Enhanced security against falsification and misuse is a key advantage of the new electronic passports, residence permits and identity cards, according to the Federal Office for Information Security (BSI). An important security feature of the official documents is the contactless security chip. The biggest supplier of these semiconductors in Germany is NXP semiconductors, one of the world’s leading providers of identification chips. Around 80 percent of all countries that have already introduced electronic passports rely on the company’s highly secure chips.

NXP not only supplies the right hardware for the national printing houses, but also the software that allows the personal data to be read securely using access-approved readers. When it comes to choosing a card operating system, NXP has relied on T-Systems for years. With its Telesec Chipcard Operating System (TCOS), the ICT service provider offers a multifunctional and highly secure smartcard operating system which, apart from being used on chips for identity documents, is also used on chips in toll, tachograph, signature, and company cards. TCOS is now used worldwide on more than 100 million smartcards.

**AT A GLANCE**

- National printing houses are seeking suppliers for contactless chips in the course of converting to electronic passports, residence permits, and identity cards.
- NXP supplies its SmartMX chips for the electronic passport, the new identity card, and the residence permit card.
- With TCOS, T-Systems offers a highly secure, fast, and flexible operating system for secure microprocessors.
- TCOS allows administration and protection of the data stored on the chip.
- The latest cryptographic procedures are used to protect the data from external access.
- T-Systems implements TCOS on NXP’s P60 chips (Common Criteria EAL 6+ certified).
- TCOS Passport is security-certified in accordance with Criteria EAL4+ and fulfills the strict security requirements of Guideline TR 03116 issued by the Federal Office for Information Security (BSI) in 2013.
THE CUSTOMER

NXP semiconductors is one of the world’s leading suppliers of chip solutions used for protecting transactions and authenticating people and objects. The special chips encrypt personal data, thus preventing its misuse. Around 80 percent of all countries that have already introduced electronic passports now rely on these chips. This business area generated revenue of around 986 million U.S. dollars in 2012. NXP is Germany’s largest supplier of security chips for passports and the new German identity card. The Center of Excellence for Security Technology in Hamburg has also developed a technology with SmartMX and SmartMX2 chips, which is characterized by its excellent security and performance together with very low energy consumption. Thanks to such research and development activities, production as well as worldwide business responsibility for three of the five business units, NXP semiconductors Germany plays a very prominent role in the company group.

THE TASK

The terrorist attacks in the United States on September 11, 2001 played an important role in the development and introduction of electronic passports. The U.S. wants to use the machine-readable documents to reinforce international border security and prevent illegal immigration. The countries agreed to design the passports in accordance with the specifications of the International Civil Aviation Organization (ICAO) for machine-readable travel documents. This also provided for the integration of a contactless chip. Many national printing houses were therefore seeking a suitable supplier and opted, among others, in favor of NXP Semiconductors. The company meanwhile is also responsible for equipping the new identity cards available in Germany with a contactless chip in accordance with the BSI guidelines. In order to also use the official documents’ chips, NXP required a powerful operating system with a high level of security.

THE SOLUTION

T-Systems implements its smartcard operating system TCOS on the chip developed by NXP. The operating system protects and manages the personal data saved on the chip, such as name and date of birth, statutory residence and work permit provisions or biometric details. A Public Key Infrastructure (PKI) ensures that only authorized devices can access the data. Communication between the chip and card reader is handled by means of the Password Authenticated Connection Establishment (PACE) security protocol and Extended Access Control (EAC). Introduction of the PACE protocol is mandatory for European Union countries by the end of 2014. Internationally, PACE is deployed under the name Supplemental Access Control (SAC).

EU guidelines provide for evaluation and certification of the chip and the operating system. T-Systems developed the TCOS smartcard operating system back in 1985 and has continued to enhance it through the years, especially from a security perspective. TCOS has therefore undergone regular security tests and certifications since the nineties. NXP and T-Systems began developing the first generation of the electronic passport in 2004. Since then, the third passport generation has successfully completed the evaluation and certification process. The MX2 P60 smart chip is integrated in the current generation (2013) of passports. For T-Systems, every new generation means that the operating system needs to be reconfigured virtually from scratch. For example, the security experts had to port the software to a new hardware architecture for the third generation. This step was also essential for the chip in the new identity card. Today, TCOS can be found on more than 100 million smartcards around the world, including not only passports, identity cards, and residence permits, but also toll, tachograph, signature, and company cards.

CUSTOMER BENEFITS

With the Telesec Chipcard Operating System (TCOS) from T-Systems, NXP benefits from a fast and highly secure operating system for its chips. The semiconductor manufacturer can therefore rely on T-Systems as an experienced and dependable partner. Thanks to certification of TCOS, NXP can position itself more prominently on the market for security-critical solutions. T-Systems has also programmed and implemented TCOS fully in machine language. The programming language is characterized in particular by its hardware proximity. The ICT service provider can thus optimize the operating system for the hardware architecture of the NXP chips and make optimum use, for example, of the hardware’s inherent security functions. Thanks to its hardware-based programming, TCOS offers excellent performance and is optimally positioned for security evaluation and certification. Customers of NXP also benefit from highly secure and flexible implementation.

CONTACT

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
E-mail: referenzen@t-systems.com
Internet: www.t-systems.com

PUBLISHED BY

T-Systems International GmbH
Hahnstraße 43d
60528 Frankfurt am Main
Germany