The eIdentity (eID) Card Project in Germany

- German Government eCard strategy
- German eID card
- eCard-API Framework / Architecture
- eCard and Middleware Components
- European Perspective: eID-Large Scale Pilot

Bernd Kowalski
Federal Office for Information Security (BSI)
Head of Department 3 – Certification, Approval and Conformity Testing, New Technologies

Bernd Kowalski
10th ICCC Tromsø – Norway, September 22nd 2009
German Government eCard strategy

EU Directive
January 2005

Cabinet Decision (March 2005)

- ePass
  - Biometrics
- ePA
  - ECC
  - eResidence Card
- eHealth Card
  - Authentication
  - optional Signature
- ELENA
  - (Jobcard)
- ELSTER
  - Authentication
  - optional Signature

Increasing political importance for Common Criteria Certified Products

Enable smart card interoperability and security standards based on the Common Criteria

Bernd Kowalski
10th ICC Tromsø - Norway, September 22nd 2009

tirsdag 8. september 2009
Key Security Components to be certified:

**eHC** – Electronic Health Card for 80 Mio citizens replacing the KVK (health insurance card).

**HPC** – Health Professional Card for more than 500,000 health professionals.

**SMC** – Security Module Card to be used by an institution under control by a health professional.

**Connector** – Connects and controls the doctor's practice and the Telematic Infrastructure (access rights etc.).

**Card Terminal** – Write and read the different cards.
BSI Evaluation Standards in the context eHealth

Protection Profiles (PP):
- PP for eHC
- PP for HPC
- PP for SMC Type A
- PP for SMC Type B
- PP for Connector
- PP for card reader terminal
- PP for an eKiosk

Technical Guidelines (TR):
- TR 03114 for electronic signature (batch processing)
- TR 03115 for convenient processing
- TR 03116 Security requirements crypto catalogue

Posted on the website of BSI (www.bsi.bund.de)
Key Facts of the New German National ID Card

- All visual identity card functions remain preserved
- Long-lasting polycarbonate for the ID card body
- Minimization from size ID-2 to credit-card-size ID-1
- New security characteristics integrated

Proximity card interface (ISO 14443) for biometrics
- Based on the electronic passport (ICAO compliant)
- Storage of digital photograph and if requested two fingerprints

Proximity card interface (ISO 14443) for E-Government, E-Business
- For secure electronic identification (networks, computers, vending machines) \(-\) Replacement of insecure password / PIN procedures
- Optional qualified electronic signature certificates (as an electronic equivalent of handwritten signature)
The new ID card combines properties of the traditional card with electronic functions.

### Important Certification Projects (2)

<table>
<thead>
<tr>
<th>Card body</th>
<th>New electronic functions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard:</strong></td>
<td></td>
</tr>
<tr>
<td>- All non-biometric data electronically stored</td>
<td></td>
</tr>
<tr>
<td>- Digital photograph (only for entitled authorities, e.g. police and border control)</td>
<td></td>
</tr>
<tr>
<td><strong>Upon request (no extra charge):</strong></td>
<td></td>
</tr>
<tr>
<td>- electronic ID function (access only to certain non-biometric data fields)</td>
<td></td>
</tr>
<tr>
<td>- Two fingerprints (only for entitled authorities, e.g. police and border control)</td>
<td></td>
</tr>
<tr>
<td><strong>Upon request (extra costs):</strong></td>
<td></td>
</tr>
<tr>
<td>- Qualified electronic signature</td>
<td></td>
</tr>
</tbody>
</table>

From 1 November 2010: credit-card-size ID

Protection Profile for Electronic Identity Card (PP–ePA)
Demand for a Secure Identification in the Internet

Percentage of the German Internet users who would use an electronic identity card for identification

<table>
<thead>
<tr>
<th>Online Services</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banking</td>
<td>55 %</td>
</tr>
<tr>
<td>E-Government</td>
<td>54 %</td>
</tr>
<tr>
<td>Auctions</td>
<td>41 %</td>
</tr>
<tr>
<td>Shopping</td>
<td>39 %</td>
</tr>
<tr>
<td>Games</td>
<td>36 %</td>
</tr>
</tbody>
</table>

Quelle: BITKOM/forsa; Basis: deutsche Internet-Nutzer ab 14 Jahren
Citizen – eID Card Holder:
Is the service provider able to prove its electronic identity?

Service providers identify themselves with an authorization certificate

Citizens and service providers can rely on the identity of the counterpart!

Citizens identify themselves with the eID card

Service Provider:
Is the requesting person able to prove her/his electronic identity?

Mutual Authentication between Citizen and Service Provider
Electronic Authentication Procedure

**eID Card Holder**
- Citizen’s PC
- Data request
- First name
- Last name
- Date of birth
- Confirmation by entering PIN

**Service Provider (e-business, e-government)**
- Request on service
- Service on web page
- Service is authorized and asks for personal data
  - or:
  - Secret key of eID card
  - Service provider ID
  - Pseudonym

**Government**
- Access Certificate
- Certificate:
  - Name of service provider
  - Service provider ID
  - ... Authorized for:
  - First name
  - Last name
  - Age
  - ...

**Provisioning of service**
- Data transmission
eID Application Testing Milestones

November 20th 2008
Registration start for application testing

February 28th 2009
Registration end for centrally co-ordinated application testing

End of May 2009
Selecting participants for centrally co-ordinated application testing

January 1st 2010
Start for open application testing

October 1st 2009
Start for centrally co-ordinated application testing

End of June 2010
Report on Testing Results for centrally co-ordinated application testing

End of October 2010
Conclusion for centrally co-ordinated application testing

November 1st 2010
Rollout
eID Application Testing
Participants

Bird.i ag & co. kg
D-hosting die rackspace & Connectivity GmbH

Bernd Kowalski
10th ICCC Tromsø – Norway, September 22nd 2009
Components of the Authentication Function of the eID Card

 Acts, regulations, technical specifications (standards)

<table>
<thead>
<tr>
<th>eCard</th>
<th>Terminal</th>
<th>Middleware</th>
<th>Certificate</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chip OS</td>
<td>online offline</td>
<td>eCard API Framework</td>
<td>CA</td>
<td>Hotline</td>
</tr>
<tr>
<td>eID Application (e-business / e-government)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Bernd Kowalski
10th ICCC Tromsø – Norway, September 22\textsuperscript{nd} 2009

tirsdag 8. september 2009
eCard-API: Aim of Middleware Solution (1)
1. Arbitrary Applications

2. Standardized and easy use of arbitrary eCards
1. Arbitrary Applications

2. Standardized and easy use of arbitrary eCards
Implementation

eCard-API and eID Service

Direct Middleware Implementation

 Middleware as a Service

Service Provider

eCard-API (BSI-TR-03112)
server
Access Certificate

eCard-API (BSI-TR-03112)
citizen

HSM
Access Certificate

Mgmt.

eID Service (BSI-TR-03130)
eCard-API (BSI-TR-03112)
server

Service Provider

eCard-API (BSI-TR-03112)
citizen
Normative IT-Security Standards

- Legislative Authority
  - Directives, Council Regulations, National Laws

- Federal Office for Information Security
  - IT-Security Standards, Technical Guidelines (TR), Protection Profiles (PP)

  Certification, Type Approval

  Certified Products
### Overview: Technical Guidelines (TR) and Protection Profiles (PP) in the field of eCards

#### Technical Guidelines (TR):
- **TR-02102**: Cryptographic Techniques: Recommendations and key lengths
- **TR-03104**: Production data acquisition, testing and transmission for passports (TR-PDÜ)
- **TR-03105**: Conformity Tests for Official Electronic ID Documents
- **TR-03110**: Extended Access Control (EAC2.0/PACE)
- **TR-03111**: Elliptic Curve Cryptography
- **TR-03112**: eCard-API-Framework - Client and Server Middleware
- **TR-03116-2**: eCard projects of the German Government (eCard/eHC)
- **TR-03117**: eCards with contactless interface
- **TR-03119**: eCard reader with ePA – support
- **TR-03121**: Biometrics for Public Sector Applications

#### Protection Profiles (PP):
- **PP for Electronic Identity Card (PP-ePA)**
- **PP for Inspection Systems (PP-IS)**
- **PP for ePass with “ICAO Application” (EAC)**
- **PP for Secure Signature Creation Device**

#### Key Figures:
- **80 Million Citizens**
- **6,000 Authorities**

---

80 Million Citizens

6,000 Authorities

- TR-03123: XhD-Data model for Production Data
- TR-03124: Conformity Testing for XhD
- TR-03127: ePA Architecture
- TR-03128: PKI for ePA
- TR-03129: Communication Protocols for Extended Access Control (EAC)
- TR-03130: eID-Server
- TR-03131: EAC-Box
- TR-03132: Scenarios for secure communication processes in the field of official documents
- TR-03133: Conformity Testing for TR-03132
- PP for German Electronic ID Card

---

Bernd Kowalski
10th ICCC Tromsø - Norway, September 21st 2009
The European eID Large Scale Pilot

- **Competitiveness and Innovation Framework Programme (CIP)**
  - specific programme: Information and Communication Technologies Policy Support Programme (ICT PSP)
  - eID LSP (Pilot Type A) builds on national eID initiatives

- **driver: EU service directive**

- **objective: build pan-european eID management (eIDM) backbone**

- eID LSP contributes to
  - accelerate the development of eID for public services
  - coordination between national and EC initiatives
  - test secure and easy-to-use eID solutions

→ **build interoperable national pilots**
STORK – Secure Identity Across Borders Linked

### STORK consortium members (representing 14 member states)

| 1. | ATOS   | 1. | IS MoF  |
| 2. | CAPGEMINI | 2. | LU LSC |
| 3. | AT BKA | 3. | NL MOI |
| 4. | BE FEDICT | 4. | PT AMA |
| 5. | DE BSI | 5. | SE VERVA |
| 6. | EE SK | 6. | SI MPA |
| 7. | ES MPA | 7. | UK IPS |
| 8. | FR DGM | 8. | ES CRUE – UJI |
| 9. | GOV2U | 9. | ES CATCERT |
| 10. | IT POLITO | 10. | IT CNIPA |
| 1. | IT Lombardia |
| 2. | PT IST |
| 3. | PT Multicer |
| 4. | EEMA |
| 5. | E–Forum |
| 6. | IS Nat. Registry |
| 7. | AT TUG |
| 8. | BE Soc Security |
STORK Common Technological Design

direct SP connector

S-PEPS connector

possible extension

possible extension

Modular Authentication Relay Service

DE eID Service

AT MOA ID

C-PEPS connector

national C-PEPS

configurable components

tirsdag 8. september 2009
European Authentication for (German) Service Providers

Direct Middleware Implementation or Middleware as a Service

authentication request

direct SP connect

DF eID Service

AT MOA ID

e-PEP connect or

Modular Authentication Relay Service

national C-PEPS

national C-PEPS

national C-PEPS

national C-PEPS

national C-PEPS

citizen environment

eCard-API (BSI–TR–03112)
citizen

citizen card environment
Conclusions & Perspectives

- eID solutions in Europe will improve security and authentication mechanisms in the Internet significantly
- Wide distribution of Smart Card–based security solutions
- All security related components will be certified in compliance with CCv3.1 Protection Profiles
- In Germany: Protection Profiles are obligatory
Federal Office for Information Security (BSI)

Bernd Kowalski
Godesberger Allee 185–189
53175 Bonn
Germany

Bernd.Kowalski@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de