Challenges for electronic identity documents

Mirosław Kutyłowski

Wrocław University of Technology

LIT 2011

Challenges for E-ID Documents

why E-ID cards?
personal ID card
goals of E-ID

remote identification
PACE
TA
ChA
confirming data

restricted identification
health care
law enforcement
social networks
e-auction services
Bürgerkarte
anonymous credentials
German RI
our RI

Outline

1. why E-ID cards?
   - personal ID card
   - goals of E-ID
2. remote identification
   - PACE
   - TA
   - ChA
   - confirming data
3. restricted identification
   - health care
   - law enforcement
   - social networks
   - e-auction services
   - Bürgerkarte
   - anonymous credentials
   - German RI
   - our RI

Motivation for Electronic Personal ID Cards

Personal ID cards

goals

Today

- a certified copy of some personal data
- a kind of a token

Usage

- proves authenticity of data in an offline setting
- some procedures are based on the principle “one person - one personal ID document”

Personal ID cards

goals

Today

- a certified copy of some personal data
- a kind of a token

Usage

- proves authenticity of data in an offline setting
- some procedures are based on the principle “one person - one personal ID document”

Do we really need personal ID cards?

Online versus offline

- data can be checked online in a central database
  sometimes online contact is inevitable
  – checking if the card has not been revoked
- the only advantage is that the holder of the card has control whom he shows the personal data

As a token?

- the new tendency is to admit ID document for only a single purpose: presenting it by the owner
  (forbidden by law to retain the ID document)

Do we really need personal ID cards?

consequences

Loosing business motivation for personal ID cards

In the traditional setting the ID card with whole security printing features is becoming unnecessary from practical point of view

- print yourself an ID card just as a flight ticket or a boarding card!

Electronic personal ID cards

goals

What are the goals for introducing ID cards with a chip?

- **preventing forgery**
  - it is infeasible to break well designed cryptographic protection even if the manufacturer is malicious
  - protection mechanism independent from graphical security measures
- **machine readable ID card:** for automatic border control, automatic registration ..

  (traditional MRZ codes consist of just a few bytes)
- **a personal device for remote services**
  - a service provider can check that an ID card is on the other side ...

Electronic personal ID cards

goals

What are the goals for introducing ID cards with a chip?

- **preventing forgery**
  - it is infeasible to break well designed cryptographic protection even if the manufacturer is malicious
  - protection mechanism independent from graphical security measures
- **machine readable ID card:** for automatic border control, automatic registration ..

  (traditional MRZ codes consist of just a few bytes)
- **a personal device for remote services**
  - a service provider can check that an ID card is on the other side ...

Electronic personal ID cards
goals

What are the goals for introducing ID cards with a chip?

- **preventing forgery**
  - it is infeasible to break well designed cryptographic protection even if the manufacturer is malicious
  - protection mechanism independent from graphical security measures
- **machine readable ID card:** for automatic border control, automatic registration ..

  (traditional MRZ codes consist of just a few bytes)
- **a personal device for remote services**
  - a service provider can check that an ID card is on the other side ...

Why personal ID cards
opportunities

Advantages

- one user – one eID card
- ID cards under strict control of the state
- well trained correct behavior of the owners

Limitations

- each ID card has a limited memory
- ID cards often get lost, stolen, and damaged

What services with eID cards?

Remote services

proving presence of eID card: – if the eID card is on the other side, then most likely its owner is there, too

confirming documents, transactions: – a signature or a transaction code for a document issued by eID, then most likely it has been created by its owner

replacing login & password: an eID (with appropriate cryptography) can replace tons of passwords

Remote Identification

Remote identification

requirements

Activating smart card by the owner

- a password must be used
- the password must not transmitted to the smart card in clear (eavesdropping possible), but no keyboard on a smart card, no prior secret apart from the password

Sounds to be infeasible...

In the future

- biometric reader directly on the smart card?
- a card with a display and simple keyboard

Remote identification

requirements

Activating smart card by the owner

- a password must be used
- the password must not transmitted to the smart card in clear (eavesdropping possible), but no keyboard on a smart card, no prior secret apart from the password

Sounds to be infeasible...

In the future

- biometric reader directly on the smart card?
- a card with a display and simple keyboard

Owner authentication

PACE

- password included in key agreement protocol executed to set up a session key - modified Diffie-Hellman protocol
- no replay attacks possible - for each authentication attempt there is a different challenge
- implicit proof of knowledge of the password:
  - the password is not used as a PIN to unblock the device
  - communication encrypted with a key that is derived from the password

Challenge

nothing can improve entropy of the password – it cannot be too high, otherwise the owner cannot memorize it, password guessing is possible

Terminal Authentication

Challenge

checking identity of a terminal necessary before:

- the terminal gets some non-trivial data from the card (like digital image of the owner's face)
- the card starts any important protocol, for example:
  - allowing the terminal to instal a qualified signature
  - confirming presence for a medical transaction

Requirements

- no replay attack should be possible
- protocol transcript cannot serve as a proof for a third party that the interaction took place

Terminal Authentication

Solutions

- Zero Knowledge Protocols - faking a transcript is easy, transcript useless for a third party
- static Diffie-Hellman protocol
- no “man-in-the-middle” attacks possible
- at the same time session key established
- the terminal need not to be a a local one – the protocol can be executed remotely

Still, this is not a mutual authentication!

Chip Authentication

Challenge

checking identity of a smart card:

- to check authenticity of the eID card and its presence,
- to confirm data transmitted later by the chip

Requirements

- no replay attack should be possible
- protocol transcript cannot serve as a proof for a third party that the interaction took place

Chip Authentication

Solutions

- Zero Knowledge Protocols - faking a transcript is easy, transcript useless for a third party
- static Diffie-Hellman protocol
- no “man-in-the-middle” attacks possible
- at the same time session key established
- the terminal need not to be a a local one – the protocol can be executed remotely

similarity to TA is not incidental!

Chip Authentication and Terminal Authentication

ordering the operations

French-German war on Chip Authentication

France	ChA first, then TA
Germany	TA first, then ChA

Ordering of operations may be fixed for a given smart card!
a war for the market

Challenge

- travel document inspection case (ICAO): no TA executed, the biometric passport is showing data just to anybody
- personal data protection: the eID must not reveal personal data to unauthorized terminals

Confirming personal data

Concept 1: digital stamp

- every data item confirmed by a digital signature ...
- ... by the document issuer

high quality data confirmation, enables selling these data and creating copies of state registries

Concept 1: ZKP

- data authenticated since told by an authenticated chip
- no explicit authentication, no transferability of the proof
- encryption with a session key prevents data modifications on the way between the chip and the terminal

Restricted Identification

Restricted Identification
idea

The main idea of restricted identification

- concentrate on rights of a user
- hide identity of a user ...
- but bind the rights with a physical person

Pseudonyms, attribute certificates?

pseudonyms are not enough:

Sybil attacks: one person may acquire many pseudonyms for interaction with the same system

identity transfer: pseudonym (and authentication data) may be sold to a third person

Restricted Identification

idea

The main idea of restricted identification

- concentrate on rights of a user
- hide identity of a user ...
- but bind the rights with a physical person

Pseudonyms, attribute certificates?

pseudonyms are not enough:

Sybil attacks: one person may acquire many pseudonyms for interaction with the same system

identity transfer: pseudonym (and authentication data) may be sold to a third person

Concept of sectors

Idea of sectors

1. activity areas divided into independent sectors
2. strict data separation between sectors, interaction only if explicitly defined
3. for each sector different authentication

Sector examples

- health care system
- employment authority
- citizen-police contacts
- children protection
- local referenda
- . . .

Concept of sectors

Idea of sectors

1. activity areas divided into independent sectors
2. strict data separation between sectors, interaction only if explicitly defined
3. for each sector different authentication

Sector examples

- health care system
- employment authority
- citizen-police contacts
- children protection
- local referenda
- . . .

Access to medical data

Idea

- medical data stored in a central system
- a patient has access to his own data
- identity of the patient not revealed, even not known by the Web system
- strong authentication before revealing data

Motivation

- patient awareness
- patient's control over charges to insurance company

Access to medical data

Realization

user authentication — restricted identification with his e-ID card

1. a patient has a single identity for the health care system
2. impossible to get access to data of a different person
3. identity from the health care system not linkable with identities from other sectors
   dishonest system administrator cannot sell high quality digital data

Citizen-police contacts

Motivation

1. the witnesses of crime are often afraid to inform police:
   - they fear that policemen and criminals may cooperate
   - they fear that during court procedures they will be forced to act as witnesses

   ... but afterwards the (organized) crime may revenge
2. identity of a person is important during court procedure but not during investigation

Electronic witness

1. strong authentication that a message comes from a physical person
2. the messages from the same person should be linkable

Citizen-police contacts

Realization

user authentication — restricted identification with his e-ID card

1. police knows that somebody holding an ID card is sending a message
2. not feasible to identify the informer – cryptographic protection
   (some disclosure procedures possible, but with involvement of a third party (Supreme Court?)
3. still one person cannot send messages on behalf of many people (no Sybil attack)

Citizen-police contacts

Realization

user authentication — restricted identification with his e-ID card

1. police knows that somebody holding an ID card is sending a message
2. not feasible to identify the informer – cryptographic protection
   (some disclosure procedures possible, but with involvement of a third party (Supreme Court?)
3. still one person cannot send messages on behalf of many people (no Sybil attack)

Citizen-police contacts

Realization

user authentication — restricted identification with his e-ID card

1. police knows that somebody holding an ID card is sending a message
2. not feasible to identify the informer – cryptographic protection
   (some disclosure procedures possible, but with involvement of a third party (Supreme Court?)
3. still one person cannot send messages on behalf of many people (no Sybil attack)

Citizen-police contacts

Realization

user authentication — restricted identification with his e-ID card

1. police knows that somebody holding an ID card is sending a message
2. not feasible to identify the informer – cryptographic protection
   (some disclosure procedures possible, but with involvement of a third party (Supreme Court?)
3. still one person cannot send messages on behalf of many people (no Sybil attack)

Social networks

Threats of Social Networks

1. people discovered social life over Internet, and like it
2. people are exposed to all possible threats - personal safety at risk

Motivation

as people will not stop to use social networks, give them pseudonyms such that:

- one cannot change a pseudonym within one network
- some data can be released (like age, sex, . . .)

Social networks

Realization

user authentication — restricted identification with his e-ID card

1. no cheating (*I am over 18 years old ...*)
2. Internet trolls easily banned
3. no playing different persons at the same time

Social networks

Realization

user authentication — restricted identification with his e-ID card

1. no cheating (*I am over 18 years old ...*)
2. Internet trolls easily banned
3. no playing different persons at the same time

Social networks

Realization

user authentication — restricted identification with his e-ID card

1. no cheating (*I am over 18 years old ...*)
2. Internet trolls easily banned
3. no playing different persons at the same time

Social networks

Realization

user authentication — restricted identification with his e-ID card

1. no cheating (*I am over 18 years old ...*)
2. Internet trolls easily banned
3. no playing different persons at the same time

Electronic auctions

Motivation

services like e-Bay (Germany), Allegro (Poland),... :

1. exchange of goods between the citizens over Internet an important part of economy (used books, rare products, ...)
2. the cheaters have good play grounds
3. recommendation systems are fairly weak *criminals threaten the victims if they put negative comments*

Electronic auctions

Realization

user authentication — restricted identification with his e-ID card

1. easy age verification (Polish civil law forbids children to make civil contracts)
2. a cheater cannot change his pseudonym
3. recipients really anonimized, so can put comments freely
4. tax authorities have possibilities to disclose identity of a seller

Electronic auctions

Realization

user authentication — restricted identification with his e-ID card

1. easy age verification (Polish civil law forbids children to make civil contracts)
2. a cheater cannot change his pseudonym
3. recipients really anonimized, so can put comments freely
4. tax authorities have possibilities to disclose identity of a seller

Electronic auctions

Realization

user authentication — restricted identification with his e-ID card

1. easy age verification (Polish civil law forbids children to make civil contracts)
2. a cheater cannot change his pseudonym
3. recipients really anonimized, so can put comments freely
4. tax authorities have possibilities to disclose identity of a seller

Electronic auctions

Realization

user authentication — restricted identification with his e-ID card

1. easy age verification (Polish civil law forbids children to make civil contracts)
2. a cheater cannot change his pseudonym
3. recipients really anonimized, so can put comments freely
4. tax authorities have possibilities to disclose identity of a seller

Electronic auctions

Realization

user authentication — restricted identification with his e-ID card

1. easy age verification (Polish civil law forbids children to make civil contracts)
2. a cheater cannot change his pseudonym
3. recipients really anonimized, so can put comments freely
4. tax authorities have possibilities to disclose identity of a seller

Technical Solutions: Austrian Bürgerkarte

Austrian Bürgerkarte

mechanism

Details

1. Bürgerkarte computes a password for each sector, the password computed from personal number and sector ID
2. central password verification – just like for PIN numbers of bank cards
3. **given two passwords from different sectors – it is unfeasible to say if they belong to the same person**

Disadvantages

1. the passwords are static
2. the recipient can impersonate the owner

Technology

shared secrets, symmetric cryptography

Technical Solutions: Anonymous Credentials

Anonymous credentials

idea

Separation of roles

identity provider manages user's attributes and issues credentials

service provider grants access based on presented credentials

Anonymous credentials

details

A typical procedure

1. user receives a request for credentials from a service provider
2. user submits the request to identity provider
3. identity provider
   - checks the request against user's attributes
   - issues anonymous credential for the user
4. the user presents the credentials to the service provider

Anonymous credentials
idea

Minimal properties

- an identity provider knows the attributes but not the target service
- a service provider learns the attributes but not the identity

Technology

from simple solutions based on symmetric cryptography up to sophisticated ones using asymmetric cryptography and more anonymity

Technical Solutions: German Restricted Identification

German restricted identification

on personal ID cards

Procedure

login in a sector:

1. e-ID card computes a unique password for each sector
2. the terminal of service provider:
   a) checks that it is talking with an e-ID card
   b) receives a password
   c) checks the password against the blacklist of this sector

German restricted identification

Personalausweis

Properties

1. an e-ID cannot generate a different password, so blacklists are effective
2. very strong personal data protection mechanism
3. strong guarantees for unlinkability of passwords from different sectors

strong cryptography, some infrastructure necessary

Technical Solutions: our approach

White list approach

Wroclaw University of Technology

somewhat similar to the German scheme, but

1. management of users in a sector with
   - white-lists (list legitimate users) and/or . . .
   - . . . blacklists (list of excluded users)
2. each time a different password –
   the terminals need not to be trusted

Primary application areas

access to medical data from National Health Fond (NFZ)

Technology

- one private key on E-ID card for all sectors
- even sector signatures with the same key are possible (Jun Shao (P.R.C.) & M.K.)

Restricted identification

technical overview

State of the art

- different techniques and architectures possible
- sometimes specific for specific application areas
- a universal solution does not exist so far – and probably we do not need such a solution
- based on strong cryptography with **provable properties**
  if it fails, then everything fails
- based on well studied and available components (like static DH protocol, DLP, independent of particular algebraic structures, ...)

Restricted identification

technical overview

State of the art

- different techniques and architectures possible
- sometimes specific for specific application areas
- a universal solution does not exist so far – and probably we do not need such a solution
- based on strong cryptography with **provable properties**
  if it fails, then everything fails
- based on well studied and available components (like static DH protocol, DLP, independent of particular algebraic structures, ...)

Restricted identification

technical overview

State of the art

- different techniques and architectures possible
- sometimes specific for specific application areas
- a universal solution does not exist so far – and probably we do not need such a solution
- based on strong cryptography with **provable properties**
  if it fails, then everything fails
- based on well studied and available components (like static DH protocol, DLP, independent of particular algebraic structures, ...)

Restricted identification

technical overview

State of the art

- different techniques and architectures possible
- sometimes specific for specific application areas
- a universal solution does not exist so far – and probably we do not need such a solution
- based on strong cryptography with **provable properties**
  if it fails, then everything fails
- based on well studied and available components (like static DH protocol, DLP, independent of particular algebraic structures, ...)

Restricted identification

technical overview

State of the art

- different techniques and architectures possible
- sometimes specific for specific application areas
- a universal solution does not exist so far – and probably we do not need such a solution
- based on strong cryptography with **provable properties**
  if it fails, then everything fails
- based on well studied and available components (like static DH protocol, DLP, independent of particular algebraic structures, ...)

Acknowledgment

Many thanks for support form

- Polish Ministry of Science and Education
- Foundation for Polish Science, Programme “Mistrz”

FNP
Fundacja na rzecz Nauki Polskiej

I would like to thank

- Mr. Witold Drożdż, former Polish Undersecretary of State,
- my former colleagues from Ministry of Interior and Administration, and
- Dr Dennis Kügler and Dr Jens Bender from Bundesamt für Sicherheit in der Informationstechnik.

Thanks for your attention!

Contact data

1. Miroslaw.Kutylowski@pwr.wroc.pl
2. http://kutylowski.im.pwr.wroc.pl
3. +48 71 3202109, fax: +48 71 320 2105