

MARCIN WOŁEK
ŁUKASZ TAMKUN

Uniwersytet Gdański

SYSTEM URZĘDÓW CERTYFIKACYJNYCH JAKO ELEMENT PRODUKTU TERYTORIALNEGO

Abstract: System of Certification Authorities as an Element of Territorial Product. The system of certification authorities may take a form of a public project due to persisting low efficacy of commercial certification authorities. Certification services may be provided by self-government on regional or local level. The growing competitiveness among self-government is a factor that local authorities must take into consideration and develop innovative instruments that may be the source of their predominance. The fulfillment of this aim may be achieved by taking advantage of employing the system of certification authorities as a partial product of territorial megaproduct.

Wprowadzenie

W latach 70. pojawiła się koncepcja *marketingu społecznego*, w myśl której „zadanie organizacji polega na określeniu potrzeb, wymagań i interesów rynków docelowych oraz dostarczeniu pożądanego zadowolenia w sposób bardziej efektywny i wydajny niż konkurenci, przy jednoczesnym zachowaniu lub podniesieniu dobrobytu konsumenta i społeczeństwa” [2, s. 26]. Elementem wyróżniającym *marketing społeczny* od tradycyjnego ujmowania marketingu jest dostrzeganie potencjalnych konfliktów między indywidualnymi potrzebami konsumenta w krótkim okresie, a długookresowymi potrzebami społeczeństwa [3, s. 25]. Tradycyjnie postrzegane relacje rynkowe występowały między przedsiębiorstwem a nabywcą, i to jego potrzeby były punktem wyjścia dla wszystkich działań marketingowych. Koncepcja *marketingu społecznego* przez zwrócenie uwagi na społeczeństwo jako najważniejszego adre-

sata działań marketingowych przedsiębiorstwa stała się przyczyną całkowitej reorientacji strategii funkcjonowania wielu firm. Społeczeństwo przez lepsze możliwości edukacyjne i organizacyjne (organizacje pozarządowe, sieci obywatelskie, konsumeryzm) staje się wymagającym i ważnym partnerem dla przedsiębiorstw, a powstające konflikty między przedsiębiorstwem a nabywcą są natychmiast przenoszone na relację przedsiębiorstwo – społeczeństwo. Źródłami konfliktów mogą być problemy ekologiczne, społeczne, ekonomiczne oraz demograficzne – są one wynikiem powstawania kosztów zewnętrznych ponoszonych przez ogół społeczności, a nie przez indywidualnego konsumenta. Dlatego też *marketing społeczny* przenosi ciężar zainteresowania z pojedynczego konsumenta na zbiorowość, która w społeczeństwach rozwiniętych zorganizowana jest w społeczności lokalne, miejskie, regionalne lub narodowe o różnym zakresie autonomii. Potrzeba adaptacji koncepcji marketingu społecznego związana jest także ze zmianami strukturalnymi zachodzącymi na świecie, takimi jak wzrost zainteresowania problematyką ekologiczną, globalizacja oraz rosnące różnice w zamożności poszczególnych krajów.

Współcześnie na świecie można zaobserwować zmiany idące w kierunku urzeczywistnienia społeczeństwa informacyjnego, którego niezwykle ważnym elementem jest elektroniczna administracja. Zagadnienie to obejmuje działania w sferze wewnętrznej i zewnętrznej administracji. Wewnątrz administracji w praktyce dąży się do pełnego elektronicznego obiegu dokumentów w ramach poszczególnych urzędów oraz elektronicznej wymiany danych między instytucjami publicznymi. Aby osiągnąć należytą efektywność i w pełni skorzystać z zalet informatyzacji niezbędny staje się *reengineering* procesów wewnątrz administracji, skutkujący automatyzacją procedur. Takie podejście do informatyzacji administracji publicznej jest gwarancją skuteczniejszego i tańszego świadczenia elektronicznych usług publicznych za pośrednictwem Internetu, oraz pełnej ich dostępności *on-line*. Prawdopodobnie przeprowadzona informatyzacja znacznie ułatwi, a niekiedy wręcz umożliwi pewnym grupom społecznym załatwienie spraw administracyjnych, w szczególności osobom niepełnosprawnym. Efektywne działanie elektronicznej administracji w polskich realiach jest zdeterminowane funkcjonowaniem podpisu elektronicznego. Wynika to z narzucenia, przez polskie ustawodawstwo, wymogu korzystania z bezpiecznego podpisu elektronicznego w relacjach klient-administracja. Rozwiązanie takie zostało przyjęte w art. 8 *Ustawy z 18 września 2001 r. o podpisie elektronicznym* (Dz.U. 2001 r. nr 130 poz. 1450 z późn. zmian.), zwaną dalej *Ustawą o podpisie elektronicznym*, zgodnie z którym jedynie

bezpieczny podpis elektroniczny wywołuje skutki prawne równoważne z formą pisemną. Natomiast *Ustawa z 14 czerwca 1960 r. Kodeks postępowania administracyjnego* (Dz.U. 2000 r. nr 98 poz. 1071 z późn. zmian.), w art. 14 przyjmuje zasadę pisemności postępowania przed organami administracji publicznej, które w dużej mierze stosują tę *Ustawę*.

1. Produkt terytorialny

Tradycyjnie postrzegany proces wymiany sprowadzany był do relacji *stricte* komercyjnych zachodzących między podmiotami, których nadrzędnym celem było osiągnięcie zysku lub inny cel o charakterze ekonomicznym. Współcześnie, procesy wymiany odbywają się na wielu płaszczyznach z zaangażowaniem podmiotów, które za najistotniejszy cel stawiają sobie usatysfakcjonowanie klienta i utrzymywanie z nim długofalowych, partnerskich relacji.

W przypadku miasta zarówno przedmiot wymiany, jak i jego nabywcy są tak dalece zróżnicowani, że zachodzi potrzeba ciągłego dostosowywania oferty miasta do oczekiwań jego „użytkowników” kształtowanych przez proces konkurencji terytorialnej.

Ponadto, sam przedmiot wymiany, „produkt terytorialny” traktowany całościowo jest w praktyce niemożliwy do zdefiniowania jako konkretna kategoria rynkowa. Ze względu na poziom agregacji, produkt w marketingu miasta może być rozpatrywany jako:

- megaprodukt miejski,
- produkt cząstkowy, stanowiący część *megaprodktu miejskiego*, mogący być jednak osobnym przedmiotem w procesie wymiany.

Megaprodukt miejski jest sumą wszystkich potencjalnych korzyści oferowanych konkretnemu nabywcy w wyniku procesu wymiany. Jest przedmiotem wymiany tylko w przypadku podmiotów podejmujących decyzje strategiczne, dotyczące np. lokalizacji przedsiębiorstwa lub miejsca zamieszkania.

Produkty cząstkowe będące elementami składowymi megaprodktu, ale też niezależnymi przedmiotami wymiany, bliższe są codziennemu życiu „użytkowników” miasta. Są przedmiotem wymiany na rynkach cząstkowych w mieście, takich jak rynek nieruchomości, rynek usług komunalnych czy rynek pracy.

Dla mieszkańców miasta, *megaprodukt miejski* postrzegany jest przez pryzmat poszczególnych produktów cząstkowych, mających dla nich relatyw-

nie największe znaczenie. Dysfunkcja jednego z nich, przy istnieniu pozostałych na wysokim poziomie może być elementem zmniejszającym poziom satysfakcji odczuwany przez nabywcę. Jako przykład można podać sytuację, w której nieefektywny system transportowy miasta utrudnia dostępność do różnych produktów cząstkowych położonych na terenie danego miasta, zwiększając tym samym koszty ich nabycia o koszty zewnętrzne kongestii transportowej. Prowadzić to może do znacznych dysproporcji, których wyrazem jest m.in. urbanizacja nieproporcjonalna.

Najbardziej ogólny podział adresatów działań marketingu miasta związany jest z miejscem zamieszkania lub lokalizacji danej grupy docelowej. W przypadku mieszkańców i podmiotów zlokalizowanych na terenie danego miasta mówi się o tzw. *marketingu wewnętrznym*, utożsamianym z regułą z funkcjonowaniem administracji publicznej. Zwraca się przy tym uwagę na to, że jakość obsługi mieszkańców w danym urzędzie może być przedmiotem oceny w kontekście tzw. *jakości technicznej*, czyli konkretnej usługi wykonywanej przez pracowników urzędu lub innych jednostek miejskich na rzecz klienta oraz tzw. *jakości funkcjonalnej*, która dotyczy sposobu i formy obsługi klienta [6, s. 87]. W przypadku podmiotów zewnętrznych jest to tzw. *marketing zewnętrzny*. Zasadnicze różnice przedstawiono w tabeli 1.

Należy zwrócić uwagę na to, że najistotniejszym aspektem przesłania w odniesieniu do marketingu wewnętrznego są wartości lokalne i tożsamość, które jednak przy spełnieniu pewnych dodatkowych warunków mogą stać się ważnym elementem komunikacji zewnętrznej.

Rozwój technologii teleinformatycznych i rosnąca mobilność mieszkańców jest przyczyną, dla której komunikacja administracji miejskiej z otoczeniem napotyka na nowe szanse i wyzwania.

Tabela 1

Porównanie marketingu wewnętrznego i zewnętrznego

Wyszczególnienie	Marketing wewnętrzny	Marketing zewnętrzny
Adresat (grupa docelowa)	Zlokalizowany w mieście	Niezlokalizowany w mieście
Przesłanie	Wartości lokalne, tożsamość	Uniwersalne
Kanały komunikacji marketingowej	Media lokalne i regionalne,	Media ogólnokrajowe i międzynarodowe
Organizacja	Na podstawie zasobów wewnętrznych miasta	Przy współpracy z podmiotami zewnętrznymi

Źródło: Opracowanie własne na podstawie [8, s. 173].

Jednym z instrumentów mogących w istotnym stopniu wpłynąć na kształtowanie relacji na linii urząd miejski – mieszkaniec są systemy urzędów certyfikacyjnych.

2. System urzędów certyfikacyjnych

System urzędów certyfikacyjnych to struktura hierarchiczna podmiotów świadczących usługi certyfikacyjne, który może stać się elementem marketingu wewnętrznego miasta. Usługi certyfikacyjne polegają m.in. na wydawaniu certyfikatów, którymi opatruje się podpis elektroniczny. Jeżeli certyfikat wydany przez urząd certyfikacyjny jest certyfikatem kwalifikowanym, mamy do czynienia z bezpiecznym podpisem elektronicznym. Certyfikat i kwalifikowany certyfikat to elektroniczne zaświadczenie przyporządkowane do osoby składającej podpis elektroniczny, umożliwiające jej identyfikację. Kwalifikowane certyfikaty mogą być wydawane jedynie przez kwalifikowane podmioty świadczące usługi certyfikacyjne, wpisane do właściwego rejestru.

Podpis elektroniczny i bezpieczny podpis elektroniczny nie różnią się między sobą pod względem technicznym. Są generowane w jednakowy sposób, zachowują te same właściwości oraz służą identyfikacji osoby składającej podpis elektroniczny. Różnica powstaje natomiast przez stosowanie odpowiednich przepisów, które odmiennie regulują te podpisy. Najważniejsza różnica występuje na płaszczyźnie wywoływanych przez nie skutków prawnych.

Istnieją dwa modele, które tworzą strukturę działania podpisu elektronicznego. Pierwszy jest oparty na tzw. kręgu zaufania (*ring of trust*), drugi funkcjonuje na podstawie infrastruktury klucza publicznego (*public key infrastructure*). W pierwszym modelu, strony stosunku prawnego dbają o należytą budowę bazy danych zaufanych partnerów, i to na nich ciąży odpowiedzialność skutecznego powiązania klucza publicznego z właściwą osobą, zanim przystąpi się do korzystania z podpisu elektronicznego. Natomiast w modelu drugim, obowiązek rzetelnego przyporządkowania klucza publicznego do odpowiedniej osoby nie spoczywa na stronach transakcji *a priori*. System ten funkcjonuje na podstawie hierarchicznej budowy podmiotów (tzw. zaufanych stron trzecich), które są gwarantem właściwej identyfikacji osób korzystających z podpisów elektronicznych i wystawienia ważnego certyfikatu, w którym zawarte są podstawowe dane osobowe posiadacza podpisu elektronicznego.

Oba modele mają na celu wyeliminowanie podstawowego problemu dotyczącego bezpieczeństwa obrotu prawnego, jakim jest zagwarantowanie au-

tentyczności przekazu w warunkach, gdy strony porozumiewają się i składają oświadczenia woli na odległość [4, s. 85].

Model infrastruktury klucza publicznego może być tworzony na podstawie komercyjnego systemu podmiotów świadczących usługi certyfikacyjne, w którym przedsiębiorcy występują w roli zaufanych stron trzecich, świadczących usługi certyfikacyjne. Rozwiązanie takie zostało przyjęte w Polsce. Obecnie działają trzy kwalifikowane podmioty świadczące usługi certyfikacyjne: Unizeto Technologies S.A., Krajowa Izba Rozliczeniowa S.A. oraz Polska Wytwórnia Papierów Wartościowych S.A. Podmiotem nadrzędnym w hierarchii jest Narodowe Centrum Certyfikacji, działające przy Narodowym Banku Polskim.

Pozostawanie przy procedurach tradycyjnych, wykorzystujących obrót papierowy jest droższe dla państwa, niż zastosowanie procedur całkowicie elektronicznych. Ponadto, ograniczenie ilości stosowanego papieru, drukarek oraz materiałów eksploatacyjnych do drukarek jest rozwiązaniem proekologicznym. Dlatego też w interesie publicznym jest całkowite przejście na obrót elektroniczny, oczywiście z zachowaniem zasad gospodarności. Celowi temu powinno służyć przedsięwzięcie, które umożliwiłoby, jak najszybsze i najtańsze w skali całego państwa, upowszechnienie bezpiecznego podpisu elektronicznego. Przedsięwzięcie to mogłoby przybrać postać projektu publicznego, gdyż do tej pory podmioty świadczące usługi certyfikacyjne o charakterze prywatnym nie spełniają swojej funkcji i nie przyczyniają się, z powodu utrzymywania wysokich cen, do istotnego rozpowszechniania bezpiecznego podpisu elektronicznego w Polsce. Najtańszy zestaw obejmujący kwalifikowany certyfikat, kartę kryptograficzną, czytnik oraz oprogramowanie kosztuje jednorazowo 401,38 zł, a odnowienie certyfikatu 115,90 zł [5, s.76]. Dodatkowym argumentem świadczącym o dysfunkcjonalności systemu urzędów certyfikacyjnych opartego na rozwiązaniach komercyjnych w Polsce jest wycofanie się z rynku i zakończenie działalności Centrum Certyfikacji Signet – 4 stycznia 2007 r.

Art. 9 ust. 3 *Ustawy o podpisie elektronicznym* stanowi, że jednostka samorządu terytorialnego może świadczyć usługi certyfikacyjne na zasadach niezarobkowych, dla członków wspólnoty samorządowej. Zatem każda jednostka samorządowa zarówno na poziomie lokalnym, w tym miejskim, jak i regionalnym może świadczyć usługi certyfikacyjne. Zawężony jest tylko krąg odbiorców tych usług do członków wspólnoty samorządowej, czyli obywatele stale zamieszkujących na obszarze danej jednostki samorządu terytorialnego.

Z tego względu działania, wykonywane w ramach świadczenia usług certyfikacyjnych przez organy jednostki samorządowej, są elementem marketingu wewnętrznego. Rozwiązaniem najefektywniejszym i najtańszym wydaje się być utworzenie urzędu certyfikacyjnego w miastach wojewódzkich. Pozwoliłoby to objąć, jak największą liczbę mieszkańców oraz wyeliminować powielanie się urzędów certyfikacyjnych w przypadku realizacji tego projektu na szczeblu lokalnym. Ponadto, art. 9 ust. 2 *Ustawy o podpisie elektronicznym* wskazuje, że jednostki samorządu terytorialnego mogą również świadczyć usługi certyfikacyjne na potrzeby własne oraz innych organów władzy publicznej.

Wdrożenie projektu publicznego, w którym jednostka samorządu terytorialnego będzie pełniła funkcję urzędu certyfikacyjnego nie jest wyzwaniem technologicznym ani finansowym. Infrastrukturę urzędu certyfikacyjnego najprościej można zbudować, bazując na systemie Windows Server 2003. System ten zawiera już wbudowane usługi niezbędne m.in. do wydawania, archiwizacji oraz zawieszania i unieważniania certyfikatów, a także publikowania listy certyfikatów, które uległy zawieszeniu lub unieważnieniu [10, s. 166]. Koszty zakupu licencji do oprogramowania firmy Microsoft można wyeliminować stosując jedną z wielu dystrybucji Linuksa. Oszczędności będą wynikały nie tylko z zakupu samego systemu, ale także z oprogramowania niezbędnego do zapewnienia bezpieczeństwa serwera, na którym będą przechowywane oraz publikowane kwalifikowane certyfikaty. Ponadto, system Linuks charakteryzuje się kodem ogólnodostępnym (otwartym) nie stanowiącym tajemnicy handlowej przedsiębiorstwa w przeciwieństwie do Windows Server 2003. Jest to rozwiązanie korzystniejsze z punktu widzenia bezpieczeństwa – kluczowego aspektu dla podmiotów świadczących usługi certyfikacyjne.

Następną kwestią, która może generować koszty dla podmiotu świadczącego usługi certyfikacyjne jest przygotowywanie bezpiecznych urządzeń do składania podpisu elektronicznego. *Rozporządzenie Rady Ministrów z 7 sierpnia 2002 r. w sprawie warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*, zwane dalej *rozporządzeniem w sprawie warunków technicznych i organizacyjnych*, określa w par. 3 ust. 1, że bezpieczne urządzenie do składania podpisów elektronicznych składa się z oprogramowania podpisującego, oraz współpracującego z nim, komponentu technicznego. Par. 5 ust. 1 tego rozporządzenia określa także warunki, jakie powinien

spełniać komponent techniczny, na który składają się: karta kryptograficzna wyposażona w pamięć, procesor i własne oprogramowanie oraz czytnik kart chipowych. Przygotowanie takiego zestawu to koszt kilkudziesięciu złotych [11, s. 152]. Koszty te mogłyby być znacznie mniejsze, gdyby w ww. rozporządzeniu nie wskazywano na konkretne rozwiązanie komponentu technicznego, jakim jest karta kryptograficzna oraz jej czytnik. Trzeba również zaznaczyć, że zakup komponentu technicznego jest wydatkiem jednorazowym i nie wymaga odnowienia, jak w przypadku kwalifikowanego certyfikatu.

Warto w tym miejscu zwrócić uwagę, że nie mniej ważne od zabezpieczeń związanych z komponentem technicznym jest utrzymanie wysokiego poziomu bezpieczeństwa dla oprogramowania obsługującego podpis elektroniczny. Znane są przypadki występowania w oprogramowaniu do podpisywania dokumentów elektronicznych, luk bezpieczeństwa umożliwiających np. podmianę podpisywanego dokumentu [9, s. 12]. Z powyższego przykładu wynika, że najważniejsze jest nie zabezpieczenie komponentu technicznego, ale całego bezpiecznego urządzenia do składania podpisu elektronicznego. Zatem wskazywanie konkretnego rozwiązania w rozporządzeniu w postaci karty kryptograficznej oraz czytnika nie zwiększa bezpieczeństwa składania podpisu elektronicznego, a powoduje, że stosowanie bezpiecznego podpisu elektronicznego wiąże się z nieuzasadnionymi większymi kosztami.

Na koszty utworzenia urzędu certyfikacyjnego na poziomie miejskim lub regionalnym będą składały się również koszty osobowe, lokalowe, a także zakupu serwera, oprogramowania oraz zorganizowanie produkcji komponentów technicznych. W przypadku przyjęcia wariantu oszczędnościowego cena wydania kwalifikowanego certyfikatu po raz pierwszy może wynosić kilkadziesiąt złotych, a jego odnowienie najwyżej kilka złotych.

Wprowadzenie systemu urzędów certyfikacyjnych, działających na poziomie miast wojewódzkich, spowodowałoby wymierne oszczędności dla całego sektora administracji publicznej. Dzięki realizacji takiego projektu funkcjonariusze administracji publicznej mogliby otrzymać pełny zestaw do składania bezpiecznego podpisu elektronicznego po znacznie niższych kosztach, niż w przypadku jego zakupu za pośrednictwem komercyjnych podmiotów świadczących usługi certyfikacyjne. Przykładowe całościowe wdrożenie bezpiecznego podpisu elektronicznego w Mazowieckim Urzędzie Wojewódzkim, przeprowadzone przez podmiot świadczący usługi certyfikacyjne Sigillum ostatecznie wyniosło 28 500 zł. Kwota ta uwzględnia 55 bezpiecznych urzędów do składania podpisu elektronicznego, szkolenia oraz instalację [1,

s. 46]. Wymierne oszczędności przyniosłoby świadczenie tych usług certyfikacyjnych przez jednostkę samorządu terytorialnego. W wyżej opisanym przypadku alternatywą byłoby wdrożenie bezpiecznego podpisu elektronicznego w porozumieniu z Mazowieckim Urzędem Marszałkowskim. Nie licząc jednorazowego wydatku na utworzenie urzędu certyfikacyjnego, jego koszt wynosiłby wtedy ok. 5500 zł, zakładając że wartość bezpiecznego urządzenia do składania podpisu elektronicznego wynosiłaby 100 zł, a szkolenie oraz instalacja zostałyby wykonane za pomocą zasobów własnych urzędu. Za taką cenę urząd certyfikacyjny mógłby także świadczyć usługi dla całego sektora administracji publicznej znajdującego się w województwie oraz dla wszystkich obywateli mieszkających na jego obszarze.

Opisana wyżej idea odgrywania roli urzędu certyfikacyjnego terytorialnego w mieście lub regionie, służy zmniejszeniu, w jak największym stopniu uciążliwości finansowej wprowadzenia bezpiecznego podpisu elektronicznego dla obywateli. Rozporządzenie w sprawie warunków technicznych i organizacyjnych określając szczegółowe wymagania dla komponentu technicznego oraz wskazując pośrednio na konkretne rozwiązanie techniczne, nie przyczyni się do zwiększenia bezpieczeństwa składania bezpiecznego podpisu elektronicznego. Składowym elementem bezpiecznego urządzenia, służącego do składania podpisu elektronicznego jest oprogramowanie współdziałające z komponentem technicznym, któremu zapewnia się bezpieczeństwo w taki sam sposób, jak z zastosowaniem innego komponentu technicznego niezgodnego z rozporządzeniem, lub bez szczególnego rozwiązania technicznego np. przechowywanie bezpiecznego podpisu elektronicznego na płycie CD, DVD, dyskietce lub innych nośnikach danych. Zatem utrzymanie właściwego poziomu bezpieczeństwa jest tak samo trudne w przypadku rozwiązania z komponentem technicznym wymienionym w rozporządzeniu, jak również z innymi rozwiązaniami wymienionymi powyżej [9, s. 12]. W związku z powyższym bezzasadne jest wskazywanie pośrednio w rozporządzeniu na konkretne rozwiązanie w postaci karty kryptograficznej i czytnika, biorąc pod uwagę zarówno bezpieczeństwo, jak i aspekt finansowy. Z pewnością można stwierdzić, że bezpieczny podpis elektroniczny wykorzystujący inne nośniki danych niż karta kryptograficzna, może być znacznie tańszy, w granicach kilku złotych za pierwsze wydanie oraz kilku złotych za odnowienie.

Art. 6 ust. 3 *Ustawy o podpisie elektronicznym* wskazuje, że nie można powoływać się na argument, że podpis nie został złożony za pomocą bezpiecznych urządzeń. Zatem w praktyce nie jest możliwe udowodnienie, że

bezpiecznego podpisu elektronicznego nie złożono za pomocą bezpiecznego urządzenia. W kontekście powyższych rozważań wskazanie w rozporządzeniu cech, jakie powinno mieć urządzenie do składania podpisu elektronicznego, a w szczególności jego komponentu technicznego nie jest uzasadnione. Zatem obecnie nie ma odpowiednich warunków prawnych, aby skutecznie pokonać barierę finansową, która wydaje się być największym hamulcem, powodującym że stosowanie podpisu elektronicznego nie jest powszechne. System urzędów certyfikacyjnych działający w mieście na szczepku wojewódzkim może stać się głównym czynnikiem, który spowoduje, że zostanie pokonana bariera finansowa, oraz może przyczynić się do zredukowania obaw społecznych przed stosowaniem bezpiecznego podpisu elektronicznego do załatwiania spraw urzędowych za pośrednictwem Internetu. Zaprezentowane rozważania wypełniają znamiona celowości przeprowadzenia projektu publicznego, w którym działałyby urzędy certyfikacji w miastach wojewódzkich.

3. Świadczenie usług publicznych z wykorzystaniem taniego podpisu elektronicznego

Zastosowanie systemowego rozwiązania, w którym będą funkcjonować urzędy certyfikacyjne w każdym mieście wojewódzkim, umożliwi świadczenie usług publicznych drogą elektroniczną, które są tańsze niż usługi świadczone w sposób tradycyjny. Przedsięwzięcia mające na celu upowszechnienie i rozwój elektronicznej administracji są wspierane przez Komisję Europejską, która podejmuje się wypracowania i wdrażania planów działań w skali całej Unii Europejskiej. Plany te funkcjonują pod wspólną nazwą eEurope, a aktualna strategia, która dotyczy m.in. rozwoju elektronicznej administracji została nazwana i2010. Komisja Europejska nadała priorytet pewnym usługom publicznym, spośród 600 zidentyfikowanych, które powinny być w pierwszej kolejności informatyzowane i świadczone za pośrednictwem Internetu.

Usługi te zostały poddane analizie i podzielone na te, które z zasady są świadczone dla obywateli, oraz te, które skierowane są do przedsiębiorców. W przypadku polskich realiów do priorytetowych usług dla obywateli zalicza się: rozliczenie podatku dochodowego, przeszukiwanie ofert pracy i pomoc w jej znalezieniu, uzyskanie prawa do zasiłku dla bezrobotnych, prawa do emerytury, renty i innych zasiłków, stypendium studenckiego, uzyskanie dowodu osobistego, prawa jazdy, paszportu, rejestracji pojazdu, pozwolenia na budowę, zgłoszenia na policję, dostęp do katalogów bibliotek publicznych

i ich przeszukiwanie, zgłoszenie do Urzędu Stanu Cywilnego spraw podlegających rejestracji i uzyskiwanie odpisów aktów, złożenie dokumentów o przyjęcie na studia, zmiana zameldowania, zapisanie się na wizytę u lekarza [7, s. 392].

Przedsiębiorcy natomiast, zgodnie z wytycznymi Unii Europejskiej, powinni mieć możliwość załatwienia w pierwszej kolejności następujących spraw *on-line*: rejestracja oraz rozliczenie dotyczące obowiązku ubezpieczenia społecznego pracowników, rozliczenie podatku dochodowego od osób prawnych, podatku VAT, rejestracja działalności gospodarczej, przekazanie danych statystycznych, zgłoszenie celne, uzyskanie pozwolenia i wnoszenie opłat za korzystanie ze środowiska naturalnego, udział w zamówieniach publicznych [7, s. 393].

Lista ta jest oczywiście pewną propozycją, która została sformułowana z uwzględnieniem wielu czynników m.in. takich, jak: łatwość wdrożenia, doniosłość społeczna, wymierne oszczędności dla administracji publicznej, obywateli i przedsiębiorców. W żaden sposób nie ogranicza ona działań w zakresie innych usług publicznych, które dzięki funkcjonowaniu taniego podpisu elektronicznego mogą być rozwijane i skutecznie wdrażane. Przykładami prób wdrożenia systemów elektronicznych urzędów, służących jako platformy elektroniczne do świadczenia usług publicznych za pośrednictwem Internetu jest projekt Urząd On-line, zaimplementowany przez Urząd Miasta Gdańsk oraz platforma elektroniczna Wrota Małopolski skupiająca możliwość załatwienia spraw z zakresu zadań własnych szczebla gminnego, powiatowego i wojewódzkiego, zadań zleconych, a nawet zadań z zakresu administracji rządowej, które wykonuje wojewoda [7, s. 396]. Projekty te nie odniosły oczekiwanych efektów, w dużej mierze ze względu na to, że bezpieczny podpis elektroniczny jest zbyt drogi dla obywatela.

Podsumowanie

Omówiony system traktowany jako cząstkowy produkt marketingu terytorialnego ma szansę stać się jednym z istotnych elementów kształtowania pozytywnego wizerunku administracji publicznej oraz samorządu miejskiego.

Obniżenie kosztów funkcjonowania administracji publicznej, możliwość bardziej efektywnego wykorzystania zasobów ludzkich oraz implementacja nowoczesnych rozwiązań to korzyści bezpośrednio odczuwalne przez urząd miasta. Z punktu widzenia nabywców usługi administracji samorządowej zaletami będą oszczędność czasu poświęconego na załatwianie spraw urzędowych oraz

wyższa akceptacja działań władz jednostki samorządu terytorialnego. Nie bez znaczenia jest również pewnego rodzaju edukacja mieszkańców polegająca na konieczności dostosowania się do wymogów nowoczesnej technologii.

Miasta poszukują coraz to nowych produktów marketingowych ze względu na to, że ciężar procesów konkurencji terytorialnej przenosi się z poziomu krajowego na regionalny i miejski. Potraktowanie systemu urzędów certyfikacyjnych jako elementu umożliwiającego tworzenie zintegrowanego systemu wewnętrznej (w znaczeniu całego miasta) komunikacji marketingowej w istotny sposób przyczynia się do podniesienia konkurencyjności miasta.

Literatura

- [1] Jendra M., 2005, *Elektroniczne otwarcie już za rok*. „Gazeta Samorządu i Administracji” 19.
- [2] Kotler Ph., 1997, *Marketing. Analiza, planowanie, wdrażanie i kontrola*. Wyd. Gebethner i spółka, Warszawa.
- [3] Kotler Ph., Bowen J., Makens J., 1999, *Marketing for Hospitality and Tourism*. Prentice Hall.
- [4] Kreft K., Makusak M., Tamkun Ł., 2006, *Uwierzytelnianie i autoryzacja transakcji w internecie*, [w:] *Konsument i firma w dobie internetu*. Olsztyn.
- [5] Kuczyński D., 2006, *Zastosowanie podpisu elektronicznego w sektorze bankowym w Polsce*, [w:] *Bankowość elektroniczna a rozwój banków w Polsce*. Print Group, Szczecin.
- [6] Purgat A., Reszek R., 1997, *Zarządzanie gminą w teorii i praktyce*, E. Wysocka (red.). Zachodnie Centrum Organizacji, Warszawa – Poznań – Zielona Góra.
- [7] Tamkun Ł., 2007, *Obecny stan zastosowania podpisu elektronicznego w polskiej administracji publicznej*, [w:] *Komputerowo Zintegrowane Zarządzanie*, t. 2, R. Knosala (red.). Polskie Towarzystwo Zarządzania Produkcją, Opole.
- [8] Wołek M., 2005, *Marketingowe kształtowanie przewagi konkurencyjnej miasta*. Praca doktorska napisana w Katedrze Rynku Transportowego Uniwersytetu Gdańskiego pod kier. prof. dr hab. A. Rucińskiego, marzec maszynopis.
- [9] Zagórski F., 2005, *Złamany długopis*. „Chip” 12.
- [10] Żmudziński J., 2005, *Stempel dla każdego*. „Chip” 11.
- [11] Żmudziński J., 2006, *Nie do podrobienia*. „Chip” 01.