

ID Security – Made in Germany

Holistic Solutions for Biometrics and eIDs



Personal Identity: Unique, Secure, Multifaceted.

Everyone has unique characteristics by which he or she can be clearly identified. When we interact with other people, we use these characteristics to help us recognise them. As more and more areas of life now shift towards the Internet, however, face-to-face identification is seldom possible – we have to find new ways for identification. In this context, biometrics have become the internationally established method for ensuring reliable digital personal identification. Personal characteristics are recorded, digitised and saved as electronic data, for example in passports and identity documents.

This technology has two decisive advantages:

1. Biometrics ensure that identities are just as distinctive and reliable on the Internet as they are in the analogue world and that they are equally secure. The data cannot be easily manipulated or counterfeited.

2. With the introduction of passports and identity documents that are protected using biometric identifiers, this technology already plays a part in the everyday lives of many people and provides numerous convenient and pioneering application possibilities in wide ranging business sectors, such as

- automated security for national borders,
- identification of travellers,
- ensuring secure transactions on the Internet,
- legitimate procurement of government services,
- authentication for access to sensitive rooms or areas, or to networks, mobile terminals and workstations.



Globally Secure Identities – Thanks to Expertise “Made in Germany”

The German Federal Office for Information Security (BSI) is committed to incorporating biometric identifiers in official documents. Amongst other things, the experts at BSI have

- provided vital input to the main standardisation committees to ensure the creation of secure yet practicable international standards
- carried out the world’s largest field test to evaluate the biometric modalities that are most suitable for use in identity documents
- initiated and supported the development of open, modular and standardised products. Many states have tested the interoperability of their documents, using the Golden Reader Tool, for example, at various international meetings of experts.

Thus, the BSI has made a comprehensive contribution to global identity protection and is now internationally recognised as a forerunner in the field of biometrics. A good reason to have confidence in future-proof biometric products that are “made in Germany”.

Global Systems for a Secure Identity Worldwide.

In Germany, modern, highly-secure identity protection for every citizen has long been considered a self-evident part of German culture. Identity documents from Germany are among the most forgery-proof in the world; and Germany is also at the forefront internationally with regard to electronic identity documents, campaigning actively for the highest possible level of identity protection. Biometrics is THE technology that makes unambiguous proof of a person's identity possible, even in the digital age, and protects personal data from manipulation and misuse – and all states worldwide generally agree. These states have therefore agreed that biometrically protected identity documents in the form of electronic, machine-readable passports shall be introduced worldwide by the year 2015. In order to ensure the advantages of using national documents also in an international context, the International Civil Aviation Organisation (ICAO) has produced unified international standards that will ensure the

global interoperability of electronic passports and shall be binding for all 194 states. Additional requirements are specified by the EU and national passport regulations.

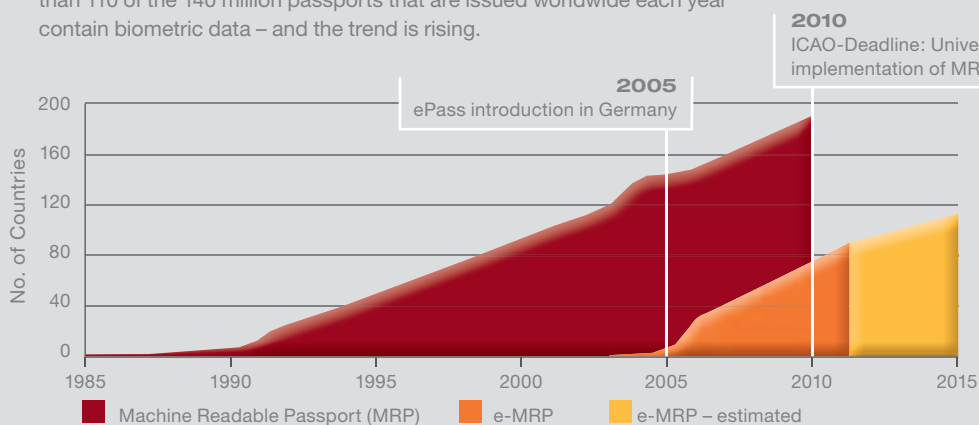
A secure identity involves more than just a forgery-proof identity card, however. The identity protection systems (ID systems) behind them must also be designed to be highly secure. They cover

- the registration and management of personal data,
- the production and issuance of the documents,
- the reading of the saved data – for example at border controls,
- applications on the Internet.

All the stages of this process chain, the so-called eID life cycle, depend on digital networks that are highly complex and, in some cases, globally connected.

The Changing Travel Documents Landscape*

More than 90 states are already issuing electronic passports and more than 110 of the 140 million passports that are issued worldwide each year contain biometric data – and the trend is rising.



Global identity protection – an important and complex task. All states must rise to this challenge.

The Highest Level of Identity Protection. With secunet's Holistic Expertise.

The need for safety and transparency is increasing: authorities, public institutions and companies worldwide are confronted with increasingly strict legal and global requirements. The correct use of data and the transparency of IT-based processes have become fundamental. Biometrics provide new, innovative possibilities and solu-

tions for reliable identity protection. To be able to put these into practise, specialists are needed who understand the complexity of the requirements and the highly fragmented market and are proficient in understanding and managing connected processes and technologies on a global scale.

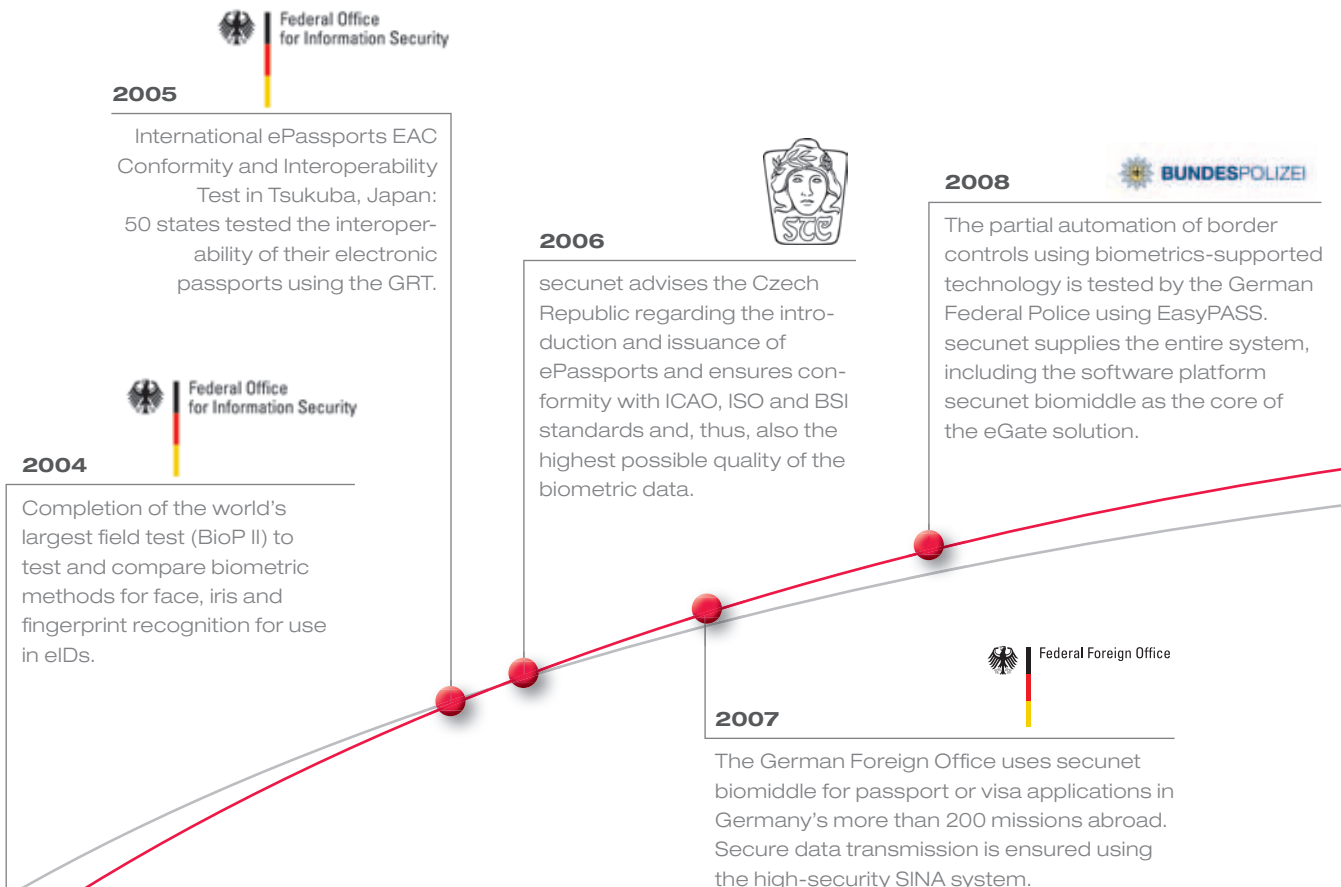
secunet offers you ...

... the highest level of security at all times

secunet's biometric solutions guarantee the highest level of identity protection at all times. As IT security experts and specialists in high-security solutions, we combine biometrics with other relevant security technologies to optimise our customers' systems with regard to security and economic efficiency.

... a holistic view of the entire eID process chain

We do not see identity protection as a single solution; we always have the whole process chain in mind. This is a decisive advantage for our customers: the biometrics specialists at secunet have a better understanding of the effects a new project will have on previous or subsequent process stages than anyone else. For our customers, this guarantees smooth integration of their solution into the overall process.



... innovative, tried and tested solutions for every type of requirement profile

secunet's experts are actively involved in the international committees that are setting standards worldwide. All our solutions are developed in strict adherence to these standards and we are able to apply the essential expertise and experience gained in the standardisation committees to our customers' projects and solutions. Our customers benefit from proven consultation and solutions that cover the latest standards and technologies at once.

... an optimal cost-benefit ratio

The more diverse the fields of application, the more secunet ensures that solutions are implemented on a needs-oriented basis. Whether the customer requires solution modules, the development of individual software components or competent technical consultation – secunet is committed to accurately tailored and precise implementation of the customer's requirements. We take into account all the relevant aspects and deliver solutions that can be integrated simply and seamlessly into the target systems. Our customers profit from low "total cost of ownership".

... innovations and quality "made in Germany"

secunet is security partner of the German Federal Government and has been working closely with the BSI in the field of biometrics for many years now; these partnerships continue to expand our solid understanding of customer requirements in the public sector environment and of the requirements of the market. Working together with the BSI, we develop products that are conform to modern standards and internationally recognised as reference implementations. At the same time, we work intensively with BSI experts on research into subjects of future interest and transform established biometric procedures to produce new generations, such as the NFIQ algorithm.

Service portfolio:

- Consulting and concepts
- System evaluation and assessment
- Ready-made solution modules and customised solutions
- Products for every phase of the eID life cycle
- Integration, service, support

2008



The European Union tests the use of biometric technology for visas with eight states taking part; Germany and Belgium decide in favour of using secunet biomiddle.

2010



The Austrian Federal Ministry for the Interior chooses secunet biomiddle as their strategic platform for border controls and application procedures for electronic residence permits; 500 representative authorities abroad are equipped with the software.

2014

SAC

ICAO regulations come into force: Supplemental Access Control (SAC) becomes the new standard for improved protection of biometrics in eIDs.

2009

Bundesministerium für europäische und internationale Angelegenheiten

The Austrian Foreign Office uses secunet biomiddle for visa applications in its 120 representative authorities abroad. secunet supplies the complete visa package and the hardware for fingerprint capture.

2011



Working in a transatlantic team of experts, secunet develops an improved algorithm for assessing the quality of fingerprint images (NFIQ 2.0).

The secunet eID Life Cycle. Holistic Identity Protection, All from One Source.

secunet has developed market-leading technologies for each process stage in the eID life cycle. These protect digital identities, create automated and thus optimised processes for our customers and can be modified to accommodate future requirements. Solution modules from secunet are tried and tested, mature and ready for use. They are resolutely in compliance with the standards, multifaceted, modular, globally interoperable and can be seamlessly inte-

grated into our customers' systems, creating high-performance comprehensive solutions. For our customers, this equates to maximum security with low "total cost of ownership".

In combination with the holistic consulting expertise of our IT security specialists, these high-security solutions ensure that identities are uniquely secure and uniquely multifaceted, even in the digital age.

Biometric solutions from secunet are always guaranteed to ensure ...

- ... high security for the entire eID life cycle,
- ... consistent quality "made in Germany",
- ... low "total cost of ownership",
- ... secure investment and future-proof systems due to technologies that are resolutely standard-compliant,
- ... cutting-edge solutions through development guarantees and expertise from standardisation committees.

Applications

Types of use

Holistic solutions for enrolment and the high-security transfer of this data

secunet technology secunet biomiddle –

for quality-assured capture and recording of biometric data; middleware that is platform-independent, standard-compliant and recommended by the German BSI as a reference-implementation for biometrics and identity documents

SINA –

BSI approved high-security solutions for protected processing, saving and transmission of classified or sensitive data via open networks

Production

Types of use

Proven components for the production of interoperable, standard-compliant ID documents

secunet technology GRT Platinum Edition –

for reliable and secure readouts of electronic identity documents; passport producers can subject their products to a quality check before dispatching them

eID Test Suite –

formal testing tool for producers of electronic passports / individual passport components

ePassportAPI

eID PKI Suite

Issue

Types of use

Modules to ensure reliable quality control and verification

secunet technology ePassportAPI –

standard interface for electronic identity documents; enables secure communication with these documents and allows reading devices to be linked in

secunet biomiddle GRT Platinum Edition

The Middleware that Brings Together Biometrics and eIDs.

All the biometric applications in the eID life cycle have to be absolutely up-to-date at all times. This means that they must be extremely adaptable: it should not be necessary to replace the entire system every time biometric technologies or standards undergo further development in this highly dynamic market; or whenever new methods are introduced to improve anti-counterfeiting protection; or when new requirements relating to biometric applications are introduced. Flexible solutions that nonetheless provide investment security can be achieved using adaptable architecture concepts that are conform to the standards. The basis for these solutions is secunet biomiddle.

This software functions as middleware that connects client applications with all the established biometric technologies available on the market. These include hardware, such as fingerprint scanners, passport readers, or cameras for face recognition, as

well as software and complex background and authorisation systems. secunet biomiddle uses interfaces that comply with the standards and enable all the technological sub-components in the overall system to be used as modules – as a result the replacement or upgrading of components is not restricted in any way.

On the application side, secunet biomiddle minimises complexity and expenditure by using internationally accepted biometric standards and the manufactured components connected to the system: All biometric functions are made available to the application as bundled data via a service-oriented interface and can therefore be integrated quickly and easily into existing systems. The SOAP interface creates greater flexibility on the client side with regard to performance, scalability and independence from platforms and programming languages.

Use

Types of use

Secure systems for reliable, worldwide check of identities

secunet technology

EasyPASS –

complete solution for modern automated border controls

eID PKI Suite –

central infrastructure for international certificate exchange and -management

secunet biomiddle

GRT Platinum Edition

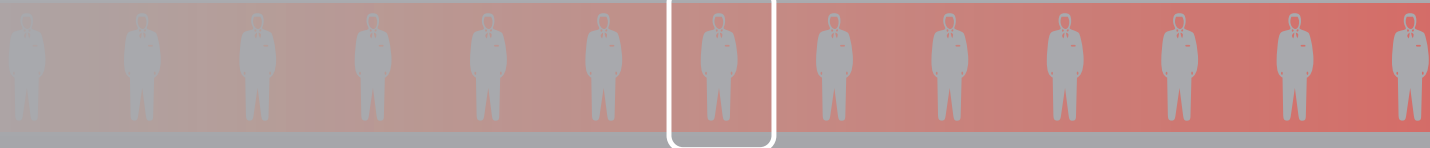
ePassportAPI

secunet biomiddle at a glance:

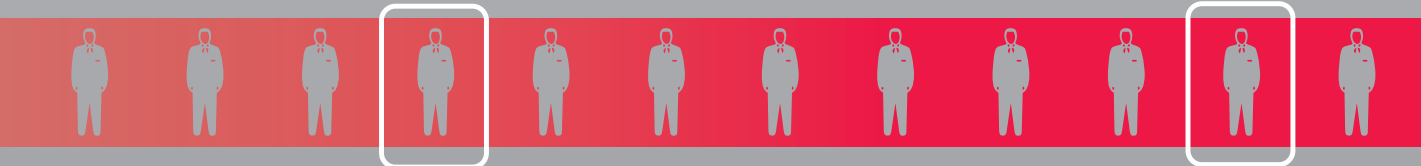
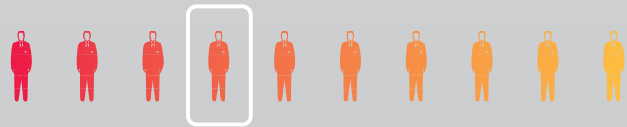
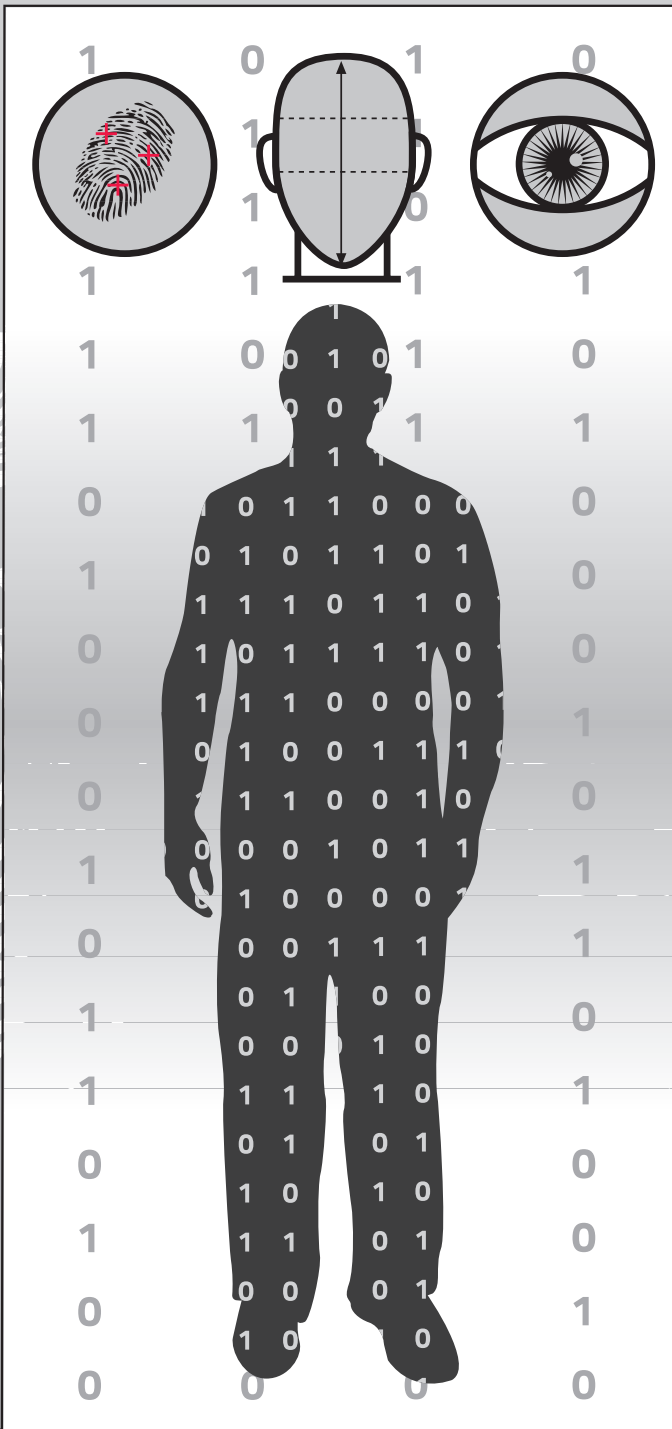
- Standard-compliant: internationally standardised interfaces (BioAPI 2.0 / ICAO/BSI) ensure flexibility and independence from specific manufacturers.
- Modular: subcomponents in the overall system can be replaced at any time.
- Adaptability: can be integrated easily into existing systems.
- Investment security: guarantee of continuous development until at least 2020.
- Made in Germany: developed in cooperation with the German Federal Office for Information Security (BSI).

Border Crossing Scenario

secunet biomiddle can be used for all types of verification and identification – for example at border crossings, as illustrated here.



Phase 1:
Verification of the passport
or travel document



Phase 2:
 Verification of the
 biometric identifiers

Phase 3:
 Border crossing after
 positive verification process

The Future of Automated Border Controls is Called EasyPASS.

The constantly rising number of passengers and a simultaneous increase in the level of security awareness present a huge challenge to both, the technology and personnel at airport border controls. Thus, the main focus today is on new and efficient solutions based on biometric technology – a task for the biometrics specialists at secunet.

At Frankfurt Airport in Germany, passengers carrying an electronic passport can experience first hand just how quickly and securely a modern border control system can operate. This is where the first eGate system in Germany (EasyPASS) was installed. The system checks the authenticity of the



document automatically, reads the electronic facial image and compares the biometric data with a live photograph of the passenger. As general contractor for the German Federal Office for Information Security (BSI), secunet was responsible for the entire project implementation and supplied the central components, the secunet biomiddle integration platform, the control software and the monitoring application for the border officials. The BSI has also commissioned the experts at secunet with modifying the semi-automatic border control system to handle the new national identity card, so that even more passengers will be able to benefit from shorter waiting times.

The advantages of EasyPASS at a glance:

- Optimum security due to
 - » checking of optical and electronic security identifiers
 - » biometric comparison at a high security level
 - » online retrieval from police background systems
 - » monitoring by border officials
- flexible replacement of all technical components possible by means of open and standardised architecture
- fast overall process (approximately 18 seconds)
- easy integration into existing infrastructure
- quick and intuitive operation by passengers
- testing of the security and reliability of the system by the BSI



“The use of electronic travel documents and biometric technologies requires entirely new test-mechanisms and systems. Evaluating the security of such procedures is one of the core tasks of the BSI. Our evaluations of the pilot project EasyPASS show that biometric procedures and electronic test-processes are consistently reliable if the complete system is suitable designed.”

Bernd Kowalski, Head of Department,
German Federal Office for Information Security (BSI)

Mobile Personal Identity Checks and Border Controls – Highly Secure and User-friendly.

Mobile devices that are used for verifying electronic documents and checking the biometric data contained in these documents are gaining significance in proportion to the increasing use of electronic passports and personal identity cards in everyday situations and the increasing number of passengers travelling across borders by bus or train. Within this context, the German Federal Police are planning to strengthen

their mobile border controls significantly in future. This will include the acquisition of mobile hardware for checking electronic documents and biometric data. In using devices that are equipped with secunet biomiddle, the German Federal Police are establishing a future-proof system that guarantees long-term flexibility, investment security and interoperability.



Deutsche Lufthansa checks travel documents at international hot spots using secunet's mobile verification system

secunet has developed an automated, mobile passport verification system for Deutsche Lufthansa. The system provides trained Lufthansa personnel with support in checking travel documents optically before check-in. The essential optical security identifiers of the documents are checked in UV, infrared and visible light and their validity and accordance with the reference database is verified. Forged travel documents carried by passengers heading for or stopping over in Germany can thus be identified in the country of departure and the illegal carriage of persons can be prevented at an early stage.

The necessary hardware – a document reader and a laptop – is housed in a robust carrying case and is controlled via verification software developed by secunet with an underlying document database. The mobile system can be operated intuitively by Lufthansa staff and is thus extremely flexible in its scope of application. The system is used alternately at various “hot spots” abroad – that is at airports with a high potential for abuse. The integrated middleware secunet biomiddle ensures additional flexibility: other reader devices can be added without difficulty, if necessary, and future technologies can be integrated later as required.

Whether with eID Card, ePass or biometric visas, at mobile or stationary checkpoints, in national or international use – every border control is guaranteed to be secure, flexible and cost-effective with secunet biomiddle at its core.

The Solid Trust Anchor for Secure Identities Worldwide. Comprehensive Protection for ePass, Residence Permits and National eIDs.

Modern identity documents such as the ePass make it possible to expand established processes extensively and make them more efficient and secure. The possibility of saving personal data digitally on the integrated RF chips, for example, enables border control processes to be automated and mobile control scenarios to be established. Before these new processes can be implemented, however, all 194 states worldwide must first exchange information, such as certificates, with each other – for an estimated one thousand million air passengers each year as well as for passengers travelling by land or sea. Complex infrastructures are required in the background if the visible processes are to be made significantly faster and more secure.

In each case, comprehensive Public Key Infrastructures (PKIs) form the backbone of the security framework. While the ICAO PKI ensures the integrity and authenticity of the documents, a second PKI, the EAC PKI, is required to provide extended access protection. The implementation of comprehensive control processes is particularly complex due to the necessary exchange of the required certificates in both PKI worlds and across all states worldwide: a wide range of

information, such as various certificates or revocation information is required in order to check the authenticity and integrity of a document. For access to the fingerprints, there is also a requirement for authorisation certificates and keys that need to be updated regularly, in some cases daily.

To this end, secunet has created a security infrastructure that is both innovative and comprehensive: The eID PKI Suite establishes a high level of security while also minimising the complex requirements on the verification system. A central control system, the so-called Terminal Control Centre (TCC), is able to provide the service of carrying out the cryptographic processes for the verification system, i. e. the complex and security-sensitive handling of certificates and keys need no longer be carried out by the local verification system.

All software modules of the eID PKI Suite put together are a high-performance complete system, yet they can also be integrated individually into an existing system architecture. Thus, secunet contributes significantly to the improvement of global identity verification and paves the way for modern processes in border controls.

The eID PKI Suite at a glance:

- All in one: covers the requirements of issuance, infrastructure and verification (ICAO, EAC)
- Flexible: modular, scalable, standard-compliant
- Advanced: supports all EAC versions
- Cross-linked: with SPOC for the national and international exchange of certificates
- Central: Terminal Control Centre for passive and terminal authentication including certificate management
- Mature: builds on knowledge and experience from over 250 PKI and eID projects



Deutsche Post Signtrust offers authorisation certificates in accordance with EAC 2.0 for the new eID card with the help of secunet eID PKI Suite

The trust centre of Deutsche Post is an accredited provider of certification services in Germany and issues authorisation certificates for the new identity card. As the software solution for its certification services, Deutsche Post Com GmbH uses secunet's eID PKI Suite. This PKI solution issues authorisation certificates for service providers and performs the role of a central communications interface between the parties involved, i.e. citizens, service providers, government agencies and the root certificate authority. Targeted management of the information flow ensures that each party receives only the information that it needs and is entitled to receive.

"With electronic identity verification, citizens and service providers alike now know exactly who they are dealing with, also on the Internet – this increases the level of mutual trust. We are pleased that in our role as certification service provider we have been able to make a contribution in this regard. The new service represents an important milestone for the Deutsche Post portfolio. For the technical implementation of the service, we opted for eID PKI Suite and the support of our long-term partner secunet and kept perfectly to the ambitious time schedule."

Sabine Buchhalter, Director of Signtrust,
Deutsche Post Com GmbH

Proven Security for Reliable Readouts of Identity Documents. Equipped to Accommodate Future Generations.

The secunet Golden Reader Tool (GRT) Platinum Edition can be used in all areas where it is necessary to read out identity documents reliably and securely or to verify their authenticity:

- Passport producers and authorities that are responsible for issuing identity documents can use the GRT to check the functionality and verify the data of the document before dispatching them.
- Stationary and mobile border controls can use the GRT to verify passports and electronic residence permits.
- Security authorities are able to identify forged passports.

The GRT system was developed in cooperation with the German Federal Office for Information Security (BSI) and has proved itself internationally, setting new standards worldwide and creating important bases for the interoperability of electronic travel documents in accordance with ICAO and EU requirements. The further development and commercial version, the secunet GRT Platinum Edition, continues to set standards: it already supports the Supplemental Access Control (SAC) mechanism, i.e. the ICAO standard that from 2014 on will ensure that access to identity documents is even more secure.

GRT Platinum Edition at a glance:

- **Advanced:** supports SAC and all EAC versions
- **Expandable:** works in biometric scenarios via BioAPI / biomiddle
- **Adaptable:** multiple functionality, flexible design and various areas of application
- **Internationally proven:** recognised as the reference implementation worldwide
- **Made in Germany:** developed in cooperation with the German Federal Office for Information Security (BSI)

A project on behalf of



Moving towards New Generations of Biometrics – New Approaches and Improved Processes with secunet’s Expertise

On behalf of the German Federal Office for Information Security (BSI), secunet has been researching since 2005 the so-called biometric cryptosystems as part of the BSI BioKeyS project series. These cryptosystems combine the advantages of biometrics with tried and tested cryptographic processes and will help make it possible in future to use biometrics with particular efficacy in terms of data protection. In order to ensure maximum flexibility, the BSI aims to develop open biometric cryptosystems that are able to adapt to the widest range of application scenarios and requirements – an enormous challenge that requires innovative approaches and research at the highest level. A good task for secunet’s biometrics experts.

The biometric cryptosystems ensure that, as in passport processes, biometric data read from identity documents is no longer stored in clear text form but as a public reference dataset. Reconstruction of the biometric information from reference data is impossible, as this can only be used for the testing of a single characteristic or feature submitted for the purpose of comparison. The electronic identity thus remains strictly personal and confidential.

secunet: Premium IT security Made in Germany.

secunet is one of Germany's leading specialists in innovative and sophisticated IT security. In close dialogue with our customers, we have been developing high-performance products and advanced IT security solutions since 1996. At secunet, more than 280 experts concentrate on issues such as cryptography (SINA), eGovernment, business security and automotive security, with the aim of always being one step ahead of the competition in terms of quality and technological advance.

We provide comprehensive security for the IT infrastructures of our customers and create intelligent, efficient processes and sustainable added value. Our speciality is

the diverse range of issues that encompass the security of the internal and external communications of authorities, the protection of entire process chains in eGovernment, the security of critical infrastructures, and the further development of security technologies, such as the ePass, electronic tax declarations and De-Mail.

The close partnership with the German Federal Office for Information Security (BSI) and our security partnership with the German Federal Government are particular indicators of our comprehensive competence and trustworthiness in the public sector – quality “made by secunet”, quality “made in Germany”.

Customised solutions for every type of requirement profile with secunet

- Proven, future-proof product quality “made in Germany”
- Technological and system competence combined with in-depth know-how in the field
- Expertise acquired in the international standardisation committees
- Close cooperation with the German Federal Office for Information Security (BSI)
- Comprehensive identity protection, all from one source

Holistic Solutions for Comprehensive Identity Protection, Economic Efficiency and Convenience

Our specialists think of biometrics not as an individual security solution but as an integral part of the overall field of IT security. When designing solutions for identity protection, they look far beyond the horizon of pure biometrics: other relevant matters, such as the effective protection of personal data and electronic identities during data transmission, are also taken into consideration.

Working together, the German Federal Office for Information Security (BSI) and secunet developed the high security solution SINA, of which almost 30,000 components are already in use both in Germany and abroad. SINA, which stands for “Secure Inter-Network Architecture”, enables the protected processing, saving and transmission of classified or sensitive data via open networks. SINA is the only IPsec-based cryptosystem that is approved for all levels up to the highest national confidentiality level, “TOP SECRET”, in Germany and is a further product that carries the “made in Germany” seal of quality.





secunet

secunet Security Networks AG
Kronprinzenstrasse 30
45128 Essen, Germany
Telephone: +49-201-5454-0
Fax: +49-201-5454-1000
biometrics@secunet.com
www.secunet.com

