task of BSI is not only to make available these communication channels but to also guarantee their confidentiality and integrity.

National Situation Awareness

The findings from these technological and non-technological sources finally result in regular situation reports. They reflect the current status and carry out an impact assessment of the disturbances occurred. Based on this knowledge well-founded decisions can be taken. The BSI operations centre therefore constitutes a central point for information assimilation, consolidation and distribution. Quite rightly the motto in this context is: “Know what is happening and react accordingly!”

Outlook

The National Information Infrastructure Protection Plan is the point of departure in a further development step to extend the crisis reaction centre and to improve the response in capacity and time. A fundamental part of further development is the formalisation of communication details with other local and sector- related crisis management organisations. The focus lies on connecting BSI with other operations centres of individual authorities of the federal administration and the operations centre of the Ministry of the Interior or the Federal Office of Civil Protection and Disaster Assistance. On the one hand the warning and alert channels can be optimised and on the other hand the information assimilation and processing capacity can be increased.

The BSI operations centre continues to adapt to the changing requirements. It is cutting edge!

2.2 The Implementation Plan KRITIS

Within the "National Plan for Information Infrastructures Protection" (NPSI) BMI and BSI in 2005 were assigned to work out a plan for "Critical Infrastructures". The so called Implementation Plan KRITIS (UP KRITIS) is now available – as a result of a cooperation between the state and the business community: 30 leading operators of critical infrastructures participated in its development.

- **Critical infrastructures** are the lifeline of our society. To a large extent these infrastructures are operated by private enterprises. None of these organisations and bodies can provide their services without adequately protected infrastructures.

- **Critical infrastructures** are organisations and bodies and highly important for the public domain. Their failure or limitation could result in sustainable supply shortages, considerable risk for the public security or other dramatic consequences. This involves for example hospitals, airports, banks, traffic management centres and police stations.

The providers are aware of this. Thus, on their own initiative they have already established a high level of IT security. Adequate protection of information infrastructures cannot be achieved by measures taken by the individual businesses and organisations on their own. Accompanying and cross sector measures on a national and international scale are necessary.

To this end 30 providers have set up a cooperation with the Federal Ministry of the Interior and the Federal Office for Information Security in order to identify necessary measures for the protection of information infrastructures and to summarise them in the "Implementation Plan KRITIS". Its foundation will be the strategic objectives defined in the National Plan for Information Infrastructures Protection: prevention, reaction, sustainability.

This cooperation reflects the common responsibility of the private sector and the state. The providers' know-how is concentrated and IT security in Germany will also in the future be consolidated sustainably.

The common motto states the following: "Our cooperation aims at describing the competence and the expert knowledge of the German private sector and the federal government for IT security in processes related to critical infrastructures. Through recommendations and measures a contribution is made in order to maintain and further consolidate an adequately high level of security in information infrastructures in

general and the IT used in the enterprises. This long term cooperation for the identification and overcoming of IT crises will be promoted across sectors and in cooperation with the federal government. It is our aim that operators of critical infrastructures actively support the common principles and that they, on the basis of the recommendations (summarised in the UP KRITIS) increase the IT security level in the critical infrastructures."

Airport Berlin Tegel also belongs to Germany's critical infrastructures. Without secure IT the operation of the airport would be impossible.

The police, the fire brigade and disaster control, trains and airports are dependent on secure internet connections. Without, many areas in society would not function any more.

Exercises and Dry Runs

On September 5th 2007 the federal cabinet acknowledged the UP KRITIS. The status quo of the security level presented in the implementation plan shows that the providers of critical infrastructures are already well prepared. There is still a need for action in the field of cross enterprise measures especially with regards to an IT crisis management across different sectors. On the basis of a roadmap developed in cooperation with the providers, the tasks identified in the UP KRITIS are supposed to be faced in forthcoming years under the technical and organisational supervision of BSI. To this end four working groups were formed, which deal with:

- Emergency and crisis exercises,
- Crisis reaction and management,
- Maintenance of critical infrastructure services and
- National and international cooperation.

By means of exercises and dry runs the working groups are supposed to test emergency and crisis plans at regular intervals and identify possible improvements. Better communication between the operators of critical infrastructures is also a priority task. BSI with its IT operations and analysis centre will collect and evaluate information and provide their partners with the processed information.

Furthermore the exchange of information between the operators of critical infrastructures and the federal government will be intensified in order to, jointly and on an international level, be able to drive forward with IT security in critical infrastructures. Thus, in a common process the risk which results from the increasing dependency on information technology also in the field of critical infrastructures is supposed to be minimised.

The implementation plan KRITIS can be ordered under publikationen@bundesregierung.de or downloaded in the internet under www.bsi.bund.de/fachthem/kritis/veroeff_upkritis.htm.

Comments and criticism regarding the implementation plan KRITIS are very welcome any time. Please direct communications to the following address:

Bundesministerium des Innern, Referat IT 3
Alt-Moabit 101 D, D-10559 Berlin
Phone: +49 (0) 30 186 81-0
E-Mail: it3@bmi.bund.de

The private sector plays a vital role in the implementation plan KRITIS (UP KRITIS). Circa 85 per cent of the critical infrastructure in Germany nowadays is in private hands. Cooperations of this kind between the public and the private sector but also other public private partnerships contribute to an improved protection of critical infrastructures.

2.3 The Data Security Competence Centre

The Data Security Competence Centre established in 2002 is an advisory service offered by BSI. The advisory services were closely linked to the initiative "BundOnline". Since the beginning of 2006 the required services must be funded by the authority taking advantage of the services.

The BSI competence centre supports its clients with analysis, advice, concepts, coaching and inspection in all issues related to IT security. These advisory services can be taken advantage of by all institutions and authorities of the federal government.

Enquiries can be related to current or future projects. The advisory services should not only consider the public authorities' issues but also the ideas and interests of the general public, associations and the private sector.

Fields of Implementation of the Competence Centre Data Security

The following fields are the priority areas in which the competence centre is primarily working:

- The field of IT security concepts primarily deals with technical and organisational issues related to ensuring the business processes of public authorities. In this case not only the conceptual design of the new electronic procedures is offered, but also enhancement development of already existing solutions.

  Examples are: Protection needs assessment, risk analyses and comprehensive IT security concepts within ISO 27001 on the basis of IT-Grundschutz.

  This advisory area becomes particularly relevant in relation to the activities resulting from the National Plan for Information Infrastructures Protection – Implementation Plan Bund.

- In the area of communication security, the focus lies on issues related to data protection and data security in the transmission and processing of confidential (personal) data and the revision security of electronic administrative processes.

The priority in this context is the adoption of technologies for the electronic signature, authentication and encryption. An adequate technical implementation of legal requirements as well as the interoperability of the different solutions are of particular importance. One of the important tasks in this field is the integration of the basic component data security into the already existing IT infrastructure.

- The data security competence centre will accompany major projects of the federal government related to IT security, for example with regards to citizens' portals. (See chapter 5.1)

  Furthermore, the competence centre is available for the support of the staff responsible for the projects "Official Documents" including the E-Card-API and federal register of residents.

- The project-related work is complemented by analyses of the IT security market, providing basic knowledge, determining best practices and training. This guarantees the necessary knowledge transfer between the competence centre and the users.

Specialists Guarantee Continuity

At the competence centre, particularly experienced consultants with specialist knowledge are working in the essential areas of IT security. In order to guarantee continuity, some of the staff members had already worked on the project Bund Online.

2.4 Legislation and Law – On IT Security-Related Legal Developments

IT security is not only a technical but also a legal problem. Security gaps in software programmes raise the question of who can be made liable in the case of damage. Which measures must be taken by whom? Who is liable for risks and to what extent? Who must prove what in a case of a dispute?

All persons involved in the manufacturing and the application of IT products – manufacturers, service providers, users – have an interest in receiving reliable answers to these questions. Only then will it be possible to guarantee legal certainty.

From a legal point of view, the question also arises as to what extent legislation with its tools at its disposal, is able to sufficiently respond to new risks. To what extent can manufacturers, users and service providers be involved in legal terms, in order to react efficiently to IT risks? In the light of rapid developments in the IT sector can legislation play a determining role at all or will it always be lagging behind the constant technical innovations? Also from the point of view of the state, these questions arise when it comes to assuming responsibility for infrastructures in the field of IT security.

Interdisciplinary Approach

As federal authority responsible for IT security, it is BSI's task also to deal increasingly with legal aspects of IT security. Here, BSI pursues an interdisciplinary approach where IT experts closely cooperate with lawyers.

The first project was implemented under the heading "Legal developments in IT Security". In 2006 a study was commissioned in which initially the security requirements regarding the manufacture and the application of information technologies were defined, which are required by the current legislation. These requirements are partly laid down in special legal acts but primarily they are deduced from the interpretation of already existing laws.

The study "Manufacturers', Users' and Intermediaries' Responsibilities in Legislation and IT Security" ("Verantwortlichkeiten von Herstellern, Nutzern und Intermediären im Recht der IT-Sicherheit") is available on BSI's homepage under www.bsi.bund.de/literat/studien/recht/IT-Recht.pdf.

Awareness Raising for Legal Aspects in IT Security

The analysis of the current legal situation as point of departure, BSI increasingly aims at raising the general public's awareness for legal aspects of IT security and will try and enter into a discussion with all the institutions concerned. Studies and events will accompany the developments in IT security legislation. To this end, on 13th June 2007 BSI in its series of events "Dialogue with BSI" invited representatives from the business community, consumer protection associations, from the scientific community and from public administration, to the visitors' centre of the Ministry of the Interior in order to discuss the topic "IT Security Through Regulation?". The lectures held here from different perspectives analysed the needs for legal regulations in IT security. The lectures of the speakers can be downloaded from the BSI's homepage.

The development of an independent IT security legislation has only just begun. BSI will continuously increase its commitment to this area. To this end it will monitor European as well as international trends and furthermore contact associations and last but not least also enter into discussions with IT security experts and lawyers in order to be able to develop its own proposals on a broad basis. Ultimately BSI is assuming that in legal literature this topic will also be dealt with and that as a result, from a cooperation between the scientific community and the practitioners, there will be a productive discussion.

IT Security:
Civil and Public Law

"Harmonised regulations or an interdisciplinary approach for guaranteeing basic IT security – contractual regulations aside – are missing; the structures seem to be inhomogeneous. Only regulations in data protection legislation regarding an organisation which guarantees data protection and which include elements of IT risk management in the form of IT-related rules and regulations cover numerous users and IT providers. Under current legislation it is therefore necessary essentially to resort to the general regulations of civil and public law."

Taken from the final result of the expert opinion

2.5 The Report on the IT Security Situation in Germany 2007

Every two years BSI publishes a Report on the IT Security Situation in Germany giving an overview of current and future risks, challenges and trends. The objective is to inform the general public and to raise awareness for IT security. A reliable use of information technologies to the benefit of all social groups in Germany can only be guaranteed in this way.

In this report, threats are analysed and evaluated which result from technical security gaps and their use. Opportunities and risks in the implementation of innovative technologies are presented as well as trends from the private sector, society, technology and legislation. It also provides an overview of the use of information technology by different groups in society and illustrates which tools the BSI provides for the different target groups. Dr. Udo Helmbrecht, president of BSI, presented the second "Report on the IT Security Situation in Germany" at a press conference at the 10th German IT Security Congress.

Increased Threat Potential

The report shows clearly that the threat potential has increased compared to the year 2005. The increasing number of business and private activities in the virtual world goes hand in hand with a professionalisation and commercialisation of IT threats. There is a continuously high level of threat in IT security for private users as well as for businesses and the public administration.

In 2006, 7.247 new security gaps in programmes and operating systems were detected – this is an increase of 40 per cent compared to the year before.

Malware is the most frequent form of attack against IT systems; the largest group is formed by trojans and worms.

The number of attacks against the availability of IT systems or IT services also rose dramatically in 2006. This is caused by the increasing number of existing Bot networks which are set up especially for these attacks or are used for sending SPAM.

Trend towards Modular Malware

Not just the quantity but also the quality of attacks against IT systems of enterprises and private users has been increasing. One of the trends regarding malware is to structure them in a modular way. Small programmes, so called downloaders, aim at being active on the computer as long as possible without being detected. They are able, at a certain point in time or following the orders of the attackers, to load further damaging functions via the internet. Thus the attacker will be able to substitute the malware on the infected system by optimised versions. A regular change of the files makes it difficult for anti-virus programmes to detect them.

Consequently efforts for increased IT security by the manufacturers, administrators and public authorities are constantly being challenged by the continuously changing and adapted methods employed by the attackers.

Nowadays, the authors of this malware preferably aim their attacks at security gaps in standard software such as office applications or web browsers. Most frequently, computers belonging to innocent users in the private or professional environment are victims of infections. This malware is usually spread via e-mail attachments or specially prepared websites. Not only the executable files are dangerous; unsuspicious image files or documents can also be misused for an attack.

BSI-President Dr. Udo Helmbrecht with Head of Division Günther Ennen (on the right) and BSI Press Officer Matthias Gärtner (on the left).

Awareness for Problems is Increasing

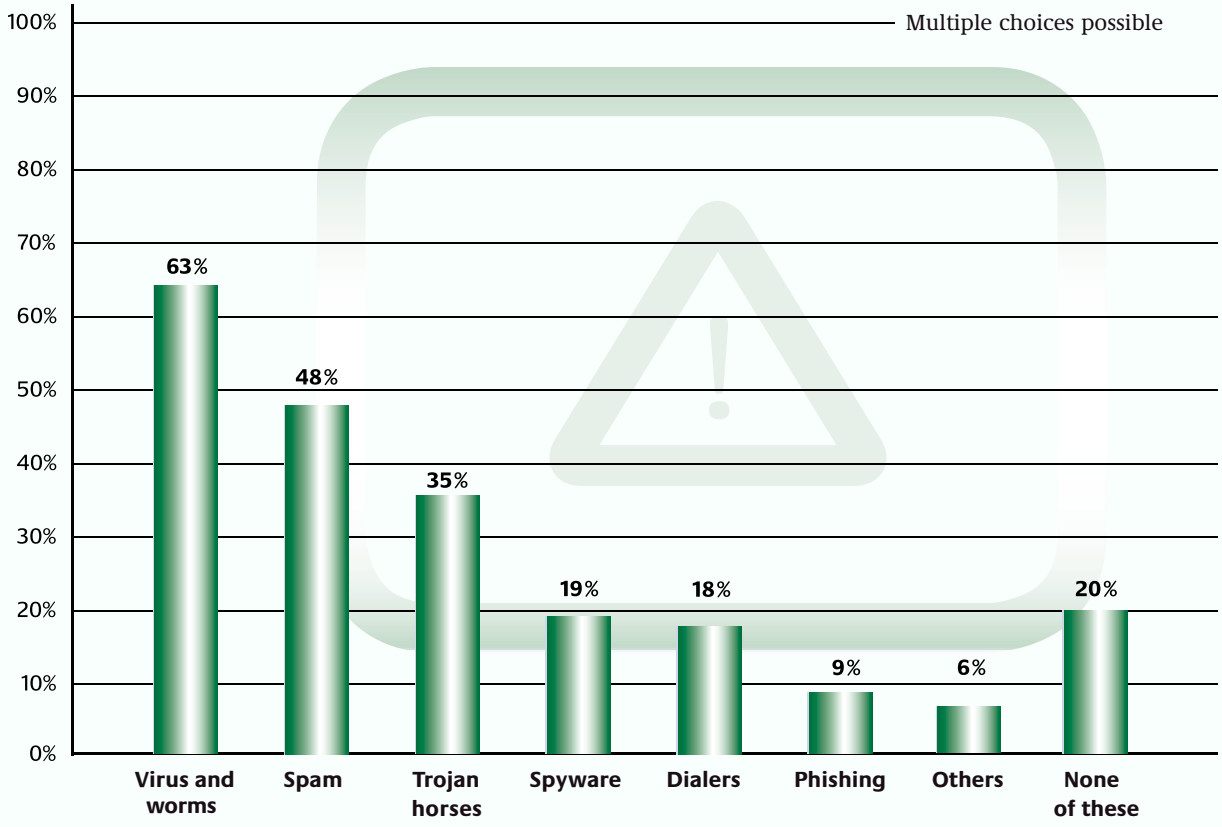
The BSI report “The IT Security Situation in Germany 2007” includes furthermore, indications on the level of awareness among the general public, the private sector and public administration regarding IT threats. Compared to the 2005 report, the level of awareness for risks in the use of information technologies has been increasing in some social groups. There are some positive trends which can be explained not least, by BSI’s education work.

According to a study conducted by BSI in 2006 90 per cent of the general public have installed a virus scanner on their computers. This is an increase of 14 percentage points, compared to the year before. 52 per cent of the people interviewed are also using a personal firewall. This corresponds to an increase by six percentage points compared to the year 2004. Among businesses, however, there is a more heterogeneous picture. Even though IT security is continuously recognised as being extremely important, businesses overall are still investing too little money in IT security.

Further Improving Security Competence

Despite these positive trends: The current situation urgently makes it necessary to further improve the security competence of all groups in society. Primarily the increased quality of the attacks, alongside the professionalism of IT crime makes this improvement of the essence. For years, BSI has taken comprehensive measures towards education and raising awareness, offering practical support.

Personal Experience with Online Threats

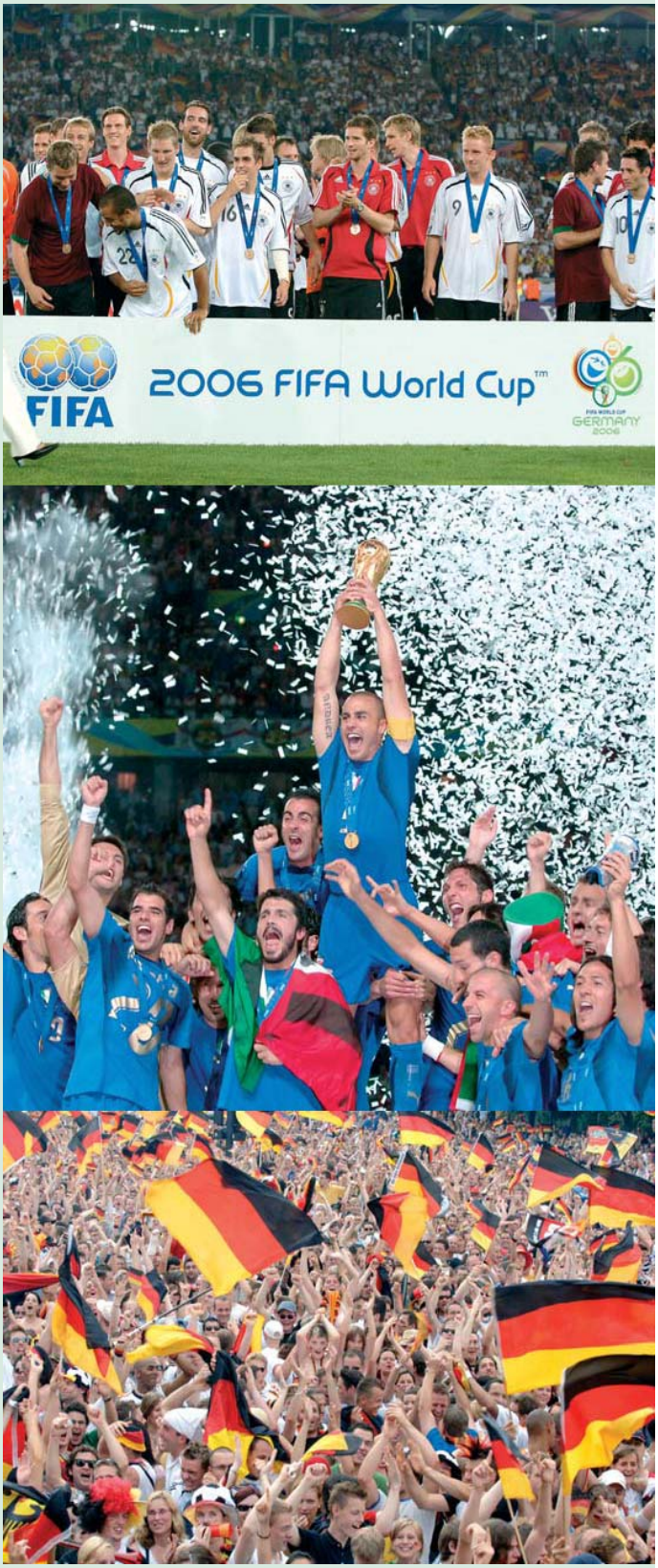


Source: BSI

More than half of the users interviewed do not register themselves on their computer with restricted user rights as is recommended by security experts. One consequence is: Infections with malware can have a severe impact. The table shows: Only every fifth person interviewed believes they have not been affected so far.

A Leather Ball and IT Security

"A Time to Make Friends" – this was the official motto of the FIFA World Cup in 2006. Making friends implies feeling safe. The number of staff in service at the BSI operations centre was increased during the World Cup in 2006, in order to be able to detect risks and acute security threats at an early stage and react accordingly. Apart from the expected phishing attacks, which aimed at spying for confidential data of football fans, no significant disturbances were registered during the World Cup.



Furthermore, BSI was also engaged in the "National Information and Cooperation Centre" (NICC) which was set up by the Federal Government before and during the FIFA World Cup 2006 in the Federal Ministry of the Interior. The task of the personnel from all security authorities from the federal level was to collect and condense information and control it within the field of responsibility of the federal government. The NICC also developed a daily report on the "National Situation World Cup 2006". As from mid May until the mid June 2006 IT experts from BSI as so called liaison officers coordinated the communication between the BSI operations centre and NICC. —› www.itsecurity2007.de

3.1 Current Developments in Security Technology

Solutions for computer workspaces, where confidentiality is vital, the further development of encryption devices and end-to-end security also in wireless telecommunication – these are examples of security technology within public authorities and ministries which constantly need to be adapted to the highest level of efficiency. BSI always advises and develops according to the state of the art.

For IT workspaces with internet connection increased security measures against external access are necessary. Due to the prevalent regulations when processing classified information (VS), a physical separation of open networks and those classified secure is imperative. As a basic principle it is prohibited at IT workspaces to carry out internet research while working on classified information if no accredited security measures are in place.

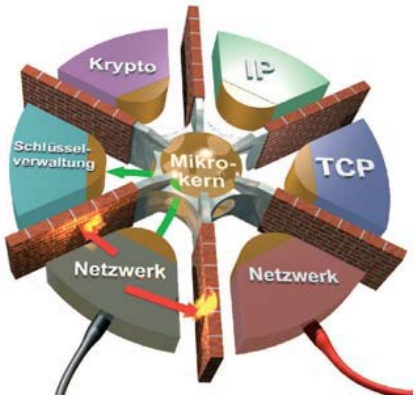
Secure Platforms

One possible solution is the introduction of a multi-session IT workspace. Here a session is defined by the user interface of an operating system. The change of the workspace environment between the sessions can be achieved by a so called virtualisation of the hardware. For the virtualisation, special software (a virtual machine monitor) is necessary. In close cooperation with a central trustworthy operating system unit (e.g. microkernel, hypervisor) and a hardware security module (e.g. Smartcard, TPM) it represents the most important components of a high security platform. The virtualisation of the hardware allows different operating systems to coexist on only one single physical IT system and also facilitates the controlled distribution of the hardware resources such as the shared access to the network. The microkernel facilitates the monitoring of the system interfaces and realises the encapsulation of different applications within the system by means of protected memory areas.

On the other hand, the principle of virtualisation for the encapsulation of a guest operating system which is generally not trustworthy also provides extra protection for the host operating system. Accesses of the guest operating system to the system resources are authorised by the virtualisation machine monitor only by means of the communication structure provided by the microkernel. With the virtualisation technology L4-VM the basic components of an innovative and highly modular microkernel-based security architecture are provided. The structure of the architecture is demonstrated in the figure (see below) and is available as a prototype. Multi-session IT workspaces provide the users with flexibility and added convenience. Internet

research and online bookings are popular applications. Using these applications is authorised by network regulations but due to the filtering of active content or Java Script they are very often not usable. These limitations can be removed by isolating non-trusted operating systems. Virtualisation also makes it possible to operate parallel sessions of different classifications or cryptographic parameters in the high security area. The condition for the application of all secure solutions is the use of trusted minimalised subsystems (Trusted Computing Base) within a modular security architecture.

Microkernel-based security architecture for multi-session operation with "compartments". By means of appropriate virtualisation techniques the direct access of the guest operating systems to the shared system resources and the microkernel can be controlled.



Configurable Crypto Modules

Crypto devices which have so far been used for the processing of classified information classified "secret" or higher according to the security philosophy by national and NATO standards necessitate hardware based realisation of crypto functions. To this end e.g. SINA components for the encryption of data classified "secret" contain a crypto module (Pluto-ASIC) developed especially for this purpose. Mask programmed ASICs to a large extent with fixed functionality have so far been most appropriate for the realisation of the high standards required in confidentiality due to their inherent security properties. They impeded manipulations of the component produced on the basis of a trustworthy finished element as well as the disclosure of the contained crypto functionality. Nevertheless the static functionality of such ASICs is also a disadvantage, as rapid adaptations to specific and/or new requirements, specifications or application scenarios are virtually impossible. For this reason BSI, in an internal study, has worked out basic concepts for security modules which correspond to the high demands in the governmental secrecy protection area and which at the same time facilitate a high degree of flexibility – also for crypto functionality. Departing from and based on these concepts, BSI has commissioned the development of a new crypto components generation.

By means of reprogrammable logic modules, so called FPGAs, BSI will be able to react more swiftly to changing requirements. In this context, the loadable part of the security functionality is protected by strong cryptographic mechanisms and the technical protection cover of the security modules, which allows only BSI approved and authorised device configurations to be loaded onto the device.

Due to the availability of several secured device configurations in the device at any one time, the new capability for the high security area is developed allowing the use of the existing hardware consecutively and exclusively with the selected configuration. Every device configuration prepared in this way within the project is called a device class. By means of an appropriate chip card, when booting, the user configures which ever of the security functionalities, which in terms of security policy might exclude each other, he or she needs and which of the device classes the user wishes to load. A national device class is being developed. First development results have been presented to BSI for analysis.

A so called wafer with the new Virtex 5 platform for high speed data acquisition.

Security Management of Modern Crypto Systems

ElcroDat 6-2

In cooperation with the company Rohde & Schwarz, BSI developed this crypto system for telephone and data traffic on the basis of Euro-ISDN. This is the first crypto device accredited in Germany which realises a key distribution with a public key mechanism for the transmission of information classified strictly confidential. The public key infrastructure used in the security management of the system virtually relieves the user of supplying the devices with key material. This infrastructure is based on crypto mechanisms which are based on the group arithmetics defined in elliptic curves. The curve parameters necessary for the application of the system are produced by BSI, then tested and made available for the user. Within the security management, ElcroDat 6-2 crypto systems are supplied with the necessary parameters at the management station via Smartcards. The noise generator realised in the crypto devices together with public key cryptography facilitates the mutual authentication and key unification.

SINA

With the “Secure Inter Network Architecture” (SINA) BSI provides a technology whereby highly secure connections can be established via the internet. The cryptographic mechanisms involve the application of asymmetric cryptographic mechanisms e.g. in certificate management and in establishing connections. These cryptographic mechanisms are also based on group arithmetics of elliptic curves. The curve parameters necessary are generated by BSI with mainframes, their quality is ensured, they are processed in conformity with SINA, tested and made accessible for the user. The na-

tional accreditation regulations stipulate that these curve parameters are substituted regularly in accordance with each individual case of implementation. The curve parameters necessary for establishing a connection can be exchanged online if a SINA online crypto management is in place. This occurs on the basis of a lifecycle model by means of secure access to the new parameters via an LDAP server set up by the crypto management. Offline, these parameters are substituted either manually by update CDs or by changing the SINA Smartcards. Regarding the curve parameters used with certificate management, the substitution is realised by an appropriate exchange procedure within a lifecycle model.

On the left: A chip card protects this computer from any possible attack by malware. ElcroDat 6-2 (below) is compatible with all ISDN basic services, even via satellite links, for telephone-, fax-, data- and video communication. This device is approved for the transmission of classified information of all degrees of classification of the Federal Republic of Germany.

Safeguarding Government Communication

In the light of rapidly developing telecommunication networks, adequate security solutions must be constantly updated. Today even with a simple telephone call incalculable networks and transmission technologies are used. The “secure” line therefore is definitely a thing of the past. The use of cryptography on both ends of the transmission path e.g. with telecommunication end-devices or just before them provides the best protection. This is also known as end-to-end encryption. Numerous security solutions developed by BSI are based on this approach which is a convincing concept. Therefore the ISDN encryption system ElcroDat 6-2 constitutes the central end-to-end security solution for speech based government communication. In the past two years this system, in technical terms, has been further developed and adapted to the requirements of modern systems. The contract for the development of the crypto telephone ElcroDat 5-4 commissioned by the German Bundeswehr was supervised and largely organised by BSI. A first accreditation already exists for this telephone which can be used in analogue and digital networks. In wireless telecommunication, end-to-

end encryption is also gaining importance. For the new digital BOS Network of the Federal Republic of Germany an encryption of this kind was designed by BSI on the basis of a chip card. In the past two years the most essential parts of this new development were completed for implementation. They will be operational just in time for the introduction of this new network.

GSM/UMTS-based mobile telephony has become an important factor in government communication. For the secure use of radio networks, end-to-end encryption is of the essence. BSI in cooperation with Rhode & Schwarz SIT, has started the development of a device-independent, external solution. This way a permanent integration into the end devices is avoided. The rapidly changing mobile phone generations would make constant new developments and consequently a great deal of investment necessary.

View onto the television tower in Stuttgart. The mast also serves as wireless transmitter for telephone calls and internet data.

3.2 Approved Security for the High Security Area

In cooperation with industry and public administration, BSI is actively engaged in several major future-oriented projects. Among the new technological challenges are inter alia the Software Defined Radio (SDR) project and the satellite system of the Bundeswehr SAR-Lupe.

The purpose of SDR is to substitute a large number of radio systems which are used in the military field with one single technology. So far radio systems for the military tactical sphere were specifically geared towards the demands of individual operations and platforms and were provided with a clearly defined radio behaviour and a specific cryptography. The result is many supported radio standards and device platforms with numerous very different security functions. Thus it seems obvious to look for a solution which constitutes a convergence towards a platform, which is capable of integrating all the different requirements with regards to radio standards, application platforms and security mechanisms on a national scale and on an alliance level.

SDR – The Secure Military Radio System

At the core of the solution aimed at lies the substitution of a “hard” inflexible with a “soft” flexible technology i.e. the change from hardware defined radios to software defined radios (SDR). This applies to nearly all parts of the radio system (radio). Similar to a high-performance computer, with software, the waveform application software, every radio standard and every security mechanism can be “loaded” and configured according to respective requirements. This technology should be available for the different platforms so that the waveform application software can be operated in the same way on all application platforms.

The Joint Tactical Radio System (JTRS) Programme from the US Army shows that this type of system is technologically feasible. For the area of tactical data links, the MIDS/JTRS was developed as a four channel system and in at least three channels it should be fully software programmable. The requirements regarding the verifiability for the determination of the trustworthiness within a NATO accreditation increase considerably and constitute a huge challenge.

Network operation management depends on first class information. Here software supported radios are indispensable.

New security requirements must be tackled in addition to the substitution of a hardware-based to a software-defined cryptography for the encryption of data and perhaps for frequency hopping. A multi-channel SDR should, channel-independently, be able to operate different waveform application software. Thus the channels must be separated in such a way so as to ensure that there is no compromising interference between them. This is vital when data of different security classifications and various origins (national, NATO, EU) are transferred on these channels. Therefore a separation of this kind must correspond to the highest possible security classification. On the other hand, it is necessary that software and data (keys, configurations) be administered centrally within the system and be distributed among the channels. A change of waveform application software must be possible within one single channel; this also implies a possible change of the cryptographic parts.

All these new requirements must comply with various international standards. At this point in time, there is no system in place which fulfils these standards and is internationally recognised. There is no solution in sight which complies with internationally harmonised requirements. Within the SDR project, BSI is therefore involved in the platform development as well as in the processes for the international recognition of solution approaches.

The Evaluation of SAR-Lupe

Information security systems which process data and classified information (classified information directive – VSA), must be accredited by BSI. In the accreditation process, an evaluation of the products in question must be carried out. This evaluation process is highly product specific and must therefore be customised. This process will be described as follows on the basis of the German reconnaissance satellite SAR (Synthetic Aperture Radar)-Lupe. In December of 2006 the first German reconnaissance satellite – SAR-Lupe – was launched. In the meantime it has passed all the tests in space. The second satellite of this series was launched successfully on 2nd July 2007. Next year, three further satellites of the same type will follow. They will form an entire system in space.

A technician testing the capacity of the solar cells of the SAR-Lupe satellite.

BSI has been contributing considerably to the IT security of these satellites and the entire system for years and through all project phases. Firstly a cryptographic concept was developed and the system producer was advised on the implementation. Then BSI carried out the evaluation. This project was and continues to be exceptional. So far there are no comparable systems in Germany. In addition, new solutions for problems constantly had to be found for the specific requirements of the aerospace industry. This applied especially to the evaluation: There was no prototype of the device being tested. Tests have therefore been carried out at the manufacturers in Bremen over the past three years.

Despite the first satellite having started its operations in orbit, BSI's work is far from conclusion, as system tests must also be conducted for the three satellites which will follow at intervals of four months. In the meantime, BSI has granted the accreditation for the processing of data and information including for the classification confidential. Nevertheless the project has not been concluded yet. The next step will be an extension of the system in terms of a cooperation with other nations. Here BSI is in demand again when it comes to guaranteeing IT security and national secrecy.

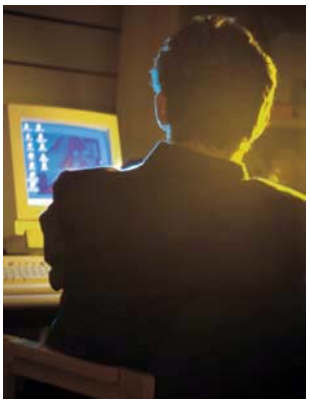
SAR-Lupe is Germany's first satellite-based reconnaissance system. It is made of five identically constructed small satellites and a ground segment. The computer model shows one of the satellites circling the Earth.

3.3 Emission Security

Compromising emission has also become a security issue for civil computer users, especially for businesses. A good shielding from this electro magnetic emission by means of the surrounding building fabric impedes unauthorised reception and decryption. A BSI study in cooperation with the University of Hanover is analysing how efficient shielding can be guaranteed at low cost.

In the active mode, every electronic device produces more or less strong interference emissions. In the case of IT devices these emissions can also transport the data that is being processed. Whoever receives the emission can read the processed data from a certain distance. Confidentiality of this data is not guaranteed any more. This way e.g. through interference emission of computer screens it is possible to reconstruct the screen content which is being exhibited. This kind of emission is called "compromising emission". An appropriate means of measuring the level of risk of eavesdropping resulting from compromising emission on site is the so called zone model developed by BSI (see BSI Annual Report 2005).

Eavesdropping by emission is an alternative especially when a computer network resists any attack or data are encrypted. It is assumed that in Germany alone, there are hundreds of attempts every year to use the emission of screens, computers, key boards and printers for the purpose of collecting information.



Post Construction Changes are Costly

If analyses of a building establish that the shielding effect of the building fabric does not meet security requirements, measures conducted afterwards may be necessary and this can be cost intensive. It would be more beneficial if the necessary shielding effect were determined during the planning phase. So far forecasts concerning the attenuation behaviour of buildings in the planning phase could only rely on empirical findings.

From Concrete to Copper

In order to consolidate the empirical findings resulting from a series of measurements on buildings by laboratory experiments and to make these results systematically accessible for the general public, BSI has commissioned the study “Analysis of the Electromagnetic Attenuation of Buildings”. A Technical Guideline (TL) was developed with this study. This guideline evaluates forty different building materials: from concrete walls to copper wall covering. It will be easier to select the building materials by integrating this into the planning process of buildings with certain security requirements. At the same time the TL is also a good adviser when it comes to protecting buildings from interference emissions (keyword electro smog). In 2008 the Technical Guideline will be published on BSI’s website.

View into a measurement booth. This type of magnetic field measurement provides information on the level of shielding.

3.4 Programme for the Strengthening of Internal Security (PSIS)

Prevention lies at the centre of BSI's action. Weaknesses in hardware, software and networks are analysed and eliminated in cooperation with producers, providers and users. The current level of threat considerably influences the perception of this task.

The terror attacks uncovered and prevented in 2006 make very clear that Germany is located in the centre of a threatened area which is directly determined by international influences. A decrease of the level of threat cannot be expected in the near future. The potential perpetrators and their suspected targets can only be identified with a high level of personnel and logistical efforts. This results in new and complex challenges which have to be addressed by public authorities. In accordance with its legal obligations laid down in § 3 BSIG, BSI supports the security agencies with concepts and methods regarding IT security and the appropriate information technology.

As the central organisation responsible for IT security in Germany, BSI has been dealing with the basics and the potential applications of biometrics for many years. Biometrics has been applied for the ePassport (electronic passport) and the planned electronic identity card. Biometric processes are also capable of effectively and safely supporting necessary identification and controls of individuals in special situations of threat.

Government networks and critical infrastructures in the business community are tempting targets for terrorist attacks. In 2005 the EU ministers of Justice and of the Interior identified cyber attacks as one of the new types of threat and initiated the fight against them. The development of technical solutions for the detection of and defence against terrorist infiltration in critical communication networks by BSI form the technical conditions for the measures taken by security agencies.

For a successful detection and defence, immediate early warnings distributed reliably and confidentially to all relevant bodies is of the essence. In order to provide a confidential and quickly available communication infrastructure for the rapid, mobile and transborder exchange of information, the BSI IT security components have to be reliably in place.

For the PSIS programme BSI received no extra staff but an increase in budget of 4 million Euros. These additional funds were used for the development and evaluation of new conceptional approaches and mechanisms. BSI initiated projects in three areas, which are subdivided in several individual measures:

1. Biometrics-Supported Early Detection of Terrorist Suspects in Image Processing Controls

- **Auto-Identification**
  Developing a mechanism for the automatic registering and identification of biometric data under real-time conditions;

- **MitarbeiterIdent (Personnel-Ident)**
  Developing a method in order to optimise controls of staff working in critical areas, such as airports by means of electronic staff IDs with biometric properties;

- **Trackingsystem**
  Developing a combination of RFID- and biometrics-based mechanisms for tracking of individuals and baggage/goods being transported in especially vulnerable public transport areas.

IT security has become a critical part of internal security. View onto a government building in Berlin.

2. Detection of and Defence against Terrorist Infiltration in Critical Communication Networks

- Creating the technical infrastructure for monitoring control channels of Bot networks;
- Developing measures for the prevention of Bot networks by means of shutdown, takeover or overload;
- Working out measures for the protection of critical communication networks against denial-of-service-attacks.

3. Secure Communication Infrastructures for the Early Detection of Terrorist Activities

- Designing secure and available communication architectures and infrastructures geared towards the special requirements in the distribution and evaluation of early findings from the terrorist environment;
- Intensified advisory and support of the security agencies in the construction of secure networks;
- Development of innovative and secure communication components.

In total, BSI initiated 22 projects which will bring about appropriate solutions in order to achieve the set targets. This includes projects for awareness raising among citizens and public authority staff, to legal expert opinions and monitoring of Bot networks as well as the development of hardware systems, which are capable of transporting highly confidential classified information.

PSIS Projects (Selection)

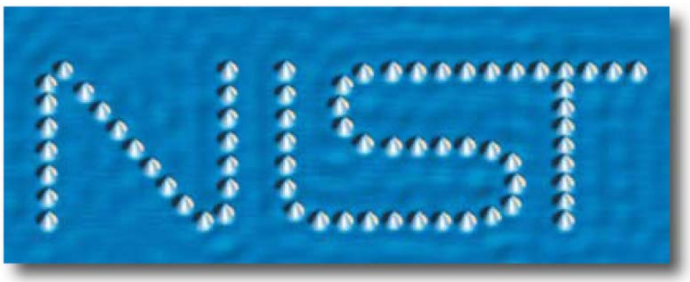
- Analysing weaknesses, design vulnerabilities, typical configuration errors of Windows Vista, which can be used for the distribution and installation of Bots.
- Legal opinions on measures for the monitoring and combating of Bot networks.
- Development of a secure boot token including an anti-tamper mechanism for mobile SINA clients.
- Protection of the EU visa sticker by the development of typographic integrated electronic security properties for the protection of machine readable data and photos against counterfeiting and falsification.
- Extension of Gpg4win and S/MIME functionality as well as improving the integration into Outlook and the manuals/documentation in order for public authorities, citizens and businesses to be able to send and receive e-mails with automatic authenticity, integrity and confidentiality assurance.
- Analysing the feasibility of a signature independent protection programme for the defence against Bot networks.
- Dubbing of a Dutch instruction film on malware in order to educate internet users in a succinct and understandable way on the risks resulting from malware when using the internet.
- Prototypical implementation of biometric staff passes using BioMiddle and EA EAC chip cards.

3.5 Current Developments in Cryptography

Signing, ciphering, encrypting – to a large extent research on cryptographic techniques is based on international cooperation. An insight into the "field of responsibility cryptography" – a field in which BSI occupies a leading position in the relevant research.

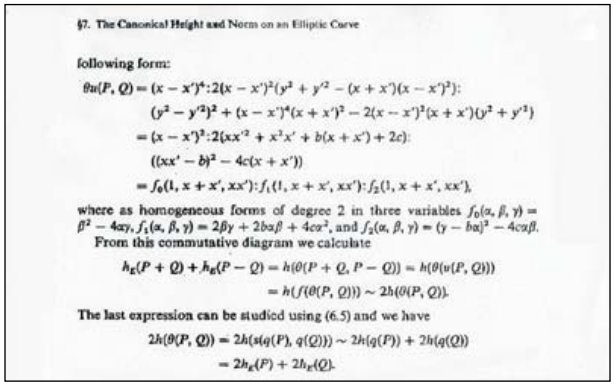
Cryptographic hash functions play a central role inter alia in creating digital signatures. In this context the so called collision resistance is fundamental: i.e. it should be practically impossible to indicate two different objects which have the same hash value. Internationally the SHA-1 algorithm standardised by the US Agency National Institute of Standards and Technology (NIST) is very wide spread. As opposed to e.g. the MD5 hash algorithm, so far there are no SHA-1 collisions known of but in 2005 a Chinese group of researchers could for the first time reveal some weaknesses of the SHA-1 algorithm.

Since then it has become obvious that the security level of SHA-1 is considerably lower than experts had assumed. In the meantime a group of researchers from Graz has found collisions for a reduced SHA-1 variant. At the present time, this group is searching for a collision for the entire SHA-1-algorithm. To this end they are looking for partners who will make free computing time available for this project.



The US agency NIST therefore decided to initiate a competition for the determination of a new hash standard. In October 2005 and August 2006 two international preparation workshops with 170 representatives each, from universities, public authorities and the industrial sector, took place in the USA. The field of responsibility cryptography at BSI was represented with lectures at both workshops. After a further workshop in May 2007 in Spain, NIST is planning to start the announced competition in the near future. The new standard should be in force by the end of 2012.

Office building of the Federal Network Agency in the former government district in Bonn (on the right). Every year it publishes the relevant "Catalogue of Algorithms".
Nowadays mathematics plays an ever increasing role when it comes to new cryptographic mechanisms (below).



§7. The Canonical Height and Norm on an Elliptic Curve

following form:

$$\theta u(P,Q) = (x-x')^4 : 2(x-x')^2(y^2+y'^2-(x+x')(x-x')^2):$$
$$(y^2-y'^2)^2+(x-x')^4(x+x')^2-2(x-x')^2(x+x')(y^2+y'^2)$$
$$= (x-x')^2 : 2(xx'^2+x^2x'+b(x+x')+2c):$$
$$((xx'-b)^2-4c(x+x'))$$
$$= f_0(1, x+x', xx') : f_1(1, x+x', xx') : f_2(1, x+x', xx'),$$

where as homogeneous forms of degree 2 in three variables $f_0(\alpha,\beta,\gamma) = \beta^2-4\alpha\gamma$, $f_1(\alpha,\beta,\gamma) = 2\beta\gamma+2b\alpha\beta+4c\alpha^2$, and $f_2(\alpha,\beta,\gamma) = (\gamma-b\alpha)^2-4c\alpha\beta$.

From this commutative diagram we calculate

$$h_E(P+Q)+h_E(P-Q) = h(\theta(P+Q,P-Q)) = h(\theta(u(P,Q)))$$
$$= h(f(\theta(P,Q))) \sim 2h(\theta(P,Q)).$$

The last expression can be studied using (6.5) and we have

$$2h(\theta(P,Q)) = 2h(s(q(P),q(Q))) \sim 2h(q(P))+2h(q(Q))$$
$$= 2h_E(P)+2h_E(Q).$$

Hash Functions and their Influence on the Signature Law

Considering the lead times and the life cycles of chip cards, it can be assumed that hash functions other than those constituting the future standard will be around at least until 2018. In cases of security critical signature applications it is absolutely fundamental to substitute the SHA-1 algorithm as soon as possible. As a "transitional solution", representatives of the SHA-2 family could be particularly appropriate until the new standard is in force. The (in-)security of hash functions such as SHA-1 is amongst others also relevant for qualified electronic signatures (q.e.S.) according to the German signature law (SigG). Legally permitted algorithms and parameters (inter alia the key length) for q.e.S. are determined by a paper published yearly in the Bundesanzeiger by the Federal Network Agency (BNetzA) called "Catalogue of Algorithms".

The SHA-1 algorithm currently used most frequently for signature applications is still authorised for q.e.S. For the past two years due to the developments outlined above, BSI has been of the opinion that the validity period of the SHA-1 algorithm should be curtailed.

New Stream Ciphers Required

A few years ago, the block encryption algorithm AES was standardised by NIST. Despite stream ciphers playing a vital role in many applications there is no standardised stream cipher. In November 2004 the first Call for Primitives in the algorithm competition "eSTREAM – ECRYPT Stream Cipher Project" was published. The declared objective is to identify new stream ciphers which can be considered appropriate. The competition is expected to end in May 2008.

Asymmetric Cryptographic Algorithms

Due to international agreements (EU/NATO) at least for the area of high security the key lengths will be increased. For symmetric mechanisms the minimum key length will typically be 256 Bits, for asymmetric mechanisms based on elliptic curves 384 Bits. The fundamental decision was taken in favour of elliptic curves; the final and general decision regarding algorithms is being hampered due to patent issues. In future, modern cryptographic devices will no longer be based on special ASICs. Rather they will allow the secure download of algorithms which can be executed on reconfigurable hardware. It is therefore important to develop innovative methods for protecting these downloads, which are quantum computer resistant and which continue to be secure even if the hash function being used is broken.

Progress in crypto analysis also determines an increase of key lengths with q.e.S. according to SigG. With the signature cards currently used, the RSA mechanism plays a central role. Until the end of 2007 a key length of 1024 Bits for RSA is considered sufficient by the Catalogue of Algorithms (see “hash functions”), whereas from the beginning of 2011 a minimum key length of 1976 is required. In the long term q.e.S. mechanisms based on elliptic curves could also gain importance.

ECC for Official Documents

As has already been referred to, public key mechanisms based on elliptic curves are becoming increasingly more common. Consequently BSI has been participating considerably in the development of standard curves and the definition of security criteria for curves which occurred within the ECC Brainpool. Besides BSI, among the members of the Brainpool are numerous enterprises and universities which are committed to ECC technologies; altogether the working group comprises approximately 25 member enterprises and institutes. Further information can be found under www.ecc-brainpool.org.

The standardised parameters are also available here. The Brainpool curves are being discussed also in terms of an IETF Internet-Draft; the corresponding Draft is available under https://datatracker.ietf.org/drafts/draft-lochter-pkix-brainpool-ecc/.

Two of these curves are already being used as basis for the calculation of signatures that serve as authenticity assurance of data saved on the RF chips of German travel documents. For instance, the German Country Signing Certification Authority, which is operated by BSI uses the Brainpool curve brainpoolP256r1 and the German Document Signer, operated by the German Bundesdruckerei GmbH, uses the Brainpool curve brainpoolP224r1. Similar mechanisms will be employed with the future electronic identity card. Furthermore, as from 2010 the use of standardised Brainpool curves is planned for the Health Card.

Quantum Cryptography and Quantum Computer-Resistant Crypto Mechanisms

If quantum computers with the respective capacity are realised, currently very common cryptographic algorithms (e.g. RSA) will de facto be broken. Even though quantum computers are still in the phase of basic research, researchers are already working on this topic in terms of data, the confidentiality, integrity and authenticity of which have to be guaranteed for a longer period. To this end, attempts are being made on the one hand, in order to develop “classic” algorithms which are resistant against attacks with quantum computers, on the other hand, quantum cryptography is using quantum mechanical properties (of photons) for encryption. In the context of the future fund (Zukunftsfonds) BSI is leading the “Quantum computer resistant cryptography and security technologies” cluster.

Side Channel Attacks Against Hardware and Software Implementation

The security of cryptographic systems primarily depends on the security of the used cryptographic algorithms and the protocols against crypto analytical attacks. The resistance of the implementation against side channel attacks is also fundamental. Side channel attacks have been studied extensively at universities and in the industrial sector for about the past ten years. Side channel attacks for instance through the running time of a cryptographic operation, try to determine the electricity consumption or the electromagnetic emission to identify a secret key. In the first few years, there was a concentration on chip cards but now software implementations have also become targets (e.g. cache-based attacks). It can be assumed that side channel attacks will also play an important role in forthcoming years.

Fault Attacks

Similar to side channel attacks, fault attacks try to make use of possible implementation weaknesses. As opposed to side channel attacks, the attacker is not just passive (i.e. only monitoring). Instead, the attacker by deliberate influences tries to provoke faulty computations in a chip card or a software implementation in order to derive the key from these faults. Fault attacks are expected to play an important role in the near future.

Random Number Generators for Cryptographic Applications

Many cryptographic mechanisms need random numbers (e.g. as session keys). Weak random number generators can decisively weaken cryptographic mechanisms which are normally resistant. Within the German certification scheme, AIS 20 and AIS 31 have for some years been mandatory. They define the evaluation of deterministic and physical random number generators. These two evaluation regulations have proven their efficiency in practical application. Central ideas of AIS 31 have been

integrated into the ISO norm 18031 “Random Bit Generation”. Groups of researchers from universities and semiconductor manufacturers regularly present new design proposals for physical random number generators.

Anti-counterfeit chip cards are part of the security-related research work at BSI.

IT-Grundschutz Days
Annual Meeting – IT Security Representatives

Record Number of Visitors at the Meeting in Berlin

Despite most enterprises and public authorities being familiar with IT-Grundschutz for some time, there is always some news to report on. BSI presents further developments and projects at congresses and trade fairs or organises its own events. In 2006 and 2007 BSI realised eight IT-Grundschutz Days with more than 1.500 participants. The first IT-Grundschutz Day 2007 on 2nd of July 2007 broke a record with 400 visitors. Among the topics were emergency management, security in a distributed IT landscape and infrastructure security. The content and the results can be read on the website www.bsi.bund.de/gshb/.

Annual Meeting of the IT Security Representatives

On September 4th and 5th 2007, around 100 IT security representatives in public administration convened for their annual meeting 2007 in Bonn. This meeting organised in a cooperation of the Federal Academy of Public Administration (BAköV) and the Federal Office for Information Security (BSI) is a platform for the up-to-date knowledge transfer and exchange of experiences. Specialised lectures deal inter alia with security products, organisational aspects in IT security, computer-related crime and anti-virus programmes for public authorities on the federal level (VSP-Bund). The annual meeting was opened by Michael Hange, vice-president of the BSI (see photo on the right).

4.1 IT-Grundschutz and High Availability Compendium

Technical issues alone do not define IT security. To a considerable extent it also depends on organisational and personnel framework conditions. BSI's work in the field of IT-Grundschutz has long since taken this insight into account. Additionally BSI is currently developing a high availability compendium, which describes specific measures of how the availability of IT resources can be maintained even in the case of an error. This compendium is especially directed at IT representatives.

Part of the IT representatives' tasks is to maintain an overview of the business processes which must be guaranteed and to maintain the respective IT as well as identifying adequate security measures and their implementation. With IT-Grundschutz, BSI developed a simple method for these tasks. With a combination of IT-Grundschutz procedures defined in the BSI Standard 100-2 and the IT-Grundschutz catalogues, BSI provides a collection of IT security measures as well as the relevant methodologies for the selection and adaptation of appropriate measures.

News from IT-Grundschutz

In order to be in line with the state of the art with regards to technology and management methods, the IT-Grundschutz catalogues and the BSI standard recommendations on information security management are constantly updated and further developed on the basis of regular requirement analysis and discussions with the users.

Currently the BSI Standards are increasingly geared towards information security as well as towards the developments in the field of risk management and data protection. The IT-Grundschutz catalogues address different topics and contain collections of precise descriptions of threats and measures which are summarised in various modules. They are constantly updated and extended. In December 2006 the 8th supplement of the IT-Grundschutz catalogues was published. This issue includes the following new modules: Windows 2003 Server, storage systems and networks, WLAN, VoIP and SAP system. The module "data bases" was totally revised in order to include new technological developments of recent years. This module includes for example a safeguard aimed at reducing risks resulting from SQL-Injections. In the first quarter of 2008 the 9th supplement will be published. The extended IT-Grundschutz catalogues will then contain topics such as electro technical wiring systems as well as IT wiring,

network printers, multifunctional devices, and mobile storage media. The catalogues as well as the BSI Standards are published in a printed version and also electronically under www.bsi.bund.de/gshb.

The IT-Grundschutz catalogues now comprise three files with more than 3.000 pages. This collection of recommendations and measures always corresponds to the state of the art in technology.

Easy Introduction: Web Courses and the GSTOOL

Many users associate IT-Grundschutz with extensive catalogues and their numerous precise recommendations for different typical IT environments. But IT-Grundschutz can also be imparted in a different way. BSI offers further tools besides the standards, for achieving an adequate security level, e.g. the web course on IT-Grundschutz which provides an easy introduction to this comprehensive topic, or the GSTOOL.

The GSTOOL supports the entire approach according to IT-Grundschutz, starting with historical data acquisition, identifying security requirements, target-performance analysis (basic security check), the implementation up to and including the resulting security revision. This also includes the ISO 27001 certification on the basis of IT-Grundschutz which designates testing the information security management as well as precise IT security measures.

After launching the slightly revised GSTOOL 3.1 in 2004, BSI provided its licence clients now numbering over 9000 with a considerably more extensive and optimised version of this tried and tested product in the shape of the 4.0 version in 2006. Among the considerable extensions of the GSTOOL 4.0 are the adaptation to the structure of the IT-Grundschutz catalogues which were fundamentally revised in 2005, the possibility of reconstructing deleted objects and the extension of the report function.

With the service package 1 (SP1) the range of functions of GSTOOL 4.0 was extended. These include the function “IT-Grundschutz management” which was realised with the kind support of Bayer Business Services GmbH. It allows for a versioning i.e. the storage of alternative file versions. With the support of the Centre for Information Processing and Information Technology (ZIVIT) the function “Multiple Standard Work Areas” was added. It has extended the possibility of various users being served by the same server, i.e. the multi-tenancy capability. In addition, a more rapid

logical and technical linking of target objects was facilitated by means of the mode “Structure Target Objects”. Currently version 4.5 of GSTOOL is being developed which allows risk analysis to be carried out. With this version, primarily the full implementation of BSI Standard 100-3 will be achieved.

The GS (Grundschutz)-Tool has been further developed according to the user’s wishes and will be available as GSTOOL Version 4.5 shortly.

Eight IT-Grundschutz Days

BSI publishes further tools on IT-Grundschutz on a regular basis. At the beginning of 2007 for example, the study “Security Properties of Dedicated Line Technologies” was published. It deals with the issue of how different offices of the same public authority or enterprise can be securely connected to each other if the technology used is based on the IT-Grundschutz component “B 3.302 Routers and Switches”. The study gives an overview of frequently applied technical solutions for the connection of different offices and the corresponding security properties. BSI presents the different updates and projects related to IT-Grundschutz at congresses, trade fairs and workshops. In 2006 and 2007 BSI organised in total, eight IT-Grundschutz Days.

The BSI's High Availability Compendium

The capacity of systems in information technology has been multiplying over the past decades. In the course of this process they have become more complex and more dynamic. This is partly due to the increasing integration of existing systems into new systems and also due to new functionalities which are added without entirely understanding the interaction with already existing components. Furthermore, IT infrastructures are increasingly made of generic software and hardware components which are produced according to the principles of interoperability and re-usability rather than high availability. A system is considered highly available if an application continues to be available in cases of faults and can continue to be used without direct human interference.

Furthermore, considering the increasing dependence of public and private life on the flawless and unrestricted functioning of information technology systems, it becomes clear how complex the challenges are which IT management is facing today. An example: After the severe earthquake on the coast of Taiwan in December 2006 access to the internet was limited for millions of people in Asia. International telephone lines were also affected as well as regional data traffic. Banks and investment firms complained about network failures. In South Korea trade with the national currency temporally came to a halt (Source: German news magazine "Spiegel", December 27th 2006, „Erdbeben bremst Internet in Ost-Asien"). These events make clear that in many places working without information and communication technologies is virtually impossible and that many business processes depend on regulated and safely functioning IT. It is not possible to avoid errors, accidents and natural disasters. Nevertheless, reducing vulnerabilities in a system in order to avoid a total breakdown is feasible.

This means: The IT resources necessary for services on a day-to-day basis have to be designed in such a way as to allow expected as well as unexpected events only to influence the availability of single components and not limit the availability of the entire system. BSI is currently developing a high availability compendium (HV-Kompendium) which describes appropriate measures. The implementation will also be part of the compendium.

The High Availability Analysis

High availability analyses (HV analyses) are an important area of risk management. The requirements of an IT system result from the analysis of the business processes in question: They define the target. The methods described in the HV compendium for the analysis of the employed IT resources facilitate an evaluation of the actual service delivery. By comparing the target and the actual service delivery the necessary measures can be deduced and the residual risk can be determined. In most cases the availability must be improved and the residual risk needs to be reduced.

A special characteristic of the HV analysis is its comprehensive approach. Service availability can only be evaluated if all IT resources contributing to the service are taken into consideration, including their interdependency. When modelling the IT resources, an object oriented approach is pursued which forms the basis of the analysis of the interdependencies. When identifying the actual service delivery, different qualitative and quantitative methods are applied according to the area and data basis being analysed.

This smooth running of IT processes requires adequate orientation to standards. Furthermore, an orientation towards different standards is indispensable for an improved comparability of the analysis results with those of other methods. The methodological approach of the HV analysis is geared to standards for IT organisation and IT systems (e.g. ITIL, COBIT, ISO, IEEE, IT-Grundschutz).

Realising High Availability

A system's availability is defined by the probability of it being available at a certain point in time in order to fulfil its tasks. This can be expressed in numbers (e.g. "99.99 per cent") or by indicating a certain level (e.g. "generally available").

Normally the task of an IT representative lies in achieving the availability level identified in the target with finite measures. The need for action resulting from the HV analysis is expressed in the compendium by scenarios, architectures and bundles of measures, each of them being classified at a certain availability level.

Basic principles of availability (e.g. redundancy, fault tolerance or robustness) are described with a hands-on orientation. It contains recommendations for the procedures and tools for the implementation. Expert knowledge from different areas (e.g. networks, infrastructure or organisation) is essential in order to realise the individual steps towards a highly available system. The publishing date of the first edition of the HV compendium, after presentation and discussion of the content with experts, is planned for 2008.

Secure Mobile Communication

Mobile telephones are constantly “online” via the mobile communication network. They are threatened by attacks via the mobile network in a similar way as stationary computers are via the internet. Without security mechanisms correctly activated, wireless interfaces such as WLAN or Bluetooth allow for data to be read or for access to the end device.

For many years BSI has been dedicated to “mobile security” and has defined precise protection measures for different application scenarios, user groups and demands for certain security requirements.

The latter have been published

- in the brochures “GSM Cellular – Threats and Security Measures”, “Wireless Communication Systems and their Security Aspects” as well as “Mobile End Devices and Mobile Applications: Security Threats and Protection Measures”,
- in the “Technical Guideline Secure WLAN” (TR-S-WLAN),
- on the website www.bsi-fuer-buerger.de,
- in the IT-Grundschutz catalogues www.bsi.bund.de/gshb/

This BSI brochure provides administrators, security officers and end users of wireless communication systems with valuable advice for the evaluation and secure use of these systems.

Under the name of SiMKo (Secure Mobile Communication) T-Systems has developed a product which facilitates the establishment of encrypted access to the government network IVBB with mobile end devices and via it the synchronisation of e-mails with the e-mail server of their own administration. For this product BSI has issued a specific application recommendation for classified information (VS) classified “Only for official use“. The synchronisation service SiMKo is constantly being updated by T-Systems. Furthermore, BSI developed a mobile telephone detector for the purpose of monitoring mobile telephones where banned, (e.g.) for example in VS conference rooms. Four separated channel receivers sequentially scan the frequency bands GSM900, GSM1800, UMTS and DECT. The device will activate an alarm if a mobile telephone connection is detected.

4.2 ISO 27001 – Certificates in Compliance with IT-Grundschutz

By providing ISO 27001 certification in compliance with IT-Grundschutz BSI created a specific type of system certification. It constitutes a combined assessment according to ISO/IEC 27001 and IT-Grundschutz.

ISO 27001 is a standard norm for information security management systems. Additionally, IT-Grundschutz catalogues and their recommendations have meanwhile become de facto standards for IT security.

The IT-Grundschutz catalogues do not only explain how information security should be designed. They also provide very precise advice on how the implementation (including technically) could work. A procedure according to IT-Grundschutz is a proven and efficient possibility of meeting all requirements according to ISO 27001. An ISO 27001 certification in compliance with IT-Grundschutz is with respect to testing concrete security measures considerably more convincing than a basic ISO 27001 certification.

The series of standards ISO 270xx includes different ones, some of which are still under development. Out of this series the standard ISO 27006:2007 “Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems” came into force in March 2007. It deals with the requirement of the authorities issuing certificates according to ISO 27001. BSI has implemented these requirements and therefore some minimal changes to the certification scheme have been made. For example, the lengthening of the validity to three years with annual monitoring audits or the possibility of performing a pre-audit. Further information and a list of all certificates are available under www.bsi.bund.de/gshb/zert/.

4.3 Introducing Technical Guidelines and Conformity Evaluation

By developing Technical Guidelines BSI aims to define technical requirements for the development, application and evaluation of secure and interoperable IT solutions.

Technical Guidelines (TR) describe functional and qualitative requirements regarding IT products and systems which are fundamental to their interoperability, integration and security. They are developed by BSI in close cooperation with the industrial sector and the business community as required. The necessity for TRs arises from national security requirements or public interest.

The relevant provisions particularly affect IT products and systems which are intended for application in sovereign and therefore security critical areas of the Federal Republic of Germany. Interoperability apart, requirements regarding electronic protection against counterfeiting and operational reliability are of particular priority. Initially, these guidelines have the formal status of recommendations. They are binding however, when required in calls for tender, explicitly demanded by the user for their area of responsibility or when mentioned specifically in a law or any form of legal regulation.

Technical Guideline for Electronic Passports

For the production of electronic passports the applicant's data, has to be registered in adequate quality with the authority responsible (e.g. the local registration office) and has to be transferred to the passport manufacturer. The Technical Guideline on the registration, quality inspection and transmission of production data for passports (TR-PDÜ) is considered binding for all technical systems which are employed to this end.

Evaluation Criteria for Electronic Travel Documents

Ensuring international interoperability of the passports and the corresponding passport readers turned out to be the greatest challenge in the introduction of electronic documents. The technical guideline on electronic passports (TR-ePass) defines evaluation criteria which ensure interoperability.

Conformity Evaluations according to Technical Guidelines

Within the extension of its accreditation and certification activities, BSI has since 2006 been offering a so called “certification according to technical guidelines”. Manufacturers and distributors can have the conformity of their IT products and systems confirmed by a BSI certificate. Prerequisite is a successful conformity evaluation. Conformity evaluations ensure that an IT product or system correctly and completely fulfils the requirements of the respective TR from BSI. Technical Guidelines also provide all evaluation regulations and specifications relevant for conformity evaluation. Independent evaluation facilities carry out the evaluation. They are accredited by BSI and have demonstrated their technical competence to the accreditation authority of BSI.

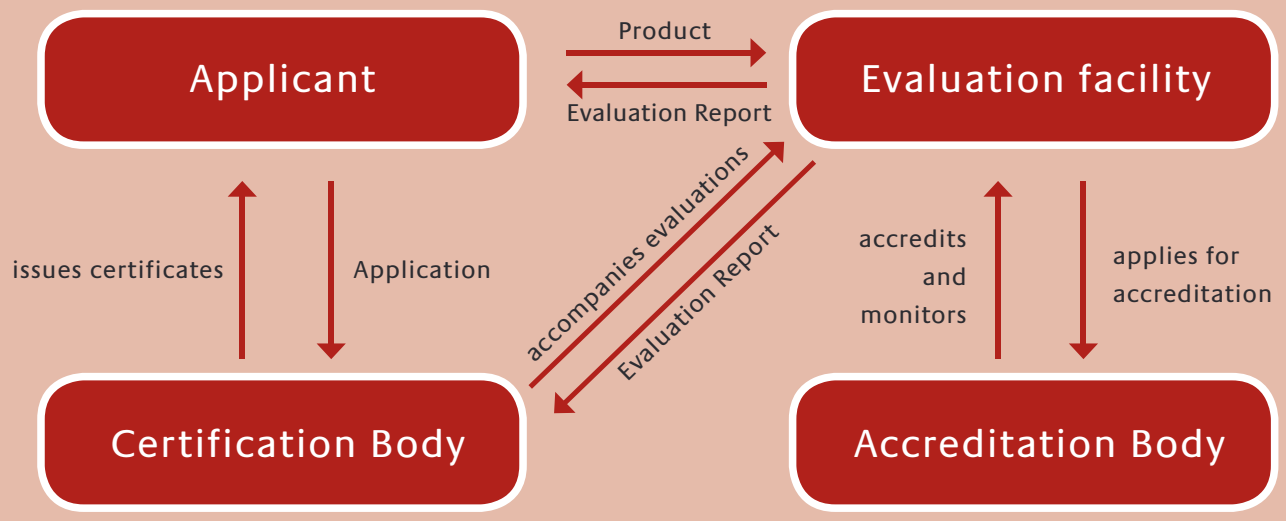
As of November 2007, the holders’ finger prints will be registered on the electronic passports of the Federal Republic of Germany. In order to ensure adequate quality of the finger prints only optical sensors which have been certified according to BSI’s TR (technical guideline) 03104 may be used. Among the certified sensors are the finger print scanners produced by Cross x displayed below.

Accrediting Evaluation Facilities

The successful introduction of new technical guidelines and the corresponding conformity evaluations in 2006/2007 was actively accompanied by the accreditation of new evaluation facilities. The accreditation of appropriate evaluation facilities is a central element of the certification. Apart from demonstrating their technical competence, it has to be ensured that an evaluation facility fulfils all requirements to be able to carry out independent, objective and high quality evaluations. In this context, an operational quality management system according to DIN EN ISO/IEC 17025 is essential. An evaluation facility is accredited by BSI and is allowed to carry out conformity evaluations only after providing all the necessary evidence.

As early as September 2006 the accreditation of “CETECOM ICT Services GmbH” as an evaluation facility for electronic travel documents (TR-ePass) was finalised. In 2007 “Fraunhofer Institut für Angewandte Optik und Feinmechanik” in Jena (TR-PDÜ) as well as the test centre “Secunet Security Networks AG”, Essen (TR-ePass) followed. Further evaluation facilities for different areas regarding TR-PDÜ and TR-ePass are in the accreditation process.

Certification According to Technical Guidelines



The diagram shows the parties involved in the certification process and their corresponding tasks according to the technical guidelines.

Certificates and Technical Guidelines

Based on the introduction of the electronic passport (ePass phase 2) on November 1st 2007 the introduction of conformity tests according to technical guidelines was quickly accepted by manufacturers of the respective IT products. Therefore numerous certifications could already be completed by September 2007. Amongst others, the conformity of a total of seven fingerprint sensors according to TR-PDÜ was confirmed with certificates. Not only national but also European and international manufacturers are showing interest in the technical guidelines and the BSI's new certification scheme.

4.4 Field of Technology “Official Documents”

In 2006 and 2007, BSI worked continuously on its projects on official documents. Field experiments paved the way for the practical implementation of biometric systems. Since 2007, the second generation ePass has been issued whereby two fingerprints are saved additionally on the passport chip.

Passport with Biometric Properties – ePass

On the 1st of November 2005 Germany introduced the electronic passport (shortform ePass). The first biometric feature saved on the passport was the facial image of the passport holder. According to the EU regulation in question two fingerprints must also be saved on the ePass chip. New passports as from November 1st 2007 already comply with this requirement. BSI contributed considerably to the formulation of technical specifications on boards of organisations such as the International Civil Aviation Organization (ICAO), the International Organization for Standardization (ISO) and the EU. BSI’s main task was the realisation of the IT security concept of the new ePassport. As central point of reference for all technical issues, BSI is operating an ePassport hotline which can be contacted daily between 8 a.m. and 5 p.m. under +49 (0) 1805 27 43 00.

Registration of Passport Applications

With the Technical Guideline for production data acquisition, -quality testing and transmission for passports, BSI has presented an entire body of regulations from the registration of application data of the applicant via the quality assurance of the biometric data to the transmission of the data. Furthermore, in cooperation with the Federal Police Office BSI developed a procedure which guarantees a high quality fingerprint registration. The software components developed by the passport manufacturer were tested and optimised in a field test. This guideline became binding for all involved authorities by the decree for passport data acquisition and transmission (PassDEÜV).

Certification of Fingerprint Sensors

High quality is required for the registration of the fingerprints of the passport applicant, otherwise they will not be unequivocally verifiable. For this reason BSI designed a special certification programme for fingerprint sensors which independent of the manufacturer, measures the quality of the sensors. Only certified sensors can be used for the registration.

Biometrics in Border Controls

In the context of ePassport and VISA, BSI has entered into a cooperation with the federal police on various pilot projects testing the processing of biometric data at border checkpoints and in mobile contexts. The objective is to develop a mechanism for the implementation of biometrics-supported border controls.

Extended Access Control – Protection of Particularly Sensitive Data with ePass

For reasons of data protection, the fingerprints which have to be saved besides the facial image on the EU passport must be particularly well protected. To this end BSI developed the Extended Access Control Protocol (EAC). According to the decision of the EU commission, the application of this protocol is binding for the passports of all member states. The EAC protocol requires an authentication mechanism for the authentication of the so called radio frequency chip (RF chip) on the ePassport as well as for the passport readers. The reader is equipped with a special pair of keys and a certificate verified by the RF chip defining which data can be accessed. This guarantees that the readers will only be able to access data for which they have been legitimised.

For the planned electronic identification card BSI extended the EAC specifications by additional functions and protocols. In the next version e.g. with the "online authentication" a secure and data protection friendly authentication of the user can be carried out via the internet.

By means of biometrics-supported border controls the misuse of genuine documents by unauthorised individuals who resemble the passport holder (so called look-alike-fraud) can be prevented.

PKI Structures for the ePassport

For the production of ePassports, BSI as superior certification authority for the digital signature (Country Signing Certification Authority – CSCA) provided the pass manufacturer (the Bundesdruckerei GmbH) with Document Signer Certificates (DS). The manufacturer is therefore able to protect the data saved on the RF chip of the ePassport with a digital signature against later falsifications or manipulations. At the same time in November 2007, BSI became the superior certification body for readers in the context of the ePassport (Country Verifying Certification Authority – CVCA). In this capacity, BSI provided the bodies authorised for the reading of fingerprints in Germany and abroad with Document Verifier Certificates (DV).

Protection Profiles for ePassports

BSI certifies the RF chips integrated into the ePassports according to the so called protection profiles (PP). They describe the security criteria which must be complied with. The RF chips intended for German passports were certified according to the new PP of the Technical Guideline EAC. The security criteria of these Protection Profiles are applied Europe-wide for the testing of ICAO-conform chips.

The “Golden Reader Tool”

The “Golden Reader Tool” (GRT), the development of which was commissioned by BSI is a software application for the reading of ICAO-conform machine readable travel documents (eMRTD). With the GRT, BSI aims to create the conditions for worldwide interoperability in the field of eMRTD based on ICAO requirements. The Golden Reader Tool is constantly updated and has already become the international standard for the reading of ePassports.

In November 2005 the electronic passport (ePassport) was introduced in Germany. It contains a digital passport photo on the passport chip as the primary biometric feature. The second generation ePassport has been issued since 2007; additionally it contains two fingerprints on the chip. With this new technology, the highest level of protection against falsification and misapplication has been achieved.

4.5 Middleware – Specifications for Electronic Application Projects

On March 9th 2005 the federal cabinet approved the outlines of a common eCard strategy. It summarises the different card and application projects of the federal government i.e. electronic passport (ePass), electronic identity card, electronic health card (eGK), electronic income statement (ELENA) and electronic tax return (ELSTER). For the business community and public administration this constitutes a considerable innovation leap.

The objective in this context is to create uniform standards, use synergy effects and to guarantee the interoperability between the different applications and technologies. In accordance with the eCard strategy of the federal government and in cooperation with the relevant public authorities and the remaining market participants under the auspices of BSI, a specification for an eCard API framework was therefore developed. With the framework it was also fundamental not only to take into consideration the "official" card projects but to also include the (signature) cards issued by the business community.

Standards Required

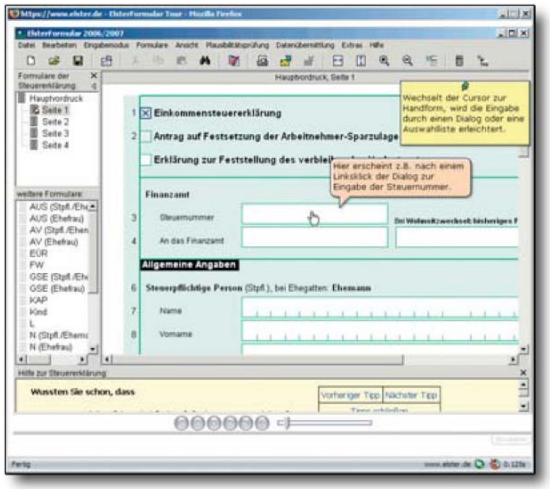
An analysis of the already established standards in the market concluded that none of the standards was able to cover all necessary requirements. Some of them displayed grave security deficits, others required certain operating system platforms and yet others required detailed technical knowledge about Smart-Card-Technology on the part of the application developer. In order to be able to make use of the advantages of the common eCard strategy it had to be guaranteed right from the beginning, that on the side of the developer, the framework could be activated with minimal effort and that the end user can apply the resulting solution intuitively if possible. The result was a layer model which uses webservices. It goes without saying that existing standards insofar as they could be implemented sensibly, were retained. High level interfaces were introduced in order to facilitate the application developers' work and consequently to promote the use of Smart-Cards. In cases where standards had to be extended, the change was carried out with caution – but from the beginning, always in cooperation with the responsible bodies at national, European and international level (e.g. DIN, CEN und ISO).

The software architecture laid down in the BSI's technical guideline ensures that in future, manufacturers will have to carry out costly and time consuming reconfirmations according to SigG/SigV less frequently.

A challenge for IT security: Eventually, 80 million persons with medical insurance will be provided with an electronic health card. The card which is issued by the approximately 200 existing health insurance companies will link 21.000 pharmacies, 123.000 doctors working in the community, 65.000 dentists and 2.220 hospitals. Tests with real data are being conducted in three regions of Germany. For more information on the electronic health card consult: www.die-gesundheitskarte.de

Manufacturers can prove Conformity

In the meantime the specifications resulting from the work have been published as Technical Guideline BSI 03-112. Manufacturers who have implemented this technical guideline entirely can, by means of special tests, prove the conformity of their solutions and when all requirements are fulfilled will be granted a corresponding seal of approval. The same applies to application software and hardware producers. Consequently, if all components have been tested successfully, the end user can be sure that the card, the reader and the software will function together smoothly. In future the end user will not only be qualified to sign electronically – this is possible already – but will also for example, be able to identify him- or herself electronically in an online shop with their ID or can obtain a medical prescription stored on the health card at an online pharmacy. BSI in its role as a public authority will not provide any implementation measures for the technical guideline in order to avoid distortions of competition in the market. Commercial suppliers have already announced the launching of corresponding products.



The software ELSTER provides the opportunity of electronically transferring tax returns to the tax authorities via the internet.

“Innovation Driver IT Security”

was the motto of the 10th German IT Security Congress which was organised by BSI from May 22nd until May 24th 2007 in Bonn-Bad Godesberg. In his opening speech the Federal Minister of the Interior Dr. Wolfgang Schäuble said: “Increasingly IT security is developing into the key factor of a future-oriented security policy. Every user must take on responsibility. We need an IT security culture within which all users act responsibly.” In the future, BSI as the only state IT security authority will have to guarantee IT security internally and externally.

At the congress, the diverse developments and aspects in IT security were analysed in lectures, round tables and in an exhibition accompanying the event. The booklet on the 10th German IT Security Congress was published by the editor SecuMedia-Verlag and can be ordered at http://buchshop.secumedia.de.

5.1 Citizens' Portals – an Infrastructure for Secure Communication

The project Citizens' Portal aims at providing a secure communication infrastructure for citizens, enterprises and public administration. One of its main goals is enhanced usability for all parties involved. This project is one of the core elements of the programme E-Government 2.0 of the Federal Government. It belongs to the four fields of federal action which aim at driving forward e-government in order to modernise public administration and Germany as a location. BSI contributes considerably to the conceptual design of this project.

Today, the running of public administration, the business community and our society is unimaginable without electronic communication. The internet opens up global communication spaces. However, using the internet is heavily flawed with respect to security aspects. The causes for this are a lack of trust, the insecurity of involuntarily giving away personal data or the feeling of being spied upon by an outsider when establishing electronic connections.

In principle the following can be stated: Confidentiality and the legally binding effect of communication are not guaranteed in open networks. Furthermore, proving certain actions is difficult, authentication is complicated and there might be a dangerous spam, worm or phishing attack hiding behind an apparently harmless e-mail. Problem-specific solutions already exist, however they are generally very complex and find little acceptance. The modern state therefore is confronted with the task to provide a basic level of security, liability and trust in the electronic communication space. State regulation can and does not have to mean the construction of an own infrastructure. The state can limit itself to defining regulations and to monitoring their compliance, if a basic security level is achievable by these means. With the project Bürgerportal (Citizens' Portal) the Federal Government is adopting this approach and is developing a concept for secure communication for all internet users.

Apart from information on organisations and on IT applications in e-government, this loose-leaf information collection which is constantly being extended, also and especially contains IT security related recommendations.

The Concept of Secure Electronic Communication

Citizens' portals should provide a secure place within the internet not just to citizens but also to users from the business community and public administration and should also facilitate confidential communication via the internet. Therefore documents and data after having been transmitted by the user via an authenticated and encrypted communication channel to his or her citizens' portal, are then transferred integrity protected and encrypted to the citizens' portal of the recipient.

Immediately before the transmission of the data to the recipient, the citizens' portal decrypts the data, verifies its integrity and sends it to a client application of the user via an authenticated and encrypted communication channel. The communication between different citizens' portals is realised encrypted and signed in the same way as within a single citizens' portal. Several providers may provide citizens' portals which differ from each other, offering extra services beyond the basic ones. The existing citizens' portals will be linked in a citizens' portal network in order to provide the basic services beyond the border of the individual portals as well. The users in this network are acting within a "closed user group", hence within a particularly protected area.

Basic Services

The aim is to facilitate confidentiality and to bind the communication in the case of the unequivocal address given. For this purpose, the citizens' portals are required to offer the following services:

- The account is available to the user as an electronic letter box. With this account, the user can receive, save and administer electronic messages. The account can be accessed by a unique electronic citizens' portal address which clearly identifies the individual citizen. To send electronic messages reliably, the user can use a mailing service. Via this service it is possible to prove if, how and when the message was delivered.

- To send electronic messages reliably, the user can use a mailing service. Via this service it is possible to prove if, how and when the message was delivered.

- The documents safe can be used for long term storage and administration of electronic documents.

- The authentication service carries out a reliable authentication for third parties whom the user wishes to contact.

Whoever wishes to make use of these services must be registered. For this procedure the person must be indisputably identifiable for the provider. Then the user will receive an unequivocal citizens' portal address in the form of an e-mail address. For the login to the citizens' portal account, the user will be able to choose from different authentication mechanisms with different authentication levels.

The future electronic ID-card can also serve as an authentication mechanism. The synergy potentials of the different e-government projects of the federal government are therefore also taken into consideration during the conceptual development. The users should be able to access the services of the citizens' portals with standard software. For this reason standard e-mail clients are supported for the access to the accounts and for sending messages via e-mail. Furthermore, access to the services will also be possible through a web browser via a web portal.

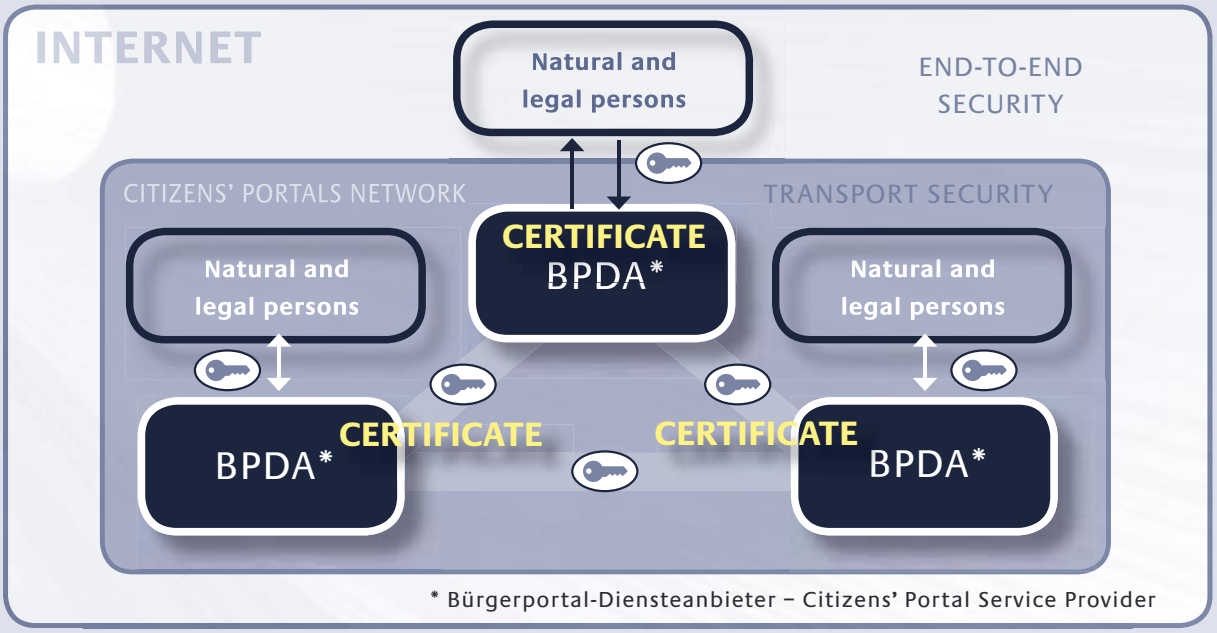
Trust through Security and Certification

It is essential for the success of the citizens' portals that they guarantee the security they promise. The basis for this is an adequate IT framework security concept which involves every aspect that is relevant for the infrastructure.

As a result: The concept must also take into consideration the application environment and the type of use. An IT framework security concept requires a comprehensive analysis of the risks and the protection needs. It defines requirements for the implementation of security targets and recommends practical measures.

The objective of the IT framework security concept for which BSI is responsible, is to facilitate an adequate security level for potential providers leaving enough scope for an individual organisation of the application environment. Thus, the providers have the opportunity of using or adapting the existing infrastructure. This way the most efficient approach can be identified by the businesses themselves. An important part of the trust in these services lies in the fact that all providers guarantee a transparent and comparable level of security. In a certification procedure they must prove the trustworthiness of their mechanisms and processes to an independent body. Apart from IT security, the functionality and interoperability of the services, data protection and consumer protection are analysed in this process. A certificate proves the conformity of the citizens' portal with the requirements and displays to the user that he or she can trust the service. Apart from the areas of data and consumer protection, the certification procedure, which is also the responsibility of BSI, should – if possible – be based on existing certification schemes.

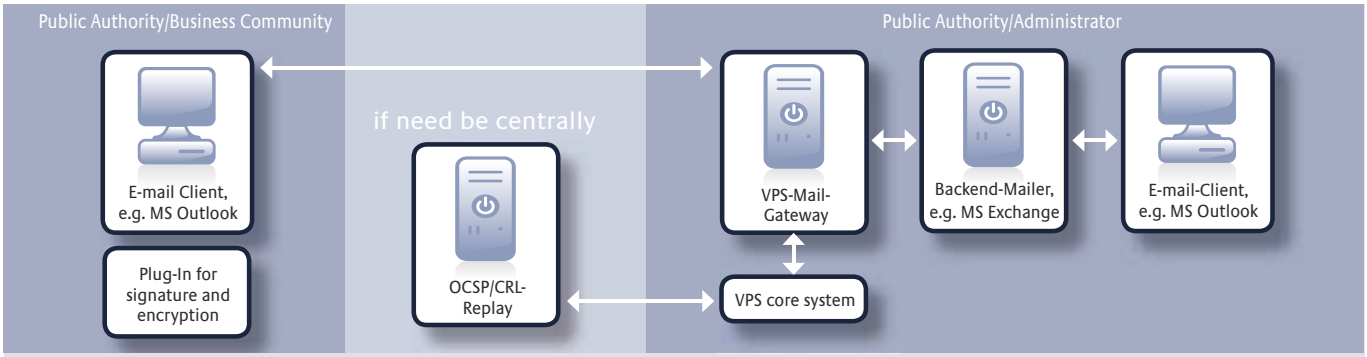
Citizens' Portals, Secure Communication Space



Citizens' portals must achieve defined security targets regarding

- Confidentiality
- Authenticity
- Integrity and
- Reliability.

The IT security certification according to ISO 27001 for example, should be carried out on the basis of IT-Grundschutz. Corresponding adaptations are only made where citizens' portal-specific properties require this. In brief, it can be stated that BSI contributes to the project with its core competencies by taking on the responsibility for the security and certification concepts. It therefore contributes considerably to the implementation of the vision of a secure and reliable infrastructure for a confidential and legally binding electronic communication.



VPS – the Virtual Post Box of the Federal Government

The virtual post box of the Federal Government (VPS), as a result of BundOnline, forms the basis for secure communication in e-government. The partial component VPS-Web has successfully been evaluated according to Common Criteria.

Since the end of 2007 the VPS, which was so far able to be applied on the basis of a manufacturer's declaration for qualified signatures according to the German signature law (SigG) has been equipped with a seal of approval of an approved signature application component. The e-mail component VPS-Mail ("Julia") is currently being used in 61 public authorities. Furthermore the process of the accreditation of the VS-NfD-mails has been started by BSI. Nevertheless "Julia" can already be used for the encryption of VS-NfD-Mails until the accreditation is finalised.

In the case of the software appliance Trusted VPS, BSI provides a secure complete solution for modern e-government which is particularly convincing due to its simple installation and administration and extends the VPS by a complete security concept. Interested users can order the VPS Live-CD via BSI which facilitates a simple test run of the VPS.

5.2 The Fund for the Future and New Technologies

The Fund for the Future (Zukunftsfonds) provides BSI with the opportunity of carrying out their own applied research in different technology fields. This fund is the basis for an IT security research programme, which is allocated funds amounting to 36.5 million Euros for a running time from 2006 until 2009.

Intensive IT security research is indispensable, in order to cope with the changed threat situation and to face the threats resulting from new technologies early enough. By involving BSI at an early stage in all new issues related to IT security in Germany there is a good chance of acting in good time instead of reacting dictated by the threat situation.

BSI Programme on IT Security Research

The funds for the IT Security Research Programme (Fund for the Future) are from the six billion Euro innovation programme of the Federal Government. New innovations in following technology fields

- Internet Early Warning Systems
- Trusted Computing as well as
- Biometrics and ID systems

are under construction.

Within this research work the following priorities are being analysed:

- **Development of Prevention Technologies for the Defence against New Types of Attacks via the Internet**

  In order to achieve the objective of preventive identification and defence against threats in the field of IT, BSI is conducting research work for new solutions. Its aim is to automatically detect security gaps during the manufacturing or use of software. It will therefore be possible to detect these gaps already in the development or before being used in security relevant areas.

- **Development of Innovative Technologies for Secure Internet Use and Data Exchange**

  The aim is to protect linked IT landscapes from hackers and malware from the internet. To this end, technologies and tools are to be developed which detect dangerous or falsified e-mails and websites as well as protecting against viruses and malicious codes.

- **Quantum Computer Resistant Crypto Mechanisms and Security Technologies**

  Alternatives to existing mechanisms (e.g. quantum cryptography) and new solutions for future application scenarios (e.g. multipoint communication) are to be identified, implemented with prototypes and hardened with regards to security. At the same time, the relevant applications will be prepared for the necessary migration.

- **Early Warning of IT Attacks for the Protection of Information Infrastructures**

  The aim is research on IT early warning as a basis for the development of IT early warning systems (IT-FWS). Another aim is the development of sensors and evaluation systems (soft- and hardware) which can identify IT attacks and malware as early as possible in order to develop counter measures and to warn the users.

- **Research, Development and Further Development of Trustworthy and Self-Protecting IT Systems**

  PC clients, server and mobile devices can be secured by means of software but also in the form of extra hardware, such as standardised security chips (TPM). The open necessary conditions in terms of architectures, network components, operating systems as well as applications for trustworthy and highly available IT systems of existing solutions (TPM) are to be analysed. At the same time also, soft- and hardware components are to be developed as alternatives to the TPM for the production of a secure IT platform.

- **Highly Secure Processor Platform for special IT Components**

  So far, modern security architectures (Mikrokernel-/Hypervisor integration, Smartcard-/TPM integration, protected memory areas, etc.) are only available for PC platforms. Within this programme they are to be realised also for embedded processor platforms.

- **New Mechanisms for Identification and Localisation**

  Besides the necessary approvements in the field of biometric authentication and the respective spoof protection mechanisms, the combined use of different biometric identifiers is expected to increase the level of security even further. The aim of the project is to evaluate existing technologies and to develop and implement new approaches for fake and live detection mechanisms, human detection and the enhancement of privacy protection.

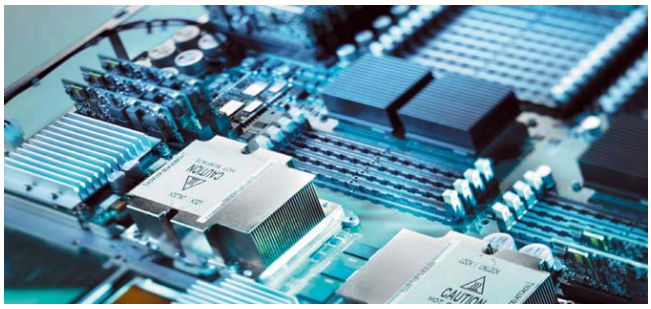
- **Development of Innovative Contactless Security Tokens for a Broad Use**

  The project aims to investigate and test new basic technologies for contactless security tokens. To this end new displays together with innovative cryptographic concepts are to be combined to contactless security tokens. This promotes a considerable increase in IT security and convenience. Furthermore, innovative contactless authentication mechanisms are being developed.

- **Security Architecture for Micro-Sensor Networks**

  The aim is to develop a broadly applicable security architecture for sensor systems focussing on secure sensor identification and communication. Based on a field experiment, a security architecture for micro sensors and actors is to be developed.

Sustainability



IT Security research will lead to new security technologies in sensitive fields. For BSI, the sustainable effect of the results of IT security research is of fundamental importance. So, besides the development of new security technologies, guidelines and testing requirements are engineered as well. This will constitute a huge step forward in the promotion of IT security in Germany. This approach further implies: IT security research can become an excellent export promotion instrument of German IT security technology.

Heads of Division and Contact Persons

President

Dr. Udo Helmbrecht,
President of the Federal Office for Information Security

Vice President

Michael Hange,
Vice President of the Federal Office for Information Security

Department 1

Dr. Hartmut Isselhorst,
Head of Department 1 – Security of Applications, Critical Infrastructures and Internet

Department 2

Dr. Gerhard Schabhüser,
Head of Department 2 – Cryptology and Counter-Eavesdropping

Department 3

Bernd Kowalski,
Head of Department 3 – Certification, Accreditation and Conformity Tests, New Technologies

Department Z

Horst Samsel,
Department Z – Central Tasks

Public Relations

Anja Hartmann,
Head of Information, Communication and Public Relations Division
E-Mail:
anja.hartmann@bsi.bund.de

Press Officer

Matthias Gärtner,
Press Officer
E-Mail:
matthias.gaertner@bsi.bund.de

Imprint

Federal Office
for Information Security

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
P.O. Box 20 03 63, D-53133 Bonn, Germany
Phone: +49 228 99 95 82-0
E-Mail: publikationen@bsi.bund.de
Internet: www.bsi.bund.de

Text and editorial staff
Sebastian Frank, BSI; Volker Thomas, Thomas Presse & PR

Translation
Isabel Meyke, Berlin; Sebastian Frank, BSI

Layout & Design
Thomas Presse & PR, Berlin/Bonn
Graphics: Annette Conradt, Pierre Boom; Screen-Version: Ludwig Lang
Phone: +49 30 21 99 66 16
E-Mail: info@thomas-ppr.de
Internet: www.thomas-ppr.de

Picture Credits
AVM GmbH, Berlin Partner/FTB-Werbefotografie, BMI/Photothek, Pierre Boom, BSI/Referat Öffentlichkeitsarbeit, Bundesanzeiger Verlagsgesellschaft mbH, Bundesbildstelle, Bundesdruckerei GmbH, Bundesministerium für Gesundheit (BMG), Cross Match Technologies GmbH, Deutsche Bahn AG, Elster/Bayerisches Landesamt für Steuern, Andreas Ernst, Fujitsu Siemens Computers GmbH, istockphoto, LinuxTag e.V., Messe Essen GmbH, Messe München GmbH, Polizei Mettmann, OHB-System AG, Reed Exhibitions Deutschland GmbH, Rohde & Schwarz GmbH, SecuMedia Verlags-GmbH, Security Networks AG, Sony Ericsson Mobile Communications AB, Studio Koslowski/Bundesnetzagentur, SWR Media Services GmbH, Günter Wicker/Berliner Flughäfen, Xilinx Inc.

Date
June 2008

This file is part of the public relations work of the German government. It is distributed free of charge and is not intended for sale.