eID and the new German Identity Card (nPA)

Innovative Security Solutions

Tuesday, 5 October 2010, 14:30 - 18:00

Introduction and Moderation: Bernd Kowalski

organised and hosted by:

TeleTrusT
Pioneers in IT security.

Federal Ministry
of the Interior

Federal Office
for Information Security

14:30 The eID Function of the nPA; Security Properties and Infrastructure Components

Marian Margraf (Federal Ministry of the Interior)

On 1. November 2010 Germany will start issuing new identity cards. One of the main differences compared to the previous version is the integration of an ISO-14443-compliant chip which contains a government application, e.g. for border control purposes, and two applications for eGovernment (authentication and signature). IT security and privacy considerations played a crucial role during the design phase of the electronical functionalities. Reliable protection for personal information required a coordinated approach to legal provisions, organisational measures and technical implementation.

15:00 AusweisApp and eID Service/Server – making online identification finally more secure –

Werner Braun (Siemens IT Solutions and Services)
Dirk Arendt (OpenLimit SignCubes)

The key components involved in using the ID card for identification purposes on the Internet are the AusweisApp and the eID service. These components form the innovative security infrastructure that makes online identification possible. One outstanding characteristic of the German eID model is its excellent interoperability with regard to the integration of smart cards, card readers, platforms and applications. This approach is also suitable for use in other countries. Siemens IT Solutions and Services and OpenLimit are playing a key role in planning and executing the "new identity card" project. Siemens IT Solutions and Services is the general contractor and responsible for the overall architecture of the IT solution, the Web portal, and the creation and integration of the application. Long-standing specialists in the field of signature and encryption technologies, OpenLimit is developing and maintaining the AusweisApp and the eID server middleware.

15:30 PostIdent Online with the nPA

Jens Terboven (Deutsche Post AG)

The business processes of many companies have created the need for a reliable method to verify the identities of their contractual partners. The issue of data security in particular has high priority in electronic networks and requires innovative and reliable solutions. This situation poses a major challenge especially to business customers who have no branch offices or only a few. In order to meet these requirements, Deutsche Post AG currently offers the Postident procedures, which allow private customers to be identified in accordance with the provisions of the German Money Laundering Act and the German Signature Act. Now the existing Postident procedures will be expanded to include the option of secure, fast and convenient identification over the internet, with the help of the new ID and its online identification function.

16:00 Coffee Break

16:30 The eID Function of the nPA within the European STORK Infrastructure

Volker Reible (T-Systems International)
Andre Braunmandl (BSI)

For official identity checks all electronic ID cards will include a digital photo; optional two fingerprints and/or a qualified electronic signature may also be stored on the chip. To use the new eID card the citizen needs a card reader as well as a client software called "Ausweis-App". Since autumn 2009 an application trial is running to test and prepare the roll-out. In parallel, the European Commission started in June 2008 the STORK project under the CIP, ICT PSP framework. STORK's main objectives are to identify existing eID infrastructures in Europe, specify and implement a common architecture which allows secure and easy to use eID solutions in Europe, and demonstrate the European interoperability in 6 application pilots. The outcome of STORK will be a prototypical infrastructure to be a working basis for the pan-European eID architecture.

**17:00 Public Administration and Electronic Signatures
    – Polish Concepts for Securing E-Government Document Flow –**

Mirosław Kutyłowski & Przemyslaw Kubiak
(Wroclaw University of Technology)

One of the basic problems in electronic documents flow in public administration is authentication of documents and fulfilling all related legal and technical requirements. The situation in public administration is in many ways easier that in general flow of legal documents, the actors of the process are well defined and known in the system (the citizens and representatives of public bodies). A number of technical and legal solutions are aimed to make electronic documents flow easier and more reliable. The main components are: electronic seal, personal signature and restricted identification. In our presentation we focus on requirements and their technical feasibility concerning personal signatures. The idea is to provide means for signing documents exchanged between citizens and public bodies so that (1) immediate disabling a signature card is possible, and (2) the signing time is undeniable.

17:30 Trusted Cloud Computing in Practice

Stefan Schröder (DATEV eG)

DATEV presents two trusted cloud computing scenarios:

1. Use of new identity card (neuer Personalausweis (nPA)) in the DATEV payroll accounting system:
    Each month 9,5 million payrolls are calculated using DATEV software. This means one of four employees in Germany. In the future DATEV will offer a new online service to grant access to payrolls via internet. For identification, the national ID card (nPA) will be used.

2. DATEV e-invoice in „DATEV Unternehmen online":
    DATEV offers a wide range of high-quality software solutions for accounting. This is shown by the number of financial accountings in Germany: About two thirds of German enterprises - a total of 2.4 million financial groups - use DATEV software solutions. One part of this accounting solution is „DATEV Unternehmen Online". It provides small companies with an easy way to collaborate online with their tax consultant for accounting needs. E-invoice is a special topic in this context. DATEV e-invoice is an easy solution for small companies to fulfil the legal requirements for e-invoices in cooperation with tax consultants.

The Moderator:

Bernd Kowalski: obtained his university degree in electrical engineering at the Rheinisch Westfälische Technische Hochschule (RWTH) in Aachen. In 1982 he joined the Deutsche Bundespost and worked first in the area of data communication networks and applications in Darmstadt. Since 1985 he is involved in information security at the Deutsche Bundespost, has been active in various security projects and several standardisation groups like, for example, the ITU work on X.509 Authentication Framework (1985-1988).

After the Deutsche Bundespost changed to Deutsche Telekom in 1990 he took over the task to set up the Productcenter Telesec in Siegen that offers secure communications products and services, e.g. Certificate and Smartcard Services for public Digital Signature and corporate Solutions. In 2002 he changed to the German Federal Office for Information Security (BSI) and took over a department that is responsible for Certification, Approval and Conformity Testing and New Technologies.

Marian Margraf 1998 Diploma in mathematics, 2001 PhD in mathematics, supported by the Deutsche Forschungsgemeinschaft (DFG), 2001-2003 Assistant Professor at the University of Kiel, 2003-2007 Cryptograph at the Federal Office for Information Security, Since 2007 Technical Project Leader of the Project Neuer Personalausweis at the Federal Ministry of the Interior.

Dirk Arendt was born in 1966. From 1988-1993 Dirk Arendt passed a training program as assistant tax accountant. Afterwards he studied law at the Freie Universität Berlin and successfully finished his studies in 1999. As Vice President, Business Development, he has been a member of the board of management of the OpenLimit Group since January 2009.

Werner Braun was born in 1964 and received his masters degree in computer science in 1991. Since then he works for the Siemens AG. Since 1995 versatile responsibilities in the IT-security area for smart card, PKI, RFID and identity management products and solutions for projects in all relevant sectors, i.e. public sector, health care, enterprises, communications and more.

Jens Eugen Terboven born on February 21, 1966, in Mannheim. After studying history and law in Berlin and Montpellier, he began working at Deutsche Post in 2000, first in strategy and later as a project head. In 2007, he became Vice President of Marketing responsible for additional and special products. Since then, his work has included expanding Deutsche Post security and identity products and making them usable online.

Andre Braunmandl studied physics at the University of Bochum and received his diploma in 1995. In 2003 he received his Ph.D. from the University of Bonn. Since 2001 he worked as a Consultant at IBM and became an expert for SAP supply chain solutions. Starting 2005 he joined the German Federal Office for Information Security (BSI). Currently his main working areas are interoperable eID solutions and applications of eID-management systems.

Volker Reible studied computer science and economics at Technical University Berlin and joined Deutsche Telekom Group in 1989 as Senior Project Manager for national and European projects in the R&D affiliate Berkom. Now he works as Vice President Large Scale Project Management in the markets telecommunications and public/e-government/healthcare with focus on security projects and solutions. In the project STORK he is the German project manager coordinating the German partners/subcontractors.

Miroslaw Kutylowski is a full professor for computer science at Wroclaw University of Technology. He received his master degree in mathematics in 1980, PhD in 1986, Habilitation in 1992, from the University of Wroclaw. He is involved in e-government issues and serving as adviser of different public institutions. In 2009 he received the award „Mistrz" from the Foundation of Polish Science in technical sciences.

Przemysław Kubiak received his master degree in mathematics in 1997 and his PhD in 2001. He is an assistant professor for computer science at Wrocław University of Technology. His research interests are in public key cryptography.

Stefan Schröder studied Computer Sciences at University Erlangen-Nuremberg with the main emphasis on pattern recognition and artificial intelligence. Since 1990 he has been working for DATEV eG. Since 2008 he is the Head of the development team financial accounting and Chairman of the working group Software as a Service (SaaS) at BITKOM e.V.