Disability Parking Permit
Lightweight but Trustworthy Identity Documents

Mirosław Kutyłowski, Piotr Lipiak

Wrocław University of Technology
Wrocław, Poland

IEEE TRUSTID 2013
People with mobility disabilities

Attempts to reduce problems due to mobility disability problems:

- make exempts from general rules that would exclude these people from normal life
- reduce mobility barriers

- European Directives
- national laws
Some rights of drivers with mobility disabilities:
- designated parking places
- waiver of parking fees
- driving and halting in restricted areas

Parking permit as the document confirming these rights:
Disability Parking Permit

- partially standardized in European Union
- obligatory fields, only necessary data
- protection of personal data

Security features:
- seal of the issuing authority
- signature of the owner

.. so practically no security features! Only legal protection - penalties for creating fake documents
Parking permit misuse

Misuse

- attractive as a free ticket enabling to park in restricted areas
- borrowing permits to unauthorized drivers
- permit not returned when the rights expire

Some estimations indicate that more than 50% of disability parking permits are either fake or issued to people with no mobility problems.

Easing misuse:

- permits issued by local authorities
- no registries, no easy online verification, no control
- permits are easy to forge
Attempts to secure the system

1. use forgery evident techniques for securing physically the document
2. control local authorities through compulsory involvement of a trusted third party
Smart cards
why it does not work

delivery  production and personalization costly and has to be centralized – inevitable delivery delays and high cost

manipulations  non-electronic cards can be overwritten unless fancy printing techniques, electronic layer with crypto is necessary

inspection  problems with inspection through the windshield

readers  wireless smart cards - expensive readers and problems with wireless communication from distance and the glass
Assumptions

production parking permits printed locally, standard (cheap) devices used

forgery resistance parking permit must be secured against forgery

cloning resistance parking permit must not be cloned (otherwise two drivers may use the same correct data)

inspection optical, wireless communication might be problematic as the parking permit should work with no battery

inspection devices smart phones
Physical protection
holograms

Holograms

- optical effect - inspection by a human eye, requires minimal training
- advanced technology for producing holograms, patented, registering holograms
- low unit price

Securing ID document

- hologram on a thin transparent film
- hologram and the film glued with the paper document in a machine (like lamination but temperature control $\approx 115^\circ C$
- hologram can be separated from the paper, but film torn and holograms comes in pieces
Physical protection
holograms

Problems solved:

- holograms with serial numbers - accountability
- cloning only by permit issuers
- manipulating printed data leaves traces on the film and the hologram

typically used for issuing car registration documents
Disability ParkingID

Kuty lowski, Lipiak

Problem
Requirements
Solution
physical protection
signatures
legal
face image
Application
-temporary
personal ID
Conclusions

Representing “electronic data”
QR codes

“ala ma kota. jasio ma pieska. piesek nazywa sie burek. ala lubi burka”

Advantages
- error correction codes
- easy for machine reading
- purely optical representation, easy printing,
- no compatibility problems for communication – as for smart card protocols
- recognized by Android applications, . . .
Cryptographic protection

Electronic signature

1. elliptic curves signatures and textual data easy to encode as QR code
2. a mediated electronic signature of the issuer
### Mediated Schnorr Signature

- Private key $x$ is partitioned into $x_1$ and $x_2$ so that $x = x_1 + x_2$.
- Two parties involved in signature creation, say $A$ and $B$, holding respectively $x_1$ and $x_2$.

#### Creating signature $(e, s)$ of $M$

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$A$ chooses $k_1 \in [1, q - 1]$ uniformly at random,</td>
</tr>
<tr>
<td>2</td>
<td>$R_1 := k_1 P$,</td>
</tr>
<tr>
<td>3</td>
<td>$R_1$ is sent to $B$,</td>
</tr>
<tr>
<td>4</td>
<td>$B$ chooses $k_2 \in [1, q - 1]$ uniformly at random,</td>
</tr>
<tr>
<td>5</td>
<td>$R_2 := k_2 P$, $R := R_1 + R_2$,</td>
</tr>
<tr>
<td>6</td>
<td>$e := H(M</td>
</tr>
<tr>
<td>7</td>
<td>$s_2 := (k_2 - x_2 \cdot e) \mod q$,</td>
</tr>
<tr>
<td>8</td>
<td>$s_2$ and $R$ are sent to $A$,</td>
</tr>
<tr>
<td>9</td>
<td>$s := (k_1 - x_1 \cdot e) + s_2 \mod q$.</td>
</tr>
</tbody>
</table>
Advantages

- signing parties: local authority and country’s registry
- key generation procedure may guarantee that no party is in possession of both part at no time
- the keys for country’s registry may be generated on-the-fly from a single secret
- neither a local authority nor country’s registry can create alone a valid signature
- the outcome is the regular signature, no adjustment of verification necessary

Main advantage

no document can be issued without knowledge of the state’s registry guarantees are not organizational but technical
Legal concept
signed data in QR as a *seal*

**A seal**

1. no explicit legal definition
2. functional properties are identical with electronic signature (machine generated) encoded in QR code and sealed

- no necessity to change legal rules concerning disability parking permit
- adjusting legal framework is a substantial part of implementation cost
Face image

**Necessity of protection**

- protect the image so that it is not changed by third persons (or even local authority) ⇒ **sign digitally**
- prevent from reading and using by third persons ⇒ **do not sign digitally**
- encoding the whole image for the electronic signature in QR code is infeasible – its volume is too high

*it seems that we have contradictory requirements and an unsolvable problem as we have no active electronic part on the parking permit*
Face image

three resolutions concept

three images obtained from one photo:

- **full resolution**: original image, stored in a central registry
- **middle resolution**: printed on the back side of the permit
- **resolution**: further reduced, digitally signed and encoded in a QR code

Feasibility of signature and low value of the electronic signature for the third parties
face image
alternative approach

concept developed by German authorities

- an image printed
- biometric features extracted
- biometric features signed

Problems:

- biometric methods for face image still not completely reliable
- simple scratches and defects on the image make derivation of biometric data quite problematic
Example design

Disability Parking ID

Kuty lowski, Lipiak

Problem

Requirements

Solution
- physical protection
- signatures
- legal
- face image

Application
- temporary
- personal ID

Conclusions
Image verification concept

- Step A: signature verification
- Step B: visual and device assisted comparison
- Step C: visual comparison
- Step D: visual comparison
- Step E: visual comparison

signature of low resolution image

low resolution image, QR code

medium resolution image, printed

document holder

high resolution picture in a database
Temporary personal ID

Problem

- thousands of personal ID documents lost, machine washed, stolen... each year,
- temporary replacement document - a simple document signed by a police officer (confirmation that ID document has been lost)
Temporary personal ID solution

Downloadable pdf document

- created after revocation of lost ID document, on request from Police station
- short validity period
- contains character fields and image data
- image and character data secured by signatures in QR codes

Difference to Disability Parking Permit

- need not to be cloning resistant
- therefore holograms unnecessary
Conclusions

1. low cost,
2. almost only consumer market devices used
3. no delays due to document delivery
4. fully distributed system
5. strong control over document issuers
6. documents forgery resistant
7. documents unclonable
Thanks for your attention!

Many thanks for Hologram Industries Polska for technical support and the Parliament Commission members for discussions

Contact data

1. Miroslaw.Kutylowski@pwr.wroc.pl
3. +48 71 3202109, +48 71 3202105
   fax: +48 71 3202105