

Dr Artur Romaszewski

Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
artur.romaszewski@uj.edu.pl

Dr hab. med. Wojciech Trąbka

Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
wojciech.trabka@uj.edu.pl

Mgr Mariusz Kielar

Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
mariusz.kielar@uj.edu.pl

Mgr Krzysztof Gajda

Uniwersytet Jagielloński - Collegium Medicum
Wydział Nauk o Zdrowiu
Zakład Medycznych Systemów Informacyjnych
krzysztof.gajda@uj.edu.pl

WPROWADZENIE USŁUG ZAUFANIA ZGODNYCH Z ROZPORZĄDZENIEM UE eIDAS W ASPEKCIE SYSTEMÓW INFORMACYJNYCH OPIEKI ZDROWOTNEJ (CZĘŚĆ II)

Wstęp

Czas wprowadzenia usług zaufania uregulowanych w rozporządzeniu eIDAS, będących tematem tego artykułu, to 1 lipca 2016 roku. Powyższa data staje się tym samym wyraźną cezurą czasową rozpoczynającą implementację systemu usług zaufania. Biorąc pod uwagę szereg zaprezentowanych w artykule problemów praktycznych i zmian wprowadzanych na mocy wchodzących w życie przepisów unijnych istotną kwestią z punktu widzenia ich konsekwencji prawnych wydaje się już być sama forma rozporządzenia (nie dyrektywy) nadana eIDAS przez ustawodawcę. Rozporządzenie Unii Europejskiej jest bowiem aktem prawnym zasadniczo różniącym się od dyrektywy. O ile dyrektywa unijna podlega implementacji przez kraje członkowskie w systemie prawa krajowego, o tyle przepisy rozporządzenia są bezpośrednio stosowane w krajowym porządku prawnym. Skutek rozporządzenia nie zależy

przy tym od krajowych środków implementujących w jakikolwiek sposób, czy też wprowadzających, rozporządzenie do krajowego porządku prawnego. Dla mocy obowiązującej rozporządzenia nie jest konieczny akt inkorporacji jego przepisów do prawa krajowego¹.

Forma rozporządzenia wyklucza możliwość korygowania tych przepisów przez państwa członkowskie. Państwo członkowskie ma jednak prawo doprecyzowania czy dookreślenia tych obszarów, które prawodawca unijny pozostawił niedookreślone, lub wprost odesłał do prawa krajowego,. Możliwe jest zatem doprecyzowanie obszarów, które w rozporządzeniu eIDAS pozostały "otwarte", ale pod warunkiem, że sposób tego doprecyzowania nie będzie stał na przeszkodzie osiągnięciu celów rozporządzenia². W Polsce trwa proces przygotowywania aktów prawnych mających za zadanie uregulowanie zagadnień nie uregulowanych na poziomie rozporządzenia eIDAS. Należy przede wszystkim określić skutki prawne dla usług zaufania, dla których skutki te nie zostały określone w rozporządzeniu eIDAS. określać zasady i przesłanki odpowiedzialności cywilnoprawnej podmiotów świadczących usługi zaufania, określenie w ustawie sposobów i środków nadzoru, monitoringu i kontroli podmiotów świadczących usługi zaufania. Ustawa winna regulować zasady funkcjonowania rynku usług zaufania określając warunki rozpoczęcia i zakończenia działalności kwalifikowanych usługodawców, jak też warunki zawieszenia certyfikatów³.

Będzie to miało szczególne znaczenie dla systemów administracji publicznej naszego kraju, w tym dla systemów informacyjnych opieki zdrowotnej. W sektorze zdrowia nadal niedokończone i nie w pełni funkcjonalne pozostają platformy teleinformatyczne zaprojektowane w ramach Systemu Informacji Medycznej. Dlatego sprawne przyjęcie zróżnicowanego modelu usług zaufania wymaganych przez eIDAS może w praktyce napotkać na liczne bariery związane przede wszystkim z głębokim niedostosowaniem infrastruktury informacyjnej naszego państwa do przedmiotowych regulacji.

W artykule omówiono ideę otwartych i zamkniętych usług zaufania oraz ich rodzaje. Przedstawiono koncepcję krajowej infrastruktury zaufania oraz narodowego centrum certyfikacji usług zaufania. Rozporządzenie eIDAS między innymi wprowadza zmiany w

¹ Wróbel A., [w]: *Traktat o funkcjonowaniu Unii Europejskiej*. Komentarz. Tom III pod red. D. Kornobis-Romanowskiej i J. Łacny, Warszawa 2012

² Mielnicki T., Wołowski F., Grajek M., Popis P., Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013

³ Tamże

istniejących usługach np. podpis elektroniczny jak również wprowadza nowe usługi jak pieczęć elektroniczna, uwierzytelnienie witryn internetowych oraz konserwację elektronicznych podpisów, pieczęci i certyfikatów.

Pieczęć elektroniczna

Nowym rozwiązaniem w polski systemie prawnym jest wprowadzenie wśród usług zaufania publicznego pieczęci elektronicznej. Pod tym pojęciem rozumie się dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych. Pieczęcie elektroniczne powinny służyć jako dowód wydania danego dokumentu elektronicznego przez daną osobę prawną dając pewność co do pochodzenia i integralności dokumentu⁴ (Rysunek 1).

Instytucja pieczęci elektronicznej nie jest koncepcją nowatorską - od ponad 15 lat funkcjonuje ona m.in. w czeskim systemie prawnym, natomiast w Belgii trwają obecnie prace nad aktem prawnym wprowadzającym to narzędzie. Co ciekawe, w Polsce także były próby wprowadzenia pieczęci elektronicznej (m.in. siedem lat temu do ustawy o podpisie elektronicznym), ale ostatecznie jednak wycofano się z tego pomysłu⁵. W rzeczywistości w Polsce pieczęcie elektroniczne były od dawna stosowane w urzędach administracji publicznej, tyle że ich instytucja nie była wprost zdefiniowana w przepisach. Po raz pierwszy pieczęć elektroniczna została objęta regulacją prawną trafiając "po cichu" do treści rozporządzenia o warunkach technicznych doręczania dokumentów podmiotom publicznym (ESP). Była ona niezbędna dla realizacji elektronicznej skrzynki podawczej (ESP) - inaczej nie dałoby się bowiem wystawiać urzędowego poświadczenia odbioru (UPO). Miało być ono wystawiane automatycznie przez system, bez udziału człowieka i z użyciem certyfikatu należącego do organizacji - czyli dokładnie przeciwnie, niż podpis kwalifikowany⁶. Zawarta w rozporządzeniu definicja urzędowego poświadczenia odbioru jako "danych dołączonych do

⁴ Art. 59, Preambuła

⁵ Zwolińska A., Szostek D., *E-pieczęć uwierzyteln firmowe i urzędowe dokumenty*, Rzeczpospolita, 23.03.2016, <http://www.rp.pl/Opinie/303239980-E-pieczec-uwierzyteln-firmowe-i-urzedowe-dokumenty.html>

⁶ Do czego posłuży pieczęć elektroniczna?

<https://ipsec.pl/kwalifikowany-podpis-elektroniczny/2010/do-czego-posluzy-pieczec-elektroniczna.html>

dokumentu elektronicznego”⁷ to funkcjonalnie niemal dokładnie to samo, co pieczęć elektroniczna, tyle że ograniczona do stosowania w skrzynce podawczej⁸.

W związku z powyższym zasadnym jest wniosek, że pieczęć elektroniczna jest usługą zaufania kierowaną do osób prawnych. Oznacza to, że z pieczęci elektronicznej nie będą mogły korzystać osoby fizyczne. Powstaje więc problem dopuszczalności wykorzystywania pieczęci elektronicznych przez jednostki organizacyjne nieposiadające osobowości prawnej. Aktualnie brak jest w systemie prawnym normy, która wyłączałaby stosowanie przepisów o pieczęci elektronicznej wobec tych podmiotów. Wydaje się, że wprowadzenie tego typu regulacji nie znajduje uzasadnienia. Jednostki organizacyjne posiadające zdolność prawną posiadają niektóre cechy osób prawnych, jak też mają odrębną podmiotowość prawną, skoro ustawa przyznaje im zdolność prawną. Skoro zatem prawodawca europejski uznał zasadność wyposażenia osób prawnych w możliwość korzystania z instytucji pieczęci elektronicznej, to w ocenie niektórych autorów zasadne jest stworzenie takiej możliwości także tzw. ułomnym osobom prawnym, których dotyczy przepis art. 33¹ § 1 k.c., a których prawo europejskie nie zna.

Odpowiednie stosowanie przepisów o osobach prawnych wobec tzw. ułomnych osób prawnych stanowi podstawę umożliwiającą wyposażenie jednostek organizacyjnych posiadających zdolność prawną, a nie posiadających osobowości prawnej, w możliwość wykorzystywania instytucji pieczęci elektronicznej w pełnym zakresie analogicznie jak to się dzieje w stosunku do osób prawnych.⁹ Do instytucji pieczęci elektronicznej szereg zastrzeżeń miał również Minister Gospodarki, w tym do jej nazwy, która kojarzy się - według jego opinii - z pieczęcią o charakterze notarialnym lub urzędowym¹⁰.

Zasady używania i wykorzystania pieczęci elektronicznej przez dany podmiot winny być regulowane przede wszystkim na poziomie dokumentów wewnętrznych określonego podmiotu, zaś do jego reprezentacji winien nadal służyć przede wszystkim podpis elektroniczny. Analogicznie, jak w przypadku pieczęci tradycyjnej, która nie służy

⁷ Uchylone rozporządzenie Prezesa Rady Ministrów z dnia 29 września 2005 r. w sprawie warunków organizacyjno-technicznych doręczania dokumentów elektronicznych podmiotom publicznym Dz.U. 2005 nr 200 poz. 1651 par. 2 ust. 4

⁸ *Do czego posłuży pieczęć elektroniczna?* <https://ipsec.pl/kwalifikowany-podpis-elektroniczny/2010/do-czego-posluzy-pieczec-elektroniczna.html>

⁹ *Pejaś J., Szulga M., Wagemann M., Stolarowa-Myć A., Wiktorczyk P., Wdrożenie rozporządzenia eIDAS w Polsce – raport*, <http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Glowna-w.-4-2.pdf>

¹⁰ Odpowiedź Ministra Gospodarki na oświadczenie Pana Senatora Ryszarda Knosali w sprawie zapisów ustawy o podpisie elektronicznym Warszawa, 10 października 2013

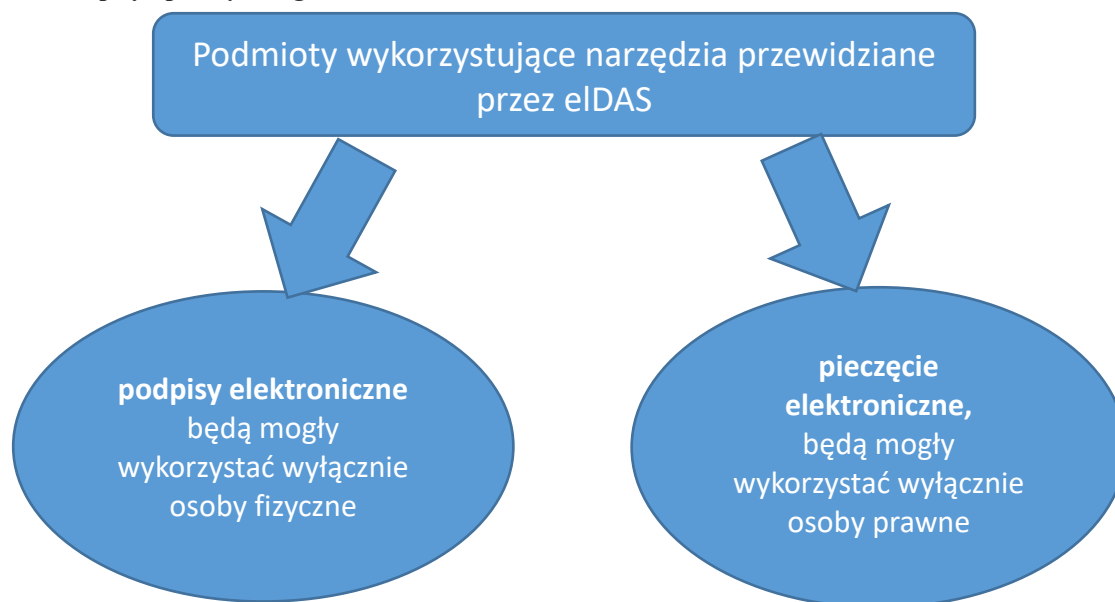
reprezentacji osoby prawnej, pieczęć elektroniczna powinna służyć przede wszystkim potwierdzeniu autentyczności pochodzenia i zapewnieniu integralności danych, nie zaś reprezentacji podmiotu¹¹.

Przepisy powinny zapewnić długoterminową konserwację informacji w celu zapewnienia prawnej ważności podpisów elektronicznych i pieczęci elektronicznych przez wydłużone okresy oraz zagwarantowania możliwości ich walidacji bez względu na przyszłe zmiany technologiczne.

Pieczęcie elektroniczne mogą być używane nie tylko do uwierzytelnienia dokumentu wydanego przez osobę prawną, lecz również do uwierzytelnienia wszelkich zasobów cyfrowych osoby prawnej, takich jak kod oprogramowania lub serwery urządzenia diagnostyki obrazowej. Pieczęcie elektroniczne powinny służyć jako dowód wydania danego dokumentu elektronicznego przez daną osobę prawną dając pewność co do pochodzenia i integralności dokumentu.

W rozporządzeniu eIDAS przewidziano pieczęcie tzw. zwykłe, awansowane i kwalifikowane. Wyróżnia się w nim certyfikat i kwalifikowany certyfikat pieczęci elektronicznej, zwykłe i kwalifikowane urządzenie do składania e-pieczęci.

Rysunek 1. Podpisy i pieczęcie wg. eIDAS



Źródło: opracowanie własne

¹¹ Tamże

Zgodnie z zapisem rozporządzenia eIDAS kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana¹². Zaawansowana pieczęć elektroniczna musi spełniać następujące wymogi:

- jest unikalnie przyporządkowana podmiotowi składającemu pieczęć;
- umożliwia ustalenie tożsamości podmiotu składającego pieczęć;
- jest składana przy użyciu danych służących do składania pieczęci elektronicznej, które podmiot składający pieczęć może, mając je z dużą dozą pewności pod swoją kontrolą, użyć do złożenia pieczęci elektronicznej oraz
- jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

Usługa rejestrowanego doręczenia elektronicznego

Na podstawie definicji „usługi zaufania” można wywnioskować, że w ramach tego rodzaju funkcjonalności świadczone mogą być także usługi¹³:

- „tworzenia rejestrowanego doręczenia elektronicznego” rozumiane jako tworzenie dowodów w wyniku działania usługi eIDAS,
- „weryfikacji rejestrowanego doręczenia elektronicznego” rozumiane jako weryfikacja certyfikatów, przy wykorzystaniu/użyciu których powstały dowody usługi EDS oraz
- „walidacji rejestrowanego doręczenia elektronicznego” rozumiane jako walidacja dowodów elektronicznych, tzn. przykładowo: podpisów pod dowodami usługi EDS, prezentowanie daty i czasu zawartego w takim dowodzie, określenie nadawców i odbiorców w oparciu o dowody usługi EDS.

¹² Art. 35 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

¹³ Art. 3, pkt. 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

W rozporządzeniu eIDAS znajduje się również definicja *explicite* odnosząca się do „usług rejestrowanego doręczenia elektronicznego” oznaczająca usługę umożliwiającą przesłanie danych między stronami trzecimi drogą elektroniczną i zapewniającą dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniącą przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiegokolwiek nieupoważnionej zmiany¹⁴.

Na działanie powyższej usługi składają się następujące działania:

- przesyłanie danych,
- wystawianie dowodów powstałych na skutek posługiwania się tymi danymi (tzn. różne dowody - nie tylko dowody wysłania i otrzymania),
- tworzenie dowodów wysłania,
- tworzenie dowodów odbioru oraz
- zabezpieczanie danych przez cały okres przesyłania.

Dowody, które powstają podczas świadczenia usługi rejestrowanego doręczenia elektronicznego, można podzielić na następujące rodzaje:

- potwierdzenie dostarczenia danych do usługi,
- potwierdzenie dostarczenia przez usługę do odbiorcy informacji o oczekiwanej przesyłce,
- potwierdzenie wydane odbiorcy dotyczące faktycznego odebrania danych od usługi,
- potwierdzenie wydane nadawcy danych dotyczące faktycznego odebrania przez odbiorcę przesyłki,
- potwierdzenie wydane nadawcy o udostępnieniu przesyłki w określonym czasie i miejscu dla odbiorcy w celu odebrania w określonym momencie udostępnienia,
- potwierdzenie wydane nadawcy o odebraniu/nieodebraniu przesyłki przez odbiorcę w określonym czasie.

¹⁴ Art. 3, pkt. 36 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Mogą również powstawać inne dowody wymagane przez procesy biznesowe lub postępowania typu administracyjnego lub sądowego (przykładowo takimi dowodami mogą być raporty/poświadczenia usług walidacji lub weryfikacji certyfikatu, podpisu, pieczęci przeprowadzone do wyżej wymienionych dowodów, potwierdzenie wysłania odpowiedzi przed upłynięciem ustalonego procesem terminu, dowody co do zgodności przekazywanych konkretnych typów danych z wymaganiami lub „wzorcami”.

Minimalnym wymaganiem dla powyższych dowodów powinno być opatrzenie ich podpisem elektronicznym lub pieczęcią elektroniczną świadczącego usługę rejestrowanych doręczeń elektronicznych, a także dołączenie niezaprzeczalnych informacji o danych przekazywanych, o odpowiednich datach poszczególnych czynności oraz o danych identyfikujących nadawców i odbiorców.

Rozporządzenie eIDAS wymienia wymogi, które muszą spełniać kwalifikowane usługi rejestrowanego doręczenia elektronicznego¹⁵:

- są świadczone przez co najmniej jednego kwalifikowanego dostawcę usług zaufania,
- z dużą dozą pewności zapewniają identyfikację nadawcy,
- zapewniają identyfikację adresata przed dostarczeniem danych,
- wysłanie i otrzymanie danych jest zabezpieczone zaawansowanym podpisem elektronicznym lub zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania w taki sposób, by wykluczyć możliwość niewykrywalnej zmiany danych,
- każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy i adresatowi danych,
- data i czas wysłania, otrzymania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu.

Do powyższych wymagań dojdzie z pewnością częsta w praktyce konieczność zintegrowania z systemami płatności internetowych lub płatnościami za pośrednictwem usługi świadczonych przez operatorów telekomunikacyjnych.

¹⁵ Art. 44, ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Usługi rejestrowanych doręczeń elektronicznych już obecnie mogą być wykorzystane przy budowie rozwiązań proponowanych jako:

- pojedyncza elektroniczna skrzynka podawcza, obsługująca wskazany podmiot z ograniczonym zakresem zdefiniowanych dokumentów kierowanych do tego podmiotu; w tym przypadku powstają pojedyncze dowody nadania i odbioru,
- elektroniczna skrzynka podawcza obsługująca wiele podmiotów oraz wiele zdefiniowanych dokumentów kierowanych do tych podmiotów; w tym przypadku powstają pojedyncze dowody nadania i odbioru,
- elektroniczna usługa rejestrowanych doręczeń posiadająca określoną liczbę odbiorców i nadawców z możliwością przekazywania zarówno zdefiniowanych dokumentów, jak również dowolnych danych (e-listy, e-obrazy); w tym przypadku mogą powstawać wieloetapowe łańcuchy dowodów nadania i odbioru,
- elektroniczna usługa rejestrowanych doręczeń posiadająca określoną liczbę odbiorców i nadawców z możliwością przekazywania zarówno zdefiniowanych dokumentów, jak również dowolnych danych (e-listy, e-obrazy) oraz posiadająca możliwość korzystania z list adresowych innej elektronicznej usługi rejestrowanych doręczeń zarówno w obrębie jednego kraju, jak również kilku krajów; w tym przypadku także mogą powstawać wieloetapowe łańcuchy dowodów nadania i odbioru.

Z praktycznego punktu widzenia obecnie obowiązująca doktryna w polskim ustawodawstwie z zakresu doręczeń stanowi, że to obywatel lub podmiot mający odpowiedni obowiązek wnosi bezpośrednio dokumenty do systemów administracji i jest przy tej czynności odpowiednio identyfikowany i uwierzytelniany. Przy czym jeżeli przy takiej czynności wymagane są szczególne wzory dokumentów lub zdefiniowane formularze, to dostawca usługi zaufania rejestrowanych doręczeń elektronicznych powinien mieć możliwość korzystania w sposób nieutrudniający z tego typu wzorów i formularzy podczas świadczenia usługi.

W przypadku postępowań administracyjnych, skarbowych, cywilnych, karnych powinna być zapewniona walidacja usług rejestrowanego doręczenia elektronicznego, przedstawiająca dowody w sposób czytelny i ogólnie zrozumiały.

Po wejściu w życie rozporządzenia eIDAS nadawca dokumentów korzystający z pośrednictwa kwalifikowanej usługi doręczeń (zarówno krajowej, jak również świadczonej przez inne kraje Unii Europejskiej) będzie miał możliwość wniesienia różnego rodzaju danych

(np. pisma, e-faktury) do każdej publicznie dostępnej skrzynki mailowej administracji publicznej.

Co więcej, wniesione w ten sposób dane muszą być rozpatrzone na podstawie skutków prawnych określonych w rozporządzeniu eIDAS¹⁶. Jest w nim mowa o niemożności kwestionowania skutków prawnych danych wysłanych i otrzymanych przy użyciu usługi rejestrowanego doręczenia elektronicznego ani ich dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że dane te mają postać elektroniczną lub że nie spełniają wszystkich wymogów kwalifikowanej usługi rejestrowanego doręczenia elektronicznego.

Podobnie, jak w przypadku instytucji pieczęci elektronicznej, dane wysłane i otrzymane przy użyciu kwalifikowanej usługi rejestrowanego doręczenia elektronicznego korzystają z domniemania integralności danych, wysłania tych danych przez zidentyfikowanego nadawcę i otrzymania ich przez zidentyfikowanego adresata oraz dokładności daty i czasu wysłania i otrzymania wskazanych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego.

Obecnie zgodnie z przepisami regulującymi zasady doręczeń w administracji publicznej lub sądownictwie doręczenie dokumentu za pośrednictwem komunikacji elektronicznej odbywa się poprzez usługi, które nie są świadczone przez kwalifikowanych usługodawców. Dlatego też nie są one świadczone jako usługi zgodne z normami wprowadzanymi przez rozporządzenie eIDAS. Jako takie zatem nie będą wywoływały bezpośredniego skutku prawnego w innych krajach Unii Europejskiej. Taki skutek prawny zaistnieje, o ile urzędowe potwierdzenie odbioru będzie zawierało podpis kwalifikowany lub podpis przy użyciu pieczęci kwalifikowanej,

Wprowadzenie narzędzi takich, jak e-doręczenia czy e-konserwacja oraz tworzenie, weryfikacja i walidacja certyfikatów uwierzytelniania witryn internetowych wymagają nowych regulacji prawnych.

¹⁶ Art. 43 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

Usługi uwierzytelniania witryn internetowych

Usługi uwierzytelniania witryn internetowych¹⁷ zapewniają środki, za pomocą których odwiedzający daną witrynę internetową może być pewny, że za tą witrynę internetową stoi prawdziwy i legalnie funkcjonujący podmiot. Usługi te przyczyniają się do budowy zaufania do prowadzenia przedsiębiorstwa *online*, ponieważ użytkownicy zyskują zaufanie do witryny internetowej, która została uwierzytelniona w ten sposób.

Świadczenie i używanie usług uwierzytelniania witryny internetowej jest całkowicie dobrowolne. Jednak aby uwierzytelnianie witryny internetowej stało się środkiem wzbudzającym zaufanie, zapewniającym użytkownikowi lepsze doświadczenie i wspierającym wzrost na rynku wewnętrznym, niniejsze rozporządzenie powinno określać minimalne obowiązki w zakresie bezpieczeństwa i odpowiedzialności dla dostawców i ich usług.

Rozporządzenie eIDAS nie powinno przy tym utrudniać używania innych środków lub metod uwierzytelniania witryny internetowej nieobjętych niniejszym rozporządzeniem ani nie powinno uniemożliwiać tego, aby dostawcy usług uwierzytelniania witryn internetowych z państw trzecich świadczyli swoje usługi klientom w Unii Europejskiej. Jednak usługi uwierzytelniania witryny internetowej świadczone przez dostawcę z państwa trzeciego można uznać za kwalifikowane wyłącznie wtedy, gdy zawarta została umowa międzynarodowa między Unią Europejską, a krajem siedziby tego dostawcy.

Rozporządzenie eIDAS definiuje także pojęcie „certyfikatu uwierzytelniania witryn internetowych” jako poświadczenie, które umożliwia uwierzytelnianie witryn internetowych i przyporządkowuje witrynę internetową do osoby fizycznej lub prawnej, której wydano certyfikat. Określono również wymogi dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych¹⁸

Skutki prawne uwierzytelniania witryn internetowych proponuje się określić w prawie krajowym w ten sposób, że osoba fizyczna lub prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której ustawa nadaje zdolność prawną, którym wydano

¹⁷ Art. 67, Preambuła

¹⁸ Załącznik IV pt. „Wymogi dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych” - rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

certyfikat uwierzytelnienia witryny internetowej, traktowane są jako właściciel witryny internetowej, dla której wydano certyfikat uwierzytelnienia przyporządkowujący tę witrynę do tej osoby lub jednostki¹⁹.

Usługa konserwacji elektronicznych podpisów, pieczęci i certyfikatów

Ten element usługi zaufanej ma na celu zabezpieczenie niezaprzeczalności autorstwa i autentyczności dokumentu podpisanego kwalifikowanym podpisem elektronicznym w wymiarze czasu obecnego i przyszłego. O ile w odniesieniu do dokumentu papierowego ewentualny proceder fałszerstwa można wykryć stosunkowo łatwo za pomocą szczegółowej analizy nośnika papierowego, pieczęci, tuszu drukarskiego czy charakteru pisma, o tyle w przypadku dokumentu elektronicznego taka weryfikacja może okazać się niezwykle trudna do przeprowadzenia. Dlatego też istnieje konieczność przeprowadzania konserwacji dokumentów podpisanych elektronicznie, która sprowadza się w praktyce do cyklicznego tzw. „znakowania czasem” z wykorzystaniem coraz to nowszych algorytmów kryptograficznych. Za pomocą znaczników czasowych potwierdza się, że dokument elektroniczny istniał w danym momencie w danej formie, co pozwala zachować bezpieczeństwo takiego dokumentu. Obecne przepisy prawa polskiego wymagają przeprowadzenia takiego znakowania co 10 lat, aby dokument elektroniczny uznawany był za wiarygodny.

Zgodnie rozporządzeniem eIDAS kwalifikowaną usługę konserwacji kwalifikowanych podpisów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który stosuje procedury i technologie umożliwiające przedłużenie wiarygodności kwalifikowanego podpisu elektronicznego poza techniczny okres ważności²⁰. W innych miejscach rozporządzenia znajdują się zapisy stanowiące m.in., że „niniejsze rozporządzenie powinno zapewnić długoterminową konserwację informacji w celu zapewnienia prawnej ważności podpisów elektronicznych i pieczęci elektronicznych przez wydłużone okresy oraz zagwarantowania możliwości ich walidacji bez względu na przyszłe zmiany technologiczne”²¹, „usługa zaufania” oznacza usługę elektroniczną zazwyczaj

¹⁹ *Pejaś J., Szulga M., Wagemann M., Stolarowa-Myc A., Wiktorczyk P., Wdrożenie rozporządzenia eIDAS w Polsce – raport*, <http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Glowna-w.-4-2.pdf>

²⁰ Art. 34, ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

²¹ Art. 61, Preambuła

świadczoną za wynagrodzeniem i obejmującą: (...) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami”²².

Co istotne, w przypadku usługi konserwacji podpisów/pieczęci elektronicznych nie jest określony dokładny termin wydania aktów delegowanych i wykonawczych. Podobnie do usługi konserwacji podpisów elektronicznych nie są określone w rozporządzeniu eIDAS skutki prawne usługi konserwacji pieczęci/podpisu elektronicznego, co wymagać będzie uregulowania skutków prawnych na poziomie krajowym, a tym samym może wprowadzić różnice pomiędzy poszczególnymi państwami członkowskimi. Analizując dostępne w rozporządzeniu eIDAS zapisy dotyczące konserwacji kwalifikowanych podpisów elektronicznych, pieczęci i certyfikatów można stwierdzić, że charakteryzują się one jednym z najmniejszych poziomów precyzji uregulowań prawnych. Taki stan rzeczy z pewnością wymagać będzie dalszych prac standaryzacyjnych i legislacyjnych.

Podsumowanie

Obecnie w naszym kraju trwają procesy adaptacyjne mające na celu dostosowanie krajowych regulacji prawnych dotyczących narzędzi uwierzytelniania i autoryzacji dokumentacji do norm eIDAS odbywające się m.in. w ramach projektów ARIADNA – Dostosowanie Profilu Zaufanego do Unijnych Wymogów rozporządzenia eIDAS oraz projektu HELIOS – Integracja Rejestrów Publicznych z Wykorzystaniem Krajowej Szyny Usług²³. Zdaniem ekspertów najwcześniejszy termin powstania standardu opisującego zaufaną usługę walidacji kwalifikowanych podpisów elektronicznych i pieczęci elektronicznych to pierwszy kwartał 2019 roku.

Obecnie realizowany jest program „Od papierowej do cyfrowej Polski”, który zakłada szereg konkretnych działań wraz z harmonogramem ich realizacji. Program ten przewiduje m.in. cyfryzację kluczowych usług publicznych, zwiększenie obrotu bezgotówkowego i wdrożenie inicjatywy tożsamości elektronicznej (eID).

²² Art. 3, pkt. 16 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

²³ Źródło internetowe: <https://mac.gov.pl/aktualnosci/publiczna-prezentacja-zalozen-kolejnych-projektow-w-ramach-popc-21>

Cyfryzacja pomoże wzmocnić fundament realizacji Planu na rzecz Odpowiedzialnego Rozwoju, jakim jest sprawne państwo. Wpisuje się także w ujęte w nim poszczególne filary rozwoju, a potencjał sektora cyfrowego jest warunkiem innowacyjności i konkurencyjności polskiej gospodarki²⁴.

Literatura

- [1.] Marucha-Jaworska M., *Podpisy elektroniczne, biometria, identyfikacja elektroniczna. Elektroniczny obrót prawny w społeczeństwie cyfrowym*. Wydawnictwo Lex, Warszawa 2015
- [2.] Mielnicki T. Wołowski F., Grajek M., Popis P. Łuczak P., Tabor M., Brakoniecki M., *Identyfikacja i uwierzytelnienie w usługach elektronicznych*, Forum Technologii Bankowych przy Związku Banków Polskich, Warszawa 2013
- [3.] **Pejaś J., Szulga M., Wagemann M., Stoliarowa-Myć A., Wiktorczyk P., Wdrożenie rozporządzenia eIDAS w Polsce – raport**, <http://www.internet.pl/wp-content/uploads/2014/07/Ekspertyza-Główna-w.-4-2.pdf>
- [4.] Projekt ustawy o usługach zaufania oraz identyfikacji elektronicznej z 03.06.2016 r. - <https://legislacja.rcl.gov.pl/projekt/12283556>
- [5.] Projekt ustawy o usługach zaufania oraz identyfikacji elektronicznej z 03.06.2016 r. - <https://legislacja.rcl.gov.pl/projekt/12283556>, art. 4
- [6.] Projekt ustawy o usługach zaufania oraz identyfikacji elektronicznej (projekt 3.06.2016)
- [7.] Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2006 r. w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania Dz.U. 2006 nr 247 poz. 1819
- [8.] Rozporządzenie Ministra Zdrowia z dnia 21 grudnia 2010 r. w sprawie rodzajów i zakresu dokumentacji medycznej oraz sposobu jej przetwarzania Dz.U. 2010 nr 252 poz. 1697
- [9.] Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania Dz.U. 2006 nr 247 poz. 1819
- [10.] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr. 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE
- [11.] Stanowisko Poczty Polskiej <https://legislacja.rcl.gov.pl/docs//2/12283556/12343437/12343440/dokument216770.pdf>
- [12.] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, Dz.U. 1960 nr 30 poz. 168

²⁴ <http://televizjarepublika.pl/dowod-osobisty-aplikacja-na-smartfon-morawiecki-zapowiada-koniec-quotpapierowej-polskiquot,34815.html>

- [13.] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz.U. 2005 nr 64 poz. 565
- [14.] Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, Dz.U. 2001 nr 130 poz. 1450
- [15.] Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym. Dz.U. 2001 nr 130 poz. 1450
- [16.] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia Dz.U. 2011 nr 113 poz. 657
- [17.] Ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa, Dz.U. 1997 nr 137 poz. 926
- [18.] Ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta Dz.U. 2009 nr 52 poz. 417
- [19.] Wróbel A., [w]: *Traktat o funkcjonowaniu Unii Europejskiej*. Komentarz. Tom III pod red. D. Kornobis-Romanowskiej i J. Łacny, Warszawa 2012
- [20.] Źródło internetowe: <http://notariat.pl/wiadomosci-notariat/374-uwierzytelnianie-w-eidas-to-nie-jest-skladanie-podpisu-elektronicznego>

Streszczenie

W artykule omówiono ideę otwartych i zamkniętych usług zaufania oraz ich rodzaje. Przedstawiono koncepcję krajowej infrastruktury zaufania oraz narodowego centrum certyfikacji usług zaufania. Rozporządzenie eIDAS między innymi wprowadza zmiany w istniejących usługach np. podpis elektroniczny jak również wprowadza nowe usługi jak pieczęć elektroniczna, uwierzytelnienie witryn internetowych oraz konserwację elektronicznych podpisów, pieczęci i certyfikatów.