

Polska Izba Informatyki i Telekomunikacji
00-511 Warszawa, ul. Nowogrodzka 31
Tel: (22) 628 2260, 628 2406, Fax: (22) 628 5536
www.piit.org.pl, E-adres: biuro@piit.org.pl

POLSKA IZBA
INFORMATYKI
I TELEKOMUNIKACJI



Tożsamość Kowalskiego w polskim systemie prawnym

Zakopane 17.11.2005

Jarosław Mojsiejuk - Wiceprezes
Polskiej Izby Informatyki i
Telekomunikacji

Tożsamość Kowalskiego

- Tradycyjne dokumenty związane z tożsamością – akty stany cywilnego, paszport, dowód osobisty, dokumenty na podstawie których można ustalić tożsamość (legitymacje uczniowskie, prawo jazdy etc.).
- Rozwój digitalnych dokumentów tożsamości w UE, BIOMETRIA.
- Tożsamość w sieci – podpis elektroniczny.

Tożsamość Kowalskiego –akty stanu cywilnego

- Jeden z najważniejszych rodzajów dokumentów - status osoby fizycznej - urodzenie, małżeństwo, śmierć – moc zupełna a.s.c
- Bardzo słabo zabezpieczony. Ilu mamy „lewych Kowalskich”? Ilu bandytów umarło a żyje?
- Brak centralnego rejestru – elementarny warunek bezpieczeństwa dokumentów (systemu)

W stronę cyfrowego dokumentu tożsamości

- W wielu państwach UE dowody osobiste wyposażono w microchip umożliwiający składanie podpisu elektronicznego (Włochy, Estonia, Belgia, Holandia, Finlandia). W innych powstają cyfrowe dokumenty tożsamości z funkcjami podpisu (Austria, Dania).
- Wprowadzenie stymuluje rozwój usług publicznych online (Włochy, Estonia, Finlandia, Belgia, Holandia).
- W ramach UE powstają coraz to nowe standardy dokumentów z elementami elektronicznymi.

Biometria – „omnia mea mecum porte” - wszystko co mam nosze przy sobie ? UE

- wizy i karty stałego pobytu dla rezydentów powinny być wzbogacone o cechy biometryczne
- kolejno zostaną wprowadzone biometryczne paszporty / dokumenty dla obywateli UE
- „obowiązkowe” cyfrowe zdjęcia twarzy, w dalszej kolejności odciski palców
- dane biometryczne (osobowe) będą przechowywane w krajowych oraz unijnych bazach danych

Odciski palców i zdjęcie twarzy

- Komisja Europejska - wymagane dwa identyfikatory biometryczne: cyfrowa fotografia twarzy oraz odciski palców. Identyfikatory te byłyby przechowywane na chipie zawartym w dokumencie. Pobieranie i gromadzenie fotografii twarzy będzie obowiązkowe. Następnie zostanie dodany kolejny identyfikator odciski palców.
- Najprostsze technologie są już dostępne. „High resolution electronic portrait” przechowuje się na chipie jako zdjęcie możliwe do odtworzenia np. w czasie przekraczania granicy. Bardziej zaawansowany "facial recognition systems" sprawdza dodatkowo zdjęcie na chipie z centralnie zgromadzonymi danymi danej osoby.

Paszport obywateli UE

Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie (Dziennik Urzędowy L 385 , 29/12/2004 P. 0001 – 0006)

CELE:

- Harmonizacja cech zabezpieczających oraz integracja identyfikatorów biometrycznych.
- Bezpieczniejsze dokumenty podróży oraz zwiększona wiarygodność autentyczności paszportów.
- Standardy Międzynarodowej Organizacji Lotnictwa Cywilnego (ICAO) m.in. Nr 9303 dotyczące dokumentów podróży odczytywanych przez mechaniczne czytniki.

Dokumenty dla cudzoziemców

1. Jednolity format kart stałego pobytu - Projekt Rozporządzenia Rady zmieniającego Rozporządzenie (WE) 1030/2002 w sprawie jednolitego formatu kart stałego pobytu dla obywateli państw trzecich

(Brussels, 24.09.2003 COM(2003)558 final 2003/0218 (CNS))

- Jednolity format kart stałego pobytu powinien zawierać cyfrowe zdjęcie twarzy, w postaci identyfikatora biometrycznego oraz dwa odciski palców.
- Informacje biometryczne powinny być przechowywane na odpowiednim nośniku, który powinien być zabezpieczony oraz wystarczająco pojemny.

2. Jednolity format wiz - Projekt Rozporządzenia Rady zmieniającego Rozporządzenie (WE) 1683/95 w sprawie jednolitego formatu dla wiz

(Brussels, 24.09.2003 COM(2003)558 final 2003/0217 (CNS))

- Jednolity format wiz powinien zawierać cyfrowe zdjęcie twarzy, w postaci identyfikatora biometrycznego oraz dwa odciski palców.
- Informacje biometryczne powinny być przechowywane na odpowiednim nośniku, który powinien być zabezpieczony oraz pojemny.

Dokumenty pojazdów i kierowców

1. Dokumenty rejestracyjne pojazdów (identyfikacja samochodu a nie osoby) - Dyrektywa Komisji 2003/127/WE z 23 grudnia 2003 r. zmieniająca Dyrektywę Rady 1999/37/WE w sprawie dokumentów rejestracyjnych pojazdów

Od 15 stycznia 2005 r. obowiązują dwa równorzędne formaty dokumentów rejestracyjnych pojazdów:

- 1) Papierowy dokument rejestracyjny (w Polsce wybrano ten model)
- 2) Dokument rejestracyjny w postaci karty chipowej.

2. Prawo jazdy - Projekt Dyrektywy WE Parlamentu i Rady w sprawie prawa jazdy (Brussels, 21.10.2003 COM(2003) 621 final 2003/0252 (COD))

- Prawo jazdy w formie plastikowej albo chipowej karty - około 2006. Państwa Członkowskie będą miały około 10 lat na wymianę praw jazdy. W przeciągu 20 lat powinno być wprowadzone jednolite prawo jazdy UE.).

Rozwój zjawiska elektronicznych d.t. w UE

1. Narodowe (państwowe) programy rozwoju cyfrowych dokumentów tożsamości rozwijają się gwałtownie w ostatnich latach - niektóre z tych programów spotkało niepowodzenie (nikłe efekty np. w Finlandii)
2. Oczekiwanie na rozwiązanie kwestii standardów pomiędzy UE a USA, zwłaszcza w zakresie biometrii, trudności technologiczne.
3. Implementacja nośników elektronicznych w dokumentach wychodzi poza ramy identyfikacji (potwierdzenia tożsamości) – zapisy biometryczne, dane osobowe posiadacza na rzecz nowych funkcji – identyfikacja na odległość – możliwość stosowania podpisu elektronicznego

Rozwój.....c.d

4. Różne pola zastosowania rozwiązań opartych na PKI:
 - dostęp do usług publicznych (e –gov, podatki, cła, etc.) – wspólne; zastosowanie telefonii komórkowej – różne
 - ubezpieczenia społeczne, zdrowotne (tylko w niektórych państwach). Brak standardów technicznych dot. EKUZ.
5. Elektroniczny dowód osobisty może być oddzielony od tradycyjnego (Austria, Dania), może nie mieć postaci karty lecz softwaru (Dania)
6. Obligatoryjny (Włochy, Estonia) czy fakultatywny (Finlandia). Inny wymiar fakultatywności w przypadku rozdzielenia z tradycyjnym d.o. (Austria , Dania)

Podpis elektroniczny –ustawa z 2001 r.

- Bezpieczny podpis elektroniczny równoważny własnoręcznemu,
- Obowiązek sprawdzenia tożsamości przez kwalifikowany podmiot wydający kwalifikowane certyfikaty (dokument tożsamości),
- Domniemanie, że ten kto się podpisał pod dokumentem elektronicznym to ten kto został w wskazany w certyfikacie. Niezaprzeczalność.
- Od sierpnia 2006 r. obowiązek organów administracji publicznej przyjmowania podań w formie elektronicznej. Wg ordynacji podatkowej niektóre kategorie firm będą miały obowiązek składania e-deklaracji.

Czy zawsze powinien być obowiązek stosowania bezpiecznego podpisu w elektronicznych procedurach administracyjnych?

- Wg ustawy o informatyzacji w częściach zmieniających procedury administracyjne TAK – kpa, ustawa o ubezpieczeniach społecznych.
- Dlaczego nie dopuścić innych form uwierzytelniania jeżeli miałyby one być tańsze i wystarczająco bezpieczne np. związanych z lokalnymi platformami usług elektronicznych ?

Problemy:

1. Czy dokumenty tożsamości w tradycyjnej formie nie zostaną wyparte skoro każdy cechy biometryczne nosi przy sobie ?

Czy dokumenty z cechami biometrycznymi to tylko środek na wypadek awarii IT ?

Jak zabezpieczyć bazy biometryczne przed wyciekami skoro w zasadzie już wszystko wyciekało ? (dokumenty „tajne”, bazy danych ...)

2. Podpis elektroniczny to oczywiście to na razie najlepszy sposób identyfikacji i przesyłania dokumentów przez Internet ale czy zawsze musi to być bezpieczny podpis elektroniczny ?
3. Kowalski ma jedną tożsamość, może występować jednak w różnych rolach społecznych stosując różne metody i instrumenty uwierzytelniania.
4. Jaki powszechny program dla obywateli (i firm) mógłby służyć do upowszechnienia podpisu elektronicznego w Polsce (d o. czy e - deklaracje) ?

Polska Izba Informatyki i Telekomunikacji
00-511 Warszawa, ul. Nowogrodzka 31
Tel: (22) 628 2260, 628 2406, Fax: (22) 628 5536
www.piit.org.pl, E-adres: biuro@piit.org.pl

POLSKA IZBA
INFORMATYKI
I TELEKOMUNIKACJI



Dziękuję za uwagę

Jarosław Mojsiejuk, HP Polska Sp. z o.o.

ul. Szturmowa 2 A, 02-678 Warszawa

Dyrektor ds. Bezpieczeństwa i Współpracy z
Administracją Publiczną

tel. (+48 22) 565 79 90

e-mail: Jaroslaw.Mojsiejuk@hp.com