



Disability
ParkingID

Kuty łowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

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

Disability Parking Permit

Disability
ParkingID

Kuty łowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

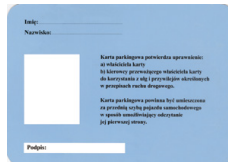
-temporary
personal ID

Conclusions

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

Disability
ParkingID

Kuty łowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

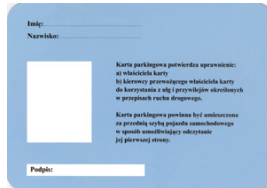
legal

face image

Application
-temporary
personal ID

Conclusions

- 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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

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



Disability
ParkingID

Kuty łowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiaki

Problem

Requirements

Solution

physical protection
signatures
legal
face image

Application
-temporary
personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

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

Disability
ParkingID

Kuty Iowski,
Lipiak

Problem

Requirements

Solution

physical protection
signatures
legal
face image

Application
-temporary
personal ID

Conclusions

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 $\approx 115^{\circ}\text{C}$)
- hologram can be separated from the paper, but film torn and holograms comes in pieces



Physical protection holograms

Disability
ParkingID

Kuty 1owski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary
personal ID

Conclusions

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



Representing “electronic data”

QR codes

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary
personal ID

Conclusions



“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, ...



Disability
ParkingID

Kuty 1owski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

- 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

- 1 A chooses $k_1 \in [1, q - 1]$ uniformly at random,
- 2 $R_1 := k_1 P$,
- 3 R_1 is sent to B ,
- 4 B chooses $k_2 \in [1, q - 1]$ uniformly at random,
- 5 $R_2 := k_2 P$, $R := R_1 + R_2$,
- 6 $e := H(M || R)$,
- 7 $s_2 := (k_2 - x_2 \cdot e) \bmod q$,
- 8 s_2 and R are sent to A ,
- 9 $s := (k_1 - x_1 \cdot e) + s_2 \bmod q$.



Advantages

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

- 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*

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary
personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary
personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary
personal ID

Conclusions

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
ParkingID

Kuty łowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions



Image verification concept

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

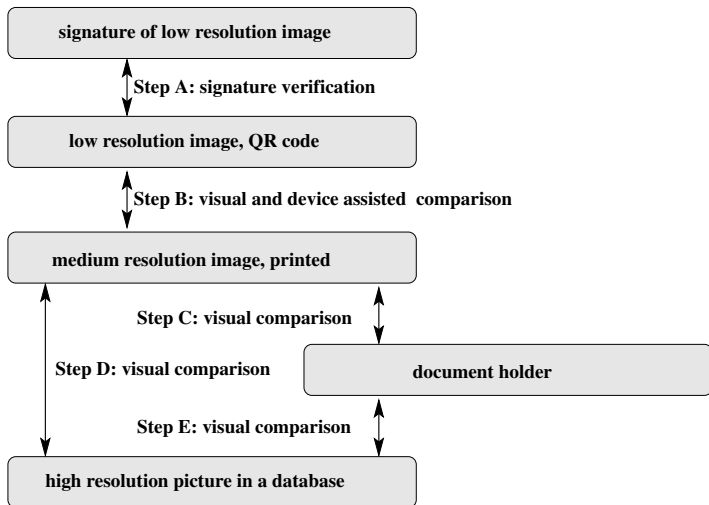
face image

Application

-temporary

personal ID

Conclusions





Temporary personal ID

Disability
ParkingID

Kuty 1owski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application
-temporary
personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application
-temporary
personal ID

Conclusions

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

Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

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



Disability
ParkingID

Kuty lowski,
Lipiak

Problem

Requirements

Solution

physical protection

signatures

legal

face image

Application

-temporary

personal ID

Conclusions

Thanks for your attention!

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

Contact data

- 1 `Miroslaw.Kutyloowski@pwr.wroc.pl`
- 2 `http://kutyloowski.im.pwr.wroc.pl`
- 3 `+48 71 3202109, +48 71 3202105`
fax: `+48 71 3202105`