Aspekty techniczne nowoczesnej karty parkingowej dla osób niepełnosprawnych

Mirosław Kutyłowski, Piotr Lipiak

Politechnika Wrocławska

Sejm Rzeczypospolitej Polskiej, 18.04.2013

Karta parkingowa
zabezpieczenia tradycyjne

Zabezpieczenia

- pieczątka
- druk

Fałszowanie

wszystkie urządzenia do fałszowania w sprzedaży detalicznej – standardowe urządzenia konsumenckie!

Karta chipowa

przykład: niemiecki dowód osobisty

komunikacja bezprzewodowa, format karty bankomatowej, wiele funkcji elektronicznych

Zalety

- niefałszowalne, łatwa kontrola produkcji
- możliwa silna kryptografia, stosunkowo duża pamięć

Wady

- **czytnik musi być blisko karty – prawa fizyki!**
- **personalizacja wymaga bardzo drogiego sprzętu**

Karty chipowe

krytycznym problemem jest odległość między czytnikiem a kartą - wymagałoby to co najmniej umieszczania karty na szybie

na większe odległości konieczne byłyby bardziej wydajne anteny dla lepszego przechwytywania energii

Podpis elektroniczny

wbrew nazwie to sekwencja cyfr

```
---BEGIN PGP MESSAGE--- Version: GnuPG v1.4.11 (GNU/Linux)
owEBYAKf/ZANAwACAQEly0BArQB+AawwYgl0ZWtzdC50eHRRbvwHQWxhIG1hIGtv
dGEuIEFsZWsgbWEgZWxlbWVudGFyei4KiQIcBAABAgAGBQJRbvwHAAoJEAEly0BA
rQB+kt4QANZkSA058jT2l0jOLL7p/P//k2SwsI46xWFBJhe/3uXPtitvEMCuOWLA
k9Pk4K3pWLAtsqQrTPl4USPFt/lnZ6IP8K3MyrwD49xT9/ez5kC+E/ABNcC7a08G
LMhHPQd4KNoGADJoMti/TDeBVBC+Slq4QT92O10LC6k7oQml7Yz7qId4N2wt3pvF
xPbNDFWyd6pdk8c9e0bdBPrWfZialCTyYru5U8MYrIr1Mn8p+ftZ/IwF5kpRz0XO
i4k90xtUN7P4CDaDDZ+4QKqSuv/HPZqNW0QLyYNt37HDXCCB2oqYdMCo+S+yneGj
l0aqDEC0uhFitSGrMZ+HjW+4GI3+rxSrM9mWw3c06IjYI1mKXSV/H+4l4+WkyFK+
K+Ku7vyNGPe1lEGn74tbKnqtlHAkXCaCf7PFQU+Gi8GQLZ+jeHkfm/lW0+cKmqbj
+G6V990NUzSohHAJquDSf1h7llFjB98ScXend9OyUAI1jtx5kDshSJo2JoU3uV9t
IwAp5chKtrbDINvVqVSf/aNlaPwybeZEq1dD246PGgl7Gqm9wob0uXLGuEJLWwjL
TUckiClScVukcCcQ15uc3Z0kLsxe6V8fVEhkz/LxuLNdpZPR/xOjCHelIdJ4IGkn
4/NB29Nw4NwvE5aaFkQfWiWLlLolHG3LnjGi/E0+YTo1Xr1D9ktr =qtzq

---END PGP MESSAGE---
```

Podpis elektroniczny

inny sposób zapisu cyfr – kod QR

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

Zalety

- korekcja błędów - uszkodzeń zapisu
- pojemne i łatwe do maszynowego odczytu

Zabezpieczenia kryptograficzne
podpis elektroniczny

Utworzenie podpisu

możliwe jedynie przy pomocy tajnego klucza podpisującego

stosunkowo prosta operacja obliczeniowa

Weryfikacja podpisu

weryfikacja podpisu możliwa przy pomocy klucza publicznego – opublikowanego!

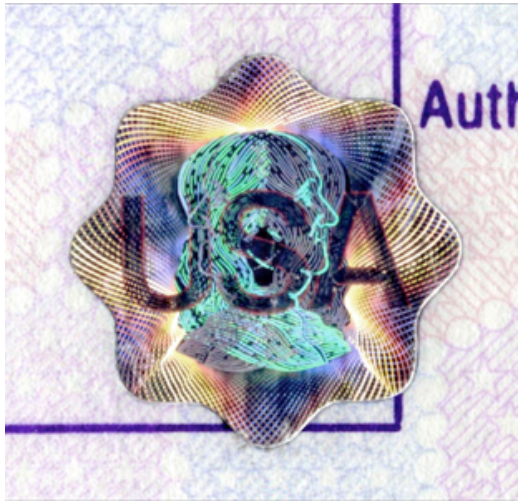
Bezpieczeństwo

- **podpisu nie da się stworzyć bez znajomości klucza podpisującego**
- **klucza podpisującego nie da się w praktyce wyliczyć z klucza publicznego, z podpisów, . . .**

Zabezpieczenia holograficzne

Idea

- efekt optyczny - weryfikacja poprzez obejrzenie
- produkcja wymaga zaawansowanej technologii
- niski koszt jednostkowy



Założenia

1. niemożność podrobienia karty
2. niemożność duplikowania kart
3. wydanie karty na poczekaniu
4. techniczna niemożność wystawienia karty bez odnotowania w rejestrze
5. niski koszt

Karta

Zabezpieczenia

podpis elektroniczny: uniemożliwia wydanie karty przez osoby nieuprawnione, lub modyfikacje danych na karcie

hologram: - przeciw klonowaniu, hologramu nie można oderwać bez podarcia

wizerunek twarzy: wydruk i podpisany w kodzie QR - umożliwia wykrycie używania karty przez osoby trzecie

Karta parkingowa
umiejscowienie danych

Dane zakodowane w kodach QR

- nr karty, data ważności, itp. - powtórzenie danych wydrukowanych znakami w zwykły sposób
- uproszczony wizerunek twarzy

Rozmieszczenie danych

ochrona danych osobowych:

przód karty: dane do wglądu przez osoby postronne

spód karty: dane do wglądu przez upoważnionego konrolera

Na wierzchu karty tylko to co **uznane za niezbędne** do kontroli uprawnień

ochrona zdjęcia - proponowane podejście

- wydruk izerunku twarzy **celowo** zredukowany w jakości
  osoba postronna mogłaby sfotografować zdjęcie posiadacza
  realizacja zasady **privacy by design** promowanej przez Unie Europejską
- podpisany wizerunek twarzy zawarty w kodzie QR – zredukowany jeszcze bardziej
  podpis dostarcza niezaprzeczalnego dowodu jak dana osoba wygląda

Karta parkingowa
wizerunek twarzy

koncepcja weryfikacji wizerunku

porównanie 3 wizerunków: z QR kodu, z wydruku, z “natury” lub z rejestru (Policja, ...)

redukcja umożliwia zawarcie wizerunku w kodzie QR

alternatywne podejście

podpis cech biometrycznych (niemiecki BSI)

nieodporne na proste uszkodzenia takie jak plama na zdjęciu

Karta parkingowa
kontrola

Efektywna kontrola

wygenerowanie podpisu **zmusza** do kontaktu z centralnym rejestrem

wytworzenie karty “na boku” technicznie niemożliwe

Sugerowana technika

podpis elektroniczny:

- oparty o problem dyskretnego logarytmu i krzywe eliptyczne (niewielki rozmiar)
- schemat z mediatorem (podpisy Schnorra)

Karta parkingowa
kontrola

Mechanizm podpisu z mediatorem

- konieczne użycie kluczy prywatnych zarówno po stronie wystawcy jak i centralnego serwera
- końcowy wynik jest całkowicie **standardowym** podpisem (brak szczególnych wymagań po stronie oprogramowania do weryfikacji)
- proste pod względem komunikacji

Weryfikacja karty - część “cyfrowa”

Oprogramowanie na urządzenia mobilne

Prototyp:

- dla telefonów pod systemem operacyjnym Android
- telefon musi być wyposażony w aparat fotograficzny
- otwarte oprogramowanie

Wydanie karty

1. osoba ubiegająca się o kartę składa wniosek (formatka na centralnym serwerze)

Wydanie karty

1. osoba ubiegająca się o kartę składa wniosek (formatka na centralnym serwerze)
2. urzędnik weryfikuje prawo do karty i wydaje decyzję (kliknięcie, zdalnie na centralnym serwerze, wymagane uwierzytelnienie urzędnika)

Wydanie karty

1. osoba ubiegająca się o kartę składa wniosek (formatka na centralnym serwerze)
2. urzędnik weryfikuje prawo do karty i wydaje decyzję (kliknięcie, zdalnie na centralnym serwerze, wymagane uwierzytelnienie urzędnika)
3. komputer urzędnika wraz serwerem centralnym generują podpis cyfrowy (podpis z mediatorem)

Wydanie karty

1. osoba ubiegająca się o kartę składa wniosek (formatka na centralnym serwerze)
2. urzędnik weryfikuje prawo do karty i wydaje decyzję (kliknięcie, zdalnie na centralnym serwerze, wymagane uwierzytelnienie urzędnika)
3. komputer urzędnika wraz serwerem centralnym generują podpis cyfrowy (podpis z mediatorem)
4. centralny serwer generuje kartę w podstaci pliku pdf i dokonuje wpisu do rejestru z informacją o wykonaniu karty

Wydanie karty

1. osoba ubiegająca się o kartę składa wniosek (formatka na centralnym serwerze)
2. urzędnik weryfikuje prawo do karty i wydaje decyzję (kliknięcie, zdalnie na centralnym serwerze, wymagane uwierzytelnienie urzędnika)
3. komputer urzędnika wraz serwerem centralnym generują podpis cyfrowy (podpis z mediatorem)
4. centralny serwer generuje kartę w podstaci pliku pdf i dokonuje wpisu do rejestru z informacją o wykonaniu karty
5. urzędnik drukuje plik pdf
   (na papierze wstępnie zadrukowanym na niebiesko ze stałymi elementami)

Wydanie karty

1. osoba ubiegająca się o kartę składa wniosek (formatka na centralnym serwerze)
2. urzędnik weryfikuje prawo do karty i wydaje decyzję (kliknięcie, zdalnie na centralnym serwerze, wymagane uwierzytelnienie urzędnika)
3. komputer urzędnika wraz serwerem centralnym generują podpis cyfrowy (podpis z mediatorem)
4. centralny serwer generuje kartę w podstaci pliku pdf i dokonuje wpisu do rejestru z informacją o wykonaniu karty
5. urzędnik drukuje plik pdf
   (na papierze wstępnie zadrukowanym na niebiesko ze stałymi elementami)
6. urzędnik nakłada hologram (laminarka, 115^oC)
   i opakowanie ochronne (twardy, gruby laminat)

Wydanie karty

1. osoba ubiegająca się o kartę składa wniosek (formatka na centralnym serwerze)
2. urzędnik weryfikuje prawo do karty i wydaje decyzję (kliknięcie, zdalnie na centralnym serwerze, wymagane uwierzytelnienie urzędnika)
3. komputer urzędnika wraz serwerem centralnym generują podpis cyfrowy (podpis z mediatorem)
4. centralny serwer generuje kartę w podstaci pliku pdf i dokonuje wpisu do rejestru z informacją o wykonaniu karty
5. urzędnik drukuje plik pdf
   (na papierze wstępnie zadrukowanym na niebiesko ze stałymi elementami)
6. urzędnik nakłada hologram (laminarka, 115^oC)
   i opakowanie ochronne (twardy, gruby laminat)
7. urzędnik wydaje kartę

Procedura

sprawność postępowania

- karta wydawana na poczekaniu **pomimo centralnego tworzenia dokumentów**
- prawie zerowe koszty nadzoru nad systemem
- brak słabych punktów mogących spowodować chaos z danymi i pracochłonne ich odtwarzanie
- możliwy bezpośredni import danych do rejestru/ewidencji

Koszty
hardware

Hardware: samorząd terytorialny

- drukarka laserowa dwustronna (druk biało-czarny)
- laminarka do hologramów (taka sama/ta sama jak dla dowodów rejestracyjnych)
- dostęp do internetu

Koszty
hardware

Hardware: samorząd terytorialny

- drukarka laserowa dwustronna (druk biało-czarny)
- laminarka do hologramów (taka sama/ta sama jak dla dowodów rejestracyjnych)
- dostęp do internetu

Hardware: centralny serwer

- serwer webowy
- interfejs do rejestru

Koszty
hardware

Hardware: samorząd terytorialny

- drukarka laserowa dwustronna (druk biało-czarny)
- laminarka do hologramów (taka sama/ta sama jak dla dowodów rejestracyjnych)
- dostęp do internetu

Hardware: centralny serwer

- serwer webowy
- interfejs do rejestru

Hardware: rejestr dokumentów

- standardowy serwer
- moduł do podpisywania (np. uruchomiony TPM na PC)

Koszty
materiały

Materiał

- blankiety (druk niebieski, gruby papier) - tak jak dzisiaj
- hologram na cienkiej folii (folia 9-12 mikronów, jak w paszportach, $\approx$ 5 PLN/szt)
- usztywniające opakowanie $\approx$ 20gr/szt - tak jak dzisiaj

Koszty
materiały

Materiał

- blankiety (druk niebieski, gruby papier) - tak jak dzisiaj
- hologram na cienkiej folii (folia 9-12 mikronów, jak w paszportach, $\approx$ 5 PLN/szt)
- usztywniające opakowanie $\approx$ 20gr/szt - tak jak dzisiaj

Logistyka

- blankiety i hologramy dostarczane **jednorazowo** do jednostek smaorządu terytorialnego
- hologramy numerowane
- wykonanie legitymacji “od ręki”

Podsumowanie

Główne cechy

- silny poziom zabezpieczeń (taki sam lub wyższy niż w przypadku paszportów) mimo stosunkowo prymitywnych środków
- niskie koszty
- zakres danych, rozmiar hologramu – do decyzji po analizie ryzyka i kosztów
- możliwość organizacji jednego/jednolitego systemu dla wielu krajów
- neutralność technologiczna w sferze cyfrowej (rozwiązania kryptograficzne nie objęte patentami, realizowalność za pomocą dowolnego sprzętu)

Kontakt

Dziękuję za uwagę!

Kontakt

1. Miroslaw.Kutylowski@pwr.wroc.pl, Piotr.Lipiak@pwr.wroc.pl,
2. http://kutylowski.im.pwr.wroc.pl
3. +48 71 3202109, +48 71 3202105
   fax: +48 71 3202105