Federal Office
for Information Security

Annual Report 2003

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

The Federal Office for Information Security (BSI) is the central IT security service provider for the German government. To promote IT security in Germany, the agency advises and supports several different target groups: IT manufacturers and users, data protection officers, security consultants, experts, testing agencies, research establishments and standardisation bodies.

Implementation of its own security products, trend research and collaboration with international organisations are other important areas of its work. In addition, as a certification authority and accreditation body, the BSI develops criteria, methods and tools for the evaluation of the security of IT systems.

Private PC users also profit from the work of the BSI. Up-to-date information about possible threats and protective measures can be obtained from a special website. Well over a million copies of a CD-ROM compilation of the main content have been distributed through various teaming partners. Precisely because information technology increasingly affects every aspect of our lives, IT security for the public is one of the BSI's primary concerns.

This Annual Report 2003 presents the main activities, functions and work of the Federal Office for Information Security BSI for the first time in a single publication. The report provides an overview of major developments at the BSI during 2003.

Services of the BSI

Information

- Education and awareness raising of the public
- Future and trend analysis

Consultancy and support

- IT Baseline Protection, IT security consultancy to government agencies
- E-Government and the BundOnline 2005 initiative
- Protection against bugging and emission security, Penetration testing
- Support to data security officers
- Support to law enforcement agencies

Risk analysis, testing and assessment

- Malicious programs, Internet security analyses
- IT platforms, Critical Infrastructures
- Biometric procedures, Mobile applications
- Certification of IT products and systems
- Licensing of products for classified applications

Development

- Evaluation and development of crypto-equipment
- Security tools, Formal security models

Operations

- German CERT (Computer Emergency Response Team)
- Technical co-ordination of the Berlin-Bonn Information Network (IVBB), Government administration PKI
- Production of key material for crypto-equipment

Committees

- Active role on national and international committees and standardisation bodies for Germany

Annual Report 2003

Federal Office for Information Security (BSI)

www.bsi.bund.de

Test, assess, research and protect – the BSI Annual Report

Dear readers,

the age of globalisation depends on information technology. With its huge potential, IT has made possible enormous change in recent years, both economic and social, that would never otherwise have occurred.
As a result, reliable and powerful information technology is today a critical element of the basic infrastructure of any modern industrial nation. Its protection is a matter of national security.

As President of the Federal Office for Information Security (BSI), I took over a committed and successful government agency in 2003. I started my new job with the aspiration of not only following previous developments but expanding and developing them further as well. As the German government's central IT service provider, we have an enduring commitment to the security of information technology in Germany. Risk prevention, quality monitoring and certification of IT products and comprehensive IT baseline protection are our foremost priorities. In this way the BSI is the guarantor of IT security in our society.

The BSI can be proud of its many accomplishments. This annual report provides an impression of the variety of fields in which it is actively engaged.

The special challenge it faces today is to perform many different tasks simultaneously. Its terms of reference are extremely wide: it has to address not only meteoric rates of advance in technology but also the enormous market-economy importance of IT security.

The BSI also contributes to Germany's overall domestic security. Our goal here is to play an active role in shaping developments in security in the information society. Thus, the

BSI will continue to play a leading role in IT security-related matters in Germany as it works together with both public administration and industry.

Anyone who accepts the challenge of organising the protection of modern information technology must adapt to its diversity and dynamics. The spectrum of our activities includes informing and raising the awareness of the public on IT security matters, quality monitoring and the certification of products against international criteria, supporting the Bund-Online 2005 initiative, developing cryptographic products and running CERT-Bund (the Computer Emergency Response Team for German federal government institutions) – to name but a few examples of our activities.

Arising from quite different areas of work, we have close relationships with everyone involved in information technology: the BSI maintains a lively exchange of information with both IT users and IT security providers. Here, the BSI assumes the role of a trusted agency that provides direction. Its position as a neutral specialist agency allows it to examine threat scenarios and protective measures independently of any particular interest.

The success of the BSI would not be possible without its motivated and committed workforce. I would like to offer them my special thanks.

Bonn, March 2004

President of the Federal Office for Information Security (BSI)

Content

Content

History

Staying in touch: it can also be done with a piece of string and two empty cans – the "tin can telephone".

Growing with the job

Information technology (IT) is changing rapidly. For years, the capability of individual systems has been rising in an exponential manner. Innovative products are pushing their way onto the market, replacing or supplementing existing solutions. In the search for ever better products, technical development may be systematic in individual cases, but in the wider context it is spontaneous and uncoordinated.

The result of this process are ever more powerful IT systems. At the same time technological islands develop, along with competing standards and incompatible networks. Today the complexity of information technology has attained proportions that are difficult to grasp.

At the same time information and communications technology (ICT) has developed into an unparalleled driving force in modern life, both economically and socially. Against this background, making IT secure is not just a complex task but one that is critically important. In Germany this responsibility is borne by the Federal Office for Information Security (BSI).

The BSI was founded in 1991 in Bonn and is one of the divisions of the Federal Ministry of the Interior. To fulfil its statutory mission of looking after IT security, the BSI has to keep up with the pace at which information

and communications technology develops. In certain areas, the BSI even defines the direction and pace itself. New areas of responsibility, new key topics and the requirement to always keep abreast of the latest developments – all this naturally requires resources. Consequently, as information technology has developed generally, the BSI has grown in size both in its workforce and in its funding.

The multi-layered nature of problems in the area of IT security means that the spectrum of tasks facing the BSI is complex.

Past and present presidents of the BSI: founding president Dr. Otto Leiberich (right), his successor Dr. Dirk Henze (left) and the present president Dr. Udo Helmbrecht.

Task spectrum of the BSI

Testing and assessing the security of IT systems

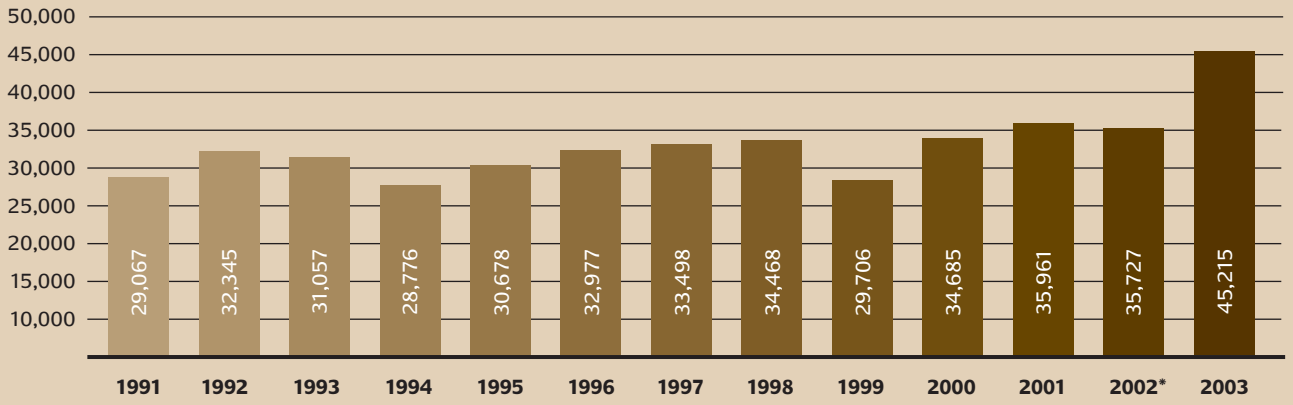
Evaluation and certification against international criteria makes the security capabilities of products transparent. In the struggle to hold one's own in hotly contested markets this is an important weapon; if a company wants to be an approved supplier to customers in government and industry which handle classified material, it is essential.

Development of IT protective measures

The BSI itself develops and markets IT security systems, ranging from products for handling classified information through to administration tools for UNIX and the implementation of IT Baseline Protection. Some of these products are developed in close collaboration with partners from industry.

The BSI's budget 1991 to 2003

(in thousands of euros)

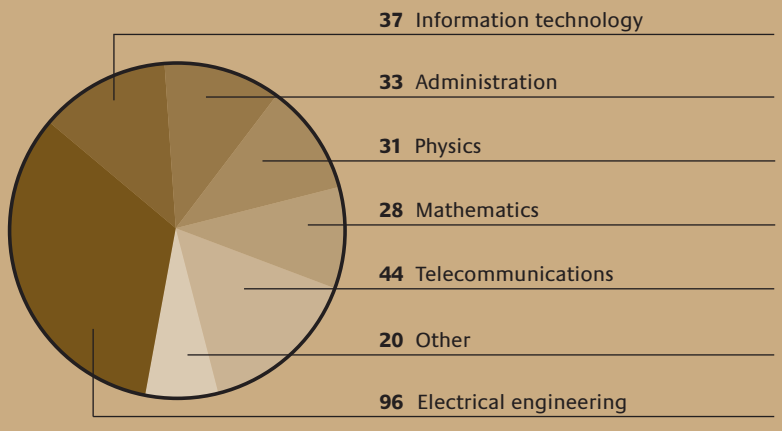


* In 2002, the BSI received an extra E 10,7 million for the purposes of fighting terrorism.

Since the foundation of the BSI in 1991 its budget has risen by over 50%. This mirrors the growth that has taken place in its areas of activity.

Fields of specialisation at the BSI

Number of staff in senior and executive grades



The complex structures of information technology require above all staff with a scientific educational background. However, the complex links between information and communications technology (ICT) and every aspect of daily life mean that there is also a need for several other disciplines, notably lawyers, administrative scientists and economists.

History

Consultancy to manufacturers, distributors and users of IT systems

The BSI's information and consultancy services are directed at private home users, those responsible for IT in government agencies, companies and manufacturers of IT products. This ensures that all those involved in the development and use of systems can pay heed to IT security considerations right from the start.

Involvement on international committees

The BSI represents and supports Germany's interests with regard to IT security through its committee work, for example in NATO and the EU. The influence of the BSI is applied with the aim of avoiding undesirable developments, promoting the exchange of information and nurturing international contacts.

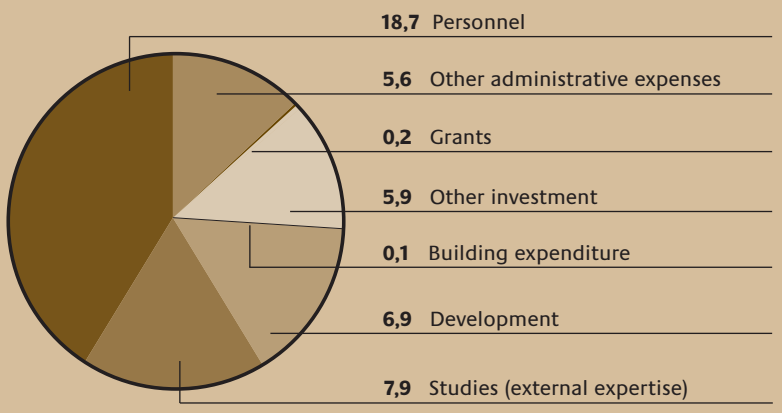
Trend research and project work relating to new technological approaches

The timely and as accurate as possible prediction of future developments allows for prompt and prudent action to be taken. For this reason the BSI is involved in working teams and projects covering all the major aspects of IT security in the future.

These include Open Source software, IT implementation in biometric systems and the activities of the Trusted Computing Group (TCG). The aim of this industrial alliance is to develop a Trusted Platform Module (TPM) security chip to protect different IT devices, e.g. PCs, smart phones and PDAs.

Contact persons in the BSI. From left to right: Anja Hartmann, head of public relations, Michael Dickopf, press officer, Dr. Udo Helmbrecht, president of the BSI and Michael Hange, vice president.

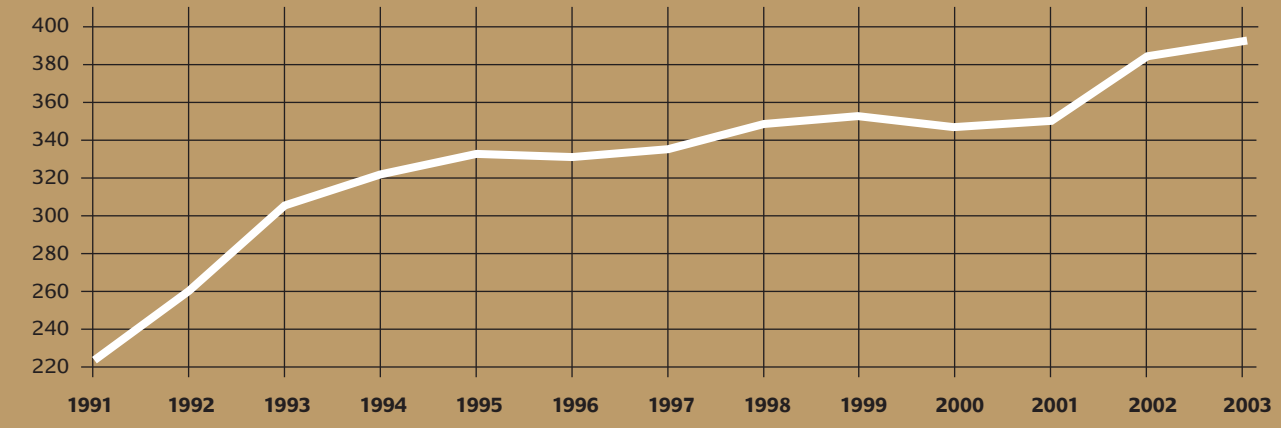
Breakdown of expenditure at the BSI by category
(in millions of euros)



The second-largest item in the budget after personnel (D 18,7 million) is studies and development which, at D 14,8 million, accounts for 33%.

With the expansion of BSI's fields of activity and the complexity of individual tasks, the number of staff has risen steadily. The rapid tempo at which information technology develops requires total commitment from the workforce. In 2003, in addition to the BSI's normal business, there were over 200 ongoing projects to be supported and driven forward. Despite the heavy workload, the dynamic and varied environment offers a stimulating working atmosphere.

Number of BSI employees 1991-2003



With its range of offers, BSI sees itself primarily as an IT security service provider for the German government. Traditionally it offers extensive services not only to government agencies but also to regional and municipal organisations. Naturally, its target groups are not confined to public sector organisations. Many products tailored to the requirements of the users concerned are available also to small and medium-sized enterprises, which, unlike most large companies, have tended to lag behind as regards reducing risks through IT protective measures.

IT security from the start of product development

This also affects the numerically largest group in Germany: private IT users who are less well versed in technical matters. The BSI has specific offers for members of the public, as their very number means that the damage potential in this area is considerable. Education and awareness raising as regards the possible dangers and protective measures are therefore very important for the BSI.

Another direction of focus for the BSI's activities is the IT manufacturers and the driving research establishments. The aim is to have a material influence on the design of future IT systems and ensure that adequate IT security is built into products from the earliest stages of development. On the other hand, IT security does not come free, either to providers or to users. Nor does the process necessarily begin with the security design of products, for only if customers consistently ask for security and are prepared to pay the higher price that this may entail will products that match these requirements be developed. For this reason, education and awareness raising play an important role in the achievement of higher IT security by both manufacturers and research laboratories.

The BSI's ongoing contact with industry and research plays a critical role in the success of its work. Only through intensive experience sharing can the more demanding requirements for security features in products be satisfied. The needs of customers – from German government agencies, industry and international organisations – must be captured and incorporated into developments in a continual process. In this way, the BSI, as a purchaser of external expertise and production resources, acts both as customer and also as partner and provider of systems and consultancy services.

Participation in international experience sharing

Due to the international nature of information and communications technology, the BSI's work is not confined to Germany. Co-operation and support in IT security issues extends to committees and project work involving other European countries or even non-European countries, e.g. at EU and NATO level. The aim is to influence security-relevant developments, obtain information and make existing expertise available.

These diverse activities lead to accurate knowledge of what is required in the market, both by the public and also in the government area. For the BSI this means that it must act as a neutral, responsible and competent interface to all the participants.

Milestones from the foundation of the BSI through to today

The history of the foundation of the BSI dates back to the year 1986, when, against the background of the rapid development of ICT technology, a working party was set up in the predecessor organisation, the Central Cipher Agency (ZfCh). Up to then the ZfCh had concentrated on the central task of information technology. The Security Working Party soon expanded to 70 members. Its job was to evaluate and certify IT products and systems. It was certification that was ultimately the trigger for the foundation of an independent agency, the BSI. In 1990 the Bundestag passed a resolution to establish a separate agency that would report to the Federal Ministry of the Interior (BMI).

The most important dates in chronological order

1986 The Central Cipher Agency is entrusted with the additional task of looking after computer security on systems that handle classified material.

1987 The Interdepartmental Committee for IT Security (ISIT) is formed under the direction of the Federal Minister of the Interior.

1989 Due to the expansion in the scope of its work, the Central Cipher Agency is transformed into the Central Agency for Security in Information Technology (ZSI). The German IT security criteria are published.

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

The direct predecessor of the BSI – at that time still the ZSI – organises the first German IT Security Congress in Bonn-Bad Godesberg.

1991 The Federal Office for Information Security (BSI) commences operation on 1 January 1991. The founding president of the BSI is Dr. Otto Leiberich.

The European IT Security Criteria (ITSEC) are developed under the direction of the BSI.
The BSI starts providing support to the Federal Data Protection Commissioner in the area of data security.

1992 IT Baseline Protection concept developed, certification and accreditation proceedings according to ITSEC/ITSEM start up.
Training system for the federal administration for over 1,000 delegates per year starts work.

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

1994 A broadly designed crypto innovation strategy in the BSI starts to be implemented. This has resulted to date in the development of important cryptographic systems such as Elcrodat 6-2, cryptosystem for the BOS digital radio, PLUTO high-performance crypto module, Elcrodat 4-2 radio system, SINA architecture and numerous innovations in the area of public key cryptography.
Support is provided to the Deutsche Bundesbank with the evaluation of electronic payment transaction systems.

1996 Version 1.0 of the Common Criteria published.

1998 The new Internet Security department addresses the growing importance of the world wide web. Management of the interdepartmental committee on Critical Infrastructures goes to the BSI. Start of future research with trend studies.

1999 The BSI provides extensive services and information relating to the "Year 2000 problem", e.g. a special brochure for the public. Set-up of and support for the public key infrastructure.

Publication of version 2.1 of the Common Criteria (CC) as an ISO standard.
The CC is now introduced into the BSI's certification scheme and the first protection profiles are developed.

With the launch of the government's Berlin-Bonn Information Network (IVBB), the BSI takes over technical co-ordination of the network.

2001 Federal Minister of the Interior Otto Schily puts in force new organisational, manpower and technical framework conditions for the further development of BSI into the central IT security service provider of the German government.
The first edition of the E-Government Manual is published.
The establishment of CERT-Bund (CERT for German Federal Government Institutions) stems from an initiative by the "Secure Internet" task force of the BMI, in response to the DoS attacks of February 2000. The CERT-Bund in the BSI is first a project team and then becomes a separate department in 2001.

As part of the anti-terrorism package, the IT Penetration Centre department and the Biometrics project team are set up.
Another initiative is to support the migration to Open Source Software, with the publication of a migration guide, studies, in-house developments and active consultancy services.

The department for Critical Infrastructure Protection (CIP) initiates extensive sector analyses in response to the terrorist attacks.
The BSI takes over the role of founding president of the Common Criteria Management Committee.

2002 Launch of the Citizen's CD, which has since been expanded into an online portal, over 1.6 million copies of which have been distributed as a CD.

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

Security / Co-operation

The world of bits & bytes extends around the globe and increasingly affects our daily lives.

Security through co-operation

Whether on national or international level, information networks are exposed to security risks. The BSI is working to promote a new "security culture", providing security concepts for the public sector and consultancy to private suppliers.

The BSI is able to collect information about IT security experiences and make it available both on international committees and also in communications with the public. A body of knowledge has grown in the course of many years of work which today is paying off in every area of IT security.

The BSI provides security concepts for government circles. It also advises and informs private users on all issues of data protection and the handling of confidential data. Warnings, online offers and other up-to-date information can be accessed from the BSI's homepage. A separate web portal containing information in a form that is easy to assimilate for the public at large is being implemented. The BSI also organises conferences and forums for the technical public.

The ninth IT Security Congress, attended by delegates from both Germany and abroad, will be held in Bonn in May 2005. The BSI is also represented at all the important trade shows, from San Francisco to Munich and Berlin, ranging from the RSA Conference, CeBIT and trade shows like "Modern State".

1. International co-operation

Global networking of communication and information systems makes it imperative that action in the area of IT security is coordinated at an international level.

For this reason the BSI plays an active role on committees organised by bodies such as the EU and NATO. Through co-operation it is hoped that developments in information security will be detected early on so that the associated security risks can be countered.

The work performed by the BSI carries weight: Germany is one of the leading states in the area of IT security, distinguished by decades of experience within the government and notable research results, and founded on the capability of the relevant industry. To promote this potential – and further expand its influence – is an urgent objective of international co-operation. Another aspect lies in promoting the market opportunities of German manufacturers.

As well as the BSI's long-standing close involvement in NATO committees and projects, its commitment is becoming increasingly important in the context of European integration. The BSI is the accredited national INFOSEC agency in the Secretariat-General of the EU Council of Ministers. It supports the European Union in drawing up and implementing security regulations for classified information. The requirement stems from the Secretariat-General's function of co-ordinating the common foreign and security policy of the EU. Co-operation takes a variety of forms: consultancy work for new networks, projects and services as well as the offer and evaluation of cryptographic devices and accreditation of systems.

Experience gained from collaborating with EU and NATO is opening up a number of fruitful bilateral contacts in the context of the expansion of the European Union and the North Atlantic Treaty Organization. This promotes dissemination of the BSI's security philosophy and opens up markets for the security products supported by the BSI. In addition, the BSI's new involvement on the OECD programme to promote a Culture of Security offers the starting point for forging further links.

The EU too calls on the consultancy services of the BSI. The picture shows Strasbourg, home of the European Parliament.

Platform for experts

FIRST (Forum of Incident Response and Security Teams) is an international coalition of approx. 100 governmental and private CERTs (warning and information services for IT threat situations). FIRST offers a platform for the sharing of experiences regarding the detection and handling of IT security-relevant incidents. Through the BSI's involvement, information for its own activities in the CERT-Bund (CERT for German Federal Government Institutions) is collected and evaluated.


FIRST TIMES

THE NECESSARY EVOLUTION OF FIRST TIMES

2003-2004

Secure IT systems for NATO

NATO and the German Foreign Office need globally interoperable, secure and capable communication and information systems. A large proportion of NATO spending flows into the procuring and maintenance of these systems, which are commissioned under the "NATO Security Investment Programme". The EU is also expanding its communication networks to incorporate the same high security requirements. Both in NATO and the EU, Germany is one of the biggest contributors. Together with its industrial partners Rohde & Schwarz (Elcrodat) and Secunet (SINA-VPN), the BSI offers powerful systems for these purposes.

2. IT security: a subject that affects everyone

The provision of information on IT security issues that is tailored to particular target groups is a high priority for the BSI. Only if the risks of information technology and appropriate protective measures are known can users protect themselves effectively against the threats.

As IT increasingly impinges upon every aspect of daily life, the BSI addresses the needs of the public, government agencies and companies with a growing portfolio of information. The BSI meets the different requirements of these target groups with a range of specific information and communication channels.

The numerically largest group is that of relatively inexperienced users, the public. Often they are not adequately informed about the risks and possible protective measures. And with fatal consequences, e.g. PCs used for private surfing without protective systems are wide open to attackers, there are no backups, any security software available is incorrectly installed and poorly maintained etc.

The Citizens' Portal contains entertaining illustrations and texts. Information is concentrated on the essentials needed to impart IT security to the public in terms that they can easily understand.

For this reason, at the beginning of 2003 BSI set up a citizens' web portal at www.bsi-fuer-buerger.de. The portal serves as a kind of manual: different sections explain how to protect oneself against viruses and worms, describe data backup procedures or show how to handle confidential data. A toolbox containing programs, a glossary and a number of useful links, offers the essentials needed to use the internet without fear of coming to harm.

Co-operation with the Stiftung Warentest organisation. Readers of this special edition received a free copy of the BSI CD "Into the internet – with security!"

The BSI has distributed the content of the Citizens' Portal widely through various collaboration partners. For example, every new consumer PC in Fujitsu-Siemens Computers' Scaleo series comes with the information already preinstalled on it. Through tradeshows and magazine inserts, for example, in a special issue of Stiftung Warentest, in"Chip" or in "PC-Welt", over 1,640,000 copies of the Citizens' Portal have already been distributed on CD.

Worms, viruses, dial-in programs, spam – anyone who follows the advice of the BSI "watchdog" has no need to worry about these nuisances.

Specialist expertise for IT professionals

IT users with some background knowledge and IT professionals can find up-to-date information at www.bsi.bund.de. Here the BSI makes available the entire bandwidth of its specialist subjects: projects, studies, background information, IT Baseline Protection offers, internet security, E-Government, the SINA and SPHINX projects, product certification and many other subjects besides. The online service also includes a newsletter that appears at regular intervals and to which anyone can subscribe.

Warnings and information supply

To ensure that those responsible for IT are promptly informed of threats and are able to take preventive measures, the BSI makes available an extensive warning and information supply. These are published on the BSI website or are sent automatically following registration with CERT-Bund (the Computer Emergency Response Team for German federal government institutions).

A compact overview of the most important security measures.

From standard work to leaflet

In addition to its online offers, the BSI provides a number of printed publications. These include standard works on IT Baseline Protection and E-Government, the "IT Security" guidelines, studies, leaflets and brochures. All publications are provided on a CD free of charge in return for a stamped addressed envelope. Unlike the Citizens' Portal, this CD and its contents are directed at the technical public.

The BSI is a committed partner

When it comes to addressing the requirements of particular target groups, the BSI attaches great importance to partnerships with industry, administration, media and academia. The BSI provides regular information on topics of current interest in the area of IT security in the BSI Forum in the specialist "<kes> – Die Zeitschrift für Informations-Sicherheit" journal (a journal devoted to information security).

Since 1 July 2003, the BSI has also disseminated its latest information via the Heise security portal (www.heisec.de). This ensures that coverage of the target groups is as wide as possible.
In 2003 the BSI organised a number of events, for example in collaboration with the Gesellschaft für Informatik (German Informatics Society), the Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e.V. (the association for security in industry), or the BITKOM.

These include appearances at trade shows

The BSI also attends all the major trade shows in its subject areas: CeBIT, Security and the RSA Conference in San Francisco. The IT security area at the Munich SYSTEMS conference is orga-

In collaboration with the Secumedia publishing house, the BSI Forum in <kes> serves as the BSI's official organ.

Typical warning on the website of heise online, another of the BSI's partners

At trade shows the BSI presents the results of its work and details of its main areas of activity. An intensive exchange of information takes place with customers and partners of the BSI as a result of personal contact.

Congress “IT security in distributed chaos”

nised by the Secumedia publishing house and is sponsored by the BSI. The BSI does not just exhibit at IT security related events but its staff frequently present papers in technical and management-oriented forums. At the “Modern State” trade show in Berlin, the BSI is the partner responsible for the area of IT security. In addition to personal discussions, the presentation of important IT security topics and current areas of focus forms a major element of these events.

In addition, every other year the BSI organises the German IT Security Congress. In recent years this has developed into one of the central meeting points for IT security specialists. Under the catchphrase, “IT security in distributed chaos”, the three-day congress held in Bonn in 2003 attracted 700 high-calibre delegates.
At an accompanying exhibition, 30 exhibitors presented new developments and solutions. The ninth congress is scheduled for May 2005. Once again the programme will offer an in-depth overview of the directions into which IT security is moving.

Bonn as a venue

The German IT Security Congress is organised by the BSI on a biannual basis. It is regarded as the central event in the area of IT security in Germany. The eighth congress in 2003 was held in Bonn-Bad Godesberg under the catchword “IT Security in distributed chaos” and built on successful developments in previous years.

Risks / threats

PCs cannot defend themselves –

they need protection.

1. The Computer Emergency Response Team: CERT
2. Basis of risk prevention: IT Baseline Protection
3. Quality officially attested: certified IT products
4. Secure E-Government

Risk prevention and threat detection

Prevention rather than cure – this is the BSI's primary concern in the matter of damage prevention.

Today computer viruses may spread so quickly that any warning can already be too late.

The BSI has set up its own Computer Emergency Response Team (CERT) for federal government institutions, whose mission is to preventively draw attention to security weaknesses in computer systems. CERT-Bund is able to respond to possible threats and attacks 24 hours a day, seven days a week, and to introduce countermeasures at short notice.

Proper IT baseline protection is equally important. With its IT Baseline Protection Manual, which now extends to over 2,000 pages, the BSI offers an integrated concept that has already been implemented in a number of government agencies and companies. The Manual has become established as a standard both nationally and internationally.
Before using IT products, one should satisfy oneself that the systems are secure. The BSI's role is to test and certify the offers available on the market with regard to their security capabilities.

The aim of all modern E-Government activities is to improve public access to data. Both at national and regional level, the BSI plays an essential role in the project of making the services provided by government agencies fit for the internet. Only if data security is guaranteed E-Government services will meet with general acceptance among the public.

1. The Computer Emergency Response Team: CERT

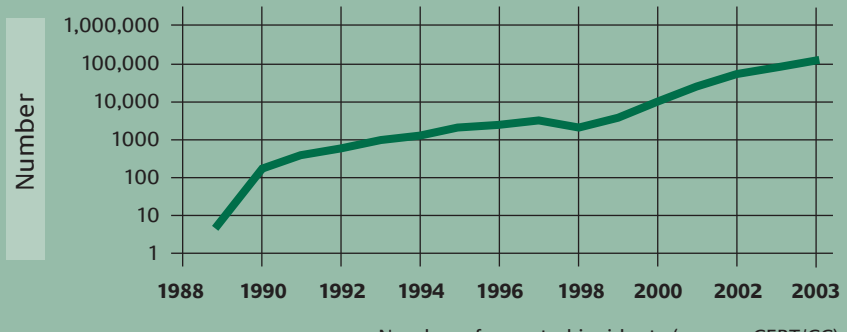
Sobig.F and Lovsan provided compelling proof to everyone in 2003 that early warnings and specific advice on available countermeasures against computer viruses, worms and trojan horses can definitely increase IT security.

In the area of federal administration, this central information service is provided by the CERT-Bund (CERT for German federal government institutions), based at the BSI. Often the delay between the start of an attack and the infliction of damage on vulnerable systems is only very short. There is scarcely any time to react. For example, in February 2003 the Slammer worm had infected 90 percent of all vulnerable systems around the world within only ten minutes. In August of the same year, the Blaster worm ("Lovsan") caused millions of euros of damage world-wide.

But in both cases, a security patch was available in time. Unfortunately, in many cases the patches were not installed. Unclear responsibilities, lack of knowledge of suitable sources of information and/or overloading of many system administrators meant that the latter did not have not up-to-date information about known security weaknesses in their systems. As a result, problems were (and still are) not detected nor were available security updates or patches implemented.

The federal administration too has been exposed to many attacks or attempted attacks on its IT systems. For this reason, in September 2001 the Computer Emergency Response Team for German federal government institutions (CERT-Bund) was set up as a centre of competence in the area of computer and network security.

Tenfold increase in security incidents



Number of reported incidents (source: CERT/CC)

Over the period 2000-2003 the number of security incidents reported rose by a factor of over 10. The central co-ordinating body for the collection, analysis and systematic forwarding of warning messages for the German federal administration is the CERT-Bund in the BSI.

"Modern State" trade fair in Berlin, 2003. Günther Ennen from the BSI explains the risks of networked systems in information technology.

CERT-Bund performs the following core tasks:

First

It serves as a central contact office that is available at all times:

- During office hours, there is a telephone hotline available on 0228CERTBUND or +49 (0)228 23782863
- Outside office hours, there is a standby service for the closed circle of users
- It can be contacted at any time by e-mail: certbund@bsi.bund.de or fax on +49 (0)228-30896-25.

Second

Incoming incident reports are analysed and evaluated by experts. Close co-operation with national and international CERTs enhances the rapid availability and quality of these assessments.

Third

Any outstanding investigations of incidents and the resumption of operations are supported and co-ordinated and, when required, support is even provided on site.

Fourth

Quality assured information, known as "advisories", is sent in digitally signed messages to the responsible points of contact in the government agencies. The warning and information service provided by CERT-Bund is particularly important here.

Between January and September 2003, CERT issued 85 major warnings. Through the new short message service that was set up in September, CERT provided information on 88 different subjects by e-mail over the next two months.

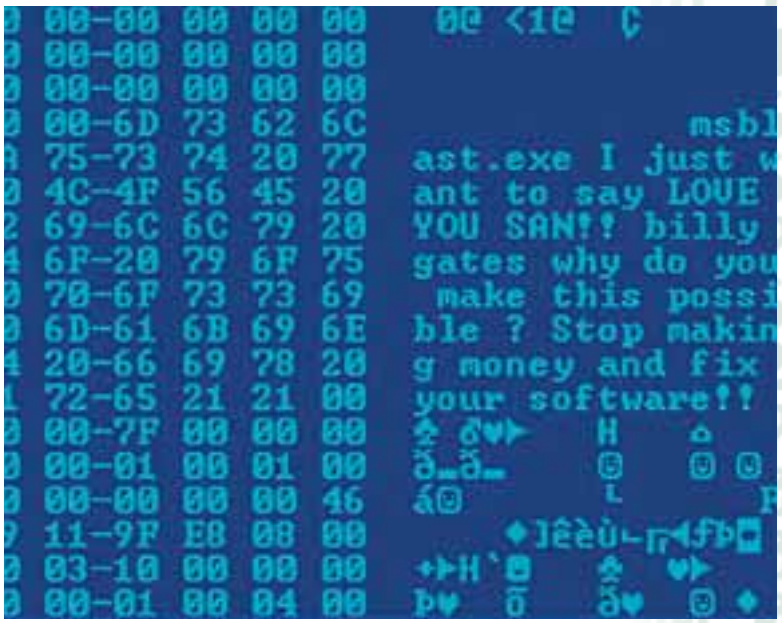
The individual advisory services are primarily available to German government agencies. Queries from companies, private persons and private institutions are only handled where resources allow for it.
CERT can relieve administrators and make a significant contribution towards the protection of information and communications technology. It is their job to collect the necessary information about security vulnerabilities and communicate information about the countermeasures required to the relevant target group in line with their needs.

They answer queries about IT security topics, issue preventive warnings of vulnerabilities and provide information on security-relevant events. On the basis of this information, concrete measures to avert a particular threat can be taken promptly by the responsible system administrators or end users. In this way, possible damage can be avoided in advance.

Prevention is the best defence against computer viruses

Even when a computer virus has already caused damage, CERT can still help. They also offer reactive services aimed at mitigating the effects of an attack, supporting the removal of the damage or directly clarifying and clearing up the security incidents.

Viewed on their own, CERTs are only one element in the fight against IT security incidents. They are no substitute for robust IT security concepts or for sensible advance contingency planning. However, they extend the spectrum of suitable individual measures and serve as extremely valuable sources of information and centres of support.



Even the latest anti-virus software cannot help: the Blaster worm spread massively within a very short period of time through a service provided in Windows 2000 and XP which was installed as standard but unfortunately was vulnerable from a security point of view. Millions of people affected throughout the world might have been helped by a patch Microsoft promptly provided.

Hacker attacks

In addition to the wide-ranging, indiscriminate damage caused by viruses and worms, more and more damage is being caused by targeted hacker attacks. The motives for these attacks are very complex and, due to the very high number of unrecorded cases, are difficult to analyse. Some examples:

- **"sportsmanship"** – the satisfaction of being able to vanquish complex security mechanisms, thereby demonstrating one's own superiority;
- pure **vandalism** – as well as demonstrating his superiority, the attacker seeks to cause as much indiscriminate damage as possible;
- **personal enrichment** – this can be achieved by misusing credit card information or other passwords;
- **industrial espionage** or, more generally, the gaining of competitive advantage;
- targeted ideational, financial or physical **damage** to an opponent.

Hackers exploit vulnerabilities that have become known so as to gain control over unprotected systems. Because of the high complexity of operating systems and applications, new security loopholes are constantly coming to light.

Methods and tools of attack are constantly being developed and refined. This means that hardening and protecting information and communications technology is not a one-off activity but has to be repeated on a regular basis.

2. Basis of risk prevention: IT Baseline Protection

Modern business processes, as found in industry and public administration, are inconceivable today without IT support. The continuity of operations depends critically on reliably functioning information technology.

Hence, inadequately protected information technology assets constitute a risk factor that is frequently underestimated, but which can threaten the very existence of many enterprises. Of course there are some very good security systems for different requirements, but precisely in small and medium-sized enterprises these are often only inadequately used and implemented. In actual fact, a basic level of IT security can be achieved with relatively modest resources.

On the other hand, full IT baseline protection means much more than just the purchase of anti-virus software, firewalls and back-up systems. An integrated concept is important: the protection requirements of a given organisation can only be determined by starting from an analysis of the present situation and then using this to work out the specific safeguards that are needed. In this area, the BSI's IT Baseline Protection Manual (BPM) has established itself both nationally and internationally as a standard. This work, which has undergone continuous development since 1994 and now extends to over 2,000 pages, provides detailed descriptions of possible threats and precautions. It contains a systematic methodology for developing IT security concepts and tried and tested standard security measures which have already been successfully implemented in numerous public bodies and companies. The fifth supplement issued at the end of 2003 contains new sections on outsourcing, electronic archiving, Microsoft Internet Information Server, Apache web server and Microsoft Exchange Server. The work is available as a set of loose-leaf binders from the Federal Gazette publishing house (Bundesanzeiger Verlag), while the electronic version will be available on the internet from the BSI's website from February 2004.

The BSI's web course is based on the IT Baseline Protection Manual. The Manual content undergoes continual further development in collaboration with partners.

The IT Baseline Protection approach entails the following major components:

Capture of information about IT systems / structure analysis

The creation and implementation of a security concept starts with examination of the existing and planned IT assets. As well as the software applications and hardware, the subjects that need to be researched here include the server rooms, the existing buildings and the specific roles of employees. The aim is to develop a solid foundation which takes full account of all the security-relevant parameters.

Assessment of protection requirements

Once the IT assets are adequately documented, the next stage is to evaluate the data. The question is, how important or critical is the information held or handled. This assessment is used to establish whether, for example, standard protection measures will be sufficient or whether special security systems are required.

Basic security check

The aim of this step is to establish which security measures are already implemented.

IT Baseline Protection modelling

From the data collected on the IT assets and the IT security requirements it is now necessary to assemble the relevant security safeguards from the Baseline Protection Manual. Systematic modules on a range of categories enable one to identify the individual security safeguards that correspond to the environment modelled. Any of these safeguards that are not yet in place are then implemented.

IT Baseline Protection Certificate

In many cases it is desirable to make the security level attained transparent both within and outside the organisation. The IT Baseline Protection Certificate documents this in a trustworthy manner. It shows that the organisation handles information responsibly and actively operates risk prevention measures.

A reputable certification process always presupposes prior testing of the object under investigation. A detailed testing scheme which specifies the testing and audit process in detail has therefore been developed for the IT Baseline Protection Certificate. On the basis of such an IT Baseline Protection audit, a decision is made as to whether an IT Baseline Protection Certificate can be issued for a set of IT assets. However, the quality of an IT Baseline Protection audit does not depend solely on the test scheme but it also depends significantly on the technical expertise and experience of the auditor. Here the BSI has introduced a licensing scheme for IT Baseline Protection auditors. To become a licensed Baseline Protection auditor it is necessary to have professional experience in the area of IT security and project experience using the IT Baseline Protection Manual. To date over 100 auditors have been licensed by the BSI.

For non-professionals, the BSI has been offering a web course since 2003 which provides an easy introduction to this wide-ranging subject. In around four hours, novices are introduced to the subject of IT Baseline Protection in a form that is easy to assimilate. The web course explains how to carry out the analysis work that is necessary for an IT security process and how to prepare the relevant documentation. An example is used to illustrate how the BPM is applied to a complete set of IT assets. Through numerous instructions, examples, exercises and tools, course participants receive the training they need to create their own security concepts using the BPM. The web course is available free of charge on the BSI's website.

As a supplement to this, since 2003 the BSI has offered the IT security guidelines, "IT Baseline Protection in brief". This document deliberately renounces the wealth of detail of the BPM so as to provide a compact, easy-to-digest overview of the most important IT security safeguards. In particular, it will assist smaller organisations with getting started on IT Baseline Protection. With the guidelines, readers can quickly ascertain what security measures are essential for them and where there is a particularly urgent need for action.

The principles and resources developed by the BSI to supplement the IT Baseline Protection Manual cover a wider spectrum of topics. These are not confined just to technical aspects, but organisational procedures, such as the transfer of know-how to the users and the practical implementation of the recommended methods, are covered as well. In the rapidly developing IT world it is extremely important to be able to react quickly to altered conditions. In particular, active sharing of experiences with the registered users and auditors contributes to ensure that the BSI's products are always tailored to current needs and is fed into ongoing further development of the IT Baseline Protection Manual.

For the implementation of IT Baseline Protection, the BSI and its teaming partner Mummert now offer Version 3.1 of the Baseline Protection software tool, GS-Tool. This assists the user to create, manage and update IT security concepts. The entire IT Baseline Protection Manual approach is supported by the tool, from the capture of information about the system through to IT Baseline Protection certification. You can download a demonstration version of the software free of charge from the BSI's website.

A functioning basic level of IT protection is essential to the entire business world.

Licences for auditors

Secure IT is a factor of competition. The fact that an organisation has implemented IT Baseline Protection shows customers, suppliers and partners that it actively operates risk prevention measures. To document the implementation of IT Baseline Protection to the outside world in a credible way, the IT Baseline Protection certification scheme was presented at the beginning of 2002. This provides for three qualification levels: self-declared entry-level, self-declared higher level and IT Baseline Protection Certificate. The issue of an IT Baseline Protection Certificate presupposes an audit by a licensed auditor.

The 100th Baseline Protection Certificate went to Holger von Rhein of SRC GmbH Bonn.

IT-Grundschutz-Zertifikat

The process of becoming a licensed IT Baseline Protection auditor has met with a gratifying amount of interest. The first twenty auditors were licensed at the beginning of 2002, and in September 2003 the 100th auditor was licensed. In addition, twelve IT Baseline Protection self-declarations have been made, the first three IT Baseline Protection Certificates have been issued and further certification processes are in the pipeline.

3. Quality officially attested: certified IT products

Trustworthiness is the decisive criterion for the use of IT products. However, it is virtually impossible for IT managers to assess the security capabilities of a particular product themselves.

The burden of proving the security of its products in a credible fashion lies squarely on the shoulders of the manufacturer, who has to rely on references or independent tests. This evidence that an IT product has been implemented in a trustworthy manner is provided by evaluation (testing and assessment) and certification. This procedure is based on objective criteria, such as the Common Criteria (CC) standard. It is carried out by neutral organisations like the BSI and accredited evaluation facilities. The aim of certification is to assess IT products and systems with regard to their security capabilities in a transparent fashion that permits comparisons.

In principle, quite varied IT products, software and hardware, from smart cards and operating systems through to firewalls and data transmission products, can be certified as long as they possess security functions in conjunction with

- availability of data and services
- confidentiality of information
- integrity of data
- authenticity of data.

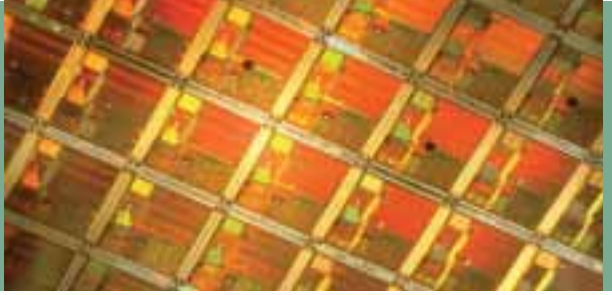
The certification process can be initiated by a manufacturer, a distributor or a government agency as user. The application is submitted to the BSI's Certification Authority.

The Common Criteria offer user groups and manufacturers the possibility of defining the requirements of a given product and system class (e.g. firewalls, cash cards, operating systems) in terms of protection profiles.

Protection profiles provide users with a means of specifying the security requirements that are needed in their particular case. In this way manufacturers can aim their product development at specific customers' needs.

Product evaluation is normally carried out by accredited and licensed evaluation facilities. All the organisations involved are bound to observe the confidentiality of trade secrets and guarantee through various measures that this important precondition will be adhered to.

International standards apply to hardware and software as well.



A common logo

In Germany, besides BSI, there are also private certification authorities. The preconditions that have to be satisfied for the certificates to be recognised are governed by bilateral agreements. The certificates recognised by the BSI can be identified by their common logo “Deutsches IT-Sicherheitszertifikat” (German IT security certificate).

Step-by-step Security

In the Common Criteria, security assurance requirements are grouped together into a series of hierarchical levels known as “evaluation assurance levels” (EAL). Altogether there are seven levels, starting from Level 1, the least demanding set of requirements, to Level 7, which de-fines the requirements for applications where highly sensitive data is to be handled. As the assurance level increases, so do the depth and scale of evaluation.

Testing starts during the development phase

The length of the evaluation and certification process can differ widely, depending on the complexity of the product and the evaluation level targeted. An initial evaluation normally lasts three months in the case of a PC security product and six to nine months for an average operating system. The evaluation can be carried out along with the development, allowing the issue of the certificate to coincide with the market launch of the product.

Whether this timing can actually be achieved will depend on the quality of the development methodology and documentation used by the manufacturer.

Usually IT products are intended for sale on the international market. To avoid multiple certification of the same product in different countries, IT security certificates can be mutually recognised. In this connection, the following agreements exist:

ITSEC and CC certificates

The European agreement relates to certificates covering all evaluation assurance levels. If a given nation does not have its own certification authority, then the recognition will be one-sided. All the certificates issued by the BSI are recognised throughout Europe.

CC certificates

An agreement covering the mutual recognition of IT security certificates based on the CC up to and including evaluation assurance level EAL4 has been signed by the national agencies of the following countries: France, Germany, the United Kingdom, Canada, the USA, the joint Certification Authority of Australia and New Zealand, Japan, Finland, Greece, Italy, the Netherlands, Norway, Spain, Israel, Sweden, Austria and Hungary.

Where a mutual recognition agreement exists, reference is made to the certified products of the other certification authorities or these are published at the same time. The associated certification reports are exchanged. Moreover, the certification authorities agree their joint procedures at regular intervals.

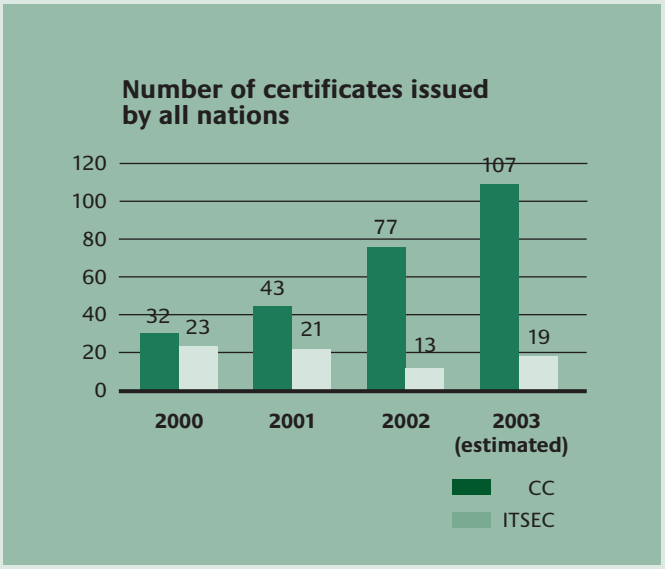
In this area, the BSI has a major influence because it played an active role in the development of the CC right from the beginning. In addition, it has extensive experience of the certification process. This derives not least from the many certificates that the BSI has issued to foreign manufacturers and from its involvement in groundwork, e.g. in the evaluation of smart cards and random number generators.

CC certificates are based on internationally agreed criteria.

In the international arena, certification is becoming more and more important. In the USA, the use of certified products has been mandatory in public administration since July 2002. In Australia it is a stipulation that certified products must be used in connection with the implementation of E-Government applications. In France, only certified smart card products can be used in both the public and private sectors. Also, a wide range of systems based on the CC is increasingly being certified for public administration.

This new impetus and the successful trend suggest that certification will become more and more important in the future for both manufacturers and users.

The BSI certifies IT products and IT systems in accordance with the international Common Criteria and the European Information Technology Security Evaluation Criteria (ITSEC).



It is estimated that in 2003 the BSI issued almost one-quarter of all the certificates issued world-wide.

International expert conference

The fourth International Common Criteria Conference (ICCC) was held between 7 and 9 September 2003. This is the most important conference of the internationally recognised Common Criteria (CC) for the evaluation of IT security. Over 300 experts met in Stockholm to discuss the use and ongoing further development of the baseline criteria.

At the conference, the president of the BSI, Dr. Udo Helmbrecht, handed out five CC certificates issued by the BSI. Philips Semiconductors received a certificate for its SmartXA2 smart card microcontroller.

The Belgian company, Banksys, was rewarded with a certificate following the successful evaluation of its hardware security module. Microsoft Corporation was handed a certificate for the Microsoft ISA firewall server, as was IBM for its AIX 5.2 operating system and the Directory Server.

The fact that even major American corporations are choosing the BSI as their certification authority testifies once again to the effectiveness and success of the international agreement for the mutual recognition of CC security certificates. The next ICCC will be hosted by the BSI in 2004.

4. Secure E-Government

The aim of the BundOnline 2005 initiative is to make available online all federal administration services that are internet-capable. The joint "Deutschland Online" project involving the federal government, Laender and municipalities is aimed at making the services provided by all government agencies available over the internet faster, more efficiently and in a standardised manner.

This will open up to the public the possibility of using almost the full spectrum of services, whether at national, regional or municipal level, 24 hours a day, seven days a week. The traditional visit to the authorities will be supplemented by a convenient access route.

The acceptance and success of E-Government services depends critically on the quality and user friendliness of communications. Data security is the central quality feature here.

Information and communication security falls within the task spectrum of the Data Security Competence Centre in the BSI. This was set up at the end of 2002 with the participation of the companies Secunet and Secartis. It became operational at the beginning of 2003.

At the forefront of its work is the protection of confidentiality of data, protection against unnoticed changes and the reliable identification of the originator. These are the primary security objectives.

Encryption, digital signatures and certificates are widely used today as cryptographic mechanisms based on public key procedures to protect sensitive data in transit. Here, transmitter as well as receiver each have two keys. One of these is kept secret and only known to them. The other half of the pair of keys is openly accessible, e.g. via a public directory.

With these two keys and the aid of trustworthy third party it is possible to ascertain three features of communication: confidentiality of messages and the impossibility of manipulation as well as the transmitter's authenticity.

To ensure that communications between government agencies and members of the public, between agencies and industry and between the agencies themselves over the internet are properly protected, the BSI is currently developing the Data Security basic component. This will significantly simplify electronic communication between government agencies and avoid multiplication of development and implementation costs.

The Virtual Post Office – your guarantee of data security

The core element of the basic component is the Virtual Post Office (VPO). This takes over the function of processing secure, traceable and confidential communications. Both e-mail and web-based communication are supported here.

The VPO provides central functions such as encryption and decryption, digital signature creation and testing and authentication to the government agency. Additional systems such as virus scanners can be integrated over open interfaces. As well as indirect e-mail communication with a central address in the government agencies, the basic component also supports strict end-to-end security with individual officials. Linking of external trust centres to the VPO is also supported.

VPO launched in the summer of 2003

The first project phase was completed in the spring of 2003 with the creation of the technical concept and the DP high-level design by IBM. In the early summer of 2003, work began on implementing the VPO. The further development of the VPO's web and core components is

continued on page 44

"Modern State 2003": Secunet and BSI shared a stand at this trade fair.

Secunet and Secartis are partners of the BSI in the Data Security Competence Centre.

BundOnline 2005

Government moves into cyberspace

The aim of the BundOnline 2005 initiative is to make all internet-capable government services available online by 2005. The BSI is supporting the implementation of these measures with a number of activities, for example, the “Virtual Post Office” and operation of the Data Security Competence Centre.

If data is to be delivered to people’s homes, as opposed to their having to make a trip to some official office, it is imperative that mistakes are avoided and fraud is ruled out. Members of the public visiting the authorities are frequently required to provide proof of identity. Similarly, the Virtual Post Office and one of the possible solutions in the matter of the digital signature are based on the provision of proof of identity via a smartcard inserted into a special input device that is connected to the home PC.

BSI President Dr. Udo Helmbrecht explains how a Virtual Post Office works to Federal Minister of the Interior Otto Schily.

based on the "Governikus" product from the Bremen Online Services company, while the product chosen for e-mail communication was Julia from the ICC company. A first version of the VPO will be in operation with BundOnline 2005 pilot users at the beginning of 2004. A further stage that is capable of wider use and implements essential parts of the concept will be available in the fourth quarter of 2004.

E-Government Manual updated

The BSI is making the E-Government Manual available as a methodology. Once again, updating of the Manual was one of the main priorities in 2003. Thus the phase plan was completed with the publication of phases 5 (implementation and test) and 6 (introduction and commissioning). The phase plan is aimed at the E-Government co-ordinators in the public agencies and describes step-by-step how a government agency can introduce E-Government.

Guidelines for government agencies

In co-operation with other government agencies, three modules were prepared for the Manual on the topics "Legal framework conditions for E-Government", "E-Government compliance with data protection legislation" and "E-shop guidelines". Version 1.1 of the "Standards and Architectures for E-Government Applications" (SAGA) document, commissioned by the co-ordination and advice office of the federal government for information technology in the federal administration (KBST), was incorporated into the Manual. In this connection, the BSI is currently providing support for the preparation of version 2.0.

Barrier-free access

The "Secure integration of E-Government applications" and "Barrier-free E-Government" modules were also completed during 2003. As of the end of the year, modules on the subjects of "Secure payment transactions for

continued on page 46

E-Government necessitates changes to existing information technology infrastructures.

The implementation of E-Government services requires that public administration IT systems which have hitherto been sealed off are made available over the internet in such a way that there are no security loopholes. The transmission of sensitive data over the internet requires that trustworthy infrastructures are created, administrative processes restructured and existing government agency applications are furnished with suitable security solutions. The BSI's comprehensive E-Government Manual provides tools for the analysis, design and reorganisation of processes and also for reassessing the subjects of data protection, IT security and the protection of electronic communications. This will ensure on the one hand that members of the public and businesses can communicate smoothly with government agencies over the internet and that transactions will be legally binding and confidential. On the other hand it will guarantee the security of communications within these agencies.

Online registration of a change of address.

E-Government" and "Secure client/server architectures for E-Government" were also under development.

Latest news on the subject of E-Government

The E-Government Manual is being published simultaneously in three versions. Initial publication is always on the BSI's "Secure E-Government" website, which is continually updated by the project team. English translations of the most important modules appear on the same website a little later. Then the Bundesanzeiger Verlag publishes the Manual as a set of loose-leaf pages. In 2003, two supplements were added.

Growing e-mail distribution list

The BSI's main contact with the users is via e-mail newsletters, in which the BSI announces new publications, events and invitations to tenders. Over 1,200 people have already registered as users. New readers sign up almost every day. Finally, the BSI receives valuable feedback about implementation practice through the advisory project work performed by its Data Security Competence Centre.

Electronic communication with government bodies from the home is more relaxed and saves money.

Government is on track

Almost 260 of the 449 government services recently identified as internet-capable were on the internet as of the end of 2003. The "BundOnline 2005" initiative is aimed at ensuring that all the relevant government services are online by the end of 2005.

The Federal Ministry of the Interior expects to save Euro 400 million per year in administrative costs once the plan is fully implemented. Thus, the customs authorities are already auctioning impounded articles at www.zoll-auktion.de. Patent applications and applications for student grants can be submitted online, while the Foreign Office accepts job applications for senior grade positions that are submitted over the internet. You can find out just what is possible online by visiting *www.bundonline2005.de*

BundOnline 2005 progress indicator

Services implemented	Up to 2002	2002	2003	Total
Provision of information	21	99	38	158
Consultancy	0	6	3	9
Preparatory work for political decisions	0	0	1	1
Collaboration with government agencies	2	6	9	17
Application procedures	1	11	10	22
Sponsorships	1	1	4	6
Procurement projects	0	1	5	6
Inspection work	0	4	4	8
Other services	5	12	12	29
All services	**30**	**140**	**86**	**256**

Date: 17 Dec. 2003

The future

Moving with the times: anyone who consults the BSI can be sure of being kept abreast in matters of IT security.

1. Knowing what is coming: trend analysis
2. Mobile communication
3. Encryption technology
4. Human beings in bits & bytes: Biometrics
5. Protection of Critical Infrastructures

Looking ahead

For anyone who wants to have a part in building the future, it is imperative to be at the forefront of technical developments even now. Wherever IT security is an issue, the BSI has a substantial involvement in significant future-oriented trends.

Of course, no one can accurately foresee the future, but forecasts do at least permit rough estimates and allow probabilities to be identified. Unless one keeps one's eyes open, threat situations cannot be detected before it is too late.

Wireless communication systems, which are already becoming widespread, offer great individual freedoms to users, while at the same time also concealing dangers. Mobile networks are easier to attack and more difficult to protect. The BSI is actively concerned with the issue of mobile security and is involved in identifying vulnerabilities and preparing technical standards for wireless communications.

High-performance encryption systems are needed not just for this type of communication. One of the tasks of the BSI is to provide state-of-the-art cryptographic systems for the exchange of sensitive information within the federal administration and law-enforcement agencies.

State, industry and society must be able to rely on information technology to function even at times of crisis. The protection of Critical Infrastructures – energy, health care, emergency services – is a challenge that the BSI has taken on with the development of a "National plan for the protection of IT-dependent Critical Infrastructures".

1. Knowing what is coming: trend analysis

What are the critical developments that will change and shape our economy and society in the future? What technologies will mould our lives over the next ten years?

In the rapidly developing world of information technology, it is not enough simply to be au fait with existing systems. In the case of threat scenarios it is important to be able to respond quickly and competently. Future events need to be predicted as accurately and as early as possible using forecasts, so as to be prepared should a critical situation occur.

With the aid of various forecasting methods (quantitative and qualitative), it is possible to make probability statements about future developments. One possible starting point for trend analysis is the theory of cyclical economic trends. As well as other short- and medium-term fluctuations, according to the theory of Kondratiev there are also long waves that last 50 to 60 years. Such long cycles are triggered by trail-blazing innovations such as the steam engine or electricity and, in the recent past, by information technology. These kinds of innovation do not occur continually but in phases, and in this way trigger periods of pronounced economic growth.

"Planetary gearing" for miniaturised motors with high rotational speed. Such nanomotors are used in Minidisk players and in surgery.

Today, the boom years of information and communications technology (ICT) are drawing to an end. At the beginning of the 21st century, we find ourselves in a downturn, i.e. the zenith of the fifth Kondratiev cycle is already behind us. The transition from one economic cycle to the next is always associated with pronounced instability in world economy.

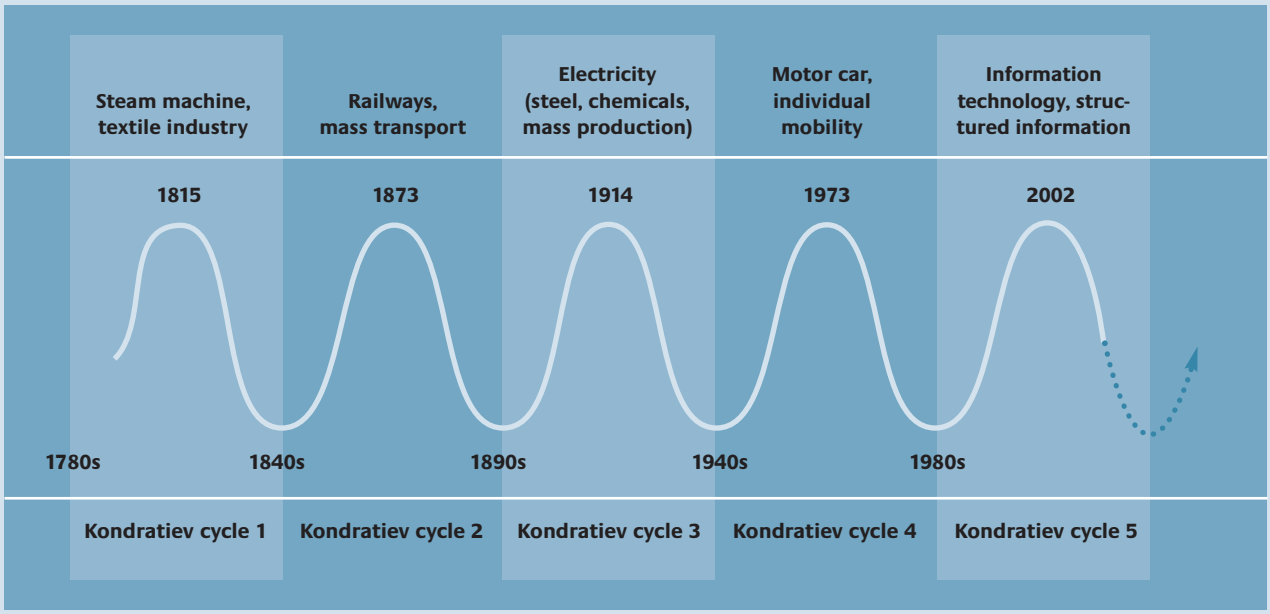
The five Kondratiev cycles to date are characterised by the following trail-blazing inventions:

- steam engine/cotton (1793-1847)
- steel/railways (1893)
- electrotechnology/chemistry (1939)
- petrochemicals/car manufacture (1984) and
- currently ICT.

All these inventions triggered an enormous upswing in the world economy. ICT alone is no longer sufficient to cope with the future social requirements and needs of humans. Another basic invention will have to follow; this in turn will trigger major global economic effects and in the long run have a significant cyclical effect on our society.

Kondratiev's economic cycles

The world economy moves in short-, medium-and long-term economic cycles. The BSI is particularly interested in the approx. 50-60 year long cycles postulated by N. D. Kondratiev in 1926. They are triggered by critical innovations, which in modern times occur at increasingly short frequencies. The recurring pattern permits a forecast of future economic and technology developments.



What trend will determine the 6th cycle?

There is at present no agreement in trend research as to the form which the next long-term cycle, the sixth Kondratiev cycle, will take. Discussion at present centres around the following possibilities:

- omnipresent information networks
- miniaturisation – microsystem technology and nanotechnology
- nanorobotics, quantum computers
- biotechnology, medical engineering, genetic engineering
- optical technology
- environment, energy technology
- health, education and networked knowledge.

Which of these basic inventions will decisively determine the tempo and direction of world economy over several decades?
Will it lead to vigorous growth throughout global economy?

Building blocks for the future: ICT

The further development of ICT will definitely be an element of this process. In combination with biotechnology and nanotechnology, it could perhaps trigger the next high-tech boom. Forecasts of specific technological ICT developments and the identification of new application areas are therefore of quite considerable importance.

The BSI's latest trend study examines especially relevant developments in the areas of ICT in depth.

The study is divided into four technology areas:

- computer technology, computer networks and communication, software technology
- databases and knowledge management
- range of application
- security technologies.

What will be the key innovation

for the 21st century?

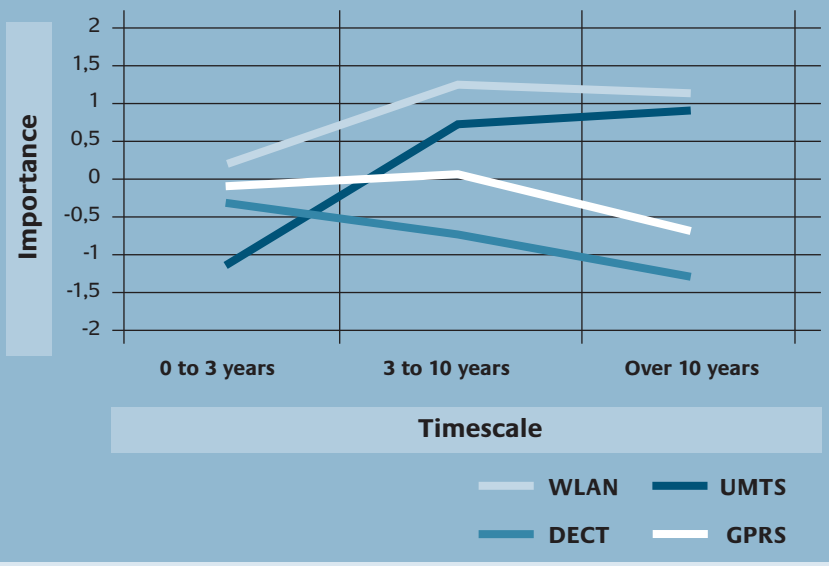
One candidate is biotechnology.

For these areas overall trends – e.g. convergence, complexity and mobility – are included and analysed. Specific technological considerations, analysis of the driving forces and overall investigation of their interaction explain what is going on. The result is a clear picture of future trends.

One thing is already clear: whatever the next key invention will be, the new economic and social potentials discovered will not be the only subjects discussed, but once again there will also be a lot of talk about possible security risks. The trend analyses are already providing information on the form that the answers could take.

The BSI is attentively following developments in information technology and the critical factors that will determine future events. The study entitled "Communications and Information Technology 2010+3: new trends and developments in technology, applications and security" and published in 2003 provides information on the latest trends.

Importance of transfer technologies for IP-based application protocols in the area of mobile communications



Mobile communication

As the number of mobile applications rises, broadband IP-based transmission technologies, especially WLAN or UMTS, will become increasingly important.

(Survey of experts conducted by the BSI in 2002 based on 185 questionnaires)

2. Mobile Communication

First we had the global networking of economic regions; now, mobile applications have made triumphant progress. The associated terminal devices, such as laptops, PDAs, organisers and mobile phones, are already an important element of everyday life.

The availability of ever smaller, more powerful products has played a significant role in transforming wireless communications systems into something that is taken for granted. But this newly gained freedom also has its risks. Through the use in private and business environments, vulnerability increases with the quantity of time-critical and sensitive data. Secure internet and mobile telephony services are therefore becoming more and more important.

Rapid changes in technology mean that IT security parameters are constantly changing. Today devices can communicate with other components in a distributed environment via cellular mobile telecommunications networks (GPRS, UMTS), fixed LANs and WLANs, satellite networks and telephone networks. Together they constitute a world-wide, mobile system.

Special standards have been developed for application protocols for mobile terminal devices. They enable access to internet services such as e-mail, surfing and the downloading of active content even on very small mobile devices.

A host of security risks lurk in open networks, such as the internet. On top of these, mobile applications face some additional specific threats starting with the vulnerabilities that are inherent in small mobile terminal devices. For example, the very portability of small, light terminal devices makes them easier to steal or lose, while at the same time they can be misused so as to record and/or intercept conversations unnoticed.

Often the mobile devices come with limited resources only. This may expose them to risks in the software area e.g. it is necessary to download code which could turn out to be harmful or little effort may have gone into security checks. Personalisation of devices enables security-critical usage profiles to be created, and movement profiles can also be recorded.

Wireless access networks introduce further risks, for example easier interception of unencrypted connections. The list of dangers is long and could be extended, for example to include the danger of disabling the encryption function or the risk of unauthorised access to networks.

As a result of these vulnerabilities, IT security has become a central issue. Since we are talking about mobile devices accessing mobile and distributed infrastructures, we use the term “mobile security”. The first step prior to setting up a secure mobile infrastructure is to draw up

a wide-ranging security policy that covers all mobile platforms, from PDA to home office. This includes, for example, analysing the security risks and defensive measures. To ensure the confidentiality of mobile applications, the following basic requirements must be satisfied:

- confidentiality of data
- authenticity of the communication partners involved
- data integrity
- legally binding force
- availability of the system
- digital access rights management.

The BSI directs a lot of effort at the issues raised above. These include the following activities relating to “mobile security”, i.e. security in wireless networks:

- the acquisition of fundamental knowledge on standards, network design and mode of operation
- design of own networks for investigation purposes
- analysis of vulnerabilities and methods of attacking wireless networks
- procurement, development, modification and analysis of attack demonstration systems in software and hardware.

The system investigations are conducted either in the laboratory or in field trials. Thus, for example, risk analyses have been carried out for the latest standard versions of the following wireless communications systems: WLAN 802.11x, Bluetooth, DECT, HomeRF, HiperLAN/2, ZigBee, wireless keyboards and mice, IrDA.

The knowledge gained has flown directly into the creation of information publications, consultancy activities and the writing of technical guidelines and test specifications. It is also of assistance both to public administration and industry when it comes to the selection of mobile system solutions. The development of technical guidelines and of product test procedures based thereon is a new area of activity started up at the BSI in 2003. Finally the BSI itself develops tools for the reliable detection and prevention of attacks.

Surfing the internet from the comfort of your sofa with a wireless terminal.

Projects 2003

LWC (Local Wireless Communication)

This project examined the security of wireless local communication systems (WLAN 802.11x, Bluetooth, DECT, HiperLAN/2, HomeRF, Zigbee, wireless keyboards and mice and IrDA).
The results have been presented to a wide public through information brochures, publications and lectures. Practical demonstrations of attacks have explained the risks to audiences in graphical terms. The countermeasures and the principles for WLAN technical guidelines which have been developed will serve as the basis for increased security in wireless communications systems.

MDS (Modular radio detection system)

This project took as its starting point previous investigations of networked mobile radio detectors. These are used to detect the interception of indoor conversations using GSM mobile phones. Building on this, in the feasibility study, the technical possibilities of radio monitoring for the additional UMTS, DECT, WLAN and Bluetooth radio standards were analysed.

TRC-DigID (Technical guidelines for the smartcard platform in the area of digital ID)

Smartcards are becoming an important means of protecting people's mobility (access control, time recording, secure mobile computer and network access, and much more besides). To ensure that the smartcards are secure, interoperable and flexible in use, this project is pursuing the goal of creating a uniform technical standard for different application profiles.

TR-S-WLAN (Technical guidelines for secure WLAN)

The BSI's technical guidelines bring together specific recommendations for the planning, procurement, installation, configuration, acceptance, administration and withdrawal from service of secure WLANs. This means that a significant reduction is possible in the cost of buying in expert knowledge for the procurement and acceptance of secure systems in public bodies and small and medium-sized enterprises.

SME (Security of mobile terminal devices)

A one-year study is examining the extent to which, with today's technical options, mobile terminal devices can be integrated into business processes of whole enterprises under security aspects.

Mobility – with security

The future of mobile application solutions depends on the one hand on overcoming the security problems and on the other hand on economic, social and political factors, such as workable business models, uniform standards, amortisation of infrastructure, unit costs, prices, social acceptance of new mobile services and political and legal framework conditions.

The BSI is actively working on the solution of security problems in the area of mobile communication so that appropriate account can be taken in the future of the need for mobility and security.

From the beach, the living room or the train – wireless data communication between IT terminals is gaining ground.

3. Encryption technology

In view of the increasing exchange of sensitive information within and between federal public administration, contractors entrusted with sensitive information and law enforcement agencies such as the police, intelligence services and the military, highly effective encryption systems are essential.

They have to satisfy the highest security requirements and yet provide sufficient bandwidth for modern applications. The state-of-the-art cryptographic systems developed by the BSI satisfy both requirements. Their use prevents unauthorised persons from either gaining access to raw data or tampering with it unnoticed. Activities in this area are centred around the BSI's Crypto Innovation Programme, initiated in the spring of 2003. The central theme of this is the long-term provision to customers of innovative cryptosystems for the most important IT applications in the area of high security.

The strategic aims of the Crypto Innovation Programme are as follows:

- to consider technology trends on a timely basis
- to reduce development and planning times
- to implement development concepts
- to reduce procurement, operational and follow-up costs for the user
- in the long run, to encourage cryptographic expertise in Germany

The Crypto Innovation Programme is creating a framework of action for the long-term provision of effective and trusted systems to security-critical areas in Germany.

Encryption systems developed by the BSI are used all over the world. Here in the German embassies in Prague (Czech Republic), Maskat (Oman) and Tbilisi (Republic of Georgia), Elcrodat 6-2 protects ISDN-based data traffic for the world-wide exchange of sensitive information at the highest security level (left to right).

The most important products and activities of the BSI in this area are as follows:

Elcrodat 6-2

Together with its partner, Rohde & Schwarz, the BSI has developed this ISDN-based cryptosystem for telephone and data traffic. With Elcrodat 6-2, the encryption functions can be used easily and inexpensively with many telecommunications systems. A public key infrastructure (PKI) that is made available relieves customers completely of the need to supply the system with cryptomaterial.

Today the cryptosystem is used by German law enforcement agencies all over the world. Moreover, for the first time the telephone and data traffic of public bodies connected to the Berlin-Bonn Information Network (IVBB) is, where necessary, being encrypted by the Elcrodat 6-2 cryptosystem. Other organisations both in Germany and abroad, for example NATO and the European Union, have already expressed great interest in the system and plan to protect their communications with ElcroDat 6-2 in the future.

Secure Inter-Network Architecture (SINA)

The SINA architecture was implemented by the BSI in partnership with Secunet. SINA constitutes the basis for the transmission and processing of classified material in local networks (LANs) over a virtual network formed through encryption. This virtual private network (VPN) procedure can also be employed where the internet is used. In this way highly classified material can be transmitted for the first time over the internet with SINA, protected by encryption. In addition, it dispenses with the need for costly material protection on the cable paths and at the workstations. Finally, the distribution channels for classified material are significantly shortened and speeded up.
Again, the use of SINA on the internet eliminates the high cost of leased and dial-up lines, while at the same time transmission bandwidth is a lot higher. Another innovation for such systems is the use of the Open Source operating system Linux in a specially hardened variant. This not only reduces dependence on vendors, but at the same time brings significant savings.

Cryptosystem for digital BOS mobile networks

For public authorities and organisations responsible for security tasks (known in German by the acronym “BOS”), the widespread use of a BSI encryption system shall be a national standard solution in the future BOS mobile network. This encryption system will protect

Continued on page 62

View of the Frankfurt banking quarter – banks and financial institutions need secure encryption technology, too.

Secure network architecture

The SINA cryptosystem constitutes a closed and securely encrypted network (VPN) within an organisation or across national borders. By this means information classified as secret can also be transmitted over the otherwise insecure internet. In the government agency or in the company, the SINA system also significantly simplifies the handling of classified data.

The IT architecture developed by the BSI for handling highly sensitive information in insecure networks operates with a combination of thin client/server processing and virtual private network (VPN) technology. SINA provides the means for implementing flexible high-security systems solutions. Thus, all Germany's foreign embassies are networked via SINA. The hardware variant of the SINA box has been classified "top secret".

At the "Modern State" trade show held in Berlin in November 2003, SINA was demonstrated to the technical public on a joint stand shared by the Secunet company and the BSI.

mobile communications against eavesdropping and interception both nationally and internationally. The use of smartcard-based encryption guarantees flexible and inexpensive adaptation to modern terminal devices. The card assumes all the cryptographic functions and it is a simple matter to adapt it to existing terminal devices. The keys are provided over a PKI. End-to-end encryption was successfully demonstrated in the TETRA prototype network in Aachen using the security card – adapted to Motorola and Nokia terminal devices. By the end of 2004, the security card should have been adapted to TETRA, TETRAPOL and GSM-BOS terminal devices and systems. TETRA, TETRAPOL and GSM-BOS are the digital mobile systems that have been identified by public authorities and organisations responsible for security tasks as candidates for the future digital BOS mobile network.

Implementation of customer-friendly cryptosystems

Supporting the objectives of the Crypto Innovation Programme requires modern cryptographic mechanisms, for example, efficient public key protocols or high-performance encryption algorithms. They are particularly necessary for use specifically in the governmental high security area. The BSI is therefore continuing with the design and analysis of these algorithms oriented towards applications for different projects. These include special narrowband protocols for satellite systems such as Terra SAR and SAR Lupe or the design of a cryptographic procedure. As digital signature applications are increasingly gaining in importance outside governments, the BSI regularly examines the security of the various procedures.

When required, the BSI makes appropriate recommendations for changes to parameters and framework conditions. To assess the suitability of signature algorithms, the BSI is also

collaborating with researchers from the University of Bonn. The result of this year's tests is a new world factorisation record that was published in April. A 160 decimal digit integer that was known to be the product of two prime numbers was split into its prime factors. Numbers of this type form the basis, for example, for the RSA encryption algorithm.

To support the strategic goals of the Crypto Innovation Programme, a flexible but nevertheless secure platform is needed as a cryptographic hardware module. The necessary design work has been driven forward. In parallel, crypto mechanisms have already been implemented on the chips by way of example in less security-critical application environments. To demonstrate the efficient implementation of highly complex public key crypto algorithms on the modules, a new elliptic curve crypto-coprocessor has been developed in reconfigurable hardware.

PC protection

In collaboration with INFINEON AG, the BSI has developed the encryption chip PLUTO. This crypto component is setting new standards for security and functional range: all the necessary basic functions such as encryption, decryption, authentication, key generation and key management are accommodated on a single chip. PLUTO contains function modules for both symmetric and asymmetric cryptographic procedures and protocols. With its impressive encryption capability of up to 2 Gbps, PLUTO has many possible applications.

At present use of the PLUTO chip is confined to the high-security variants of the SINA solution family, where it works alongside the PEPP-1 crypto card developed by Rohde & Schwarz.

4. Human beings in bits & bytes: Biometrics

Electronic procedures for protecting and checking individuals' identity – known as biometric systems – capture features that are unique to each person. They do this in a way that allows machines to recognise and distinguish between individuals. This revolutionary technology offers new possibilities for increasing internal security.

From laser-based iris scanners to temperature-monitored fingerprint systems, the list of technologies that have already been developed is varied and long. Some of the biometric systems offer specific advantages, but many of them also have some fundamental restrictions. For example, it is not yet always obvious which method is suitable for which purpose, or what form the legal and organisational framework conditions should take.

For the BSI, the key issue is to analyse biometric techniques from the point of view of IT security and to participate in international standardisation procedures. Specific solution approaches should be implemented in as realistic an environment as possible in comprehensive trials. This work is proceeding in partnership with other law enforcement agencies such as the Federal Criminal Police Office (BKA) and in close consultation with the Federal Ministry of the Interior.

Moreover, bearing in mind the urgent need for international co-ordination, the basis for harmonised and interoperable solutions must be developed. Active involvement in national, European and international standardisation processes is therefore essential.

The main purposes for which biometric technology will be used are:

- passports and identity cards
- documents for foreign nationals and residence cards
- border checkpoints
- access control in security areas.

From a strategic point of view at the present time the focus of the BSI's project activities is on facial, iris and fingerprint recognition technology. The BSI is an active member of international standardisation committees including DIN, CEN/CENELEC, ISO, ICAO. These activities are necessary to cope with the security requirements and ensure that the systems are truly interoperable.

First of all the biometric systems are being tested at the BSI under laboratory conditions to assess their recognition performance and reliability. This will allow basic conclusions to be drawn about their performance capability. Secondly, in field tests, biometric techniques are being tried out in mass field tests in realistic applications on defined target populations. This will provide information about their suitability for everyday operation.

Continued on page 66

PC keyboard with

sensor field for fingerprint.

Systems that combine smartcard and fingerprint are means of access control.

People can be fooled, but what about computers? This form of access control using automatic facial recognition is based on highly complex mathematical computations related to an elastic grid system.

Another technology aimed at the same objective: a face is measured with the aid of stripe rasters. Four digital cameras and an ordinary PC are sufficient to process the data.

The future Biometrics

Both approaches will serve to reliably assess the capability of biometric systems available on the market. At the heart of the analysis is the identification of vulnerabilities and the development of technical and organisational framework conditions that will permit reliable operation.

A number of activities aimed at studying different aspects of biometrics were started in 2002. The most important focal points and specific results from the year of 2003 are as follows:

BioFace (facial recognition)

The algorithm and field tests have been successfully completed and published. The next element of the project, to examine the influence of noise factors on recognition performance, is close to completion.

BioFinger (fingerprint recognition)

The analysed test results on its performance capability are available with system and algorithm tests.

Bio-P (a general, practically oriented series of projects)

The (mass) testing of facial, finger and iris recognition has concluded with testing of facial recognition on identity documents. The second phase, which will analyse recognition performance and operational reliability with around 2,000 users, has started.

Information database

A global market overview of application products and associated system overviews has been collected in an information database.

Security tests

Within the context of a project initiated by the BSI, standardisation requirements for biometrics have been developed. The first security tests were carried out in the new BSI internal test laboratory that was opened in 2003.

5. Protection of Critical Infrastructures

The use of modern information technologies is creating new vulnerabilities and dependencies: computers control energy systems and traffic and information flows, and without them modern payment transactions would not be possible at all.

State, industry and society rely more and more on fully functioning IT to perform their tasks. As a result, many areas can only function at all if information and communications technology reliably performs its work. If this cannot be guaranteed there could be unforeseeable consequences for state and society. In the face of a multitude of possible and conceivable threats and vulnerabilities, the "Protection of Critical Infrastructures – CIP" is a task that state and industry must tackle together.

The concept "Protection of Critical Infrastructures" differs from pure technical IT security in one major respect, namely, it also considers risks to the state or society as a whole and links them beyond the level of the state into a single general understanding of security. Critical Information Infrastructure Protection (CIIP) is a significant element here.

Organisations and establishments that are designated Critical Infrastructures are essential to the community. Disruption or failure of these systems would threaten large sections of the population with enduring supply bottlenecks or other serious consequences. State and economy can only function if the following Critical Infrastructures are available at all times without significant degradation:

1. telecommunications and information technology
2. energy
3. financial and insurance systems
4. the transport system
5. health care
6. emergency services
7. public agencies and public administration.

IT security contributes significantly to the functioning of these areas. But this alone cannot offer adequate protection. Rather, an all-embracing security concept is required that includes the following components as well as purely technical measures:

- prevention, aimed at minimising the occurrence of incidents
- early detection of threats and threat situations
- containment and limitation of the effects of breakdowns on state and society
- elimination of the technical causes of breakdowns.

New forms of co-operation are necessary

A broad, uniform protection concept for Critical Infrastructures which extends beyond technical measures requires new forms of co-operation between state, industry and society.

A number of initiatives and projects which can be rated as either directly or indirectly falling within the area of "Protection of Critical Infrastructures" as we understand it today, have already existed in Germany for about ten years. Thus, for example, the BSI has commissioned analyses of seven Critical Infrastructure areas in Germany, set up a "Co-operation KRITIS" between representatives of industry and the BSI and stepped up co-operation with the universities and research establishments.

The BSI is also creating a "National Plan for the protection of IT-dependent Critical Infrastructures" for the first time. The centrepiece of this plan is the presentation of a concept as to how to protect Germany's Critical Infrastructures over the next few years. This vision has four strategic objectives: prevention, response, awareness raising and sustainability. For each of these objectives, details have been worked out for the three areas of government, private industry and population, with specific statements on responsibilities, target groups and initial actions.

The Federal Chancellery, a railway line, Berlin-Tegel airport – IT-dependent critical infrastructures need full protection.

Critical Infrastructures affect not only state-owned structures but also private sector organisations throughout Germany. To ensure that all these areas function reliably, it is essential that all the responsible offices act together. Coordination and the exchange of information are imperative. Only through intensive collaboration between industry and state this goal can be achieved effectively. For this reason, initiatives and public-private partnerships play an important role in Germany as a connecting link between state and industry.

One initiative worth mentioning here is the D21 initiative. 300 companies have joined together into a non-profit-making, cross-industry association aimed at promoting the transformation from industrial society to information society, in collaboration with government and public administration. In the “Arbeitskreis Schutz von Infrastrukturen” (AKSIS), companies and government agencies share their experiences. They analyse the dependencies of critical sectors on IT and their interrelations with each other.

The results gained through partnership ultimately benefit everyone: the direct participants through more robust systems and, ultimately, the entire population of Germany through higher security.

Protection of Critical Infrastructures cannot be achieved by individual nations acting alone. Given the high level of international networking, to achieve comprehensive protection of Critical Infrastructures the BSI also discusses objectives and results internationally, at congresses and conferences, G8 committees and NATO.

The protection of Critical Infrastructures is becoming more and more important both nationally and internationally. Drawing on the example of 18 countries and three international or supranational organisations, this study published in 2003 presents the status of activities relating to the protection of Critical Infrastructures in a scope and approach that are unique. It is less a detailed report of results than an examination of the protection of Critical Infrastructures from programming, planning and conceptual viewpoints.

1. CD-ROM

The information published by the BSI on the internet is available to anyone interested in the form of a free CD-ROM.

How to obtain the BSI CD-ROM
Send a self-addressed envelope (DIN C5) to:
BSI CD Distribution,
P.O. Box 20 10 10,
D - 53140 Bonn, Germany.

The BSI's information offers are available from *www.bsi-fuer-buerger.de*, where they are constantly updated. A CD version of the web portal is also distributed at trade shows and with technical publications. On certain PCs, the CD contents are preinstalled.

2. BSI newsletter

Would you like to subscribe to the BSI's online newsletter? If so, please send an e-mail to:
newsletter@bsi.bund.de

3. <kes> – the information security magazine

Official announcements are published in the BSI Forum in the <kes> magazine.
<kes> – Die Zeitschrift für Informations-Sicherheit
(ISSN 1611-440X)
Price per issue: g 23, appears bi-monthly

Internet: www.kes.info
Contact details: Editorial office <kes> Lise-Meitner-Str. 4, 55435 Gau-Algesheim, Germany
or P.O. Box 1234,
D - 55205 Ingelheim, Germany
Tel: +49 (0)6725-93 04-0
e-mail: info@secumedia.de

4. Technical information

Conference Proceedings: Deutscher IT-Sicherheits-kongress – IT-Sicherheit im verteilten Chaos
Published by the BSI, 2003
ISBN 3-922746-49-7, price g 49.10
Can be obtained from: SecuMedia Verlags GmbH
P.O. Box 1234, D - 55205 Ingelheim, Germany
Tel: +49 (0)6725-93 04-0, fax: +49 (0)6725-59 94
Internet: www.secumedia.de

IT Baseline Protection Manual
(english version only on CD-ROM)
The IT Baseline Protection Manual is distributed by the Bundesanzeiger Verlag as a loose-leaf binder.
ISBN 3-88784-915-9, Basic volume, A4, approx. 2,000 pages in three binders, Set of loose-leaf pages with CD-ROM, price g 148, Please send your orders to: Bundesanzeiger Verlag
P.O. Box 10 05 34, D - 50445 Cologne, Germany
e-mail: vertrieb@bundesanzeiger.de

Leitfaden IT-Sicherheit
2003 edition, approx. 42 pages
Download as PDF file from
www.bsi.bund.de/gshb/Leitfaden/index.htm

E-Government Manual, ISBN 3-89817-180-9
(english version only on CD-ROM)
BSI series on IT security, volume 11
Loose-leaf, 1,200 pages, three binders, DIN A5
Price: g 98
Please send your orders to:
Bundesanzeiger Verlag, PO Box 10 05 34
D - 50445 Cologne, Germany
Fax: +49 (0)221-97 66 82 78
e-mail: vertrieb@bundesanzeiger.de

Drahtlose lokale Kommunikationssysteme und ihre Sicherheitsaspekte
Published 2003, approx. 62 pages
Download as PDF file from
www.bsi.bund.de/literat/doc/drahtloskom/index.htm

Internationale Aktivitäten zum Schutz Kritischer Infrastrukturen, ISBN 3-922746-54-3
Can be obtained from: SecuMedia Verlags GmbH
P.O. Box 1234
D - 55205 Ingelheim, Germany
Tel: +49 (0)6725-93 04-0, fax: +49 (0)6725-59 94
Internet: www.secumedia.de

5. Studies

Kommunikations- und Informationstechnik 2010+3
New trends and developments in technology, applications and security
Published by the BSI, 2003
ISBN 3-922746-48-9
Price: g 78
Can be obtained from:
SecuMedia Verlags GmbH
P.O. Box 1234, D - 55205 Ingelheim, Germany
Tel: +49 (0)6725-93 04-0
Fax: +49 (0)6725-59 94
Internet: www.secumedia.de

Apache Webserver – Sicherheitsstudie
Published by the BSI, 2003
ISBN 3-922746-46-2
Price: g 19.80
Can be obtained from: SecuMedia Verlags GmbH
P.O. Box 1234
D - 55205 Ingelheim, Germany
Tel: +49 (0)6725-93 04-0
Fax: +49 (0)6725-59 94
Internet: www.secumedia.de
PDF version can also be downloaded from
www.bsi.bund.de/literat/secumed.htm

Microsoft Internet Information Server – Sicherheitsstudie
Published by the BSI, 2003
ISBN 3-922746-47-0
Price: g 19.80
Can be obtained from: SecuMedia Verlags GmbH
P.O. Box 1234
D - 55205 Ingelheim, Germany
Tel: +49 (0)6725-93 04-0, fax: +49 (0)6725-59 94
Internet: www.secumedia.de
PDF version can also be downloaded from
www.bsi.bund.de/literat/secumed.htm

Leitfaden zur Einführung von Intrusion-Detection-Systemen
Can be downloaded as a PDF file from
www.bsi.bund.de/literat/studien/ids02/dokumente/Leitfadenv10.pdf

Information on other BSI publications can be found on the internet at *www.bsi.bund.de*

Appendix contact persons

Born in 1955, he studied Physics and Mathematics, worked at the Institute of Theoretical Physics at Ruhr University Bochum as a scientist until 1983. Head of department at the Bergisch University in Wuppertal until 1989, when he moved to Messerschmitt-Bölkow-Blohm (now EADS). Up to 1995 he held various management positions there. Before taking up his appointment at the BSI in 2003, he was a director and divisional manager at the Bayerische Versorgungskammer, Munich.

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

Born 1950, studied Mathematics in Bonn. In 1977, he joined the federal administration as a consultant and in 1985 was promoted to head of section, IT Security. Following the foundation of the BSI, he became head of department and played a major role in building up and expanding the work of the BSI. Since 1994 he has been the Vice President, in which capacity, as the national director for communications security, he has been the German representative on NATO and EU IT security committees.

Michael Hange, Vice President

Born 1963, studied Administrative Science in Konstanz, graduating in 1988. Worked on the academic staff of the universities of Konstanz and Bonn and also at the Nuclear Research Centre in Karlsruhe, joined the BSI in 1993. Since then has specialised in security culture, education and raising awareness of IT security issues.

e-mail: Anja.Hartmann@bsi.bund.de

Anja Hartmann, Head of Public Relations and Marketing

Born 1955, studied Jurisprudence in Bonn, lawyer. Moved to the disaster relief organisation of the Federal Republic of Germany (THW). Following the foundation of the BSI in 1991, he was appointed section leader, Organisation, and also Press Officer.

Any questions and suggestions on press releases should be sent to michael.dickopf@bsi.bund.de.

Michael Dickopf, Press Officer

The BSI on the internet

The Citizens' Portal: www.bsi-fuer-buerger.de

The Citizens' Portal offers information on a variety of topics, including

- data backup
- viruses and espionage
- protection of children on the Internet
- internet shopping

along with a download area that includes

- encryption tool
- virus scanner
- PC firewall program
- screen saver.

The portal for IT professionals: www.bsi.bund.de

Specialists and experts can find information here on subjects that include

- certification
- E-Government
- CERT-Bund (CERT for Computer Emergency Response Team)
- digital signatures
- IT Baseline Protection
- Critical Infrastructures
- malicious programs

along with information on events, training and publications.

Address
Federal Office for
Information Security (BSI)
Godesberger Allee 185-189,
D - 53175 Bonn, Germany
Tel: +49 (0)228-95 82-0
Fax: +49 (0)228-958 24 00
e-mail: bsi@bsi.bund.de

The BSI on the internet
www.bsi.bund.de
www.bsi-fuer-buerger.de

Photo Credits
Pierre Boom, Bremen Online Services, BSI Referat Öffentlichkeitsarbeit, Caro Fotoagentur, Das Fotoarchiv, Deutsche Bahn, Deutsche Telekom, Andreas Ernst, European Commission Audiovisual Library, Fujitsu Siemens Computers, Hans Georg Gaul, Geschäftsstelle Bundesprogramm Ökologischer Landbau, Paul Glaser, Institut für Mikrotechnik Mainz, Nokia, Jan Pauls, Photodisc, Presse- und Informationsamt der Bundesregierung – Bundesbildstelle, Presse- und Informationsamt der Bundesstadt Bonn, Siemens Presse-bild, Vodafone D2, Frank Weihs

Published by
Federal Office for Information Security (BSI)
D-53175 Bonn
GERMANY

Reference office
Federal Office for Information Security (BSI)
Section III.21
Godesberger Allee 185-189, D-53175 Bonn, Germany
Tel: +49-(0)228-95 82-0, e-mail: bsi@bsi.bund.de
Internet: www.bsi.bund.de

Text and editorial staff
Tobias Mikolasch, BSI; Thomas Presse & PR, Berlin/Bonn

Translation
Lettera, Staufen, Internet: www.lettera.biz

Layout and design
Thomas Presse & PR, Berlin/Bonn
Graphics: Annette Conradt
Internet: www.thomas-ppr.de

Printing
Druckhaus Dierichs Akzidenz GmbH, Kassel

Date
March 2004