Insecurity of Anonymous Login with German Personal Identity Cards

Lucjan Hanzlik, Kamil Kluczniak, Mirosław Kutyłowski

Wrocław University of Technology, Poland

SocialSec 2015, Hangzhou

1speaker
Electronic ID documents
Necessity for ID documents with a chip

- traditional security printing is not reliable enough:
  - race between authorities and sophisticated forgers
  - a personal ID document should be used for (10) years

- cryptographic protection – independent and relatively long lasting
Identity document with a memory chip - a simplest solution

- the printed data stored also on the chip,
- ... and signed by the document issuer
Identity document with a memory chip - a simplest solution

- the printed data stored also on the chip,
- ... and signed by the document issuer

Side effect: severe privacy problems
Identity document with a memory chip - a simplest solution

- the printed data stored also on the chip,
- ... and signed by the document issuer

Side effect: severe privacy problems

- personal data signed by the state authorities are attractive for illegal trading – quality is guaranteed!
Identity document with a memory chip - a simplest solution

- the printed data stored also on the chip,
- ... and signed by the document issuer

Side effect: severe privacy problems

- personal data signed by the state authorities are attractive for illegal trading – quality is guaranteed!
- for durability reasons, the chip of the e-passport should communicate via a wireless interface – so skimming is possible
Privacy protection consequences

requirements

- access to data stored in the eID must be secured by the chip of eID
- the eID has to verify that the terminal asking for data has the right to get this data

⇒ nontrivial (cryptographic) procedures
Privacy protection consequences

**requirements**

- access to data stored in the eID must be secured by the chip of eID
- the eID has to verify that the terminal asking for data has the right to get this data

⇒ nontrivial (cryptographic) procedures

**consequences:**

- eID chip has to execute cryptographic protocols (crypto coprocessor is a MUST)
Privacy protection consequences

**conclusion**

we have to employ strong cryptography for eID documents, so why not use it **online**?
ICAO standard solutions

**BAC** - Basic Access Control: session key derived from a personal data readable via an optical channel (relatively insecure protocol)
ICAO standard solutions

**BAC** - Basic Access Control: session key derived from a personal data readable via an optical channel (relatively insecure protocol)

**EAC** - Extended Access Control: both Chip Authentication and Terminal Authentication - to authenticate both the eID chip and the terminal in a cryptographic way
E-Passports

ICAO standard solutions

**BAC** - Basic Access Control: session key derived from a personal data readable via an optical channel (relatively insecure protocol)

**EAC** - Extended Access Control: both Chip Authentication and Terminal Authentication - to authenticate both the eID chip and the terminal in a cryptographic way

**PACE** - Password Authenticated Communication Establishment: the user has to enter the password to the reader, protocol immune against offline attacks
E-Passports

ICAO standard solutions

**BAC** - Basic Access Control: session key derived from a personal data readable via an optical channel (relatively insecure protocol)

**EAC** - Extended Access Control: both Chip Authentication and Terminal Authentication - to authenticate both the eID chip and the terminal in a cryptographic way

**PACE** - Password Authenticated Communication Establishment: the user has to enter the password to the reader, protocol immune against offline attacks

**CAM** - PACE combined with Chip Authentication, but more efficient than the protocol executed separately
the focus of ICAO specification

- border control - document inspection
- enabling automatic border control
- no anonymity
German personal ID card

Main components

- **Terminal Authentication** - checking terminal’s access rights
- **Chip Authentication** - checking originality of a chip
- **Restricted Identification** - anonymous authentication
- **PACE** - enabling chip operation with a password as well as place for qualified signatures

Specifications:

*BSI Technische Richtlinie 03110: Advanced Security Mechanisms for Machine Readable Travel Document*
Terminal Authentication v. 2
protocol specification of BSI

<table>
<thead>
<tr>
<th>terminal</th>
<th>e-ID chip</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. ( \text{verify } cert(PK_{PCD}) ), extract ( PK_{PCD} )</td>
<td></td>
</tr>
<tr>
<td>2. choose ( SK_{PCD} ) at random ( PK_{PCD} := g^{SK_{PCD}} ) compute commitment ( Comp(PK_{PCD}) )</td>
<td></td>
</tr>
<tr>
<td>3. ( \text{choose } r ) at random ( r \leftarrow )</td>
<td></td>
</tr>
<tr>
<td>4. ( s := \text{Sign}<em>{SK</em>{PCD}}(ID_{PICC}</td>
<td>r</td>
</tr>
<tr>
<td>5. ( s \rightarrow ) ( \text{verify } s )</td>
<td></td>
</tr>
</tbody>
</table>
## Chip Authentication

<table>
<thead>
<tr>
<th></th>
<th>terminal</th>
<th>e-ID chip</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>static key pair</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$(SK_{PICC}, PK_{PICC})$</td>
</tr>
</tbody>
</table>

### Steps:

6. $PK_{PICC} \leftarrow$

7. $\overline{PK_{PCD}}$

8. $K := (PK_{PICC})^{SK_{PCD}}$

9. choose $r'$ at random

10. $K' := Hash_1(K, r')$

11. $TAG := MAC_{K_{MAC}}(PK_{PCD})$

### Equations:

$K := (PK_{PCD})^{SK_{PICC}}$

$K' := Hash_1(K, r')$

$MAC_{K_{MAC}}(PK_{PCD})$
Restricted Identification
Domains
each domain is an autonomous system such that

- user’s personal data are processed only within the system (unless a special event occurs)
- within a domain the user appears under his domain specific identity/pseudonym
- it should be infeasible to link identities of one user in two different domains
Restricted Identification concept

Domains
each domain is an autonomous system such that

- user’s personal data are processed only within the system (unless a special event occurs)
- within a domain the user appears under his domain specific identity/pseudonym
- it should be infeasible to link identities of one user in two different domains

Background

- full disclosure of identity is not really necessary
- unnecessary data flow is a privacy risk
- a kind of privacy-by-design
German Restricted Identification
on personal ID cards

Restricted Identification:

1. e-ID card computes a unique password for each domain
2. the terminal of the domain:
   a) checks that it is talking with an e-ID card
   b) receives a password
   c) checks the password against its blacklist
**Core RI procedure**  
(notation according to BSI specification)

<table>
<thead>
<tr>
<th>Terminal</th>
<th>e-ID chip</th>
</tr>
</thead>
<tbody>
<tr>
<td>holds $\mathcal{K}'$</td>
<td>holds $\mathcal{K}'$</td>
</tr>
</tbody>
</table>

$\sigma := \text{ENC}_{\mathcal{K}'}(\text{PK}_{\text{sector}})$  

$\sigma :\rightarrow PK_{\text{sector}} := \text{DEC}_{\mathcal{K}'}(\sigma)$  

$\text{I}_{\text{sector}} := \text{Hash}(\text{PK}_{\text{sector}}^{SK_{ID}})$  

$\sigma' := \text{ENC}_{\mathcal{K}'}(\text{I}_{\text{sector}})$  

$\text{I}_{\text{sector}} :\leftarrow \text{DEC}_{\mathcal{K}'}(\sigma')$  

check if $\text{I}_{\text{sector}}$ is on sector’s black-list

$\mathcal{K}'$ is a shared key that must be established **before** running RI
Security background

- since the chip is assumed to be secure, we have to believe that the eID really sends $f_{ID}^{\text{sector}} := \text{Hash}((PK_{\text{sector}})^{SK_{ID}})$ using its private RI key $SK_{ID}$
Blacklist

- a list of values $\text{Hash}((PK_{\text{sector}})^x)$, where $x$ belongs to a banned person

Blacklisting a user

- the Issuing Authority holds the public key $PK = g^x$ of that user

- $PK_{\text{sector}} = g^{r \cdot R}$, where
  - $r$ is known to the Issuing Authority
  - $R$ is known to the domain authority

- two steps:
  - the Issuing Authority computes $P_1 = PK^r$
  - the domain authority computes $P_1^R$\[ \text{note that } P_1^R = PK^{r \cdot R} = g^{x \cdot r \cdot R} = (g^{r \cdot R})^x = (PK_{\text{sector}})^x \]
Blacklisting properties:

- the Issuing Authority does not learn the password of the revoked user
- the terminal has to know that it is really talking with a valid eID; otherwise a random response would be accepted as a valid pseudonym – it is unlikely that it appear on the blacklist

Challenge

- the terminal must check that it is talking with a valid eID
- there are many authentication protocols – but how to hide the identity of the chip?

standard solutions use something (e.g. a public key) that would link RI passwords in different domains
Design decision

- authentication of an eID via Chip Authentication with a **group key**
  - it does not mean using group signatures

- a large number of eIDs share the same group key
  - a big *anonymity set*
Realistic attack assumptions

Are group keys really protected?

- a really powerful adversary can break into an eID chip and read its secrets – breaking into just one eID of the group is enough!
- if a group key has to be installed in a large number of devices, it must be stored and protected outside the eIDs
- it suffices to provide just one tampered raw eID for personalization – it would reveal the secret (group key) in response to a secret command

what would be the consequences?
Known Attack: creating a fake eID

A fake eID

- contains a valid group key
- provides a random password during execution of the RI protocol

Properties

- the fake eID works as long as RI is used
- impossible to blacklist the fake eID
Main Attack

A powerful adversary

- learns the group key
- eavesdrops the communication with a domain server
## Main Attack
### ChA Phase

<table>
<thead>
<tr>
<th>terminal</th>
<th>e-ID chip</th>
</tr>
</thead>
<tbody>
<tr>
<td>$SK_{PCD}$ chosen at random</td>
<td>group key $(SK_{group}, PK_{group})$</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.</td>
<td>$PK_{group}$</td>
</tr>
<tr>
<td>7.</td>
<td>$\widetilde{PK}_{PCD}$</td>
</tr>
<tr>
<td>8.</td>
<td>$K := (PK_{group})^{SK_{PCD}}$</td>
</tr>
<tr>
<td>9.</td>
<td>$K := (\widetilde{PK}<em>{PCD})^{SK</em>{group}}$</td>
</tr>
<tr>
<td>10.</td>
<td>choose $r'$ at random</td>
</tr>
<tr>
<td></td>
<td>$K_{MAC} := \text{Hash}_3(K, r')$</td>
</tr>
<tr>
<td>11.</td>
<td>$TAG := \text{MAC}<em>{K</em>{MAC}}(\widetilde{PK}_{PCD})$</td>
</tr>
</tbody>
</table>

**Observation**

- the eID derives the session key with the group key $SK_{group}$ - no ephemeral random values used

$\Rightarrow$ Adversary knowing $SK_{group}$ can derive the session key $K$ from eavesdropped communication
Main Attack
RI Phase

<table>
<thead>
<tr>
<th>Terminal</th>
<th>e-ID chip</th>
</tr>
</thead>
<tbody>
<tr>
<td>holds $K'$</td>
<td>holds $K'$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$\sigma := \text{ENC}<em>{K'}(PK</em>{\text{sector}})$</th>
<th>$PK_{\text{sector}} := \text{DEC}_{K'}(\sigma)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_{\text{ID}} := \text{DEC}_{K'}(\sigma')$</td>
<td>$\sigma' := \text{ENC}<em>{K'}(f</em>{\text{ID}})$</td>
</tr>
</tbody>
</table>

Observation

- the Adversary knows $K'$!
- the Adversary can decrypt $\sigma'$ and get the domain password $f_{\text{ID}}$ of this user
The Adversary

- connects to the server with user’s account
- runs the RI protocol, with minor change:

<table>
<thead>
<tr>
<th>Terminal</th>
<th>e-ID chip</th>
</tr>
</thead>
<tbody>
<tr>
<td>holds $\mathcal{K}'$</td>
<td>holds $\mathcal{K}'$</td>
</tr>
<tr>
<td>$\sigma := \text{ENC}<em>{\mathcal{K}'}(PK</em>{\text{sector}})$</td>
<td>$PK_{\text{sector}} := \text{DEC}_{\mathcal{K}'}(\sigma)$ (^2)</td>
</tr>
<tr>
<td>$f_{ID}^{\text{sector}} := \text{DEC}_{\mathcal{K}'}(\sigma')$</td>
<td>$\sigma' := \text{ENC}<em>{\mathcal{K}'}(f</em>{ID}^{\text{sector}})$</td>
</tr>
</tbody>
</table>

\(\sigma' \leftarrow \) check if $f_{ID}^{\text{sector}}$ is on sector’s black-list

\(^2\)the step may be ignored, as the Adversary knows $PK_{\text{sector}}$.
Main Attack

Attack potential

an attacker may login to the user’s account after a purely passive attack

It looks like an obvious trapdoor in the German personal identity cards.
Possible defense
### Modified version of the protocol

**Chip Authentication phase**

<table>
<thead>
<tr>
<th>Terminal $i$</th>
<th>Chip</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chip Authentication Phase</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>choose $\rho$ at random</strong></td>
</tr>
<tr>
<td></td>
<td>$Y'<em>{\text{group}} := Y^\rho</em>{\text{group}}$</td>
</tr>
<tr>
<td>6.</td>
<td></td>
</tr>
<tr>
<td>$K := \left( Y'_{\text{group}} \right)^{x_i, r}$</td>
<td>$K := (\tilde{Y}<em>i)^{x</em>\text{group} \cdot \rho}$</td>
</tr>
<tr>
<td>choose $r'$ at random</td>
<td></td>
</tr>
<tr>
<td>$K_{\text{MAC}} := \text{Hash}(K, r')$</td>
<td>$K_{\text{MAC}} := \text{Hash}(K, r')$</td>
</tr>
<tr>
<td>$\text{Tag} := \text{MAC}(K_{\text{MAC}}, Y'_{\text{group}})$</td>
<td>$\text{Tag} \equiv \text{MAC}(K_{\text{MAC}}, Y'_{\text{group}})$</td>
</tr>
<tr>
<td>$K_{\text{Enc}} := \text{Hash}_1(K, r')$</td>
<td>$K_{\text{Enc}} = \text{Hash}_1(K, r')$</td>
</tr>
</tbody>
</table>
### Modified version of the protocol

**Restricted Identification phase**

<table>
<thead>
<tr>
<th><strong>Terminal i</strong></th>
<th><strong>Chip</strong></th>
</tr>
</thead>
</table>

#### Restricted Identification phase

1. \( \sigma := \text{Enc}_{\mathcal{KEnc}}(Y_{\text{sector}}) \)
2. \( \sigma \rightarrow Y_{\text{sector}} := \text{Dec}_{\mathcal{KEnc}}(\sigma) \)
3. \( \sigma' := \text{Enc}_{\mathcal{KEnc}}(ID_{\text{User}}) \)
4. \( \sigma'' := \text{Enc}_{\mathcal{KEnc}}(\rho) \)
5. \( \sigma''' := \text{Enc}_{\mathcal{KEnc}}(Y_{\text{group}}) \)

\[ \sigma', \sigma'', \sigma''' \leftarrow \sigma''' \]

6. \( ID_{\text{User}} := \text{Dec}_{\mathcal{K}}(\sigma') \)
7. **is** \( ID_{\text{User}} \) **on sector’s black-list?**
8. \( \rho := \text{Dec}_{\mathcal{K}}(\sigma'') \)
9. \( Y_{\text{group}} := \text{Dec}_{\mathcal{K}}(\sigma''') \)
10. **check if** \( Y^\rho_{\text{group}} \overset{?}{=} Y'_{\text{group}} \)

**data exchange**

**whole communication secured by encryption with key** \( \mathcal{KEnc} \)
Properties

- authentication of ChA phase becomes effective after establishing a secure channel
- the session key resulting from Chip Authentication depends on ephemeral values on the side of eID and therefore cannot be derived from the group key alone
Insecurity of RI
Hanzlik, Kluczniak, Kutyłowski
ID documents
E-ID
TA and ChA
RI
RI concept
RI concept
RI on German eID
Possible defense
BSI eIDAS
**Idea:** authenticating the chip via *domain signature*

- the terminal can check that the signature comes from a chip personalized by the document issuer
- no unique public key for a chip
- the public key used for signature verification derived separately for each domain (sector)
Insecurity of RI
Hanzlik, Klucznia, Kutyłowski
ID documents E-ID TA and ChA
RI RI concept RI concept RI on German eID
Possible defense BSI eIDAS

Patch by BSI

**Idea:** authenticating the chip via **domain signature**
- the terminal can check that the signature comes from a chip personalized by the document issuer
- no unique public key for a chip
- the public key used for signature verification derived separately for each domain (sector)

**Properties:** of the solution from BSI TR
- keys for an eID chip derived from **group secret key**
- ... yet each eID holds different keys
- leaking secret group key does not enable to impersonate a user
Domain signatures

of course domain signatures have also different applications

a good topic for another (long) talk

in BSI TR 03110 renamed as *pseudonymous signatures*
**Issuer’s setup**

- the secret keys $z$ and $x$
- public keys $g_1$, $g_2 = g_1^z$, $y = g_1^x$
BSI algorithm
core algorithm

Issuer’s setup
- the secret keys $z$ and $x$
- public keys $g_1$, $g_2 = g_1^z$, $y = g_1^x$

Issuing an eID for user $i$
- choose $x_{2,i} \in \mathbb{Z}_p$ at random
- compute $x_{1,i} = x - z \cdot x_{2,i}$
- install $(x_{1,i}, x_{2,i})$ in the eID of the user $i$. 
**Issuer’s setup**

- the secret keys $z$ and $x$
- public keys $g_1, \ g_2 = g_1^z, \ y = g_1^x$

**Issuing an eID for user $i$**

- choose $x_{2,i} \in \mathbb{Z}_p$ at random
- compute $x_{1,i} = x - z \cdot x_{2,i}$
- install $(x_{1,i}, x_{2,i})$ in the eID of the user $i$.

**Signing $m$ by Alice for domain $D$**

- create domain specific pseudonym $dsnym = D^{x_{1,i}}$
- choose $t_1, t_2$ at random, $a_1 = g_1^{t_1} g_2^{t_2}, \ a_2 = D^{t_1}$
- $c = \text{Hash}(D, dsnym, a_1, a_2, m)$
- $s_1 = t_1 - c \cdot x_{i,1}, \ s_2 = t_2 - c \cdot x_{i,2}$
- output the signature $(c, s_1, s_2)$
Insecurity of RI
Hanzlik, Kluczniak, Kutyłowski

ID documents
E-ID
TA and ChA
RI
RI concept
RI concept
RI concept
RI on German eID
Possible defense
BSI eIDAS

BSI algorithm
core algorithm

Signing \( m \) by Alice for domain \( D \)
- create domain specific pseudonym \( dsnym = D^{x_1,i} \)
- choose \( t_1, t_2 \) at random, \( a_1 = g_1^{t_1} g_2^{t_2}, a_2 = D^{t_1} \)
- \( c = \text{Hash}(D, dsnym, a_1, a_2, m) \)
- \( s_1 = t_1 - c \cdot x_{i,1}, s_2 = t_2 - c \cdot x_{i,2} \)
- output the signature \((c, s_1, s_2)\)

Signature verification
- compute \( a_1 = y^c \cdot g_1^{s_1} \cdot g_2^{s_2}, a_2 = dsnym^c \cdot D^{s_1} \)
- output valid if \( c = \text{Hash}(D, dsnym, a_1, a_2, m) \) and \( dsnym \) not on a blacklist
Seclusiveness problem

**Attack:**

- **break into just two eIDs**
- use private keys $x_{1,i}$, $x_{2,i}$ and $x_{1,j}$, $x_{2,j}$ to compute $x$, $z$ based on the equations

\[
x = x_{1,i} + z \cdot x_{2,i}
\]
\[
x = x_{1,j} + z \cdot x_{2,j}
\]

- ... and **create any number of fake eIDs** that would create proper domain signatures
Undeniability problem

Proof of interaction:

- every authentication based on signature leaves undeniable proof of user’s activity
- sometimes the proof is required but otherwise it is a security threat in the system as the signature can serve as evidence against third parties

security rule: one should avoid generating data that can be misused
Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.edu.pl