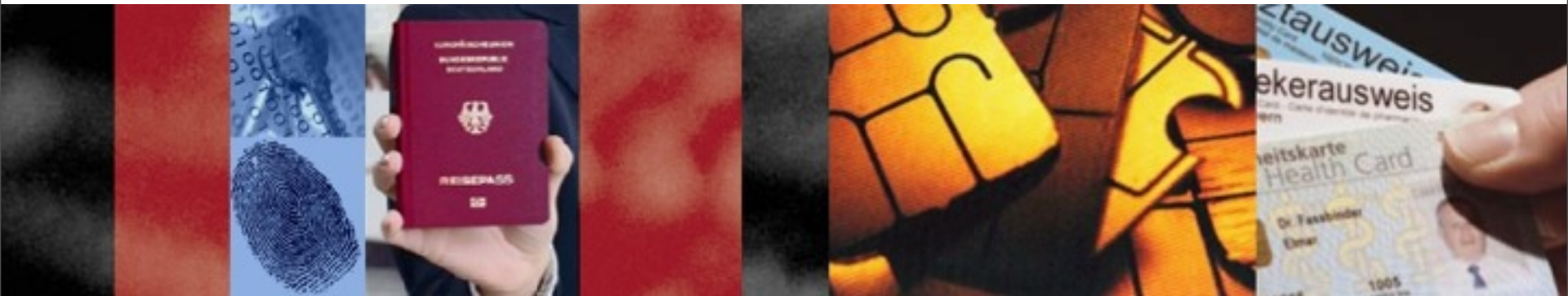


# The eidentity (eID) Card Project in Germany



- 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

# German Government eCard strategy

EU Directive  
January 2005

Cabinet Decision (March 2005)

<p>ePass</p>	<p>ePA ECC eResidence Card</p>	<p>eHealth Card</p>	<p>ELENA (Jobcard)</p>	<p>ELSTER</p>
<ul style="list-style-type: none"> <li>• Biometrics</li> </ul>	<ul style="list-style-type: none"> <li>• Biometrics</li> <li>• Authentication</li> <li>• optional Signature</li> </ul>	<ul style="list-style-type: none"> <li>• Authentication</li> <li>• optional Signature</li> </ul>	<ul style="list-style-type: none"> <li>• Signature</li> </ul>	<ul style="list-style-type: none"> <li>• Authentication</li> <li>• optional Signature</li> </ul>



Increasing political importance of  Common Criteria Certified Products

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

# National eHealth-Card



## Important Certification Projects (1)



### 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.

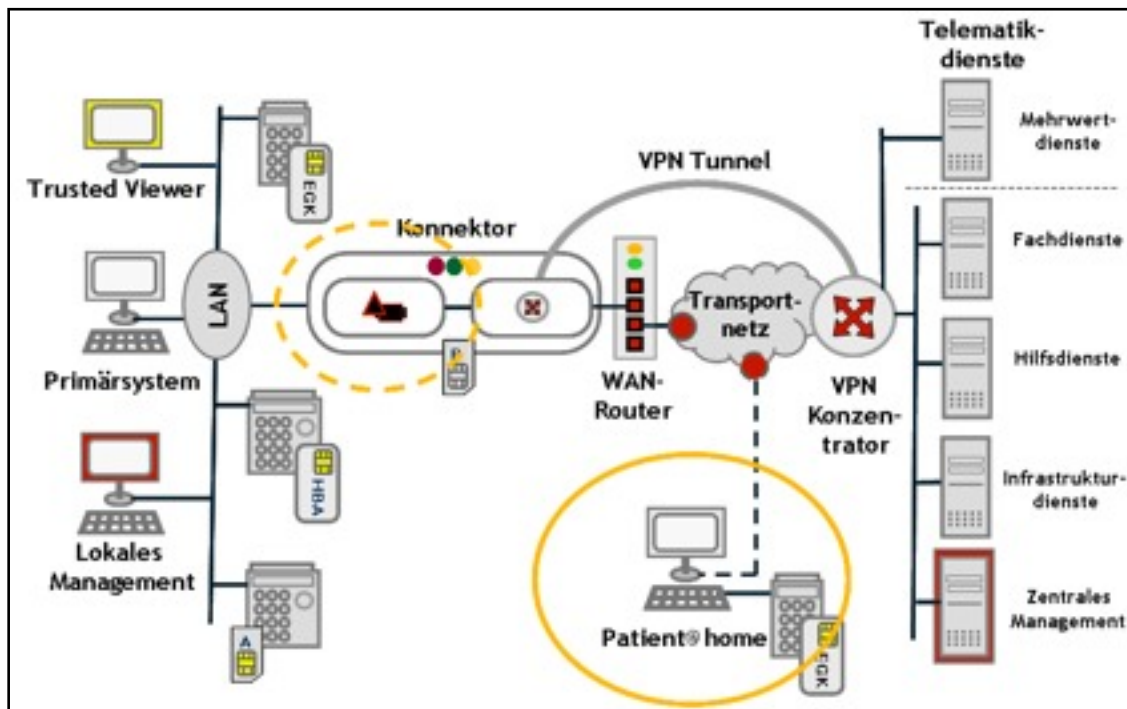
**Connector** – Connects and controls the doctor's practice and the Telematic Infrastructure (access rights etc.).

**Card Terminal** – Write and read the different cards



# BSI Evaluation Standards in the context eHealth

## Important Certification Projects (1)



### 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](http://www.bsi.bund.de))

# Key Facts of the New German National ID Card

## Important Certification Projects (2)



- 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

eID Function



QES Function



### 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)

### Card body



**From 1 November 2010:  
credit-card-size ID**

### New electronic functions

#### Standard:

- **All non-biometric data electronically stored**
- **Digital photograph** (only for entitled authorities, e.g. police and border control)

#### Upon request (no extra charge):

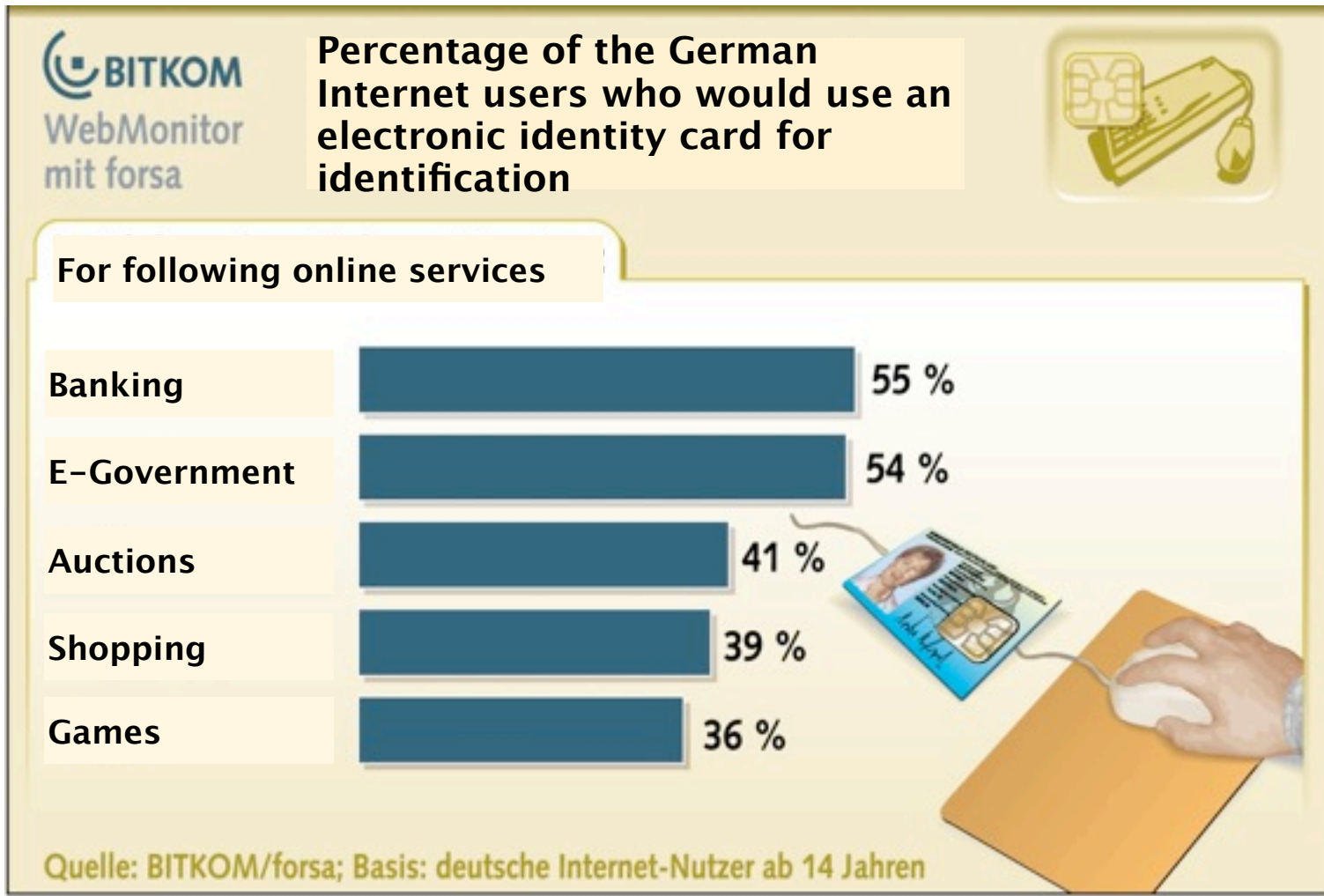
- **electronic ID function** (access only to certain non-biometric data fields)
- **Two fingerprints** (only for entitled authorities, e.g. police and border control)

#### Upon request (extra costs):

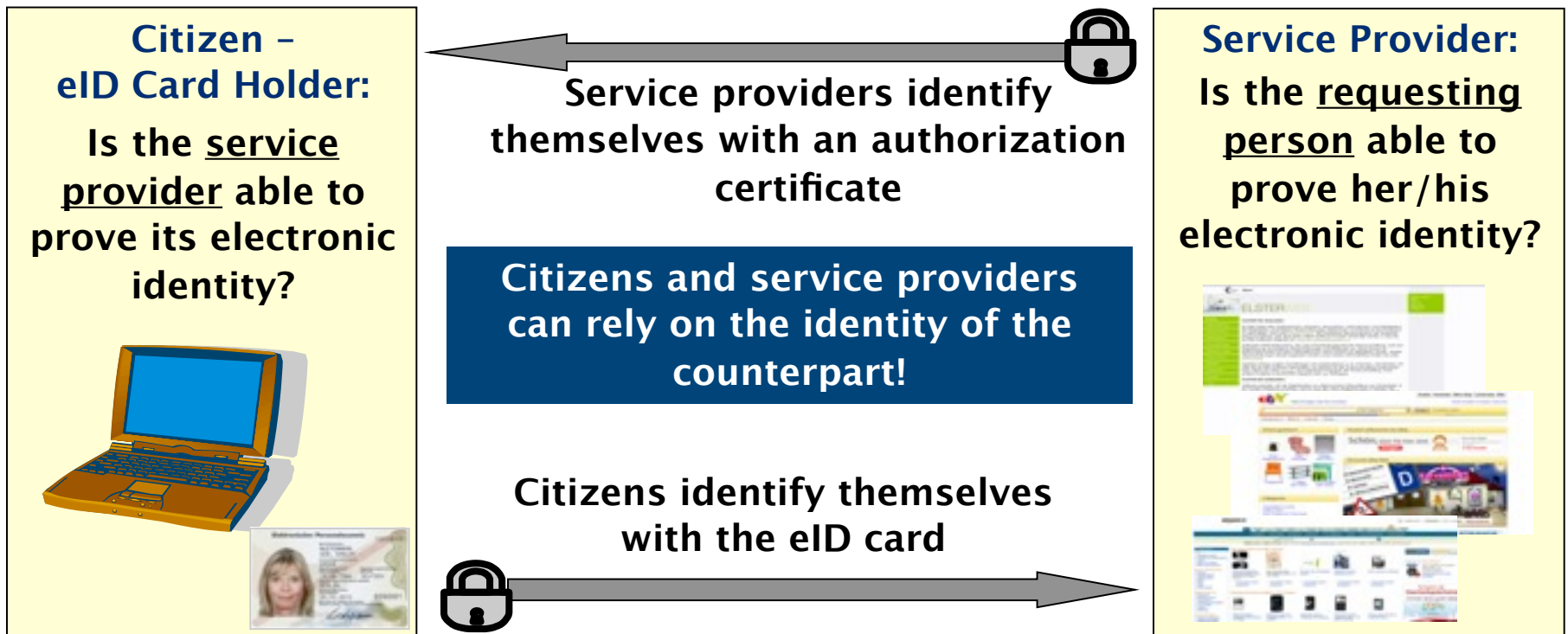
- **Qualified electronic signature**

## Protection Profile for Electronic Identity Card (PP-ePA)

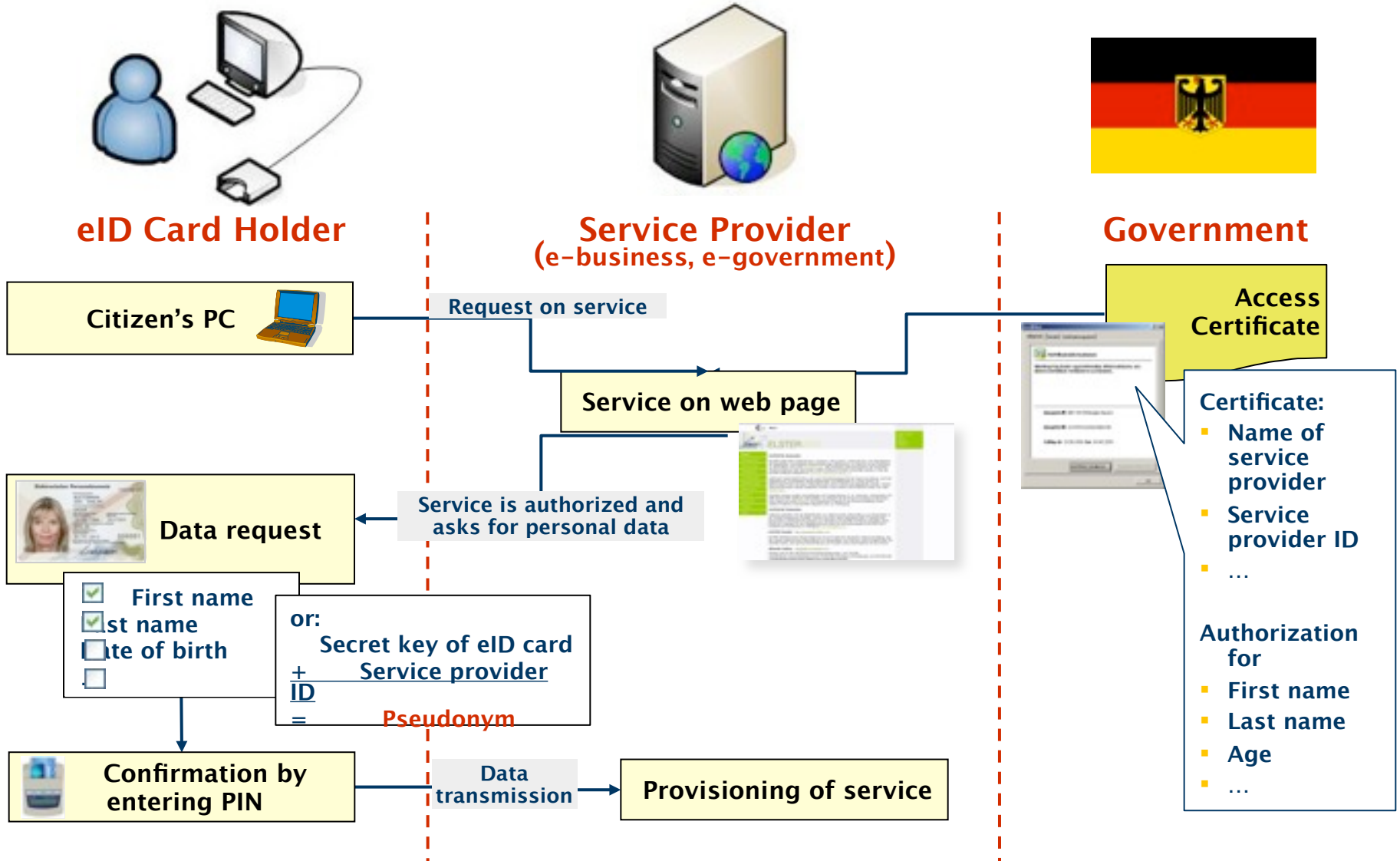
# Demand for a Secure Identification in the Internet



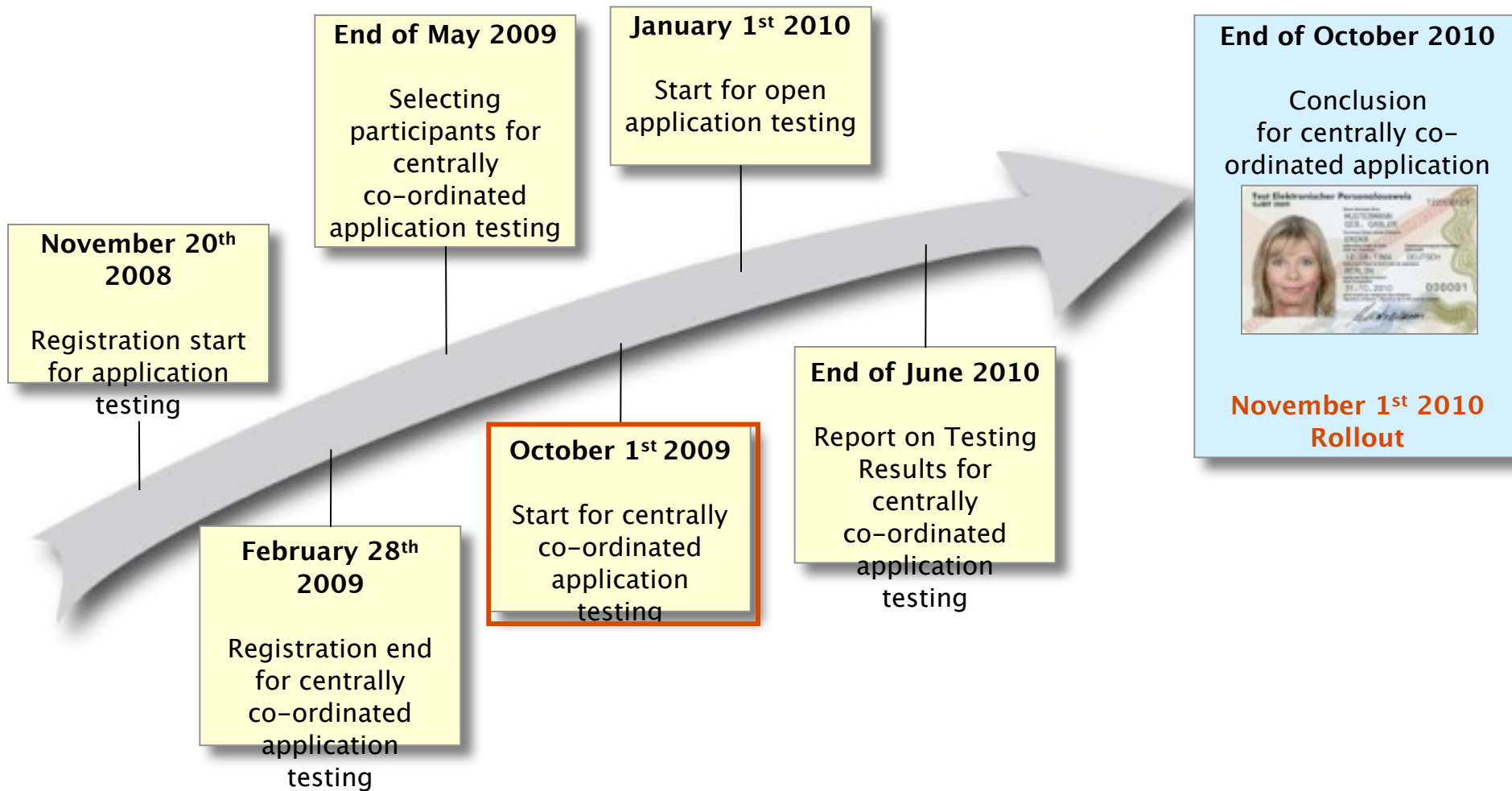
# Mutual Authentication between Citizen and Service Provider



# Electronic Authentication Procedure



# eID Application Testing Milestones



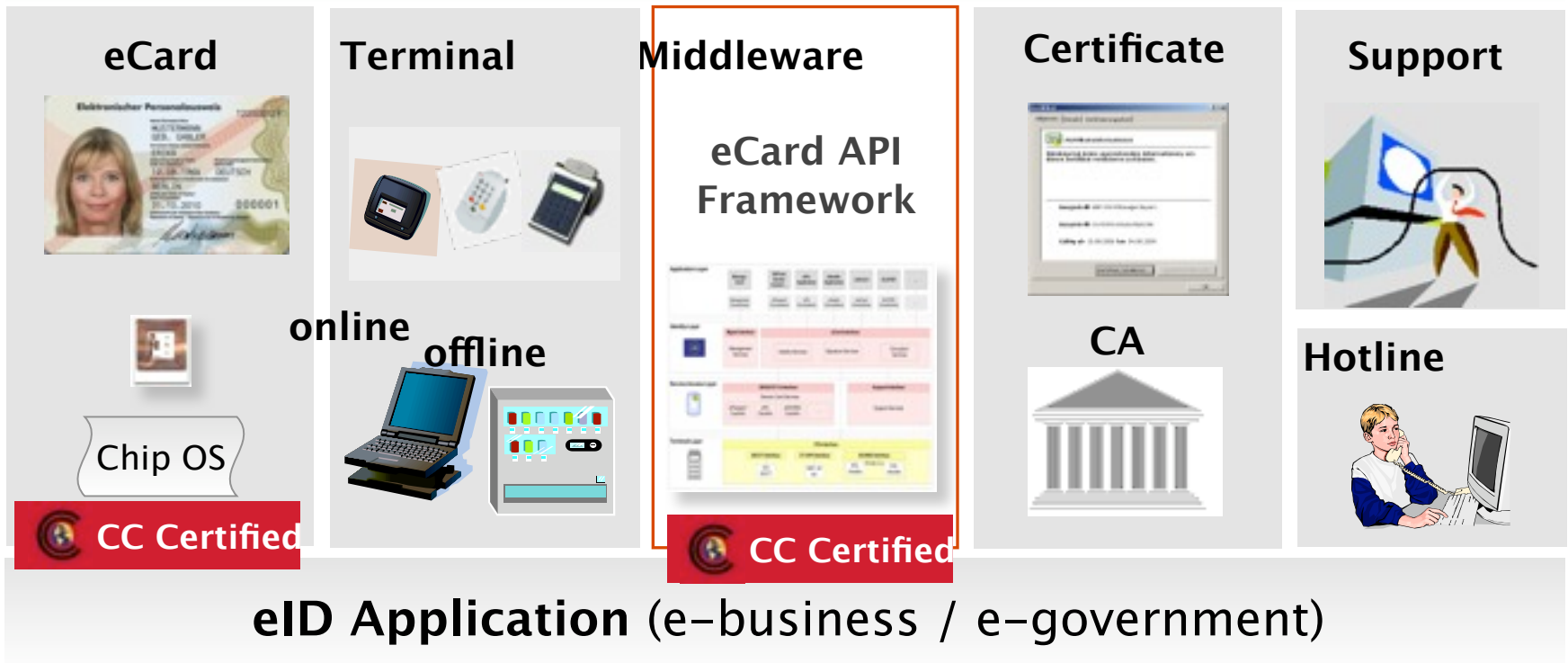
# eID Application Testing Participants



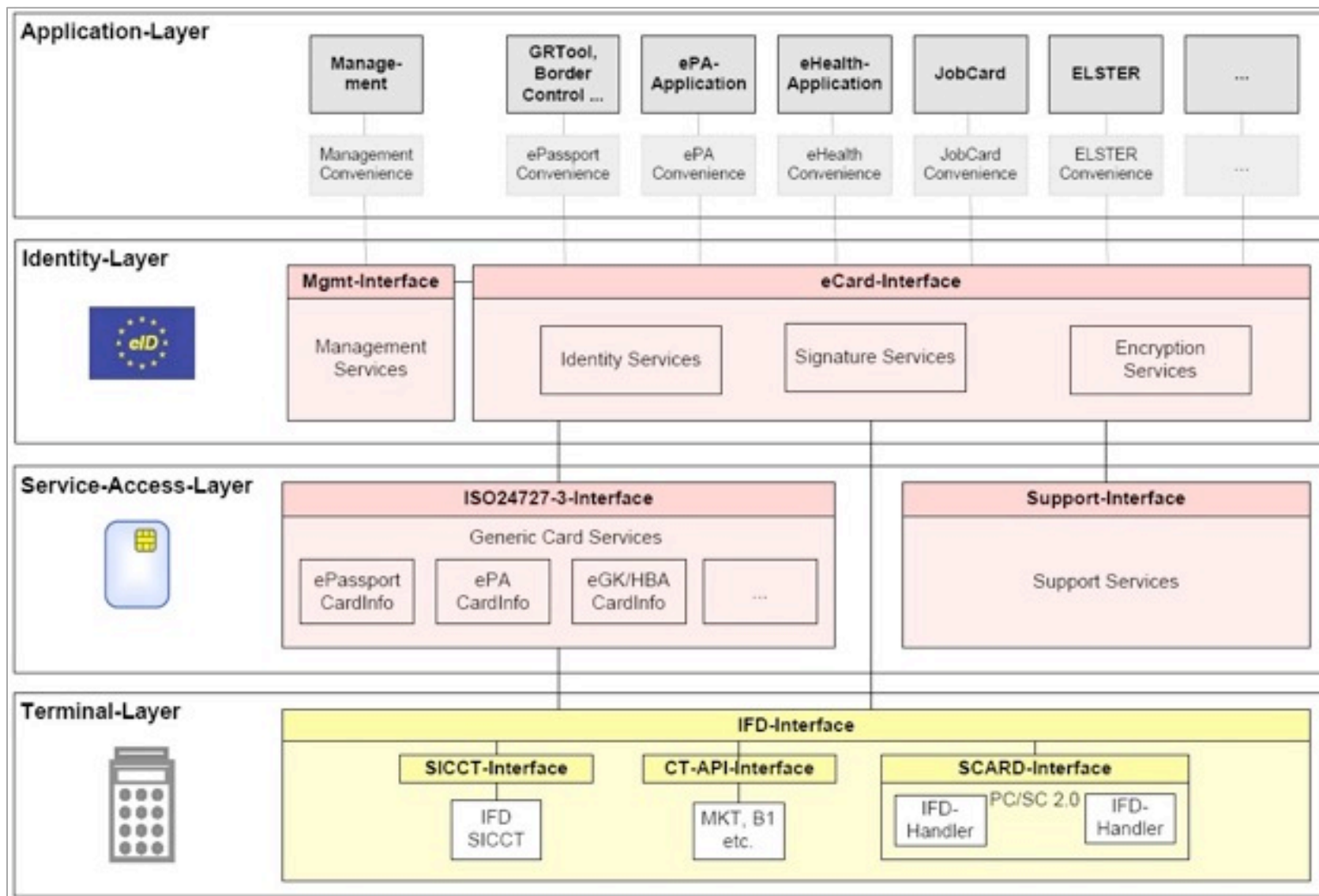
d-hosting die rackspace & Connectivity Gmb

# Components of the Authentication Function of the eID Card

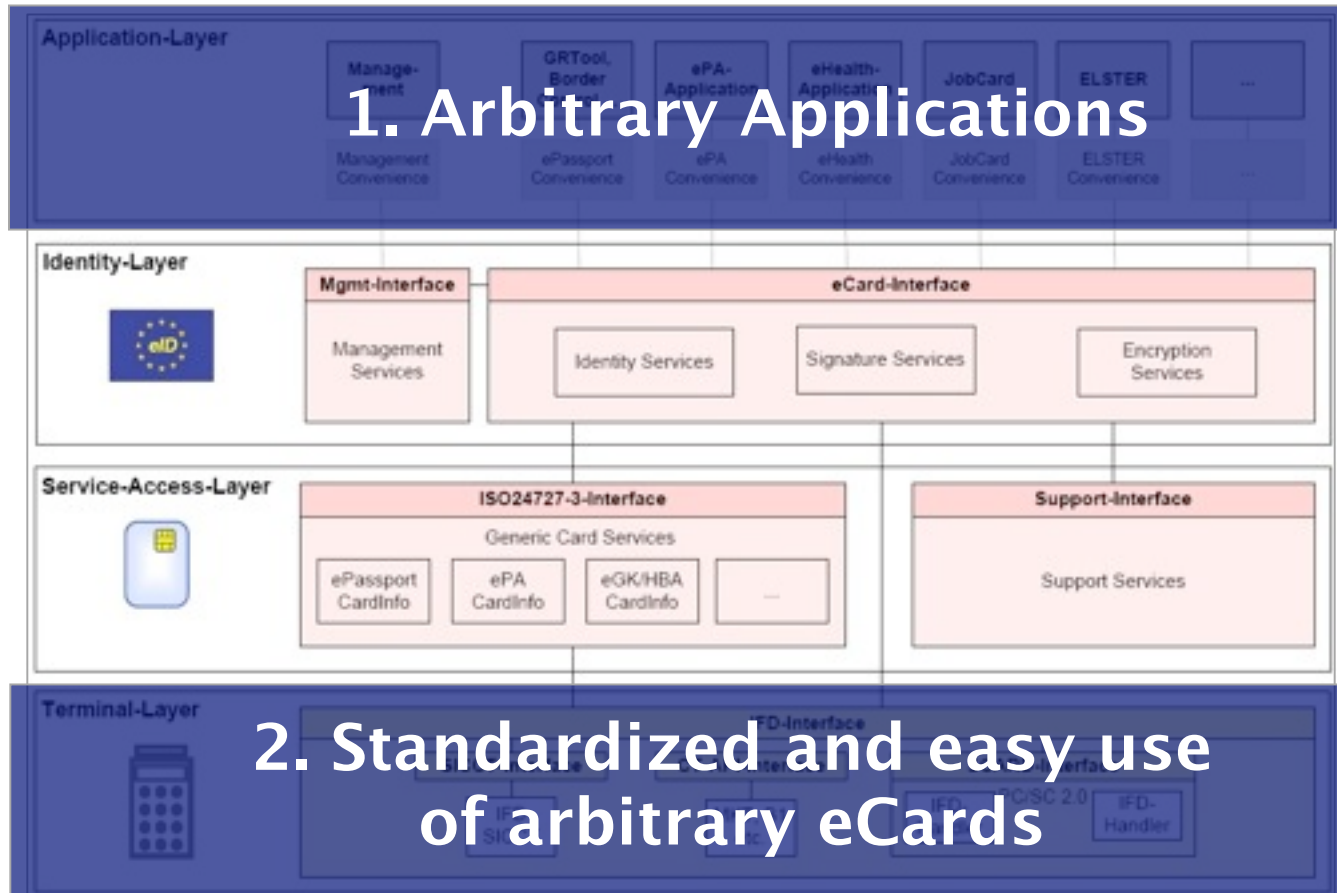
Acts, regulations, technical specifications (standards)



# eCard-API: Aim of Middleware Solution (1)



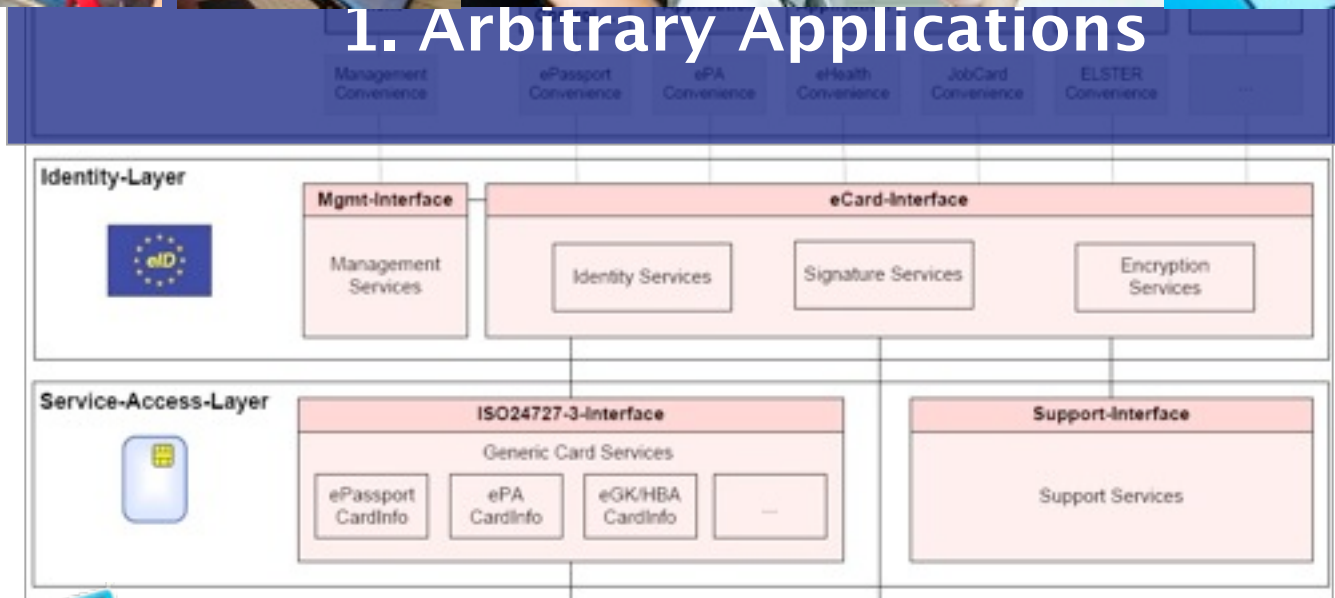
# eCard-API: Aim of Middleware Solution (2)



# eCard-API: Aim of Middleware Solution (2)



## 1. Arbitrary Applications

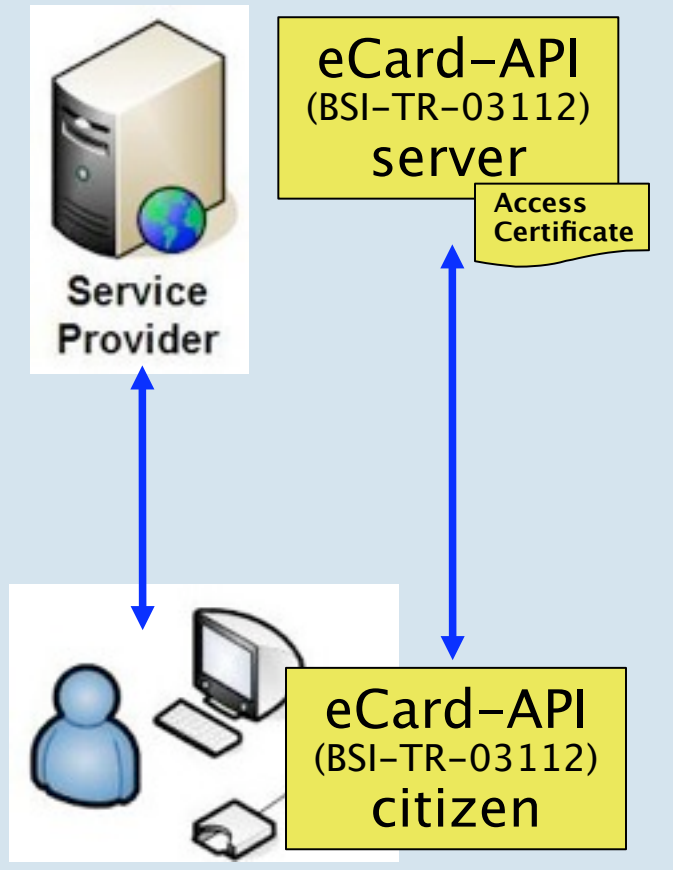


## 2. Standardized and easy use of arbitrary eCards

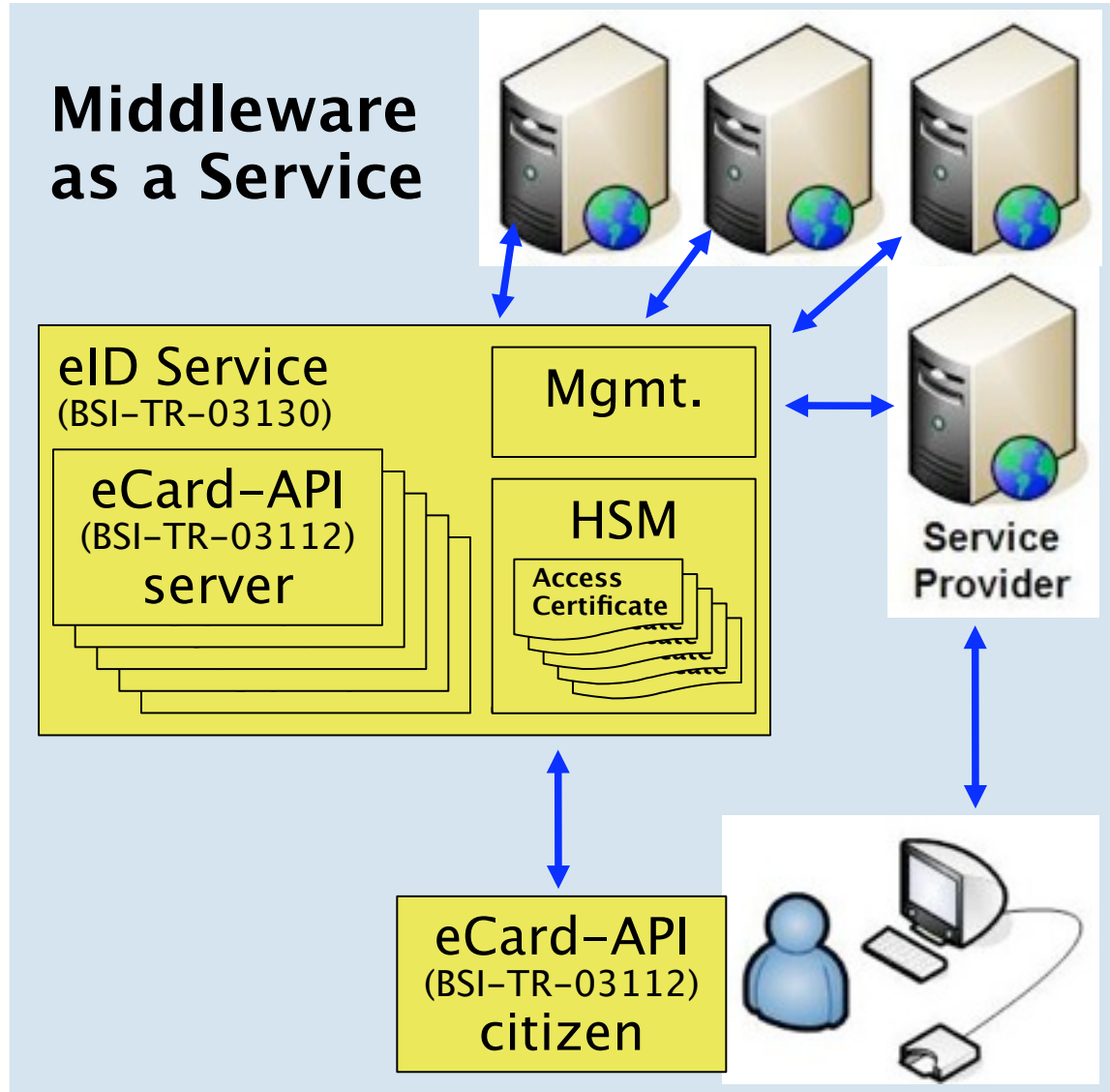


# Implementation eCard-API and eID Service

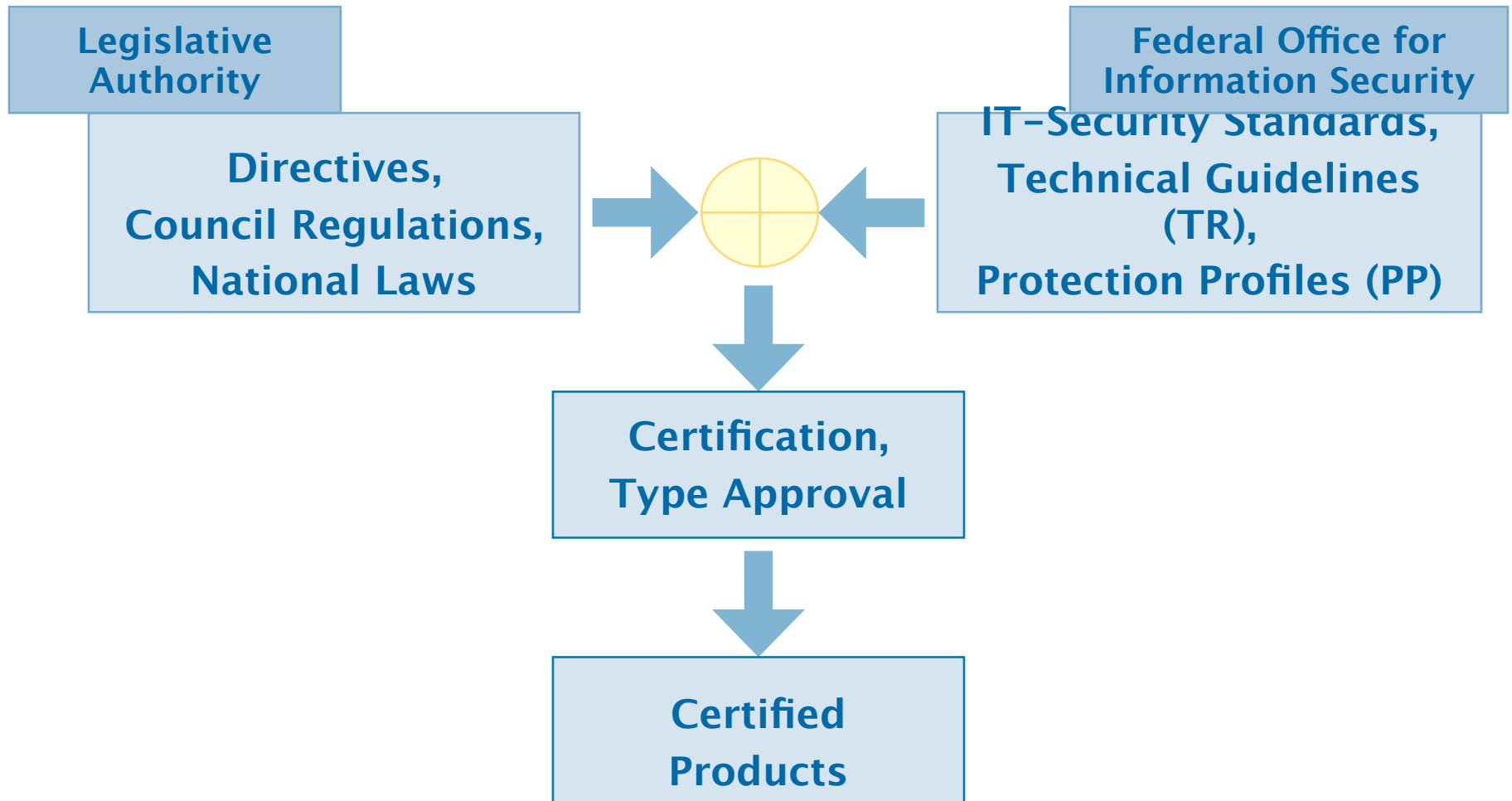
## Direct Middleware Implementation



## Middleware as a Service



# Normative IT-Security Standards



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



■ 80 Million Citizens

■ 6.000 Authorities

## Technical Guidelines (TR):

- TR-02102 - Cryptographic Techniques: Recommendations and key lengths
- TR-03104 - Production data acquisition, - quality, 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

- 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

## 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

Applications

■ PP for German Electronic ID Card

# 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



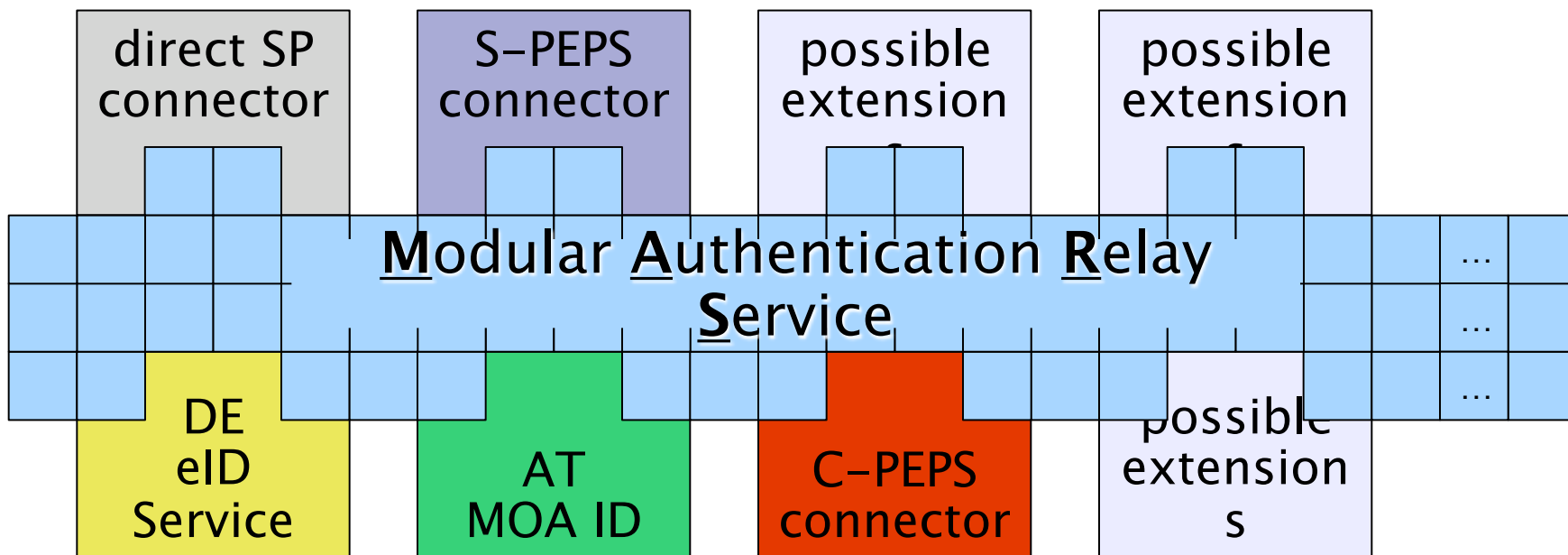
## STORK consortium members (representing 14 member states)

- |                 |                  |                                                                        |
|-----------------|------------------|------------------------------------------------------------------------|
| 1. ATOS         | 1. IS MoF        | 1. IT Lombardia                                                        |
| 2. CAPGEMINI    | 2. LU LSC        | 2. PT IST                                                              |
| 3. AT BKA       | 3. NL MOI        | 3. PT Multicer                                                         |
| 4. BE FEDICT    | 4. PT AMA        | 4. EEMA                                                                |
| 5. DE BSI       | 5. SE VERVA      | 5. E-Forum                                                             |
| 6. EE SK        | 6. SI MPA        | 6. IS Nat. Registry                                                    |
| 7. ES MPA       | 7. UK IPS        | 7. AT TUG                                                              |
| 8. FR DGM       | 8. ES CRUE – UJI | 8. BE Soc Security                                                     |
| 9. GOV2U        | 9. ES CATCERT    | 9. T-Systems                                                           |
| 10. IT POLITICO | 10. IT CNIPA     | (NXP, Fujitsu,<br>Infineon, Giesecke &<br>Devrient<br>Bundesdruckerei) |

# STORK Common Technological Design



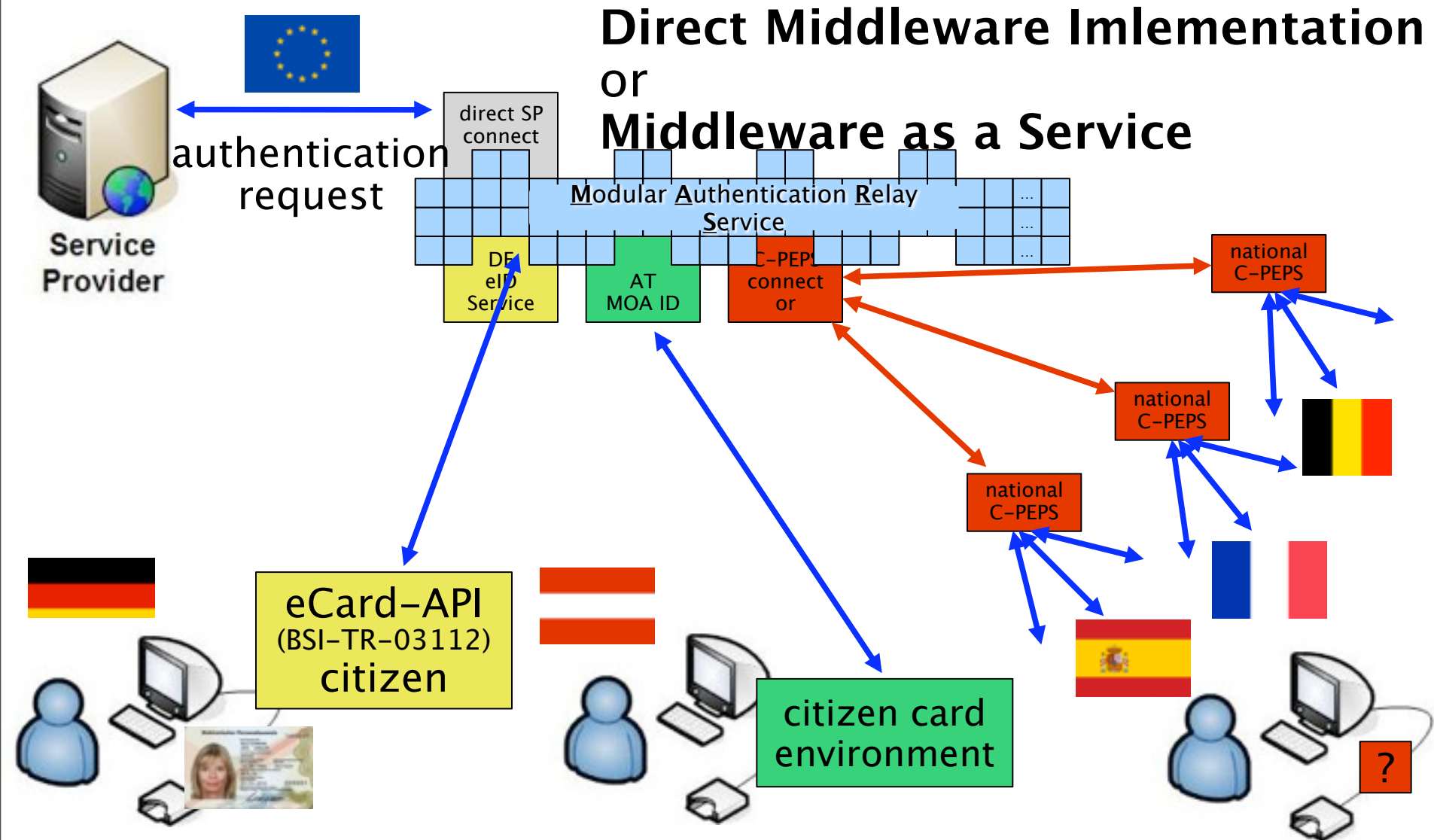
Stork MARS



**national C-PEPS**

**configurable components**

# European Authentication for (German) Service Providers



# 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

# Contact



Federal Office  
for Information Security (BSI)

Bernd Kowalski  
Godesberger Allee 185-189  
53175 Bonn  
Germany

[Bernd.Kowalski@bsi.bund.de](mailto:Bernd.Kowalski@bsi.bund.de)  
[www.bsi.bund.de](http://www.bsi.bund.de)  
[www.bsi-fuer-buerger.de](http://www.bsi-fuer-buerger.de)