Agnieszka Grudzińska-Kuna, Joanna Papińska-Kacperek

Organizacyjne i techniczne aspekty elektronicznej identyfikacji

Ekonomiczne Problemy Usług nr 104, 21-31

2013

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 762 EKONOMICZNE PROBLEMY USŁUG NR 104 2013

AGNIESZKA GRUDZIŃSKA-KUNA, JOANNA PAPIŃSKA-KACPEREK
Uniwersytet Łódzki

ORGANIZACYJNE I TECHNICZNE ASPEKTY ELEKTRONICZNEJ IDENTYFIKACJI

Wprowadzenie

W transakcjach elektronicznych ustalenie tożsamości stron jest niezbędne dla zachowania odpowiedniego poziomu zaufania. Ma to szczególne znaczenie, ponieważ usługodawca i usługobiorca mogą być oddzieleni od siebie w czasie i w przestrzeni, co uniemożliwia ich wizualną identyfikację. Rozwój systemów zarządzania elektronicznymi tożsamościami sprzyja budowaniu zaufania pomiędzy obywatelami a administracją czy biznesem. Celem artykułu jest przegląd rozwiązań systemów e-identyfikacji w wybranych krajach UE oraz próba znalezienia, na podstawie ich analizy, zachodzących prawidłowości.

1. Elektroniczna identyfikacja

Identyfikacja

Identyfikacja to ustalenie czyjejś tożsamości lub rozpoznanie kogoś na podstawie określonych cech[1]. Każda osoba posiada tożsamość, która może być określona za pomocą pewnego zestawu atrybutów takich jak płeć, wiek, kolor skóry, kolor oczu, wykształcenie, zamieszkanie itp. Idealnie byłoby, gdyby ten zestaw był niezmienny przez całe życie, a więc oparty na cechach biometrycznych, jak np. DNA, odciski palców, obraz siatkówki oka. Wybrane atrybuty tożsamości zapisywane są w postaci tekstowej i graficznej (zdjęcie) w różnych dokumentach po-

[1] *Słownik języka polskiego* PWN.

świadczających tożsamość danej osoby. Same dokumenty zaś posiadają cechy świadczące o ich wiarygodności (autentyczności).

Przed II wojną światową większość ludzi nie posiadała żadnego dokumentu tożsamości. Współcześnie obywatele wielu krajów mają obowiązek posiadania takich dokumentów. Najczęściej są one wystawiane z określonym przeznaczeniem, ale zdarza się, że zaczynają służyć innym celom, niż pierwotnie zakładano. Na przykład w niektórych krajach numer ubezpieczenia lub prawo jazdy służy do identyfikacji osób zarówno w sektorze publicznym, jak i prywatnym.

Zdalna identyfikacja

W świecie cyfrowym zarówno ustalanie tożsamości, jak i przechowywanie jej atrybutów musi odbywać się za pomocą środków elektronicznych. Elektroniczne uwierzytelnienie to technika pozwalająca zweryfikować, najczęściej w trybie zdalnym, tożsamość osoby, z którą się komunikujemy. Istnieją proste i silne metody, a każda z nich wymaga użycia czynnika uwierzytelniania, jakim jest:

- coś, co użytkownik wie (np. hasło, PIN, wzór),
- coś, co użytkownik posiada (np. karta elektroniczna, token),
- coś, czym jest (cechy biometryczne, jak np. odciski palców).

Dla zapewnienia większego bezpieczeństwa wymagane jest użycie co najmniej dwóch elementów, czyli uwierzytelnienie silne (dwuczynnikowe).

Przez ostatnie 10 lat stosowano różne metody identyfikacji użytkowników systemów informatycznych i aplikacji internetowych: od nazw i haseł, przez tokeny, certyfikaty i metody biometryczne. Większość z nich opierała się i opiera nadal na bilateralnych relacjach pomiędzy usługodawcą i usługobiorcą.

Usługi elektroniczne były w przeszłości i w dużej mierze nadal są systemami zamkniętymi, czyli dla każdej potrzebny jest inny zestaw informacji identyfikujących. Użytkownik musi zatem wielokrotnie podawać swoje dane osobowe, które są przechowywane przez różnych dostawców usług elektronicznych (od serwisów społecznościowych do banków i urzędów) oraz zarządzać wieloma swoimi e-tożsamościami. Zjawisko to może nie tylko powstrzymywać go przed skorzystaniem z kolejnej usługi, która wymaga rejestracji, ale także jest zagrożeniem bezpieczeństwa, ponieważ użytkownicy dla swojej wygody albo stosują te same słabe, łatwe do zapamiętania hasła w różnych serwisach lub zapisują je w niezabezpieczonych plikach. Każdy dostawca musi wdrożyć i utrzymywać swoją własną politykę identyfikacji klientów, co stanowi dla niego dodatkowe koszty i nie jest związane z właściwą działalnością biznesową.

Jednym z rozwiązań tego problemu jest stworzenie schematu pojedynczego logowania (*single sign on*, SSO). Metoda ta jest używana np. w aplikacjach Google, gdzie zapewniono w ten sposób integrację rozproszonych usług. SSO pozwala użytkownikowi na dostęp do zasobów różnych systemów w tej same domenie bezpieczeństwa bez konieczności ponownego logowania.

W wielu przypadkach założenie konta na portalu internetowym nie wymaga weryfikacji danych personalnych. Są jednak np. portale aukcyjne, gdzie zachęca się do potwierdzania prawdziwości danych, przez zaoferowanie lepszej lub bezpieczniejszej obsługi transakcji. Mechanizmy ograniczające się do zastosowania hasła mają podstawową wadę: użytkownicy zapominają je, szczególnie gdy rzadko korzystają z danego konta. Problem z przypomnieniem hasła jest czasem rozwiązywany przez jego ponowne ustawienie (o ile jest to możliwe i działa jeszcze konto poczty elektronicznej skojarzone z daną usługą) lub założenie nowego konta. W jednym z badań administracji USA okazało się, że agencja federalna obsługująca 44 tys. użytkowników miała ponad 700 tys. zarejestrowanych nazw użytkownika[2]. Uwierzytelnienie proste, mimo że najwygodniejsze dla użytkownika, nie jest wystarczające w relacjach wymagających odpowiedniego poziomu zaufania. Metody silnego uwierzytelniania wymagają posiadania dodatkowego elementu, np. urządzenia elektronicznego (token, karta elektroniczna z czytnikiem) i mechanizmu cyfrowego (certyfikat cyfrowy, klucz kryptograficzny). Wadą silnych metod są koszty ich zakupu i utrzymania (np. ważność kluczy z reguły trzeba przedłużać), a w przypadku braku mechanizmów ochronnych (np. PIN do karty) możliwość użycia ich po kradzieży.

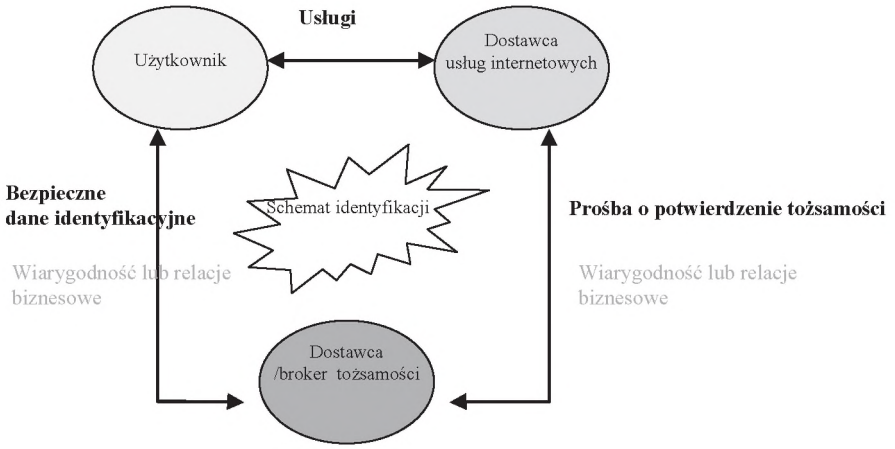
Z powyższych rozważań wynika, że od dawna istnieje zapotrzebowanie na systemowe rozwiązanie problemu zarządzania e-tożsamością i zastosowane takich metod identyfikacji, które mogą być wykorzystane w różnych sytuacjach i systemach. Rozwiązanie takie może się opierać na koncepcji dostawcy usług elektronicznej identyfikacji odpowiedzialnego za rejestrację oraz wydawanie poświadczeń tożsamości, które mogą przybierać formę haseł, tokenów[3] lub certyfikatów zapisanych na kartach elektronicznych lub innych nośnikach. Zaufanie do dostawcy usług e-identyfikacji jest uzależnione w dużej mierze od procesu rejestracji (np. konieczność osobistego stawiennictwa jest uważana za bardziej godną zaufania) oraz poziomu bezpieczeństwa wystawianych przez niego poświadczeń. Może być wiele schematów i dostawców usług e-identyfikacji, ale te wprowadzane przez państwo uważa się za najbardziej wiarygodne[4].

---

[2] *Agency response to internal U.S. Government survey*, December 2007 http://securekey.com/our-solutions.

[3] Token w kontekście uwierzytelnienia rozumiany jest jako dane cyfrowe, które zawierają poświadczenie tożsamości. Tokenem jest też urządzenie generujące takie dane.

[4] P. Valkenburg., V. Maeijers i in.: *E-identity as a business*, http://www. innopay.com/publications [dostęp 10.01.2013].



Rys. 1. Podmioty biorące udział w procesie elektronicznej identyfikacji

Źródło: opracowanie na podstawie P. Valkenburg, V. Maeijers, i in., *E-identity as a business*, http://www.innopay.com/publications.

2. Techniczne aspekty elektronicznej identyfikacji

Inteligentne karty

Karty inteligentne, czyli wyposażone w mikroprocesor, mogą być zastosowane jako hybrydowe dokumenty tożsamości, które zawierają tradycyjny nadruk, jak i zapis cyfrowy. Umożliwiają zarówno wizualną identyfikację osoby, jak i dostęp do różnego rodzaju usług elektronicznych oraz silne uwierzytelnienie. Są trudniejsze do podrobienia niż tradycyjne papierowe dokumenty. Karty inteligentne znalazły zastosowanie nie tylko jako nośnik narodowych dokumentów tożsamości (*national ID cards*), ale także w bankowości, czy jako elektroniczne legitymacje studentów lub grup zawodowych, albo karty SIM telefonów komórkowych. We wszystkich tych zastosowaniach mogą być nośnikiem poświadczenia tożsamości oraz podpisu cyfrowego.

Z technicznego punktu widzenia karty można podzielić na otwarte i zamknięte oraz umożliwiające dostęp stykowy lub/i bezstykowy. Karta zamknięta posiada system operacyjny oparty na własnym rozwiązaniu producenta. Po personalizacji i zainstalowaniu wszystkich aplikacji nie ma możliwości ani aktualizowania, ani rozszerzenia jej funkcjonalności. Aplikacje tworzone są przez producenta i przy pomocy jego narzędzi, co bardzo utrudnia lub nawet uniemożliwia audyt kodu i ustalenie np., czy zainstalowane aplikacje nie ingerują wzajemnie w wykorzystywaną przez siebie pamięć. Karta jest certyfikowana w czasie konfiguracji. Karta otwarta oparta jest na wirtualnej maszynie Javy. Najbardziej znane są tu dwa standardy: JavaCards i Multos. Maszyna wirtualna pozwala na uruchamianie apletów

realizujących określone funkcje (np. przechowywanie danych personalnych, certyfikatów czy realizacja podpisu cyfrowego). Aplety można dopisywać i kasować. W JavaCards aplikacje muszą być dostarczane w bezpiecznym połączeniu. W tym standardzie nie wbudowano mechanizmów ochrony pamięci, co oznacza konieczność sprawdzenia, czy aplikacje nie naruszają swoich zasobów i certyfikacji. Ze względu na istnienie wielu środowisk wytwórczych (np. Cyberflex, GemXpresso) w praktyce nie ma możliwości prostego zapisania kodu na kartę innego producenta bez jego kompilacji. Opisanych wad i niedogodności pozbawione są karty Multos, których aplikacje (tworzone w Javie, C lub w asemblerze) kompilowane są do Multos Executable Language. Każda niepoprawna instrukcja jest wykrywana, nie ma też możliwości współdzielenia danych. System operacyjny Multos gwarantuje pełną kompatybilność oprogramowania pomiędzy platformami różnych dostawców. W odróżnieniu od kart Java zapisywanie aplikacji może odbywać się w dowolnym połączeniu, nie musi być ono zaufane, gdyż to procesor karty dokonuje kontroli kluczy szyfrujących i zezwala (lub nie) na instalację aplikacji na karcie. W standardzie Multos funkcjonuje globalne centrum certyfikacji Key Management Authority (KMA) odpowiedzialne za bezpieczeństwo wszystkich wydanych kart. Istnieje też możliwość tworzenia lokalnych KMA np. dla projektów rządowych. W ten sposób karta Multos pozostaje pod pełną i wyłączną kontrolą wydawcy.

Zastosowanie kart inteligentnych w systemach e-identyfikacji osób w relacjach z urzędami publicznymi i biznesem jest rozwiązaniem dość drogim. Wymaga ono znacznych inwestycji w sprzęt umożliwiający personalizację kart, infrastrukturę niezbędną do realizacji systemów personalizacji dokumentów i oprogramowanie. Ponadto konieczne jest stworzenie i udostępnienie infrastruktury klucza publicznego (PKI) umożliwiającej certyfikowanie e-ID oraz umieszczonych na nich aplikacji. Konieczność wydania dużej liczby kart w krótkim czasie wiąże się z dużym wysiłkiem organizacyjnym i nakładem pracy odpowiedzialnych jednostek administracji publicznej.

Wybór określonego standardu rzutuje nie tylko na koszt, ale również na elastyczność rozwiązania. W przypadku kart zamkniętych i kart Java podmiot państwowy jest w istocie uzależniony od jednego dostawcy. Zamknięcie karty oznacza zahamowanie możliwości rozwoju tego produktu i konieczność jego wymiany w przypadku np. problemów z bezpieczeństwem. Z kolei rozszerzenie funkcjonalności kart Java wiąże się z kosztowną koniecznością ponownej certyfikacji samej karty i zainstalowanego na niej oprogramowania. Najlepszym rozwiązaniem wydaje się standard Multos, który pozwala na stosowanie kart od różnych dostawców, ponadto dobrze zarządza pamięcią i ma bezpieczną architekturę, ale na razie nie jest popularny.

Inne formy elektronicznej identyfikacji

Elektroniczna identyfikacja może być oparta na wiarygodnych procedurach rejestracyjnych oraz certyfikatach wydawanych przez instytucje zaufania publicz-

nego, umieszczanych na innych niż karty nośnikach. Kolejnym rozwiązaniem są specjalne konta (profile) na portalach administracji publicznej.

Cały schemat rozpoczyna się od rejestracji, podczas której tożsamość danej osoby jest weryfikowana na podstawie tradycyjnych dokumentów lub zawartości odpowiednich baz danych. Następnie wystawiane jest elektroniczne poświadczenie tożsamości i generowany jest token, który jednoznacznie identyfikuje daną osobę. Poświadczenie natomiast umożliwia dotarcie do danych zapisanych podczas procedury rejestracyjnej.

Inną formą e-uwierzytelniania jest korzystanie ze specjalnych kont udostępnianych i administrowanych przez instytucje zaufania publicznego (DigID – Holandia) lub profili stanowiących zestaw informacji opisujących użytkownika wiarygodnie potwierdzonych przez odpowiedni organ (profil zaufany ePUAP).

Odmianą tego podejścia są próby wykorzystania, w dużym stopniu zaakceptowanej przez obywateli, e-bankowości, w której klienci od dawna muszą się uwierzytelniać. Na przykład w Estonii logowanie do portalu www.esti.ee odbywa się albo przy pomocy e-dowodu, albo poprzez system bankowy[5]. Podobne rozwiązanie wprowadzane jest w Danii. Z powodu małego zainteresowania funkcjonalnością konta podobnego do profilu zaufanego (po wielu latach tylko 20% penetracji) rząd duński utworzył wraz z bankami centralny system identyfikacji użytkowników.

3. Elektroniczna tożsamość na szczeblu narodowym – przykłady

E-identyfikacja wymaga regulacji prawnych określających warunki konieczne do zapewnienia poprawności procedur sprawdzania tożsamości. Warunki te wyznaczane są zazwyczaj przez ustawy i rozporządzenia dotyczące ewidencji ludności, dowodów tożsamości, podpisów cyfrowych i obrotu dokumentami elektronicznymi. Wśród różnorodnych poświadczeń tożsamości spotykanych w życiu codziennym (np. poświadczenia komercyjne wydawane przez pracodawców, banki, dostawców usług medycznych, firmy ubezpieczeniowe lub operatorów telekomunikacyjnych umożliwiające dostęp do siedzib lub usług oraz systemów informatycznych) dokumenty wydawane przez państwo uważa się za najbardziej wiarygodne. Ponadto to państwo, a nie komercyjne firmy, jest uznawane za wiarygodny organ mogący gwarantować poprawność np. certyfikatów, tym bardziej jeśli dysponuje ono wiarygodnym i pełnym rejestrem obywateli. Z tych powodów oczekuje się od państwowej administracji wdrożenia odpowiednich regulacji oraz przygotowania systemu e-identyfikacji, który będzie gwarantował wysoki poziom zaufania w elektronicznych relacjach nie tylko z administracją publiczną.

---

[5] *Trendy: Autoryzacja prosta i bezpieczna*, http://mac.gov.pl/dzialania/trendy-autoryzacja-prosta-i-bezpieczna [dostęp 10.09.2012].

Coraz częściej wyposaża się obywateli albo w elektroniczne dowody osobiste (jeśli istniały wcześniej papierowe, jak np. w Portugalii), albo umożliwia zwiększenie funkcjonalności zaakceptowanych już przez wielu użytkowników kart elektronicznych wydawanych przez banki czy operatorów mobilnych (np. w Austrii). Karty elektroniczne umożliwiające identyfikację przy wszystkich usługach publicznych wprowadziły już Estonia, Austria, Belgia, Włochy, Portugalia i Szwecja[6]. Tam, gdzie istnieje obowiązek posiadania dokumentu tożsamości, obywatele otrzymują nowe elektroniczne wersje, gdy stare stracą ważność, stąd użycie nie wynosi jeszcze 100%. Nie wszystkie e-dowody zawierają podpis cyfrowy, czasem tylko pozwalają na uwierzytelnienie w serwisach internetowych.

Elektroniczne dowody w postaci karty, jak już wspomniano, to kosztowne i uciążliwe dla obywatela rozwiązanie, bowiem wymaga opłaty za wydanie dokumentu, trzeba też posiadać czytnik podłączony do komputera, gdyż nie jest to jeszcze standardowe urządzenie peryferyjne komputerów osobistych. Ponadto trzeba zainstalować oprogramowanie czytnika, a czasem także program obsługujący kartę. W przypadku kart SIM czytnikiem jest telefon komórkowy.

W wielu krajach e-identyfikacja realizowana jest często w wygodniejszy i tańszy sposób. Jednym z nich jest bezpłatny cyfrowy certyfikat tylko do kontaktów z urzędami (np. w Słowenii darmowe certyfikaty software'owe[7]). Inna metoda polega na przypisaniu obywatelowi, po wizycie w urzędzie, konta wraz z osobistym identyfikatorem i hasłem dającym możliwość korzystania z usługi e-administracji (Węgry[8]). Procedura jest podobna do polskiego zaufanego profilu – jednak w naszym kraju konto założyć można przed wizytą w urzędzie, ale dopiero po niej uzyskuje ono pełną funkcjonalność. Z kolei w Holandii założenie konta DigID w ogóle nie wymaga osobistego stawiennictwa, gdyż weryfikacja polega na sprawdzeniu danych w sieci gminnych rejestrów mieszkańców w oparciu o identyfikator BSN (*Burger Service Number*)[9]

W tabeli 1 przedstawiono porównanie narodowych systemów e-identyfikacji obywateli wybranych krajów UE. Ponieważ poszczególne rozwiązania znacznie się różnią (różnorodność stosowanych schematów i środków e-identyfikacji była podstawowym kryterium selekcji), autorki uważają, że analiza implementacji konkretnych rozwiązań pozwoli określić, na ile poszczególne narzędzia sprawdzają się w praktyce, oraz zaobserwować zachodzące prawidłowości. Wnioski mogą stanowić pewną wskazówkę dla decydentów odpowiedzialnych za realizację projektów elektronicznej identyfikacji (np. projektu pl.ID).

---

[6] D. Patos, C. Ciechanowicz, F. Piper: *The status of National PKIs – A European overview*, Information Security Technical Report 15, 2010, s. 13–20.

[7] *eID Interoperability for PEGS: Update of Country Profiles study Slovenian country profile*, http://ec.europa.eu/idabc/servlets/Docdf6b.pdf?id=32292 [dostęp 5.01.2013].

[8] *E-services/E-returns*, http://en.nav.gov.hu/e_services/E_returns_extra [dostęp 5.01.2013].

[9] *DigID*, https://www.digid.nl/index.php?id=1&L=1 [dostęp 5.01.2013].

Tabela 1

Przegląd narodowych systemów elektronicznej identyfikacji obywateli

Kraj/ Produkt /Rok	Obligatoryjny dokument tożsamości (*National ID*)	Obligatoryjność eID	Rejestr ewidencji ludności	Forrna eID*	Penetracja	Urzędy certyfikacyjne (CA)	Funkcjonalność
Włochy CIE Carta d'identità elettronica CNS Carta Nazionale dei Servizi 2000	Tak	Tak	Rejestr mieszkańców gmin	Dowód tożsamości na karcie inteligentnej	ok. 2 mln (3%) CIE ok. 20 mln (33%) CNS 2012	CIE wydawany przez Ministerstwo Spraw Wewnętrznych (SSCE), CNS różne podmioty	Podpis cyfrowy Identyfikacja Składanie deklaracji PIT Rejestrowanie umów wynajmu Wysyłanie oświadczeń np. ws. ubezpieczenia społ.
Estonia 2004	Tak	Tak	Rahvastiku-register on Eesti	Dowód tożsamości na karcie inteligentnej Karta SIM Uwierzytelnienie przez bank	80% 2010	Główny CA JUUR-SK ESTEID-SK od 2007 ESTEID-SK	Identyfikacja na eesti.ee i serwisach komercyjnych Podpis cyfrowy e-Citizen – składanie PIT Głosowanie przez Internet Zakup e-biletu i wiele innych
Holandia** DigID 2003	Nie	Nie	Sieć gminnych rejestrów mieszkańców	Konto DigID	50% w 2013	Rozwiązanie nie wymaga certyfikacji	Narzędzie uwierzytelniania obywateli w kontaktach tylko z administracją publiczną
Dania OCES 2003 NemID 2010	Nie	Nie	Det Centrale Personregister	Oprogramowanie Token Karta inteligentna **NemID** także na SIM	OCES 20 % 2009 NemID 70% 2012	OCES CA Offentlige Certifikater til Elektronisk Service	Dostęp do portali e-administracji Zeznania podatkowe Publiczne Usługi e-zdrowia **NemID** Zastosowania komercyjne
Austria Bürgerkarte 2004	Nie	Nie	Centralny Rejestr Mieszkańców CRR	Koncepcja eID Implementacje: – karty płatnicze – ubezpieczenia zdrowotnego – zawodowe – SIM	2% 2006	A-Trust, firma komercyjna wyznaczona przez państwo	Identyfikacja i podpis cyfr Nieobowiązkowo funkcja pełnomocnictwa Wnioski np. o emeryturę Zgłaszanie niektórych przestępstw Rejestracja działalności gospodarczej Składanie deklaracji PIT (FinanzOnline)

Portugalia Cartão de Cidadão 2007	Tak	Tak	Registo Civil	Dowód tożsamości na karcie inteligentnej	42% w 2010	Sistema de Certificação Electrónica do Estado	Identyfikacja na portalach e-administracji i komercyjnych Cyfrowy podpis Weryfikacja danych biometrycznych Karta usług zdrowotnych, ubezpieczenia społecznego oraz identyfikator podatnika
Polska Zaufany Profil 2010	Tak	Nie	PESEL	Konto Zaufany Profil	96 tys. (0,25%) 2013	Bezpieczne środowisko ePUAP	Uwierzytelnianie na portalu ePUAP

* W rozwiązaniach opartych na kartach inteligentnych wykorzystano technologię JavaCard firmy Gemalto.

** Od 2006 r. w Holandii wydawane są dowody elektroniczne, od 2009 r. zawierają dane biometryczne (odciski dwóch palców).

Źródło: opracowanie własne.

Podsumowanie

Państwo działając jako modelowy użytkownik, a jednocześnie regulator i ustawodawca, może ustanowić warunki do powstania odpowiedniego, uniwersalnego dla danego kraju systemu elektronicznej identyfikacji obywateli.

Główną przyczyną tworzenia narodowych systemów elektronicznej identyfikacji jest modernizacja administracji publicznej. Zakłada się, że e-identyfikacja i zarządzanie e-tożsamościami na szczeblu państwowym ułatwi korzystanie z usług e-administracji i umożliwi rozwój innych innowacyjnych rozwiązań.

Działania administracji państwowej mają głównie na celu: ograniczenie liczby profili, którymi obywatel musi zarządzać, aby mieć dostęp do usług publicznych; implementację rozwiązań umożliwiających pojedyncze logowanie i przekazywanie tożsamości. Działania te mogą przyczynić się do rozwoju rynku narzędzi silnego uwierzytelniania. Większa podaż usług wymagających silnego uwierzytelnienia spowoduje, że użytkownicy będą musieli się z nimi w jakimś stopniu zapoznać i zaakceptować.

Wdrażane rozwiązania są najczęściej kontynuacją prowadzonej od lat polityki ewidencji ludności i tradycyjnych form uwierzytelnia obywateli w kontaktach z administracją publiczną. W procedurach elektronicznego uwierzytelniania zostały wykorzystane istniejące rejestry ewidencji ludności i numery identyfikacyjne. Czasami wymagały one pewnego dostosowania, np. centralizacji rejestrów lub przynajmniej powiązania ich w bezpieczną sieć. Kraje, które wprowadziły elektroniczne dowody tożsamości, po prostu zmieniły nośnik istniejących dokumentów na kartę z mikroprocesorem. Kwestie obowiązku ich stosowania zazwyczaj pozostały niezmienione.

Czas i koszt wdrożenia rozwiązania opartego na obowiązkowych dowodach tożsamości w formie kart inteligentnych będzie zdecydowanie większy w krajach, gdzie nie ma tradycji ewidencji ludności. Czasami wdrożenie tego typu rozwiązania jest niemożliwe ze względu na opór społeczny, gdyż są one traktowane przez społeczeństwo jako zamach na wolność osobistą i próbę inwigilacji obywateli (Francja, Wielka Brytania).

Nie ma jednego obowiązującego podejścia, zastosowane rozwiązania zależą od danego państwa i zazwyczaj nie nadają się do przeniesienia do innego.

Strategie tworzenia systemów elektronicznej identyfikacji powinny zatem uwzględniać specyfikę danego państwa, modyfikować raczej istniejące procedury, do których obywatele już się przyzwyczaili, niż je rewolucjonizować.

Literatura

1. *Agency response to internal U.S. Government survey*, December 2007 http://securekey.com/our-solutions.
2. *An overview of the eGovernment and eInclusion situation in Europe* http://www.epractice.eu/en/factsheets.
3. *Cartão de Cidadão*, http://www.cartaodecidadao.pt.
4. *Citizen Card*, http://www.buergerkarte.at/index.en.php.
5. *DigID*, https://www.digid.nl/index.php?id=1&L=1.
6. *eID Interoperability for PEGS*, http://ec.europa.eu/idabc/en/document/6484.html.
7. *eRecognition: authentication and authorisation for legal entities*, http://www.eherkenning.nl/eRecognition.
8. *ID.ee* http://www.id.ee.
9. *Multos*, http://www.multos.com/.
10. *National Strategies and Policies for Digital Identity Management in OECD Countries*, OECD Digital Economy Papers, No. 177, OECD Publishing 2011, http://dx.doi.org/10.1787/5kgdzvn5rfs2-en.
11. Nazimek P.: *Inżynieria programowania kart inteligentnych*, Politechnika Warszawska, 2005, http://home.elka.pw.edu.pl/~pnazimek.
12. *NemID conditions for online banking and public digital signatures*, https://www.nemid.nu/om_nemid/regler/nemid_rules.pdf.
13. Patos D., Ciechanowicz C., Piper F.: *The status of National PKIs – A European overview*, Information Security Technical Report 15, 2010.
14. *Trendy: Autoryzacja prosta i bezpieczna*, http://mac.gov.pl/dzialania/trendy-autoryzacja-prosta-i-bezpieczna.
15. Valkenburg P., Maeijers V. i in.: *E-identity as a business*, http://www.innopay.com/publications.

ORGANIZATIONAL AND TECHNICAL ASPECTS OF ELECTRONIC IDENTIFICATION

Summary

Electronic identification is essential to provide trusted interactions between parties in the online and the physical worlds. Governments play a leading role in establishing terms and conditions for enabling high level identity assurance and as a driving force to help citizens and business adopt consistent identity management practices. The article aims to overview of solutions to e-identification in selected EU countries and to examine how they work in practice. Building on analysis authors have indicated some tendencies and the regularities.

Translated by Agnieszka Grudzińska-Kuna