Techniki elektronicznej identyfikacji użytkowników i ich rola we współczesnej komunikacji z instytucjami systemu administracyjnego

Justyna Adamus-Kowalska
Instytut Bibliotekoznawstwa i Informacji Naukowej
Uniwersytet Śląski w Katowicach

Abstrakt

Cel/teza: Celem artykułu jest przybliżenie problematyki identyfikacji elektronicznej, mającej miejsce podczas komunikacji z systemami instytucji administracyjnych. Omówione zostały najnowocześniejsze i zapewniające wysoki poziom bezpieczeństwa metody weryfikacji praw dostępu do zasobów elektronicznych, takie jak: podpis elektroniczny kwalifikowany, profil zaufany oraz planowany do wprowadzenia podpis osobisty i metody biometryczne.
Koncepcja/metody badań: Artykuł opracowano na podstawie analizy literatury i przepisów prawnych, raportów Ministerstwa Administracji i Cyfryzacji na temat wpływu informatyzacji na działanie urzędów w Polsce oraz własnych analiz korespondencji wpływającej i wychodzącej w Urzędzie Marszałkowskim Województwa Śląskiego w Katowicach. Przebadano także oferowane użytkownikom możliwości na platformie ePUAP.
Wyniki i wnioski: Wskazano techniki uwierzytelniania stosowane przez podmioty publiczne w komunikacji elektronicznej na platformie ePUAP, tj. wykorzystanie loginu i hasła, zastosowanie podpisu elektronicznego, zastosowanie profilu zaufanego. Na podstawie analizy przepisów prawnych omówiono planowany do wprowadzenia podpis osobisty. W świetle literatury przedmiotu wykazano, że coraz popularniejsze i najbardziej bezpieczne w świecie wirtualnym są metody biometryczne. Wykorzystanie elektronicznego uwierzytelniania jest konieczne dla zapewnienia bezpieczeństwa w systemach informacyjnych administracji publicznej, z tego względu, że dokument uwierzytelniony ma znaczenie prawne. Badania przeprowadzone przez autorkę w Urzędzie Marszałkowskim Województwa Śląskiego w Katowicach pokazały, że w I kwartale 2014 roku wykorzystanie narzędzi elektronicznego uwierzytelniania w administracji publicznej w Polsce dotyczy średnio 6.16% dokumentacji wysyłanej z Urzędu oraz 5.31% dokumentacji otrzymywanej przez Urząd. W wyniku przeprowadzonych badań zaobserwowano liczne bariery jakie napotykają użytkownicy w tych systemach: brak wiedzy na temat możliwości systemu, brak kompleksowości, brak formularzy elektronicznych, brak wewnętrznych zmian w urzędach.
Oryginalność/wartość poznawcza: W polskim piśmiennictwie nie podejmowano dotychczas oceny narzędzi stosowanych w celu identyfikacji użytkowników w systemach administracji publicznej oraz przebiegu procesu uwierzytelniania dokumentów elektronicznych.

Słowa kluczowe

Administracja publiczna. Identyfikacja elektroniczna. System informacyjny. Uwierzytelnianie.

Otrzymany: 1 grudnia 2014. Poprawiony: 22 stycznia 2016. Zatwierdzony: 25 stycznia 2016.

1. Wprowadzenie

Techniki elektronicznej identyfikacji mają zastosowanie w komunikacji podczas kontaktów użytkownika z systemem informacyjnym. Wśród różnych rodzajów systemów informacyjnych wyodrębnia się systemy specjalistyczne, do których należą systemy informacyjne administracji publicznej. Na tego typu system w szerokim sensie składa się sieć instytucji administracyjnych, użytkownicy (klienci, petenci) korzystający z usług administracyjnych oraz zasoby i środki realizacji procesu informacyjnego w administracji publicznej[1]. System ten należy do infrastruktury informacyjnej państwa, która jest definiowana jako kompleks infrastrukturalnych zasobów i systemów informacyjnych warunkujących funkcjonowanie państwa postrzeganego jako zinstytucjonalizowana forma organizacji życia społecznego i ekonomicznego na terytorium określonym w wyniku ustaleń międzynarodowych (Oleński, 2006). Infrastruktura informacyjna państwa stanowi podstawę sprawnego funkcjonowania państwa jako formy organizacji społeczeństwa i gospodarki oraz stanowi ona, według Józefa Oleńskiego, główny instrument realizacji obywatelskiego prawa do informacji (Oleński, 2006).

Elektroniczna identyfikacja jest stosowana obecnie w wielu dziedzinach życia. W dobie społeczeństwa informacyjnego, zwanej też erą elektroniczną, znamienne jest posługiwanie się technologiami informacyjno-komunikacyjnymi w bardzo wielu sferach funkcjonowania człowieka. Identyfikacja elektroniczna ma miejsce począwszy od zakupu produktów spożywczych opatrzonych kodem kreskowym, poprzez uruchomienie telefonu komórkowego, zabezpieczonego hasłem PIN, aż po pracę w zaawansowanych systemach produkcji i usług. Zakres występowania identyfikacji elektronicznej jest bardzo szeroki. W tym miejscu uwaga będzie skupiona na metodach weryfikacji praw dostępu do zasobów elektronicznych, które mają zastosowanie we współczesnej komunikacji z instytucjami systemu administracyjnego. Sposoby te określane są mianem uwierzytelniania, które zgodnie z definicją oznacza

> uzyskiwanie pewności, że zadeklarowana cecha danego podmiotu jest prawdziwa (ISO/IEC 27000: 2009).

Uwierzytelnianie jest zatem uzyskaniem określonego poziomu pewności, że dany podmiot jest w rzeczywistości tym, za który się podaje (PN-ISO/IEC 9798–1:1996; Gaj et al., 2003). Tak zdefiniowany proces jest częścią procesu dowodowego. Wiarygodność dotyczy w głównej mierze identyfikacji nadawcy i odbiorcy informacji. Nawiązując do elementów systemu informacyjnego, tj. nadawca, zbiór informacji i kanały przepływu informacji oraz odbiorcy informacji, problematyka uwierzytelniania i bezpieczeństwa informacji występuje we wszystkich tych elementach, w największym stopniu jednak odnosi się do użytkownika systemu. Na wyjściu systemu informacyjnego następuje przekazywanie informacji do odbiorcy (użytkownika), co wiąże się często z koniecznością jego identyfikacji przez system i udzieleniem praw dostępu do zasobów informacyjnych systemu. Uwierzytelnianie jest także integralnym elementem systemu informacyjnego administracji publicznej.

[1] Definicja została sformułowana przez autorkę poprzez odwołanie do definicji Agnieszki Pawłowskiej, która przyjmuje, że na system informacyjny składają się: informacja, narzędzia informatyczne, ludzie i struktury (Pawłowska, 2002, 78).

2. Podstawy prawne e-administracji

Podstawy prawne dla funkcjonowania systemu informacyjnego administracji publicznej w środowisku elektronicznym zostały przyjęte w Ustawie z dnia 17 lutego 2005 roku *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Ustawa, 2005). Dopuszcza się w niej zastosowanie komunikacji w formie elektronicznej, przy czym określono przede wszystkim warunki jakie musi spełniać dokument w formie elektronicznej. Zgodnie z art. 3 pkt 2

> dokument elektroniczny jest to stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisanych na informatycznym nośniku danych.

W komunikacji z administracją publiczną zastosowanie mają także przepisy Ustawy z dnia 14 czerwca 1960 roku *Kodeks postępowania administracyjnego* (z późn. zmianami) (Ustawa, 2015), w których określono, że

> dokument elektroniczny wymaga opatrzenia bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu (art. 54 § 2, art. 107 § 1, art. 124 § 1, art. 217 § 4, art. 238 § 1).

W Polsce podpis elektroniczny został wprowadzony przez Ustawę z dnia 18 września 2001 roku *o podpisie elektronicznym* (Ustawa, 2001)). Ustawa opiera się na przepisach dyrektywy unijnej w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dyrektywa, 1999). Dyrektywa definiuje pojęcie podpisu elektronicznego jako

> dane w formie elektronicznej dodane do innych danych elektronicznych lub logicznie z nimi powiązane i służące jako metoda uwierzytelnienia (Dyrektywa, 1999, art. 2 ust. 1).

Tak zdefiniowany podpis elektroniczny nie daje jednak pełnej identyfikacji osoby, która podpis złożyła, dlatego też uznaje się w polskim prawie, że obowiązkowe jest posługiwanie się bezpiecznym podpisem elektronicznym (podpisem kwalifikowanym). W ustawie o podpisie elektronicznym określono, że podpis elektroniczny są to

> dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny (Ustawa, 2001, art. 3).

Podpis elektroniczny kwalifikowany musi spełniać następujące warunki:

(1) Przyporządkowanie wyłącznie do osoby składającej podpis.
(2) Składanie podpisu za pomocą bezpiecznych urządzeń, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.
(3) Powiązanie podpisu z danymi, do których został dołączony w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

W polskim prawie przyjęto także zapis mówiący, że podpis kwalifikowany musi być weryfikowany za pomocą ważnego kwalifikowanego certyfikatu, czyli elektronicznego zaświadczenia, wystawianego przez kwalifikowany podmiot i umożliwiającego identyfikację osoby składającej podpis. Uzyskanie podpisu kwalifikowanego wiąże się jednak z koniecznością poniesienia opłaty za wydanie certyfikatu i utrzymanie go w określonym w umowie czasie. Z tego powodu forma podpisywania dokumentów i posługiwanie się

podpisem elektronicznym kwalifikowanym jako narzędziem uwierzytelniania nie jest szeroko rozpowszechniona w społeczeństwie. Natomiast urzędy administracji publicznej, które wdrożyły do swojej pracy systemy teleinformatyczne wyposażyły także uprawnionych pracowników w podpisy elektroniczne. Według badań przeprowadzonych przez Ministerstwo Administracji i Cyfryzacji w urzędach administracji publicznej w Polsce, w 2014 r., podpis elektroniczny posiadało jeden na sześciu pracowników (MAC, 2014). Największy odsetek pracowników posiadających tego typu podpis odnotowano w urzędach gminnych, a kształtował się on na poziomie 18%.

Ustawa o informatyzacji w art. 20a dopuszcza również jako formę uwierzytelniania:

– profil zaufany ePUAP, jako bezpłatny sposób uwierzytelniania udostępniany przez ePUAP, wymagający identyfikacji podczas jednorazowej wizyty obywatela w urzędzie,
– inne sposoby identyfikacji, (podpis elektroniczny weryfikowany za pomocą certyfikatu niekwalifikowanego, za pomocą loginu i hasła lub też inna forma weryfikacji) dla organów administracji publicznej korzystających z systemów teleinformatycznych do realizacji zadań publicznych.

Prace nad utworzeniem narzędzi umożliwiających identyfikację osoby w środowisku elektronicznym przy użyciu profilu zaufanego rozpoczęły się w Polsce w 2008 r. Wówczas Ministerstwo Spraw Wewnętrznych i Administracji, mając na uwadze duże opóźnienia w uchwaleniu nowej ustawy o podpisach elektronicznych, postanowiło wprowadzić tymczasowe rozwiązanie. Rozwiązanie to miało sprostać wymogom komunikacji elektronicznej na utworzonej platformie ePUAP (elektroniczna Platforma Usługa Administracji Publicznej).

Profil zaufany został zdefiniowany w znowelizowanej w 2010 r. ustawie o informatyzacji, jako

> zestaw informacji identyfikujących i opisujących podmiot lub osobę będącą użytkownikiem konta na ePUAP, który został w wiarygodny sposób potwierdzony przez organ podmiotu określonego w art. 2 (Ustawa, 2010, art. 3, ust. 14).

A zatem, profil zaufany, to informacje identyfikacyjne, które w wiarygodny sposób muszą być potwierdzone przez podmiot realizujący zadania publiczne (Ustawa, 2010). Natomiast profil zaufany jako metoda uwierzytelniania został usankcjonowany w art. 20a tej ustawy:

> Identyfikacja użytkownika systemów teleinformatycznych udostępnianych przez podmioty określone w art. 2 następuje przez zastosowanie kwalifikowanego certyfikatu przy zachowaniu zasad przewidzianych w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450) lub przy użyciu „profilu zaufanego ePUAP"(Ustawa, 2010, art. 20a).

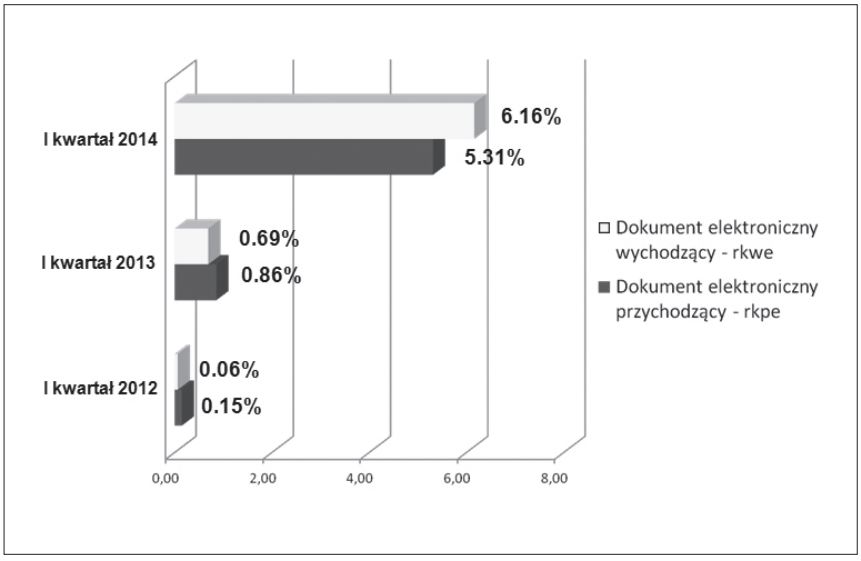
Przepisy wskazujące na profil zaufany jako narzędzie uwierzytelniania zostały przyjęte przez Ministra Spraw Wewnętrznych i Administracji dnia 9 maja 2011 r. (Rozporządzenie, 2011).

Procedura zakładania profilu zaufanego została podzielona na dwie części, tj. zakładanie konta na ePUAP i złożenie wniosku o uzyskanie profilu zaufanego. Część pierwsza obejmuje utworzenie konta użytkownika na platformie ePUAP. Część druga polega na wygenerowaniu na platformie ePUAP wniosku o nadanie profilu zaufanego, a następnie osobistym potwierdzeniu swojej tożsamości z dowodem osobistym lub paszportem, w terminie do 14 dni, w punkcie potwierdzającym profil zaufany. Miejsce potwierdzenia profilu określa paragraf 4 ust. 1 rozporządzenia w sprawie profilu zaufanego (Rozporządzenie, 2011). Zgodnie z tymi zapisami może to być: konsul, naczelnik urzędu skarbowego, wojewoda,

Zakład Ubezpieczeń Społecznych (dopuszcza się także, za zgodą ministra właściwego do spraw informatyzacji, inny podmiot wykonujący zadania publiczne).

Technika profilu zaufanego jako metody uwierzytelniania znalazła zastosowanie w administracji publicznej. Pozostaje jeszcze wiele zadań do wykonania ze strony instytucji administracyjnych, przede wszystkim udostępnienie wszystkich usług administracji publicznej na platformie ePUAP tak, aby była możliwa pełna realizacja usług administracji publicznej w formie elektronicznej. Tymczasowym rozwiązaniem jest umieszczenie na ePUAP usługi polegającej na złożeniu do wybranego organu administracji publicznej pisma (podania) w sprawie, co do której nie mają zastosowania inne formularze. Z odpowiedzi, uzyskanych na pytanie skierowane do kilku urzędów marszałkowskich w Polsce, w trybie zapytania o informację publiczną, wynika, że jedną z poważnych barier w pełnym wykorzystywaniu platformy ePUAP przez obywateli jest brak formularzy elektronicznych dokumentów dla wielu rodzajów spraw, których załatwianie umożliwia się za pośrednictwem platformy. Przyjęte wzory pism i formularze, usankcjonowane w poszczególnych rozporządzeniach, regulujących postępowanie w tych sprawach, nie uwzględniają formy elektronicznej.

Wykres 1. Udział dokumentacji elektronicznej przychodzącej i wychodzącej w stosunku do dokumentacji tradycyjnej (papierowej) w Urzędzie Marszałkowskim Województwa Śląskiego w Katowicach w I kwartale 2012, 2013 i 2014 r.



Wdrożenie informatyzacji do podmiotów publicznych nie może opierać się wyłącznie na usprawnieniu samego procesu komunikacji i wnoszenia pism drogą elektroniczną. Największym problemem jest przeprowadzenie informatyzacji wewnątrz podmiotów, tak aby całkowicie wyeliminować tradycyjne, papierowe formy pracy i obiegu dokumentacji. Dla zobrazowania tego, jaki jest w administracji publicznej udział komunikacji elektronicznej w stosunku do tradycyjnej komunikacji odbywającej się za pośrednictwem dokumentacji papierowej w latach 2012–2014, autorka zebrała dane liczbowe w Urzędzie Marszałkowskim Województwa Śląskiego w Katowicach. Na ich podstawie dokonała porównania liczby

dokumentów przychodzących do Urzędu w formie papierowej oraz liczby dokumentów przychodzących w formie elektronicznej, jak również porównała liczbę dokumentów wychodzących w formie papierowej oraz liczbę dokumentów wychodzących w formie elektronicznej. Uzyskane wyniki przedstawia Wykres 1.

Przeprowadzone badania pokazały wyraźnie, że korzystanie z komunikacji elektronicznej w Urzędzie Marszałkowskim Województwa Śląskiego jest bardzo niskie i kształtuje się na poziomie 5.31% dla dokumentacji przychodzącej oraz 6.16% w przypadku dokumentacji wychodzącej.

Podobne wyniki uzyskano w badaniach przeprowadzonych przez Ministerstwo Administracji i Cyfryzacji (MAC, 2014). W pierwszym półroczu 2014 r. urzędy otrzymały 11% dokumentacji za pomocą elektronicznej skrzynki podawczej (ESP). Dokumentacja, która została wysłana poprzez ESP, stanowiła w tym samym okresie 9% całości wysłanej koresponcencji. Przyczną niewielkiego udziału dokumentów odbieranych i wysyłanych w postaci elektronicznej względem całej dokumentacji przepływającej przez urzędyktórą wskazywano w tym badaniu, było przede wszystkim nieuznawanie przez pracowników postaci elektronicznej dokumentu jako równoważnej postaci papierowej (61% urzędów); innym powodem wskazywanym przez dużą część respondentów było przyzwyczajenie (46% urzędów). Najwieksze bariery dla komunikacji elektronicznej z administracją publiczną wynikają zatem z braku dostatecznej wiedzy i otwartości na zmiany.

3. Techniki zapewniania bezpieczeństwa w komunikacji elektronicznej w administracji publicznej

Identyfikacja osób fizycznych i podmiotów w administracji publicznej ma za zadanie zapewnić wiarygodność i bezpieczeństwo systemu informacyjnego administracji publicznej. Bezpieczeństwo jest jednym z najważniejszych aspektów prawidłowego funkcjonowania informacji w środowisku elektronicznym i obejmuje zarówno ochronę treści w zasobach informacyjnych, jak i ochronę praw dostępu do zasobów. Naczelną cechą, która sprzyja szerokiej powszechności i popularności treści rozpowszechnianych w formie elektronicznej jest łatwość i szybkość wyszukiwania informacji, łatwość dostępu do treści i coraz częściej także swobodne edytowanie treści dokumentu, choć ze względów bezpieczeństwa, ograniczane do edycji wyłącznie na własne potrzeby. W administracji publicznej rozwój komunikacji w formie elektronicznej wynika z odpowiednich przepisów prawnych, regulujących m.in. dostęp do informacji publicznej (Ustawa, 2001; Rozporządzenie, 2007; Rozporządzenie, 2012; Rozporządzenie, 2014a; Rozporządzenie, 2014b). Narzędzia, które rozwijane są w związku z tą formą komunikacji muszą nadążać za potrzebami społeczeństwa informacyjnego, dla którego pożądane jest uzyskanie dostępu do nieograniczonej ilości informacji z wykluczeniem jakichkolwiek barier i zagwarantowanie maksymalnej wiarygodności informacji, stąd też istotne jest omówienie problematyki bezpieczeństwa w tych systemach.

Jak wspomniano na wstępie, uwierzytelnianie w procesie komunikacji jest konieczne, aby zaistniał tzw. obrót prawny. Dokument w obrocie prawnym musi być odpowiednio uwierzytelniony i wówczas jest dokumentem w znaczeniu prawnym, w odróżnieniu od dokumentu jaki występuje w innych systemach informacyjnych np. systemach informacyjnych w nauce.

Proces uwierzytelniania w systemie informacyjnym administracji publicznej, który ma miejsce na platformie komunikacyjnej ePUAP, musi zapewniać wysoki poziom bezpieczeństwa. Użytkownik po zalogowaniu na swoje konto ma dostęp do systemu oferującego usługi, które udostępniają i realizują podmioty administracji publicznej w Polsce. Zgodnie z cytowaną powyżej ustawą o informatyzacji, usługi te są realizowane w formie elektronicznej po wniesieniu podania za pośrednictwem elektronicznej skrzynki podawczej; ESP na platformie ePUAP generuje automatycznie urzędowe poświadczenie odbioru (UPO). Każdy dokument kierowany za pomocą ESP musi być opatrzony podpisem, stąd też w procesie komunikacji istotny jest wybór techniki uwierzytelniania. Na platformie ePUAP możliwy jest wybór uwierzytelnienia dokumentu za pomocą profilu zaufanego lub przy zastosowaniu podpisu elektronicznego. Przy podpisie elektronicznym weryfikacji podlega certyfikat, wydany przez urząd certyfikujący. Przy weryfikacji podpisu złożonego za pomocą profilu zaufanego potwierdzenie następuje poprzez wpisanie jednorazowego hasła wysłanego na adres poczty elektronicznej przypisany do konta użytkownika.

Potwierdzenie profilu zaufanego za pomocą jednorazowego kodu autoryzacji zwiększa poziom bezpieczeństwa. Inne metody uwierzytelniania uważa się za mniej bezpieczne. Jako największe zagrożenie przy uwierzytelnianiu za pomocą loginu i hasła wskazuje się powielanie przez użytkownika tego samego loginu i hasła w różnych systemach, co powoduje ryzyko ich poznania i użycia przez osoby nieuprawnione. Problem stanowią także częste przypadki złamania haseł o zbyt prostej budowie. Zdarza się także, że hasło może zostać przechwycone w trakcie niezabezpieczonej transmisji. Hasła bywają przedmiotem ataków hakerów, którzy stosują w celu ich złamania metody słownikowe, a także metody przeszukiwania wyczerpującego. Metody te polegają na próbach włamania się do zasobów przy zastosowaniu haseł zgromadzonych w słowniku. W systemach komputerowych najczęściej zwraca się uwagę, że hasła muszą zawierać co najmniej sześć znaków, nie powinny zawierać znanego słowa, imienia, nazwiska, daty urodzenia, numeru telefonu czy też numeru rejestracyjnego. Hasła należy zmieniać tak, aby nie było zależne od starego. Haseł nie można zapisywać w widocznym czy też łatwo dostępnym miejscu oraz informować nikogo o swoim haśle.

Podpis elektroniczny jest dużo bardziej bezpieczną metodą komunikacji w administracji publicznej. Zaliczany jest on do metod uwierzytelniania dwuskładnikowego. Ten rodzaj uwierzytelniania stosuje się przy dostępie do danych lub systemów, które podlegają szczególnej ochronie. Ryzyko złamania czy przechwycenia hasła jest wówczas ograniczone dzięki wprowadzeniu dodatkowego, materialnego składnika uwierzytelniania, w postaci tokenu sprzętowego, który:

– istnieje w jednym, unikatowym egzemplarzu, co gwarantuje, że jego użycie wymaga fizycznego dostępu do niego;
– wymaga użycia potwierdzonego dodatkowo podaniem hasła (np. w postaci kodu PIN), więc bez jego znajomości token będzie nieprzydatny, nawet w przypadku kradzieży.

Uwierzytelnienie dwuskładnikowe stosuje większość banków internetowych. Stosowane są zarówno tokeny sprzętowe, jak i programowe generatory haseł oraz hasła jednorazowe przesyłane poprzez telefony komórkowe jako wiadomość SMS lub też, tak jak ma to miejsce w przypadku profilu zaufanego, przesyłane jako wiadomość na skrzynkę poczty elektronicznej.

W świetle prawa, dla osoby fizycznej najlepszym mechanizmem identyfikacji w środowisku elektronicznym jest podpis elektroniczny kwalifikowany.

Istnieją także inne metody uwierzytelniania, które co prawda nie mają zastosowania na platformie ePUAP, ale warte są szczególnej uwagi ze względu na zapewnianie wysokiego poziomu bezpieczeństwa oraz możliwe zastosowania w administracji publicznej. Poniżej odrębnie zostały więc omówione: podpis osobisty oraz o metody biometryczne, które znajdują już zastosowanie w takich urządzeniach jak smartfony czy tablety i niebawem także będzie konieczne ich wdrożenie do systemu informacyjnego administracji publicznej.

4. Podpis osobisty

Najnowszym rozwiązaniem, które nie jest jeszcze wykorzystywane na platformie ePUAP jest podpis osobisty, będący integralnym elementem nowego dowodu osobistego. Zgodnie z Ustawą z dnia 9 czerwca 2011 roku *o zmianie ustawy o dowodach osobistych i ustawy o ewidencji ludności* (Ustawa, 2011) przyjęto, iż dowód osobisty umożliwia uwierzytelnienie go w systemach teleinformatycznych podmiotów publicznych, uwierzytelnienie jego posiadacza w systemach teleinformatycznych podmiotów publicznych oraz przy dostępie do rejestrów publicznych z użyciem systemów teleinformatycznych. Nowy dowód osobisty ponadto zawiera w swojej warstwie elektronicznej miejsce na certyfikat podpisu osobistego wraz z danymi służącymi do składania podpisu osobistego.

W projekcie ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych zdefiniowano certyfikat podpisu osobistego jako elektroniczne zaświadczenie przyporządkowujące dane do weryfikacji podpisu osobistego do posiadacza dowodu osobistego (Projekt, 2010, art. 2 ust. 1, pkt 3). Dowód osobisty, według projektu ustawy, zawiera także miejsce na certyfikat podpisu elektronicznego kwalifikowanego wraz z danymi służącymi do składania bezpiecznego podpisu elektronicznego, który był już przedmiotem rozważań. Przyjęto, że:

> 1. Opatrzenie podpisem osobistym weryfikowanym za pomocą certyfikatu podpisu osobistego dokumentu w postaci elektronicznej wywołuje dla podmiotu publicznego skutek prawny równoznaczny ze złożeniem własnoręcznego podpisu pod dokumentem w postaci papierowej.
> 2. Skutek, o którym mowa w ust. 1, wywołuje opatrzenie podpisem osobistym weryfikowanym za pomocą certyfikatu podpisu osobistego dokumentu w postaci elektronicznej dla podmiotu innego niż podmiot publiczny, jeżeli obie strony wyrażą na to zgodę (Projekt, 2010, art. 16).

Zmiany także obejmować będą cytowaną już ustawę o informatyzacji działalności podmiotów realizujących zadania publiczne (Ustawa, 2005). W art. 20a ust. 1 tejże ustawy zawarto przepis mówiący o tym, by identyfikacja użytkownika systemów teleinformatycznych udostępnianych przez podmioty publiczne następowała także przy użyciu certyfikatu podpisu osobistego.

Nowy sposób wykorzystania dowodu osobistego, jako mediatora, czyli narzędzia weryfikacji, przy składaniu podpisu elektronicznego był m.in. przedmiotem prac badawczych prowadzonych przez konsorcjum Trusted Information Consulting oraz Politechnikę Wrocławską (Kutyłowski & Paluszyński, 2014). W raporcie z tych badań opisano dotychczasowe techniki podpisu oparte na algorytmach kryptograficznych oraz bezpiecznych urządzeniach do składania podpisu (podpis elektroniczny kwalifikowany). Zaproponowano mechanizm składania podpisów online w oparciu o systemy rozproszone, gdzie zachowany jest wyższy poziom bezpieczeństwa, niż w przypadku podpisu elektronicznego kwalifikowanego.

Opisana w badaniach technika umożliwia skuteczne zarządzanie bezpieczeństwem na wypadek utraty karty do składania podpisu lub próby sporządzenia jej kopii. W raporcie omówione zostały też nowe mechanizmy kontroli nad producentami, które mogłyby zwiększyć poziom bezpieczeństwa oferowanych rozwiązań. Zaproponowane tam rozwiązania zapewniają także odporność na ataki, m.in. poprzez możliwość automatycznego powiadamiana podpisującego o składanym podpisie za pomocą niezależnego kanału komunikacyjnego, monitorowanie aktywności w zakresie podpisywania i reagowanie na nieregularności oraz wykrywanie metodami matematycznymi podrobionych podpisów. Wskazano, że celem prac powinno być stworzenie rozwiązań umożliwiających uwierzytelnianie w różnych systemach z wykorzystaniem pojedynczego klucza kryptograficznego.

5. Metody biometryczne

Biometryczne metody uwierzytelniania dotyczą ludzi i polegają na wykorzystaniu cech osobowych wynikających z naturalnych różnic w organizmach ludzkich. Badania nad wykorzystaniem tych metod prowadzi m.in. Naukowa i Akademicka Sieć Komputerowa (NASK) (BioPKI, 2014). Metody biometryczne budzą jednak szereg kontrowersji natury etycznej. Dowiedziono m.in., że wykorzystywanie do uwierzytelniania cech biometrycznych może naruszać prywatność osób, ze względu na ujawnianie informacji wrażliwych, których znajomość nie jest konieczna w procesie uwierzytelniania. Cechy ludzkie, takie jak linie papilarne, mogą wskazywać na występowanie określonych schorzeń lub też mogą być zależne od właściwego żywienia matki (a z nią: płodu) w ciągu trzeciego miesiąca ciąży (Opinia, 2005). Także takie choroby jak białaczka czy rak piersi mogą być powiązane z pewnymi wzorami linii papilarnych (Liu, 2008). W przypadku korzystania z metod biometrycznych niewątpliwie pojawiają się pytania o podstawowe prawa człowieka, w tym przede wszystkim na prawo do prywatności (Krassowski, 2014).

W Polsce dane biometryczne wykorzystywane są m.in. w paszportach wydawanych od 2006 r., kiedy to wprowadzono do dokumentu paszportowego, zgodnie z zaleceniami unijnymi, rozpoznawanie twarzy (Frost & Sullivan, 2014). Następnie, od 2009 r., do paszportów wprowadzono odcisk palca[2]. Tzw. e-paszporty zostały wyposażone w mikroprocesor umożliwiający identyfikację na podstawie częstotliwości radiowej (RFID-chip), zawierający cyfrowy zapis obrazu twarzy i odcisk palca.

Krzysztof Krassowski opisał wpływ zastosowania technik biometrycznych na społeczeństwo, zwracając uwagę na szerszy aspekt, tj. na wpływ rozwoju technologicznego i związanych z nim nowych możliwości w zakresie pozyskiwania informacji, ich przetwarzania i wykorzystywania w sposób zautomatyzowany na wzrost ingerencji w prawa jednostki we współczesnym świecie (Krassowski, 2014). Obawy przed zastosowaniem technik biometrycznych odnoszą się głównie do możliwych nadużyć w postaci tzw. kradzieży tożsamości, która może służyć do celów przestępczych, w tym także terrorystycznych (Johnson, 2004). Konieczne jest zatem zapewnienie wysokiego poziomu bezpieczeństwa dla zasobów danych biometrycznych, będących w posiadaniu uprawnionych służb, w tym administracji

[2] Zgodnie z rozporządzeniem Rady (WE) nr 2252/2004. W art. 1 ust. 2 przewidziano cyfrowy obraz twarzy oraz odciski palców jako obowiązkowe cechy biometryczne zawarte w paszportach obywateli UE.

publicznej. Według badań, użytkownicy jednak w coraz większym stopniu są skłonni zrezygnować z innych form identyfikacji na rzecz identyfikacji biometrycznej, głównie ze względu na wygodę tej formy identyfikacji (Roberts & Patel, 2007, 65). Zastosowanie metod biometrycznych jest coraz bardziej popularne w korporacjach, m.in. przy kontroli dostępu oraz identyfikacji uprawnień pracowniczych, a także wśród użytkowników masowych, np. w przypadku biometrycznych odcisków palców zabezpieczających dostęp do laptopów czy telefonów (Krassowski, 2014). Te zastosowania nie budzą jednak tylu kontrowersji, co zastosowanie metod biometrycznych w stosunkach państwo – obywatel. Problemy związane z zastosowaniem metod biometrycznych na potrzeby administracji publicznej wynikają głównie z braku odpowiedniej kampanii informacyjnej. Prawo do prywatności, odnosi się do poczucia wolności oraz anonimowości (Sołtyszewski & Krassowski, 2013). Prawo to jest zagwarantowane w Konstytucji RP (art. 47), jak również w prawie międzynarodowym, m.in. w Powszechnej Deklaracji Praw Człowieka ONZ (art. 12) oraz w Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności (art. 8). Istotne jest zatem zapewnienie właściwego poziomu bezpieczeństwa dla zasobów danych biometrycznych, co wymaga uwzględnienia takich czynników jak:

- własność danych,
- ochrona danych,
- komodyfikacja danych,
- bezpieczeństwo danych i ich odporność na atak,
- dostęp do danych przez nieokreślone podmioty oraz osoby indywidualne,
- zautomatyzowana wymiana danych,
- procesy zarządzania danymi,
- korelacje danych,
- zapewnienie prywatności danych,
- outsourcing danych,
- wiarygodność danych (Lodge, 2007).

Krzysztof Krassowski omawiając badania dotyczące identyfikacji biometrycznej wyraził pogląd, iż akceptacja dla tej metody identyfikacji jest najwyższa tam, gdzie obywatele posiadają najlepszą wiedzę w jej zakresie (Krassowski, 2014). Autor ten wskazał, że organy państwa wykorzystujące metody biometryczne dla zapewnienia bezpieczeństwa publicznego i indywidualnego obywateli, powinny rozpocząć działania od budowania zaufania społecznego, planując wdrożenie tych metod powinny równocześnie kształcić społeczeństwo w zakresie biometrii oraz prowadzić konsultacje społeczne w zakresie rozwiązań legislacyjnych oraz procedur postępowania.

6. Zakończenie

Każdy system informacyjny wymaga doskonalenia. W administracji publicznej proces informatyzacji charakteryzuje duża dynamika zmian. W procesie tym korzysta się z bezpiecznych oraz przyjaznych dla użytkownika rozwiązań komunikacyjnych, w tym także metod identyfikacji i uwierzytelniania za pomocą loginu i hasła (profil zaufany ePUAP). W przypadku identyfikacji elektronicznej należy zwrócić uwagę, z jednej strony, na instytucje administracyjne jako nadawców informacji, którzy mają zapewnić dostęp do zasobów

uprawnionym do tego użytkownikom, z drugiej – na samych użytkowników, którzy muszą znać, rozumieć i akceptować mechanizmy identyfikacji elektronicznej, aby sprawnie z nich korzystać. Badania autorki przeprowadzone w Urzędzie Marszałkowskim Województwa Śląskiego w 2014 r. wykazały, że korzystanie z komunikacji elektronicznej w kontaktach z nim przez jego klientów jest bardzo niskie. Efektywność systemów informacyjnych w administracji publicznej zależy nie tylko od tego jak funkcjonuje identyfikacja, równie istotne jest świadczenie usług w sposób kompleksowy, czyli realizacja wszystkich czynności online. Systemy informacyjne, które mają cechować się szybkością, jakością i niezawodnością, nie mogą funkcjonować bez sprawnych narzędzi teleinformatycznych. Dopóki jednak administracja publiczna nie wdroży w pełni narzędzi teleinformatycznych do wewnętrznej pracy, nie zastąpi tradycyjnego obiegu dokumentacji obiegiem elektronicznym, to wśród jej pracowników trudno będzie ukształtować przekonanie, że forma elektroniczna dokumentu jest bardziej przyjazna, wygodna i usprawnia ich pracę. Wydaje się także, że użytkownicy zewnętrzni, petenci administracji publicznej nie są świadomi możliwości, które oferuje powszechnie dostępna platforma komunikacji administracji publicznej jaką jest ePUAP. Urzędy w Polsce deklarują co prawda prowadzenie kampanii zachęcających do korzystania z komunikacji elektronicznej, jednak faktyczne wykorzystanie tego kanału komunikacyjnego jest niewielkie. Dla upowszechnienia elektronicznej komunikacji z administracją publiczną bardzo istotne jest m.in. prawidłowe przygotowanie użytkowników do korzystania z narzędzi identyfikacji w środowisku elektronicznym i to zarówno po stronie nadawców informacji, a więc pracowników administracyjnych oraz po stronie jej odbiorców, czyli obywateli. Chociaż nowe rozwiązania w postaci podpisu osobistego są stopniowo wprowadzane w polskim systemie informacyjnym administracji publicznej, to niestety ich wdrażanie nie jest planowane w sposób optymalny. Nie zostały one przygotowane na czas, tj. w momencie przeprowadzania wymiany dowodów osobistych, tym samym uniemożliwiając kompleksową ich wymianę z równoczesnym uzyskaniem podpisu osobistego. Widoczny jest też opór ze strony administracji, który można tłumaczyć tym, że każda zmiana sposobu prowadzenia spraw w urzędach wymaga zmiany procedur, które przyjmuje się w odpowiednich przepisach prawnych (także tych wewnętrznych). Inicjatywa wprowadzenia zmian i popularyzacji komunikacji elektronicznej w dużym stopniu spoczywa także na urzędach administracji publicznej w Polsce, które mając odpowiednie podstawy prawne oraz narzędzia pracy muszą informatyzować się wewnętrznie.

Bibliografia

BioPKI (2014). *BioPKI – Nowoczesne dokumenty tożsamości. Projekt współfinansowany przez NCBiR* [online] [16.11.2014], http://www.biopki.org.pl/

Dyrektywa (1999). Dyrektywa Parlamentu Europejskiego i Rady nr 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych, (Dz. Urz. UE L 013 z dnia 19.01.00 r.).

Frost & Sullivan (2014). *Rosnące obawy w zakresie bezpieczeństwa oraz warunki ekonomiczne wpłyną na rozwój rynku biometrycznego* [online]. Portal Frost & Sullivan [19.11.2014], http://www.frost.com/prod/servlet/press-release.pag?docid=256202861

Gaj, K., Górska A., Górski K. (2003). *Słowniczek terminów związanych z kryptologią i ochroną informacji angielsko – francusko – polski. Enigma Systemy Ochrony Informacji*. Warszawa: ENIGMA System Ochrony Informacji Sp. z o. o.

ISO/IEC 27000:2009, System zarządzania bezpieczeństwem informacji – technologie informatyczne – techniki bezpieczeństwa – informacje ogólne i słownik pojęć.
Johnson, M. L. (2004). Biometrics and the Threat to Civil Liberties. *Computer*, 37(4), 90–91.
Krassowski, K. (2014). Identyfikacja biometryczna – nasz przyjaciel czy wróg? *Studia Prawnoustrojowe* 23, 189–201.
Kutyłowski, M.; Paluszyński, W. (2014). Finalny raport zbiorczy. Infrastruktura bezpiecznego podpisu administracyjnego. Politechnika Wrocławska, Trusted Information Consulting [online], Podpis osobisty [16.11.2014], http://podpisosobisty.pl/images/Wyniki_projektu/raport_koncowy.pdf
Liu, Y. (2008). Identifying Legal Concerns in the Biometric Context. *Journal of International Commercial Law and Technology* 2008 (3), 46.
MAC (2014). Wpływ cyfryzacji na działanie urzędów administracji publicznej w Polsce w roku 2014 [online]. Ministerstwo Administracji i Cyfryzacji [04.05.2015], https://mac.gov.pl/files/pbs_mac_cyfryzacja_fin_2014_v.pdf
Mazur, Z.; Mazur, H. (2013). Systemy automatycznej identyfikacji – zastosowania i bezpieczeństwo danych. *Nierówności Społeczne a Wzrost Gospodarczy*, 32, 193–206.
Oleński, J. (2006). *Infrastruktura informacyjna państwa w gospodarce globalnej*. Warszawa: Uniwersytet Warszawski, WNE.
Opinia (2005). Opinia nr 3/2005 w sprawie wprowadzenia w życie rozporządzenia rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących bezpieczeństwa i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie (Dziennik Urzędowy L 385 z 29.12.2004, str. 1–6 [online] [16.11.2014], http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp112_pl.pdf
Pawłowska, A. (2002). Zasoby informacyjne w administracji publicznej w Polsce – problemy zarządzania. Lublin: Wydaw. Uniwersytetu Marii Curie-Skłodowskiej.
PN-ISO/IEC 9798–1:1996, Technika informatyczna – Techniki zabezpieczeń – Mechanizmy uwierzytelniania podmiotów – Model ogólny.
Projekt (2010). Projekt ustawy z dnia o dowodach osobistych. [online] [2016–01-20], https://bip.kprm.gov.pl/download.php?s=75&id=12206
Roberts, J.; Patel, S. (2007). Biometrics: Does Convenience Outweigh Privacy? [In:] Convenient or Invasive – The Information Age. Red. Larsen K. R., Voronovich Z. A. Boulder, Colorado: Ethica Publishing, s. 62–71.
Rozporządzenie (2007). Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej (Dz. U. Nr 10, poz. 68).
Rozporządzenie (2011). Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 kwietnia 2011 r. w sprawie zasad potwierdzania, przedłużania ważności i unieważniania profilu zaufanego elektronicznej platformy usług administracji publicznej (Dz. U. Nr 93, poz. 547).
Rozporządzenie (2012). Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 17 stycznia 2012 r. w sprawie wzoru wniosku o ponowne wykorzystywanie informacji publicznej (Dz. U. poz. 94).
Rozporządzenie (2014a). Rozporządzenie Rady Ministrów z dnia 12 marca 2014 r. w sprawie Centralnego Repozytorium Informacji Publicznej (Dz. U. poz. 361).
Rozporządzenie (2014b). Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 26 marca 2014 r. w sprawie zasobu informacyjnego przeznaczonego do udostępniania w Centralnym Repozytorium Informacji Publicznej (Dz. U. poz. 491).
Sołtyszewski, I.; Krassowski, K. (2013). Wybrane aspekty zastosowania identyfikacji biometrycznej. [W:] E. Gruza (red.). Oblicza współczesnej kryminalistyki. Księga jubileuszowa Profesora Huberta Kołeckiego. Warszawa, 247–248.
Ustawa (2001). Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. 2001 Nr 112, poz. 1198).

Ustawa (2005). Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. 2005 Nr 65, poz. 565).
Ustawa (2010). Ustawa z dnia 12 lutego 2010 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw. (Dz. 2010 Nr 40, poz. 230).
Ustawa (2011). Ustawa z dnia 9 czerwca 2011 roku o zmianie ustawy o dowodach osobistych i ustawy o ewidencji ludności. (Dz. U. 2011 Nr 133, poz. 768).
Ustawa (2015). Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 4 grudnia 2015 w sprawie ogłoszenia jednolitego tekstu ustawy – Kodeks Postępowania Administracyjnego. (Dz. U. 2016, poz. 23).

Electronic Users Identification Technologies and Their Role in Contemporary Communication with Administrative Institutions

Abstract

Purpose/thesis: The aim of the article is to introduce the issue of electronic identification that takes place during the communication with the systems of administrative institutions. The author discusses the most modern solutions ensuring high level of security and allowing for the verification of access rights to electronic resources, such as certified electronic signatures, trusted profiles and personal signature and biometric methods (planned to be introduced).
Approach/methods: The study was conducted on the basis of the analysis of literature, provisions, the reports of the Ministry of Administration and Digitization on the impact of computerization on Polish administrative institutions and author' own analysis of the arriving and outgoing correspondence in the Province Marshal's Office of Silesia in Katowice. The research also involved the options offered to users via ePUAP tool.
Results and conclusions: The research identified authentication technologies employed in electronic communication by public entities using ePUAP tool, that is, the use of login and password as well as the application of electronic signature or trusted profile. The analysis of legal provisions helped discuss a personal signature (awaiting the official introduction).The analysis of the literature shows that biometric methods are getting more and more popular while at the same time being the most secure ones in the virtual world. The use of electronic authentication is necessary to ensure the security of information systems in public administration, on the grounds that the authenticated document is of legal significance. Studies conducted by the author in the Province Marshal's Office of Silesia in Katowice have shown that, in the first quarter of 2014, the use of electronic authentication tools in public administration concerns on average 6.16% documentation sent from the Office and 5.31% of that received by the Office. The results of the research show that there are numerous barriers faced by the users of these systems, including lack of knowledge about the capabilities of the system, lack of comprehensiveness, electronic forms and internal changes in government offices.
Originality/value: The communication with public entities in Poland is governed by numerous laws, which have been shown in the text. The construction of information systems of public administration results from the policy of whole country computerization. There has not been any analysis made so far which tools have been adopted to identify users in these systems, and how the process of authentication of electronic documents is implemented.

Keywords

Public administration. Electronic identification. Information system. Authentication.

Dr JUSTYNA ADAMUS-KOWALSKA – jest adiunktem w Zakładzie Zarządzania Informacją w Instytucie Bibliotekoznawstwa i Informacji Naukowej na Uniwersytecie Śląskim. Specjalizuje się w problematyce zarządzania informacją. Najważniejsze publikacje: System informacji archiwalnej w Polsce: historia, infrastruktura, standardy i metody (Katowice 2011).

Kontakt z autorką:
justyna.adamus@us.edu.pl
Instytut Bibliotekoznawstwa i Informacji Naukowej
Wydział Filologiczny
Uniwersytet Śląski w Katowicach
Pl. Sejmu Śląskiego 1
40–032 Katowice