The German eID-Card

Jens Bender

Federal Office for Information Security

Bundesamt für Sicherheit in der Informationstechnik

eID Workshop KU Leuven / 16.09.2009

The German Electronic ID-Card (Elektronischer Personalausweis)

Motivation

- Stronger link of document and holder via biometry analogous to electronic passport
- Cryptography as new security feature
- New technologies require secure electronic identity e.g. for
  - Online business
  - Financial transactions via network
  - eGovernment

Therefore: Integration of a chip

Functions of the German eID-Card

- **ePass**
  - Like ePassport
  - Only for governmental use
    - Police, border control, ..., but not eGovernment
- Electronic identity - **eID**
  - Opt-Out, may be deactivated on request of the holder
  - Contains personal and document-related data
    - E.g. name, adress, expiry date – but no biometric data
  - Used for eGovernment, eBusiness
- Qualified Electronic Signature - **QES**
  - Opt-In, activated only on request of holder
- All functions integrated into one contactless chip

State of Affairs/Roadmap

- Law promulgated 18.06.2009
- Technical specifications (TRs)
  - 10 Technical Guidelines of the BSI published
  - 6 further TRs and 3 protection profiles nearly finalized
- Test specifications for interoperability tests of several components in drafting
- Pilots and tests
  - Pilots and testing continuously since Q1 2008
  - Testing with service providers starting 01.10.2009
  - Test of enrolment in municipalities in Q1/2 2010
- Introduction of eID-Card 01.11.2010

eID and Signature

	Traditional	Electronic (1-factor)	Electronic (card & PIN)
Identification	Presentation of ID-Card	Username/ Password	**New: eID**
Transaction	Signature	TAN	Qualified Signature

Example banking

- ID-Card/eID for identification (e.g. to facilitate database query about creditworthiness of customer) – no provable authorization
- Signature/electronic signature to start actual transaction (e.g. opening of an account) – provable authorization of transaction

Opportunities and Risks

- Opportunities are obvious, e.g.
  - Better identification of customers for eBusiness
  - No 'prank'-orders using non-existing delivery-adresses
  - Faster access to governmental services
  - ...
- To look only onto opportunities would be light-headed, risk-assesment equally important
  - eID can only work if citizens trust and accept the eID-system
    - Not enough to look at eID from the perspective of the service provider
  - First-roll-out-than-fix is wrong approach
  - Therefore: Analyse risks, mitigate them already in the design

User Consent / Access Control

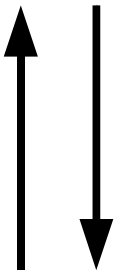
Risk: Personal data read without consent of holder

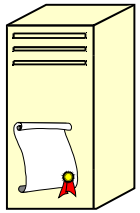
- Access to eID only after entering a secret PIN
  - Reading of data only after approval by holder
  - Additional advantage: Link of card to holder
    → authentication not only of the card but of card-holder
- User may restrict access only to certain data
  - e.g. name, adress but not age

Mutual Authentication

Risk: Phishing, access by bogus service provider

- Access only by certified service providers
  - Certificates issued by public authority
    - Authority checks provider (compliance to privacy laws ...)
    - Checked by chip, no dependency on software
  - Mutual authentication, not only of the card holder
  - Phishing considerably more difficult
- Certificate contains access rights to data
  - Access to e.g. address restricted to service providers that need an address for their business





Example banking:

- Bank identifies customer via ID-Card
- Customer identifies bank via “looking at building”

Data Integrity vs. Address Trading

Risk: Data theft/trading

- Impossible to bar further distribution of read data, only possible to reduce value of read data for third parties
- Data of the eID are not signed (no eID-certificate)
  - No forwarding of read data to third parties including a cryptographic proof of authenticity possible
- Securing authenticity/integrity of data by
  - Proof of authenticity of the chip cryptographically
  - Reading of data via encrypted & integrity protected channel
    - Eavesdropping not possible, even for local software like browser applet or trojan horse

The service provider receives data including cryptographic proof of authenticity but cannot forward proof to third parties

Age verification
Pseudonym

Risk: More infos about holder revealed than necessary

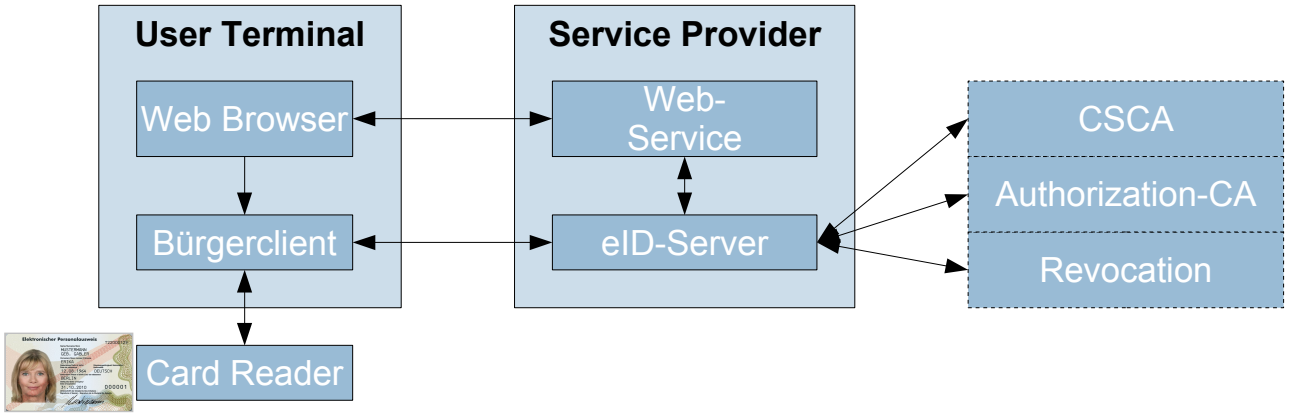
- Age verification
  - Possible by reading the date of birth – this is not desirable since date of birth reveals more about holder than only the fact being older than a certain age
  - Instead: Service provider “queries” the eID-Card if holder is born before a certain date – answer yes/no
- Pseudonym
  - Card delivers different pseudonym for each service provider
    - Different service provider cannot consolidate pseudonyms
  - A service provider is able to recognize a known eID-Card
    - Open user account by reading personal data
    - Accessing user account using pseudonym w/o reading personal data

Tracking

Risk: Tracking of card and/or holder

- Randomized UID of the chip
- Disclose system data (domain parameter, …) as late as possible during authentication
- Chip public key and signature not unique, all cards issued during certain period have same key pair and signature
- Identification of card (and holder) only possible after complete authentication procedure

Online Authentication



- Web browser calls “Bürgerclient” to start authentication
- Bürgerclient connects to eID-server of the service provider
- Bürgerclient displays the service provider's access certificate
- Chip checks PIN entered by user
- Chip checks access certificate
- Service provider checks authenticity of the chip
- Establishment of secure channel chip ↔ service provider
- Service provider gains access to data (according to access rights)

Remaining Risks

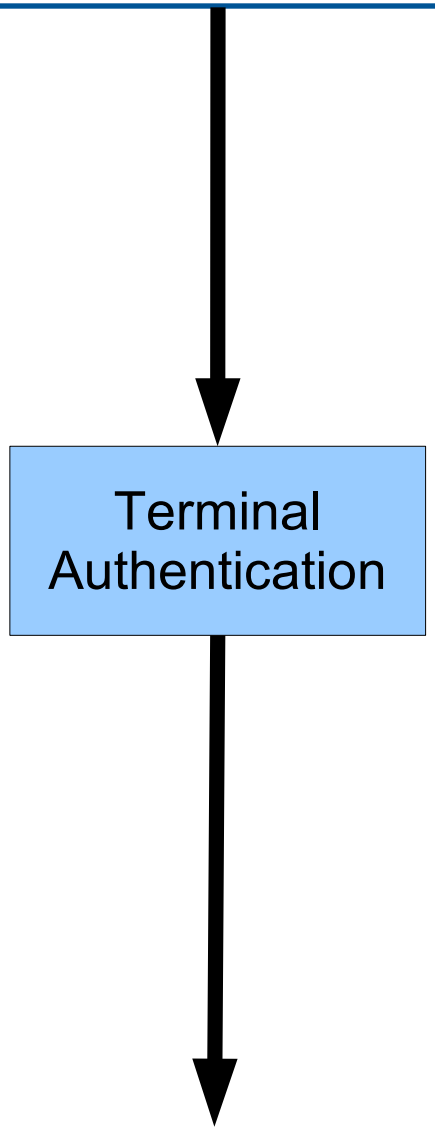
- Software/Reader may save/divulge secret PIN
  - But: Without simultaneous possession of the eID-card knowledge of PIN is worthless (2-factor authentication)
  - Countermeasures:
    - Usage of trusted software/reader (e.g. CC-certification)
    - PIN-change
- Software falsifies display of access-certificate
  - But:
    - Only trustworthy service provider get access-certificate
    - Due to end-to-end-encrypted channel data theft not possible
  - Countermeasures: Usage of trusted software

Authentication Procedure PACE

PACE
Password
Authenticated
Connection
Establishment

- Provides
  - Proof of correct password (PIN) without transmitting password, recovering of PIN from eavesdropped communication as difficult as breaking underlying symmetric cipher (e.g. AES)
  - Secure Messaging (card ↔ card terminal), strength of encryption independent of entropy of password
- Designed (by BSI) as replacement for BAC as known from ePassport
- Suitable for use with Elliptic Curve Cryptography
- Designed to be patent free

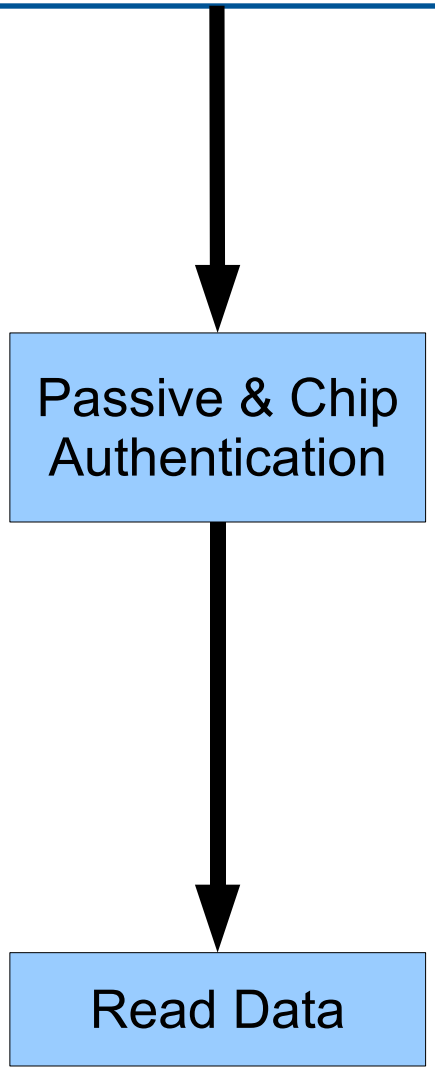
Authentication Procedure
Terminal Authentication



PKI/certificate-based proof of

- Authenticity of service provider
- Maximum access rights of service provider
- Root public key saved on chip during personalization
- Terminal sends certificate-chain starting at trusted root, chain verified by chip
- Possession of public key proven by challenge-response

Authentication Procedure
Chip Authentication

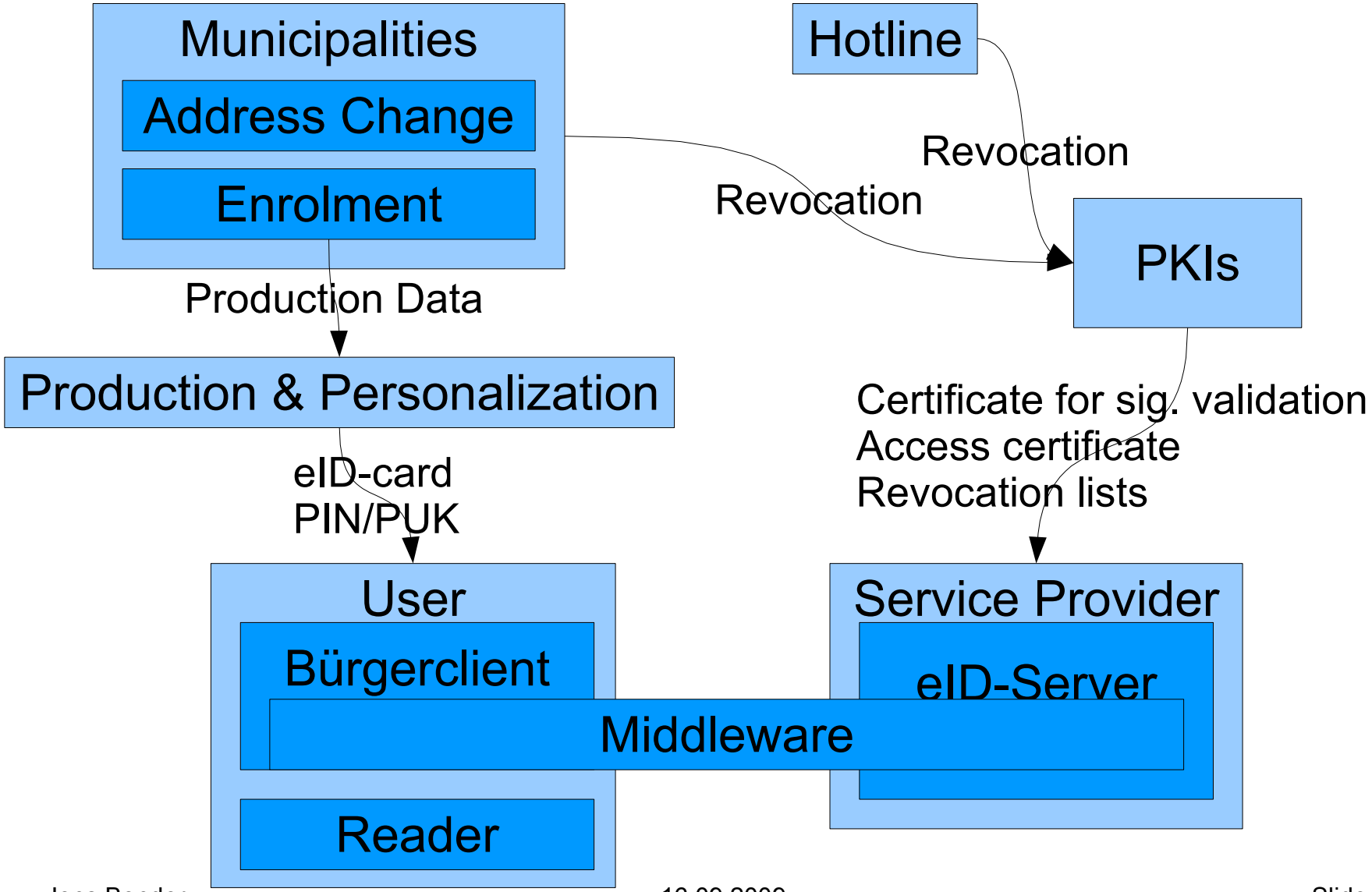


Read and verify chip public key

- PKI/certificate-based proof of authenticity of chip public key
- Proof of possession of private key corresponding to verified public key → chip is authentic
- Challenge-Response for proof of private key not advisable because of challenge semantics
- Chip Authentication based on Diffie-Hellman

Secure Messaging (card to service provider)

eID – More than a Card

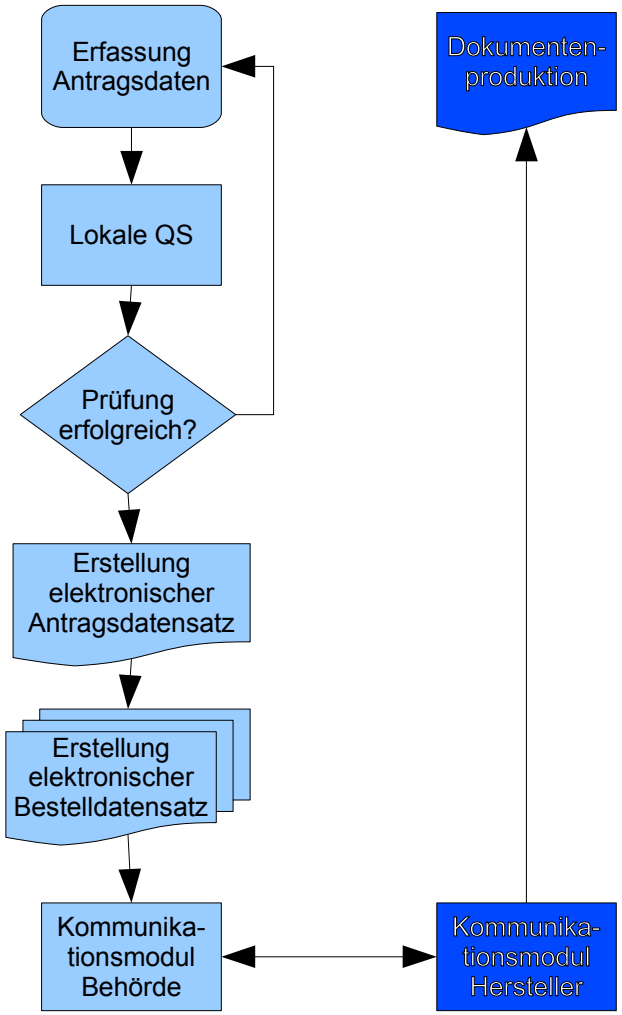


The Chip-Card
TR-03110/TR-03117/TR-.....

- The chip as carrier of the user's data and the applications has to protect those → the chip is security anchor
- Technical Guidelines as specifications
  - Data structure
  - Access control
  - Cryptographic requirements (keylength etc.)

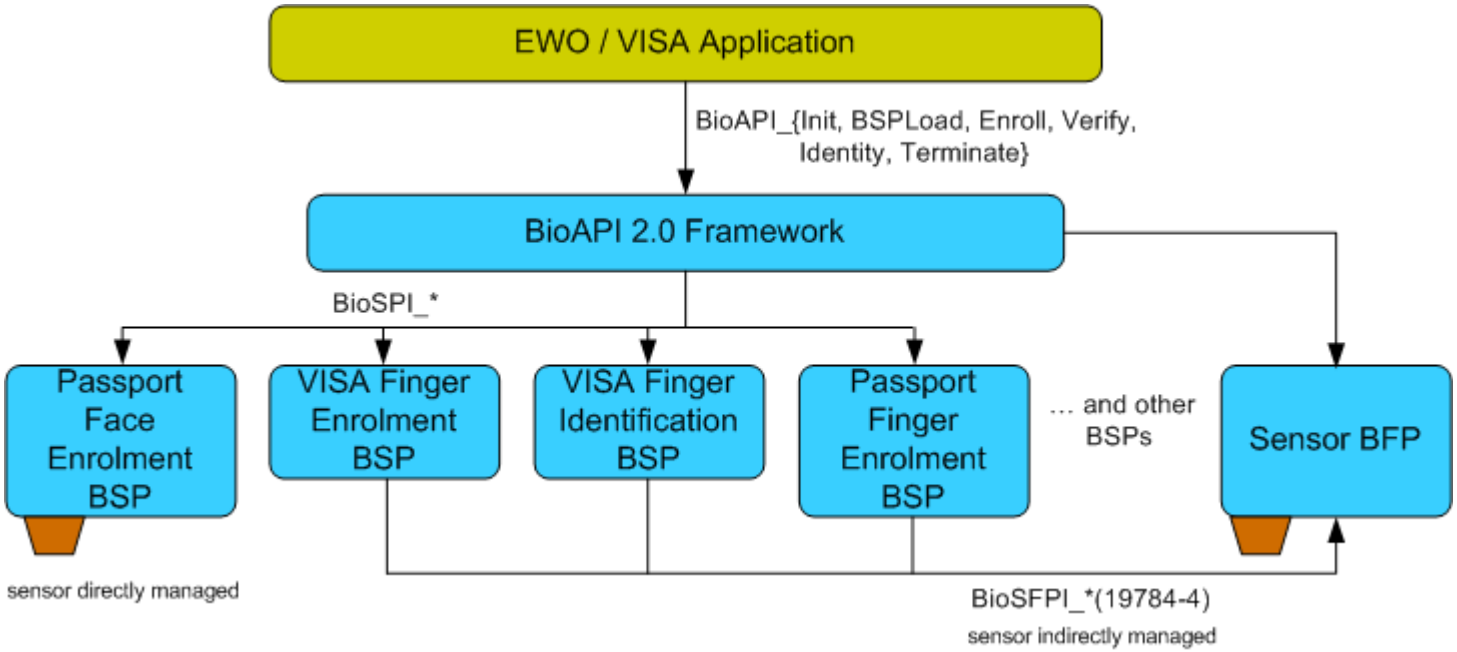
- Common Criteria Protection Profile to ensure security of chip
- Based on ICAO Doc 9303, ISO 14443, ISO 7816
- Compatible to
  - European Citizen Card (CEN TS 15480)
    - Profile 1 represents German eID-card
  - eSignK (CEN EN 14890)

Enrolment
TR-03104/TR-03123/TR-03132



- Capture of application data
- Quality assessment biometry
- Creation of electronic application
- Secure communication of application data to producer
- Document production

Technical Guideline Biometry TR-03121

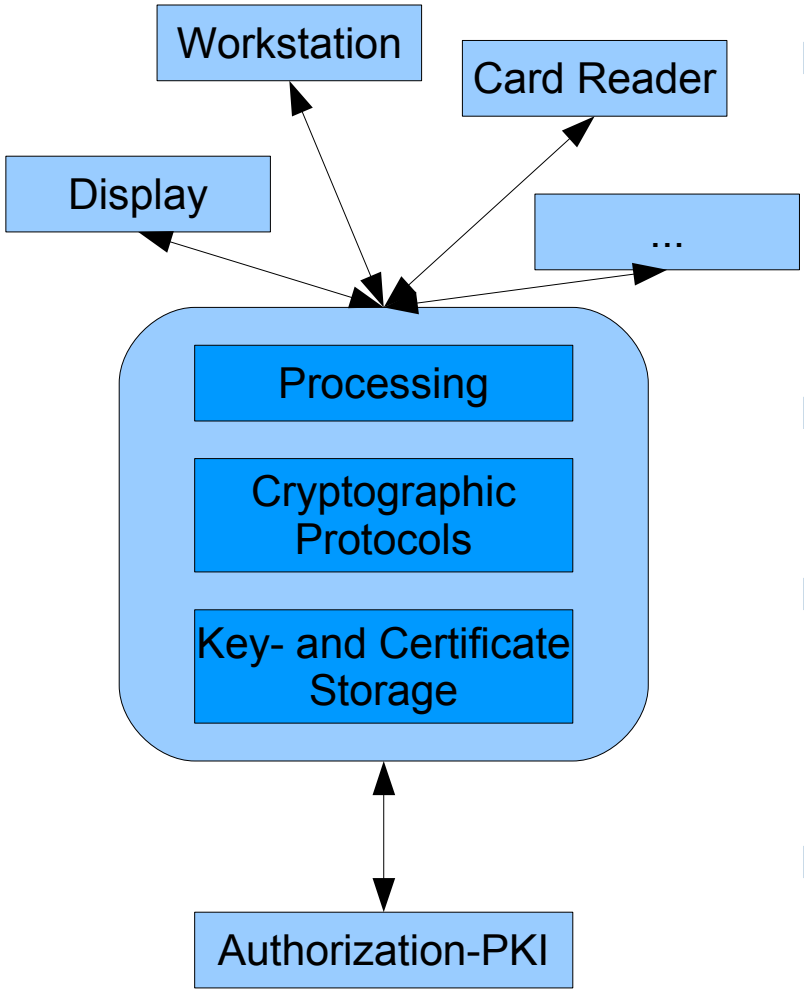


- Modular architecture based on BioAPI2.0 (ISO 19784)
- Defined interfaces
- Definition of common quality level and standardized procedures for different biometric applications in the public sector (enrolment/verification)

Change Service

- Change service in municipalities offers
  - Activiation/Deactivation of the eID-application
  - Change of address on chip – change of the address printed on the card with sticker as before
  - Change of the eID-PIN
- Secured by EAC (access certificates)
  - This ensures that changes to the chip can only be performed by municipalities
- Technical realization based on “EAC-Box”

EAC-Box
TR-03131

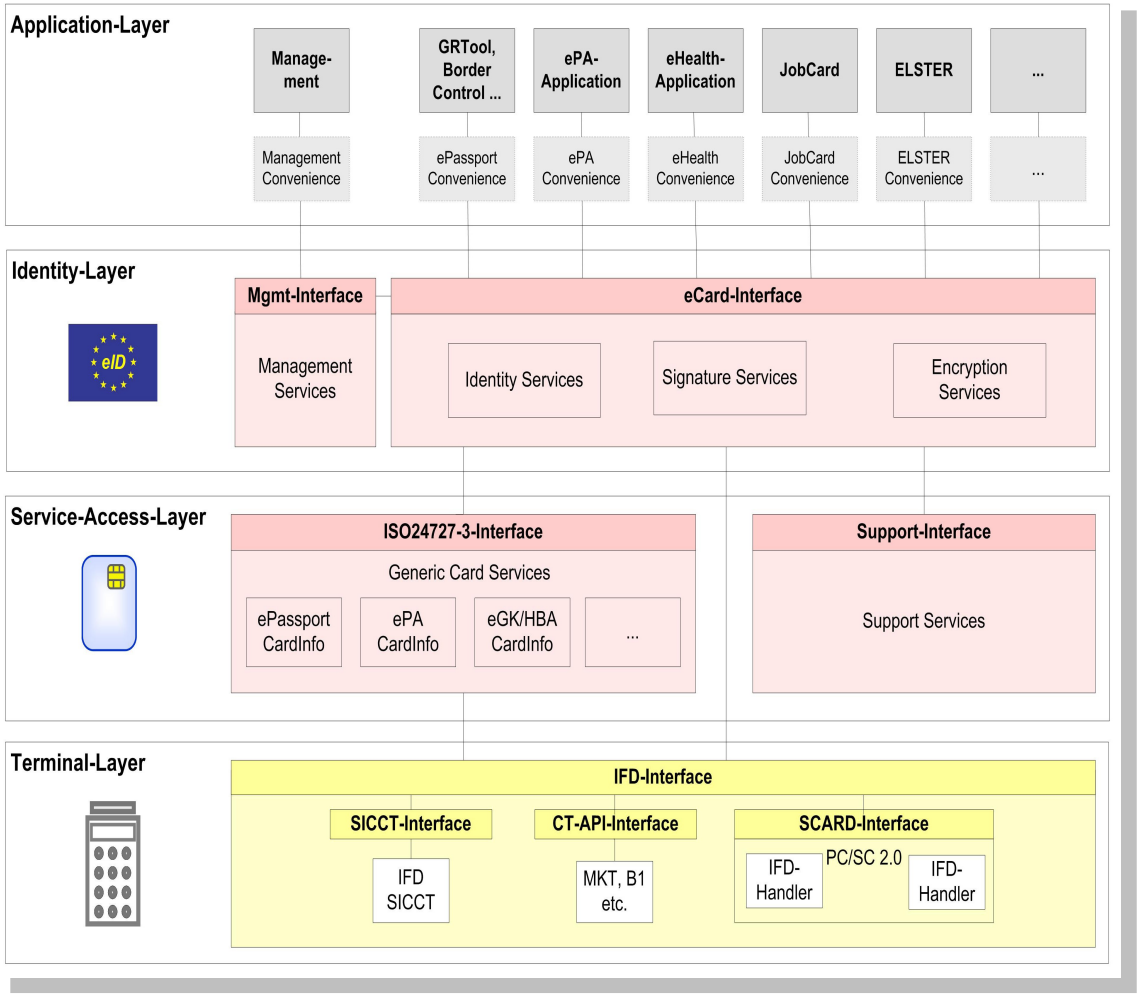


- „Black-Box“ to access eID-card
  - Change service
  - Standalone Readers
  - Mobile Readers
- Layer architecture
  - Graduated security requirements
- Common Criteria certification
  - Key-Storage (EAL4+)
  - EAC-Box (EAL3)
- Theft protection

Card Reader
TR-03119

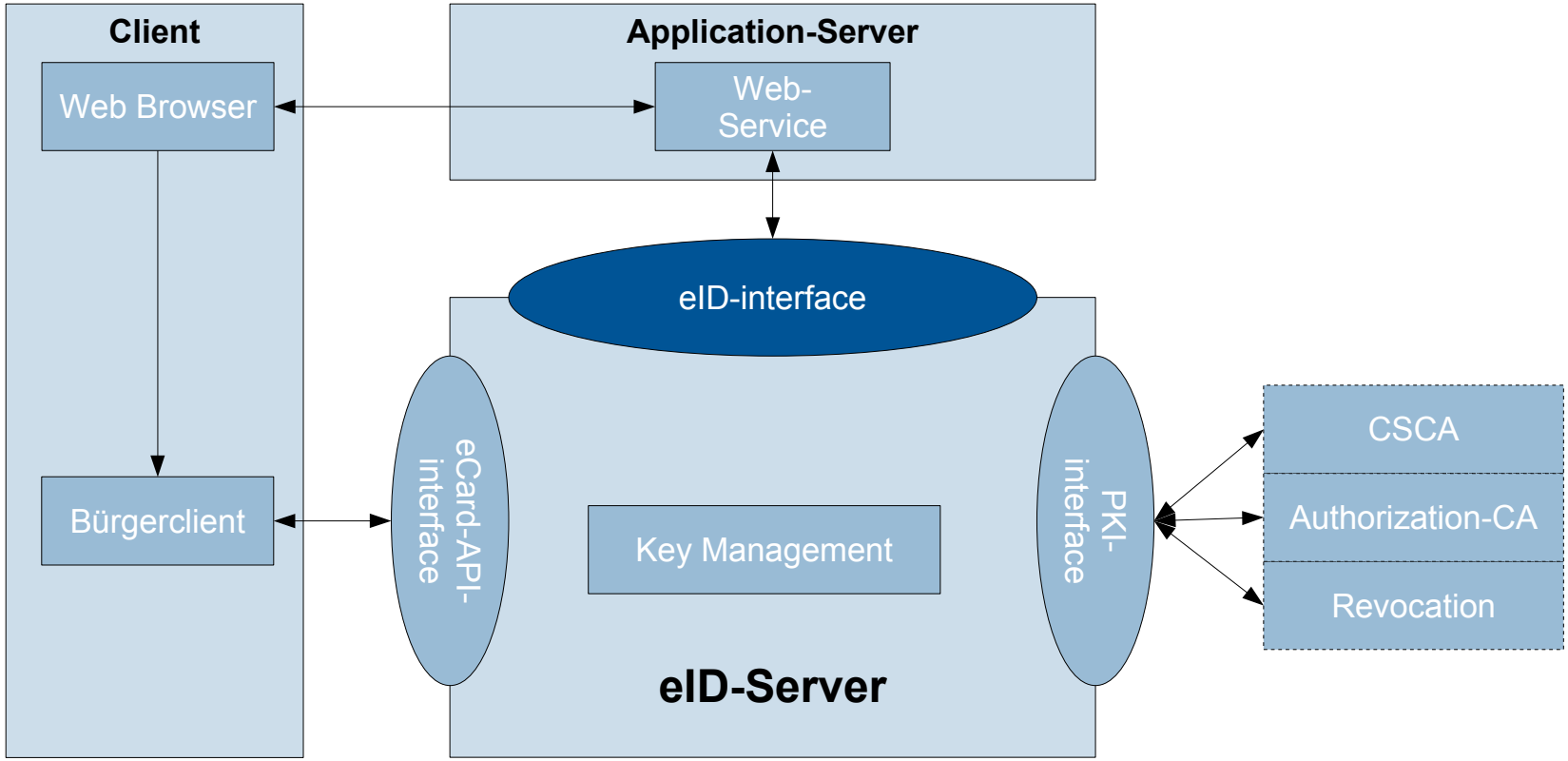
- Assurance of technical compatibility of card readers and different chip cards (contact and contactless) – health cards, signature cards etc.
- Different types:
  - Basic reader
    - Usable for mobile usage
    - Formfactor free
  - Standard reader
    - PIN-Pad for entering PIN for applications with higher security requirements
  - Comfort reader
    - Suitable for qualified signature

eCard-API-Framework TR-03112



- Technical base of Bürgerclient and eID-server
- Connection to card reader
- Execution of crypto-graphic protocols
- Communcation between Bürgerclient and service provider
- Usable for different smart cards
- Based on ISO 24727 and ECC-3

eID-Server
TR-03130

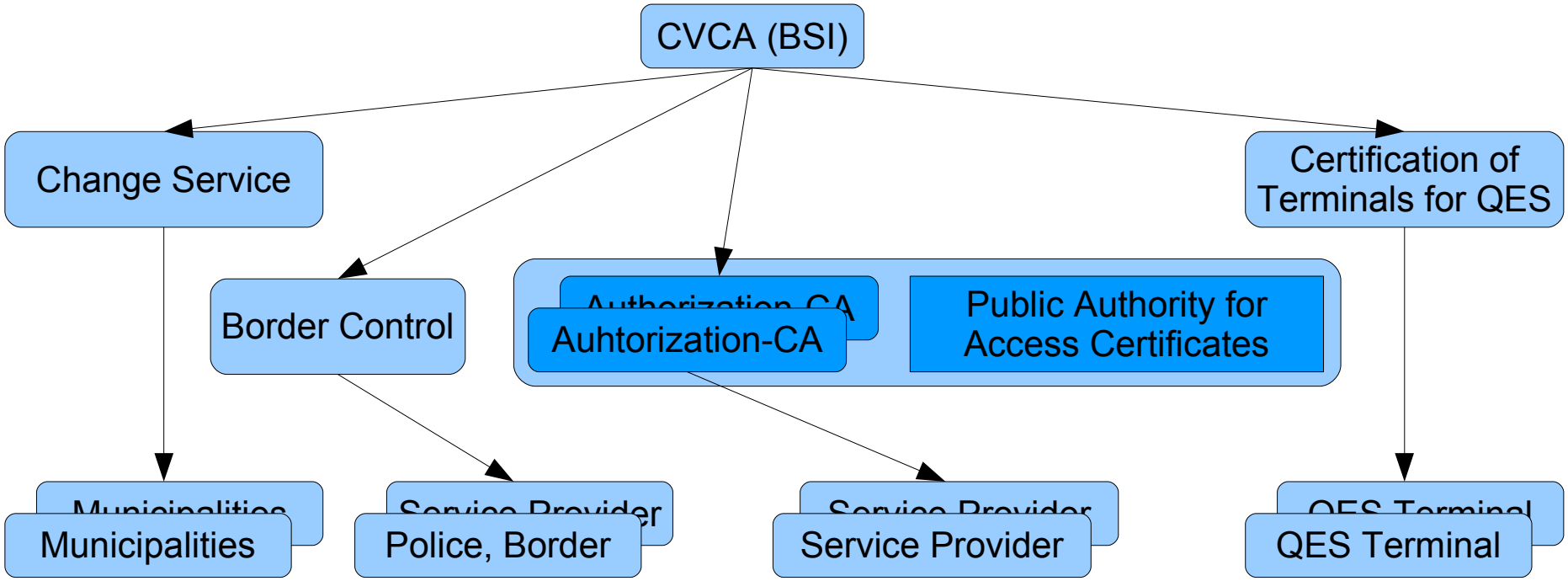


Encapsulation of technical details

Simple interface for application developers

Authorization-PKI (EAC-PKI)

Multilevel PKI for access control



eID-Revocation

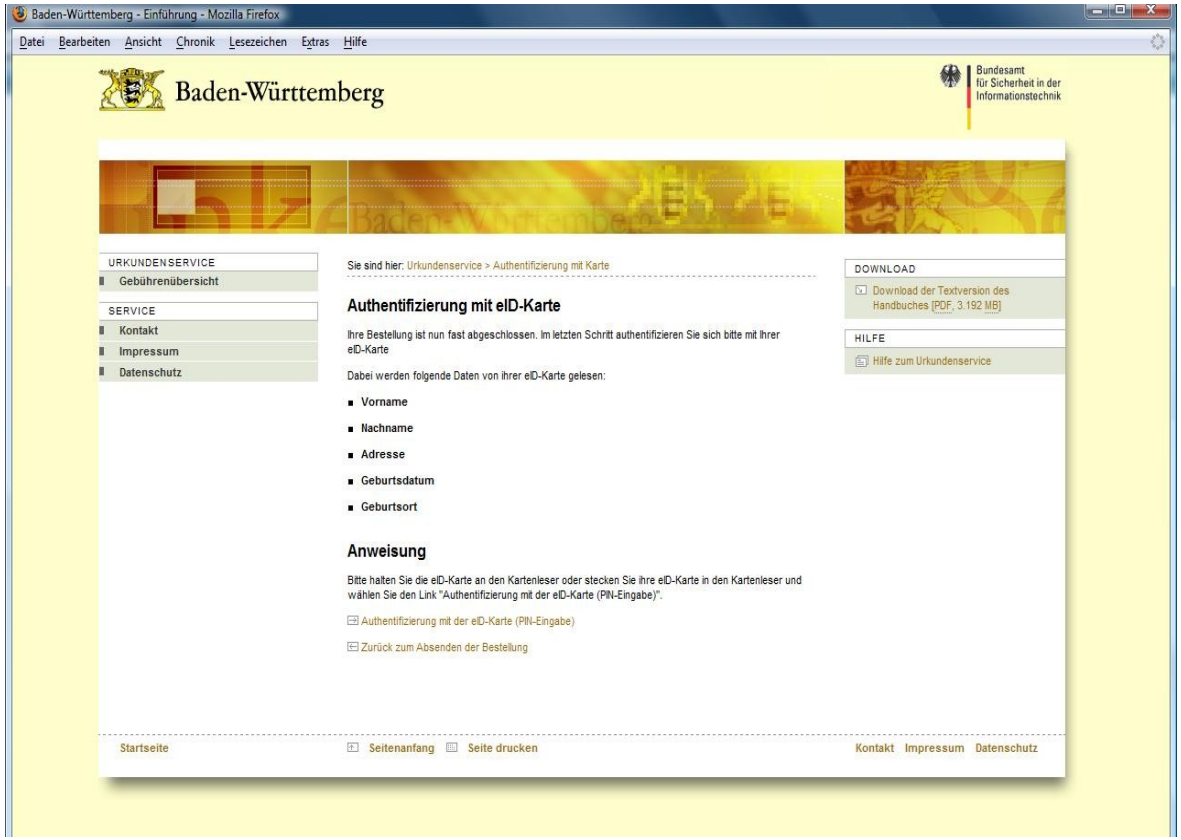
- eID-Card offers pseudonymous authentication
  - Card- and service provider specific ID
  - Not transferable between service providers
  - No “global recognition” of eID-Cards
- Revocation: eID-Card must be recognizable

Therefore: Conflict between revocation and pseudonymity

Solution: Service provider specific revocation lists

- Service provider reads provider specific revocation ID (similar to pseudonym) from eID-Card
- Lookup in provider specific revocation list

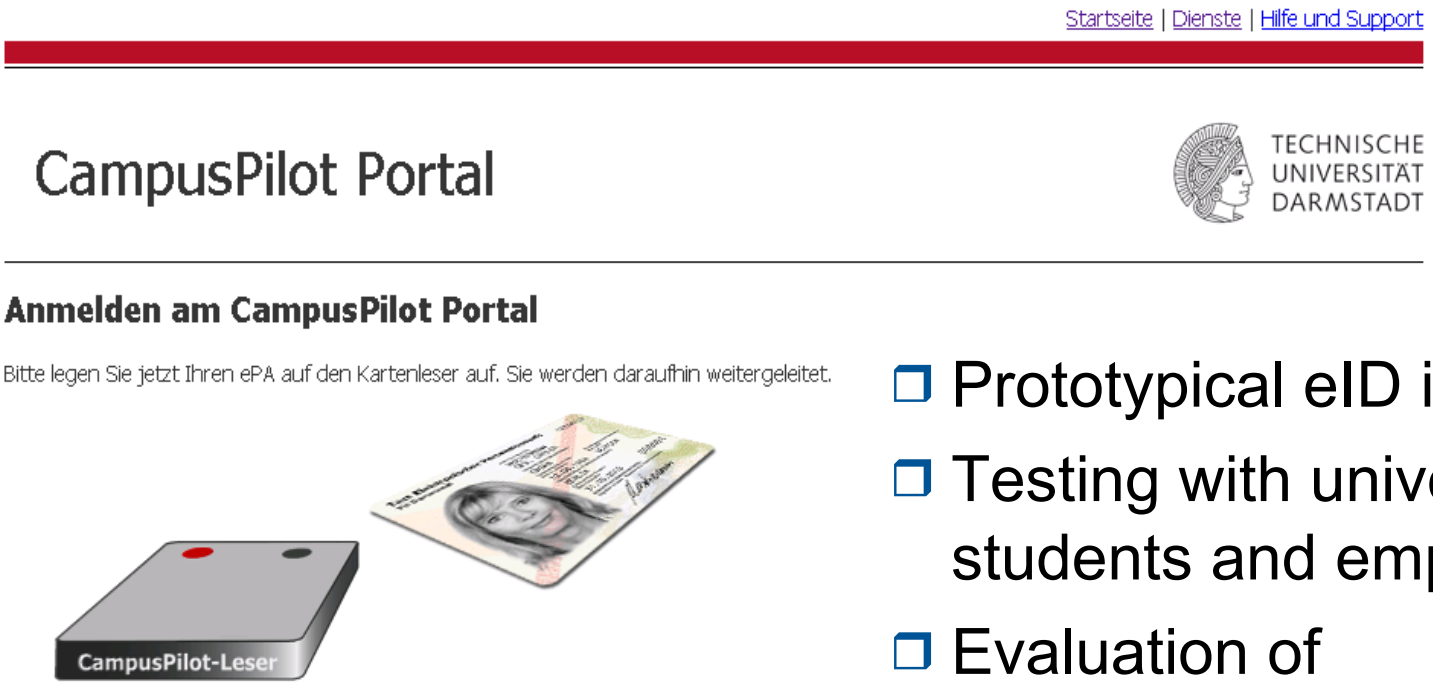
Pilot:
Serviceportal BW



Technical Proving of
Enrolment and eID-application

Project partner: T-Systems, BSI

Pilot: Campus-Pilot



- Prototypical eID infrastructure
- Testing with university students and employees
- Evaluation of
  - Reliability
  - Interoperability
  - Usability

Project partner: Consortium CampusPilot, BSI

Field Test: Enrolment

- Evaluation of systems and procedures in municipalities
  - Enrolment
  - Communication with card producer
  - Change service (incl. connection to PKI)
  - Communication with revocation service
- Preparation for country wide roll-out
- Participants
  - Ca. 25 municipalities (out of mor than 5000)
  - All software developers
  - All IT-Infrastructurs used in municipalities
- Q1/2 2010

Service Test

- **Early involvement of service providers** in evaluation of technology
- **Test of the eID-application** for eBusiness- and eGovernment-services, vending machines und offline-services
- **Broad participation of service providers** from different sectors and potential card holders as test persons
- **Optimization of support**
- **Starts October 2009**

Interoperability in Europe

- Many different eID-Cards, e.g.
  - Belgium: no biometry, personal data and eID-certificate without access control
  - The Netherlands: picture and personal data protected by BAC as known from ePassport
  - Italy: picture and fingerprints without access control, eID-certificate readable after entering of PIN
  - Spain: picture and fingerprints without access control, signature certificate but no seperate eID
- CEN TS 15890 – European Citizen Card (ECC)
  - Specification of eID-Card frame work + Middleware based on ISO24727
- eID Large Scale Pilot – STORK (CIP)
  - Development and pilot deployment of border crossing applications of electronic identity

Cryptography

- Protocols:
  - PACE
  - EAC (Terminal- and Chipauthentication) Version 2
    - Evolution from the protocols known from the European ePassport
  - Restricted Identification
    - Used for pseudonym and revocation
- All protocols suitable for different asymmetric cryptographic systems/symmetric cyphers/hashes …
- German eID-Card:
  - Elliptic Curve Cryptography with 256bit curve
  - AES-128, SHA-256
  - → high security level

Basic Access Control

- **Basic Access Control**
  - „Quick and dirty hack“ to get some privacy for eMRTDs
  - Very successful but rather limited by design
- Based on symmetric cryptography → session keys at most as strong as used password
  - Derive symmetric keys from MRZ
  - Unsuitable for PINs
- Security relies on secrecy of (parts of) MRZ
  - Document number (sequential/random, (alpha)numeric)
  - Date of Birth (partially guessable)
  - Date of Expiry (may correlate with document number)

Security of BAC against Eavesdropping

- Code Breaking Machines
  - Deep Crack (1998)
    - $250,000 → 88,000,000,000 DES Keys/s
  - COPACOBANA (2008)
    - $10,000 → 65,000,000,000 DES Keys/s

Moore's Law holds!

- Moore's Law
  - Double speed (or half the price) every 18 months
  - 10 year validity: Hardware price $10.000 → $150 (1/64)

Year	Price	Online(~20s)	½ h
2008	$10,000	33 Bit*	40 Bit
2018	$10,000	39 Bit	46 Bit

* Cryptanalysis with COPACOBANA, IEEE TRANSACTIONS ON COMPUTERS, VOL. 57, NO. 11, NOVEMBER 2008

Entropy of BAC Keys

- Maximum Entropy
  - 56 Bit for a numeric Document Number
    - ($365^2 \cdot 10^{12}$ possibilities)
  - 73 Bit for an alphanumeric Document Number
    - ($365^2 \cdot 36^9 \cdot 10^3$ possibilities)
- Redundancies, Correlations, etc.
- Examples
  - Germany (random alphanumeric numbering): ≈ 50 bit
  - Countries with sequential numeric numbering: < 40 bit
- **BAC is at the end of its life.**

Password-based Key-Agreement

- There are well-known mechanisms based on asymmetric cryptography to derive sessions keys using a short password, e.g. from ISO 11770-4
  - Mechanism 1: SPEKE
    - Jablon, 1996
    - P1363: {DL,EC}BPKAS-SPEKE
  - Mechanism 2: SRP6
    - Wu, 2002
    - P1363: DLAPKAS-SRP6
  - Mechanism 3: AMP
    - Kwon, 2000/2003
    - P1363: {DL,EC}APKAS-AMP
- … but:

Patents

- **EKE**, Bellovin & Merrit 1992
  - USP 5,241,599 1991/1993
  - USP 5,440,635, 1993/1995
- **SPEKE**, Jablon 1996
  - USP 6,226,383 1997/2001
  - USP 6,792,533 2002/2004
- **SRP**, Wu 1998
  - USP 6,539,479 1998/2003
- **AMP** not patented?

Additional problems: Security proofs? Speed?

PACE

- Provides
  - Proof of correct password (PIN) without transmitting password
  - Secure Messaging (card ↔ card terminal)
- Suitable for use with Elliptic Curve Cryptography
- Designed to be patent free
  - BSI has not applied for a patent on PACE
- One protocol, various options → Framework
  - Key Agreement (e.g. DH, ECDH)
  - Symmetric Cypher / MAC (e.g. 3DES, AES)
  - Mapping (e.g. Generic, Integrated)
- Security proof presented at ISC'09
- Speed 1sec with prototypes (brainpool256r1, AES-128, GM)

Protocol Description

	A (Card)	Shared Password π	B (Terminal)
1.	Choose random nonce s $z = E_\pi(s)$	z →	$s = D_\pi(z)$
2.	Compute ephemeral generator $\hat{g} = Map_g(s)$		Compute ephemeral generator $\hat{g} = Map_g(s)$
3.	Perform Diffie-Hellman based on the ephemeral generator $\hat{g}$ to derive common secret S.		
4.	Derive session keys from S and verify it by exchanging MACed messages. This proves that both sides use the same password π.		

Note: So far the protocol is independent of the used group (e.g. finite field or elliptic curve)

Existing Mappings

Goal: randomized embedding of s into the (EC)DH-Group

	Generic **Choose h/H by (EC)DH**	**Integrated** **B chooses K randomly**
Finite Field	$\hat{g} = g^s * h$	$\hat{g} = (E_K(s))^a$
Elliptic Curve	$\hat{G} = sG + H$	$\hat{G} = f_{a,b}(E_K(s))$

Map s into the group, randomized by h/H

a: Cofactor

$f_{a,b}()$: Icart's encoding

Integrated Mapping is faster, but Icart's encoding is patented by Sagem

Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Jens Bender
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)22899-9582-5051
Fax: +49 (0)22899-109582-5051

jens.bender@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de