ACTA IURIS STETINENSIS 3 (23)

DOI:10.18276/ais.2018.23-08

Aleksandra Monarcha-Matlak*

USŁUGI ZAUFANIA I IDENTYFIKACJA ELEKTRONICZNA

Streszczenie

Rozporządzenie e-IDAS to nowy akt europejski kompleksowo regulujący zagadnienia związane z usługami zaufania i identyfikacją elektroniczną. Poszerza ono katalog usług zaufania, wprowadza jednolitą terminologię we wszystkich państwach członkowskich UE, nowe standardy, a także obowiązek uznawania i akceptacji podpisów oraz pieczęci elektronicznych w państwach członkowskich UE. Ma to na celu podniesienie poziomu bezpieczeństwa usług zaufania i zwiększenie popularności tych usług wśród obywateli UE.

Słowa kluczowe: usługi zaufania, identyfikacja elektroniczna, podpis elektroniczny, pieczęć elektroniczna

Ogólne uwagi dotyczące rozporządzenia eIDAS

Dnia 28 sierpnia 2014 roku w Dzienniku Urzędowym Unii Europejskiej opublikowane zostało rozporządzenie Parlamentu Europejskiego i Rady UE nr 910/2014 z dnia 23 lipca 2014 roku w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrz-

* dr hab. Aleksandra Monarcha-Matlak prof. US, Wydział Prawa i Administracji Uniwersytetu Szczecińskiego, adres e-mail: aleksandra.monarcha-matlak@usz.edu.pl

nym oraz uchylające dyrektywę 1999/93/WE (DZ. Urz. UE L z dnia 28 sierpnia 2014 r.) zwane dalej rozporządzeniem eIDAS. Rozporządzenie to wraz z systemem aktów delegowanych i implementujących zastąpiło dyrektywę 1999/93/ w sprawie wspólnotowych ram prawnych dla podpisów elektronicznych oraz krajowe przepisy wszystkich państw członkowskich w zakresie regulowanym eIDAS.

Celem podstawowym nowej regulacji było wprowadzenie nowych standardów oraz podniesienie poziomu bezpieczeństwa usług zaufania, a także zwiększenie popularności usług wśród obywateli UE. Drugim ważnym celem było ujednolicenie przepisów obowiązujących w państwach Unii Europejskiej, dla zapewnienia integracyjności i transgraniczności tych usług, w tym podpisów elektronicznych. Rozporządzenie eIDAS ma przede wszystkim harmonizować europejski rynek cyfrowy w oparciu o usługi zaufania i identyfikację elektroniczną.

Rozporządzenie eIDAS wprowadza do europejskiego porządku prawnego zamknięty katalog unijnych usług zaufania. Jako „usługę zaufania" rozporządzenie określa usługę elektroniczną, zazwyczaj świadczoną za wynagrodzeniem i obejmującą: 1) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usługę rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami, lub 2) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych, lub 3) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami. Polskiemu prawu znane były dotychczas tylko podpisy elektroniczne oraz znakowanie czasem.

Natomiast „identyfikacja elektroniczna" to proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną i prawną lub osobę fizyczną reprezentującą osobę prawną.

Przytoczone wyżej definicje uprawniają do przedstawienia jeszcze jednej definicji, ściśle powiązanej z usługami zaufania, mianowicie „dokumentu elektronicznego". Nie ulega wątpliwości, że dokument elektroniczny ma szczególne znaczenie dla elektronicznego obrotu gospodarczego. Zgodnie z motywem 63 rozporządzenia eIDAS, dokumenty elektroniczne są ważne dla dalszego rozwoju transgranicznych transakcji elektronicznych na rynku wewnętrznym. Rozporządzenie wprowadziło zasadę, że nie należy kwestionować skutku prawnego dokumentu elektronicznego z tego powodu, że dokument ten ma postać elektroniczną. Należy dopilnować, aby transakcja elektroniczna nie została odrzucona wyłącznie z tego powodu, że dokument ma postać elektroniczną. Zgodnie

z art. 3 pkt 35 rozporządzenia eIDAS, dokument elektroniczny oznacza każdą treść przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne. Prawodawca unijny nie wskazuje nośnika, na jakim dokument powinien zostać utrwalony, pozostawia w tym zakresie swobodę wyboru.

We wstępie rozporządzenia wskazano, że jego głównym założeniem jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym przez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług *on-line*, e-biznesu, e-handlu w Unii Europejskiej. Rozporządzenie eIDAS ma ułatwić korzystanie z usług administracji publicznej oraz zwiększyć ich dostępność, określa ramy prawne dla podpisów elektronicznych, pieczęci elektronicznych, elektronicznych znaczników czasu, dokumentów elektronicznych, usług rejestrowanego doręczenia elektronicznego oraz usług certyfikacyjnych uwierzytelniania witryn internetowych.

Rozporządzenie bezpośrednio obowiązuje we wszystkich krajach członkowskich UE, bez potrzeby dokonywania jakichkolwiek czynności wdrażających. W preambule rozporządzenia wskazano, że budowanie zaufania do środowiska *on-line* jest kluczowe dla rozwoju gospodarczego i społecznego. Brak zaufania, spowodowany przede wszystkim odczuwanym brakiem pewności prawa, sprawia, że konsumenci, organy publiczne i przedsiębiorstwa wahają się, czy przeprowadzać transakcje elektroniczne i wdrażać nowe usługi.

Dotychczas obywatele UE nie mogli korzystać ze swojej identyfikacji elektronicznej w celu uwierzytelniania się w innym państwie członkowskim, ponieważ krajowe systemy identyfikacji elektronicznej nie były uznawane w pozostałych krajach członkowskich. Taka bariera elektroniczna nie pozwalała dostawcom usług na korzystanie z rynku wewnętrznego. Dopiero wzajemnie uznawane środki identyfikacji elektronicznej pozwolą na transgraniczne świadczenie usług i kontakty z organami publicznymi. Celem nie jest ingerowanie w systemy zarządzania tożsamością elektroniczną i w powiązane z nimi infrastruktury ustanowione w państwach członkowskich, ale zapewnienie bezpiecznej elektronicznej identyfikacji i uwierzytelniania na potrzeby dostępu do transgranicznych usług *on-line* oferowanych przez państwa członkowskie (motyw 12 rozporządzenia eIDAS). Rozporządzenie określa ogólne ramy prawne dotyczące korzystania z usług zaufania, nie dotyczy świadczenia usług wykorzystywanych wyłącznie w obrębie systemów zamkniętych przez określoną grupę uczestników

i niemających skutków dla stron trzecich, nie dotyczy także zarządzania procedurami wewnętrznymi przy użyciu usług zaufania.

Rozporządzenie eIDAS w art. 25, 35, 41, 43 wskazuje podstawowe zasady związane z usługami zaufania, tzn. podpisami elektronicznymi, pieczęciami elektronicznymi, elektronicznymi znacznikami czasu, usługami rejestrowanego doręczenia elektronicznego oraz dokumentami elektronicznymi[1]. Są to następujące zasady:

1. niedyskryminacji podpisów, pieczęci elektronicznych, elektronicznych znaczników czasu, usług rejestrowanego doręczenia, dokumentów elektronicznych,
2. równoważności kwalifikowanego podpisu elektronicznego z podpisem własnoręcznym,
3. domniemania integracyjności danych i autentyczności pochodzenia tych danych, z którymi powiązana jest kwalifikowana pieczęć elektroniczna,
4. domniemania dokładności daty i czasu oraz integralności danych, jakie wskazuje kwalifikowany znacznik czasu,
5. wzajemnego uznawania kwalifikowanych podpisów, kwalifikowanych pieczęci, kwalifikowanych elektronicznych znaczników czasu,
6. domniemania integralności danych, dokładności daty i czasu wskazanych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego.

Prawodawca europejski wprowadził także zasady, które mają służyć osiągnięciu wyznaczonych celów w rozporządzeniu eIDAS, w tym usunięcie barier prawnych, zapewnienie bezpieczeństwa usług oraz wzajemne uznawanie usług zaufania, takich jak podpisy, certyfikaty, pieczęcie elektroniczne, elektroniczne znaczniki czasu, dokumenty elektroniczne[2]. Ustanowił m.in. następujące zasady:

1. niedyskryminacji usług zaufania,
2. neutralności technologicznej,
3. równoważności kwalifikowanego podpisu elektronicznego z podpisem własnoręcznym,
4. wzajemnego transgranicznego uznawania kwalifikowanych podpisów, pieczęci i znaczników czasu,
5. wzajemnego transgranicznego uznawania notyfikowanych systemów identyfikacji elektronicznej,
6. międzynarodowego uznawania usług zaufania oraz równego dostępu do tych usług,

[1] M. Marucha-Jaworska, *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Warszawa 2017, s. 49 i n.

[2] *Ibidem*, s.47 i n.

7. zaufania do poziomów bezpieczeństwa,
8. bezpieczeństwa i ciągłości transgranicznej opieki zdrowotnej,
9. zgodności z regulacjami dotyczącymi ochrony danych osobowych.

Rozporządzenie eIDAS jest dosyć skomplikowanym aktem prawnym regulującym różne aspekty, zarówno prawne, jak i techniczne oraz organizacyjne dotyczące usług zaufania, transakcji elektronicznych i identyfikacji elektronicznej. Różne są także w rozporządzeniu eIDAS terminy, samo rozporządzenie weszło w życie 17 września 2014 roku. Natomiast 1 lipca 2016 roku uchylona została dyrektywa 1999/93/WE, od tego dnia obowiązuje większość przepisów dotyczących usług zaufania, a także przestała obowiązywać polska ustawa z dnia 18 września 2001 r. o podpisie elektronicznym[3]. Od 29 września 2018 roku obowiązywać będzie wzajemne uznawanie przez państwa członkowskie notyfikowanych systemów identyfikacji elektronicznej.

Usługi zaufania

„Usługa zaufania" jest w polskim i europejskim porządku prawnym zupełnie nowym terminem, nie był on użyty w polskiej ustawie o podpisie elektronicznym, polskiej Konstytucji, ani też dyrektywie unijnej 1999/93/WE. Prawodawca unijny zdecydował się na wydanie jednej regulacji, która obejmuje kilka usług zaufania. W polskim prawie uregulowana w pełni była jedynie instytucja podpisu elektronicznego oraz znakowanie czasem. Rozporządzenie eIDAS poszerzyło gamę dostępnych usług zaufania oraz nałożyło na państwa członkowskie obowiązek ustanowienia nadzoru. Rozporządzenie mówi o podpisie elektronicznym, zaawansowanym podpisie elektronicznym oraz kwalifikowanym podpisie elektronicznym, natomiast polska ustawa wymieniała: podpis elektroniczny, bezpieczny podpis elektroniczny oraz bezpieczny podpis elektroniczny weryfikowany ważnym kwalifikowanym certyfikatem. W związku z ujednoliceniem terminologii na poziomie europejskim również porządek krajowy musiał być do niej dostosowany.

W tym miejscu nasuwa się jednak pewna uwaga. Termin „usługa zaufania" nie został zdefiniowany w polskiej ustawie, jest on kolejnym przykładem nieporadności ustawodawcy. Nie wiadomo, co on właściwie oznacza, jest niezgodny z Konstytucją, niezgodny z zasadami poprawnej legislacji oraz zasadami języka polskiego. Podobnie jak w innych aktach prawnych, gdzie fatalne tłumaczenia podstawowych pojęć

[3] Komunikat z dnia 30 czerwca 2016 r. Narodowego Centrum Certyfikacji (NCCert), Dz.U. z 2013 r., poz. 262 z późn. zm.

powodowało spore zamieszanie terminologiczne, np. ICT, czyli „technologie informacyjno-komunikacyjne", tłumaczono jako technologie informatyczne, czy też pojęcie „komunikacji elektronicznej" zastępowano pojęciem „łączności elektronicznej".

Zgodnie z rozporządzeniem eIDAS (art. 3 pkt 16) usługa zaufania oznacza usługę elektroniczną obejmującą podpisy elektroniczne, pieczęci elektroniczne, elektroniczne znaczniki czasu, usługę rejestrowanego doręczenia elektronicznego, uwierzytelniania witryn internetowych, certyfikaty zawiązane z tymi usługami. W związku z przyjętą klasyfikacją zachodzi potrzeba bliższego określenia poszczególnych usług zaufania. Zgodnie z motywem 25 i 26 rozporządzenia eIDAS, państwa członkowskie powinny zachować swobodę określania innych rodzajów usług zaufania, oprócz tych, które znajdują się w zamkniętym wykazie usług zaufania zawartych w rozporządzeniu, do celów uznania ich na szczeblu krajowym jako kwalifikowanych usług zaufania. Jednocześnie ze względu na tempo zmian technologicznych należy przyjąć podejście otwarte na innowacje.

Podpisy elektroniczne

Rozporządzenie eIDAS wymienia trzy rodzaje podpisów elektronicznych (art. 3 pkt 10–12): podpis elektroniczny, zaawansowany podpis elektroniczny, kwalifikowany podpis elektroniczny. Wymienione podpisy mogą być złożone wyłącznie przez podpisującego, czyli osobę fizyczną.

„Podpis elektroniczny" jest najprostszym podpisem oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis (art. 3 pkt 10). Ustawodawca unijny wskazuje, że podpis nie służy do identyfikacji elektronicznej ani uwierzytelniania osoby fizycznej. Dane w postaci elektronicznej muszą być użyte jako podpis.

Drugi rodzaj podpisu, czyli „zaawansowany podpis elektroniczny" (art. 3 pkt 11), jest podpisem elektronicznym, który spełnia następujące wymogi określone w art. 26 rozporządzenia: jest unikalnie przyporządkowany podpisującemu, umożliwia ustalenie tożsamości podpisującego, jest składany przy użyciu danych służących do składania podpisu elektronicznego, których podpisujący może, z dużą dozą pewności, użyć pod wyłączną swoją kontrolą, oraz jest powiązany z danymi w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna. Dlatego też nie można używać zwrotu „dokument uwierzytelniony podpisem elektronicznym". Zaawansowany podpis elektroniczny jest podpisem o wystarczającym poziomie

bezpieczeństwa w relacjach usługobiorca a usługodawca[4]. Certyfikat, który służy do składania takiego podpisu, może być przechowywany na kartach kryptograficznych, może być także stosowany system jednorazowych kodów przesyłanych SMS-em pod numer telefonu właściciela podpisu, natomiast usługodawca takiej usługi określa poziom bezpieczeństwa podpisu jako wystarczający. Zaawansowany podpis elektroniczny według rozporządzenia to odpowiednik „bezpiecznego podpisu elektronicznego" według polskiej, nieobowiązującej już ustawy o podpisie elektronicznym z 2001 roku.

Trzeci podpis to „kwalifikowany podpis elektroniczny", najbardziej zawansowany technologicznie, oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego (art. 3 pkt 12). Kwalifikowany certyfikat wydawany jest przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku I rozporządzenia eIDAS. Kwalifikowany podpis elektroniczny, o którym mówi rozporządzenie eIDAS, to odpowiednik polskiego „bezpiecznego podpisu elektronicznego weryfikowanego za pomocą kwalifikowanego certyfikatu" obowiązującego do czasu wejścia w życie rozporządzenia eIDAS. Podobnie jak ten podpis „kwalifikowany podpis elektroniczny" ma skutek prawny równoważny podpisowi własnoręcznemu. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym z państw członkowskich musi być uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich (art. 25 ust 1 i 2).

Pieczęcie elektroniczne

„Pieczęć elektroniczna" oznacza dane w postaci elektronicznej dodane do innych danych w postaci elektronicznej lub logicznie z nimi powiązane, aby zapewnić autentyczność pochodzenia oraz integralność powiązanych danych (art. 3 pkt 25 rozporządzenia eIDAS). Pieczęć elektroniczna związana jest z osobą prawną i jest przeznaczona dla osób prawnych, nie jest jednak podpisem elektronicznym. Podpis elektroniczny może złożyć wyłącznie osoba fizyczna. Pojęcie „osób prawnych" zgodnie z postanowieniami Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) dotyczącymi prowadzenia przedsiębiorstwa pozostawia podmiotom gospodarczym

[4] Szerzej *ePodręcznik, e-usługi publiczne*, https://epodrecznik.mac.gov.pl/ (dostęp 9.09.2017).

swobodę wyboru formy prawnej, którą uznają za odpowiednią dla prowadzenia swojej działalności. Dlatego też termin „osoby prawne" w rozumieniu TFUE oznacza wszystkie podmioty ustanowione na mocy prawa państwa członkowskiego lub podlegające temu prawu, niezależnie od ich formy prawnej. Rozporządzenie eIDAS wyróżnia trzy rodzaje pieczęci: pieczęć elektroniczną, zaawansowaną pieczęć elektroniczną, kwalifikowaną pieczęć elektroniczną (art. 3 pkt 25, 26 i 27).

Pieczęć elektroniczna

Pieczęć elektroniczna zgodnie z rozporządzeniem, służy zapewnieniu integralności i autentyczności. Pieczęć elektroniczna powinna służyć jako dowód wydania dokumentu elektronicznego przez daną osobę prawną, dając pewność co do pochodzenia i integralności dokumentu (motyw 59 rozporządzenia eIDAS). Pieczęć elektroniczna może być używana nie tylko do uwierzytelniania dokumentu wydanego przez osobę prawną, lecz również do uwierzytelniania wszelkich zasobów cyfrowych osoby prawnej, takich jak kod oprogramowania lub serwery (motyw 65 rozporządzenia eIDAS).

Zaawansowana pieczęć elektroniczna

Zaawansowana pieczęć elektroniczna, oznacza pieczęć elektroniczną, która spełnia następujące wymogi określone w art. 36 rozporządzenia eIDAS: jest unikalnie przyporządkowana podmiotowi składającemu pieczęć; umożliwia ustalenie tożsamości podmiotu składającego pieczęć; jest składana przy użyciu danych służących do składania pieczęci elektronicznej, których podmiot składający pieczęć może (mając je z dużą dozę 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. Brak jest w rozporządzeniu określenia, w jaki sposób składający taką pieczęć może sprawować kontrolę nad danymi służącymi do jej składnia.

Kwalifikowana pieczęć elektroniczna

Kwalifikowana pieczęć elektroniczna zgodnie z art. 3 pkt 27 rozporządzenia eIDAS oznacza zaawansowaną pieczęć elektroniczną, która została złożona za

pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej i która opiera się na kwalifikowanym certyfikacie pieczęci elektronicznej. Zgodnie z motywem 58 rozporządzenia eIDAS, gdy transakcja wymaga od osoby prawnej użycia kwalifikowanej pieczęci elektronicznej, akceptowalny powinien być również kwalifikowany podpis elektroniczny upoważnionego przedstawiciela osoby prawnej. Przy czym dostawcy usług zaufania wydający kwalifikowane certyfikaty pieczęci elektronicznych powinni wdrożyć niezbędne środki pozwalające na ustalenie tożsamości osoby fizycznej reprezentującej osobę prawną, której świadczony jest kwalifikowany certyfikat pieczęci elektronicznej, jeżeli taka identyfikacja jest niezbędna na szczeblu krajowym w związku z postępowaniami sądowymi lub administracyjnymi (motyw 60 rozporządzenia eIDAS). Kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana (art. 35 ust. 2 eIDAS). Zgodnie z art. 35 ust. 3 kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach.

Pieczęć elektroniczna może być wykorzystywana w usługach publicznych. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej do skorzystania z usługi *on-line* oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane pieczęcie elektroniczne, zaawansowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie pieczęci elektronicznych i kwalifikowane pieczęcie elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych[5].

Elektroniczne znaczniki czasu

Elektroniczny znacznik czasu jest odpowiednikiem daty pewnej w prawie cywilnym (potwierdza czas dokonanej czynności). Uniemożliwia on antydatowanie dokumentów elektronicznych. Elektroniczny znacznik czasu oznacza dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z okre-

[5] D. Szostek, *Pieczęć elektroniczna i możliwości jej wykorzystania w polskim prawie*, w: *Media elektroniczne. Współczesne problemy prawne*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Legalis C.H. Beck 2016. (dostęp 30.05.2018 r) oraz J. Gołaczyński, D. Szostek, *Czy pieczęć elektroniczna ma szansę usprawnić administrację?*, „Monitor Prawniczy" 2009, nr 5, s. 278 i n.

ślonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie (art. 3 pkt 33 eIDAS).

Kwalifikowany elektroniczny znacznik czasu

Kwalifikowany elektroniczny znacznik czasu oznacza elektroniczny znacznik czasu, który spełnia następujące wymogi: wiąże on datę i czas z danymi tak, aby w wystarczający sposób wykluczyć możliwość niewykrywalnej zmiany danych; oparty jest na precyzyjnym źródle czasu powiązanym z uniwersalnym czasem koordynowanym; jest podpisany przy użyciu zaawansowanego podpisu elektronicznego lub opatrzony zaawansowaną pieczęcią elektroniczną kwalifikowanego dostawcy usług zaufania lub w inny równoważny sposób.

Nie można kwestionować skutku prawnego elektronicznego znacznika czasu ani jego dopuszczalności w postępowaniu sądowym tylko dlatego, że znacznik ten ma postać elektroniczną lub że nie spełnia wymogów kwalifikowanego elektronicznego znacznika czasu. Kwalifikowany elektroniczny znacznik czasu korzysta z domniemania dokładności daty i czasu, jakie wskazuje, oraz integralności danych, z którymi wskazana data i czas są połączone. Znacznik ten wydany w jednym państwie jest uznawany za kwalifikowany elektroniczny znacznik czasu we wszystkich państwach członkowskich (art. 41 rozporządzenia eIDAS).

Usługi rejestrowanego doręczenia elektronicznego

Usługa rejestrowanego doręczenia elektronicznego jest nową usługą, nieznaną dotychczas ani prawu europejskiemu, ani też prawu polskiemu. Artykuł 3 pkt 36 rozporządzenia eIDAS stanowi, że jest to usługa umożliwiająca przesyłanie danych miedzy stronami trzecimi drogą elektroniczną i zapewniająca dowody związane z posługiwaniem się przesyłanymi danymi, w tym dowód wysłania i otrzymania danych, oraz chroniąca przesyłane dane przed ryzykiem utraty, kradzieży, uszkodzenia lub jakiejkolwiek nieupoważnionej zmiany.

Kwalifikowana usługa rejestrowanego doręczenia elektronicznego

Prawodawca unijny w art. 44 rozporządzenia eIDAS wyraźnie wyodrębnia kwalifikowane usługi rejestrowanego doręczenia elektronicznego, wskazując

jednocześnie wymagania, które mają one spełniać: muszą być świadczone przez co najmniej jednego kwalifikowanego dostawcę usług zaufania; z dużą dozą pewności zapewniają identyfikację nadawcy; zapewniają identyfikację adresata przed dostarczeniem danych; wysyłanie i otrzymywanie 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 wysyłania lub otrzymywania danych jest wyraźnie wskazana nadawcy i adresatowi danych; data i czas wysyłania, otrzymywania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu.

Skutek prawny usługi rejestrowanego doręczenia elektronicznego

Podobnie jak przy wyżej wymienionych usługach zaufania, zgodnie z zasadą niedyskryminowania, także przy tej usłudze nie jest kwestionowany skutek prawny danych wysyłanych i otrzymywanych przy użyciu usługi rejestrowanego doręczenia elektronicznego ani ich dopuszczalność 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 (art. 43 ust 1 rozporządzenia eIDAS). Z kolei z uwagi na istotne znaczenie kwalifikowanych usług zaufania, także dane otrzymywane i wysyłane przy użyciu kwalifikowanej usługi rejestrowanego doręczenia elektronicznego korzystają z domniemania integracyjności danych, wysyłania tych danych przez zidentyfikowanego nadawcę i otrzymywania ich przez zidentyfikowanego adresata oraz dokładności daty i czasu wysyłania oraz otrzymania wskazanych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego.

Uwierzytelnianie witryn internetowych

W sekcji 8 rozporządzenia eIDAS zatytułowanej „uwierzytelnianie witryn internetowych" w art. 45 wskazano, że kwalifikowane certyfikaty uwierzytelniania witryn internetowych muszą spełniać wymogi określone w załączniku IV. Certyfikat uwierzytelniania witryn internetowych oznacza poświadczenie, które umożliwia ich uwierzytelnianie i przyporządkowuje witrynę internetową do

osoby fizycznej lub prawnej, której wydano certyfikat. Zgodnie z art. 3 pkt 39 rozporządzenia eIDAS, „kwalifikowany certyfikat uwierzytelniania witryn internetowych" oznacza certyfikat uwierzytelniania witryn internetowych, który jest wydawany przez kwalifikowanego dostawcę usług zaufania i spełnia wymogi określone w załączniku IV. Są to: 1) wskazanie co najmniej w postaci pozwalającej na automatyczne przetwarzanie, że dany certyfikat został wydany jako kwalifikowany; 2) zestaw danych jednoznacznie reprezentujących kwalifikowanego dostawcę usług zaufania wydającego kwalifikowane certyfikaty, obejmujący co najmniej jedno państwo członkowskie, w którym dostawca ma siedzibę, oraz w odniesieniu do osoby prawnej nazwę i numer rejestrowy, natomiast w odniesieniu do osoby fizycznej: imię i nazwisko tej osoby; 3) w odniesieniu do osób fizycznych, co najmniej imię i nazwisko, której wydano certyfikat, lub pseudonim (wtedy wymaga to wyraźnego wskazania), w odniesieniu do osób prawnych, co najmniej nazwę osoby prawnej, której wydano certyfikat oraz numer rejestrowy zgodnie z oficjalnym rejestrem; 4) elementy adresu, co najmniej miasto i państwo; 5) nazwy domen, którymi posługuje się osoba fizyczna lub prawna, której wydano certyfikat; 6) dane dotyczące początku i końca okresu ważności certyfikatu; 7) kod identyfikacyjny certyfikatu; 8) zaawansowany podpis elektroniczny lub zaawansowana pieczęć elektroniczna wydającego kwalifikowanego dostawcy usług zaufania; 9) miejsce, w którym nieodpłatnie dostępny jest certyfikat towarzyszący zaawansowanemu podpisowi elektronicznemu lub zaawansowanej pieczęci elektronicznej; 10) miejsce usług statusu ważności certyfikatu, z których można skorzystać w celu złożenia zapytania o status ważności kwalifikowanego certyfikatu.

Polska ustawa z dnia 5 września 2016 roku o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. z 2016 r., poz 1579)

Wejście w życie 1 lipca 2016 roku rozporządzenia eIDAS spowodowało zmiany w porządku prawnym w obszarze usług zaufania i identyfikacji elektronicznej oraz zrodziło konieczność dostosowania prawa krajowego do nowych uwarunkowań. Dotychczasowe rozwiązania prawne nie przystawały do nowej sytuacji, stąd zrodziła się potrzeba uchylenia m.in. ustawy z 2001 roku o podpisie elektronicznym oraz dokonania nowelizacji wielu aktów rangi ustawowej. Zmianie uległa także siatka pojęciowa – oprócz znanych dotychczas prawu polskiemu terminów, takich jak podpis elektroniczny, znaczniki czasu, pojawiły się takie

pojęcia, jak: usługi zaufania, zaawansowany i kwalifikowany podpis elektroniczny, pieczęć elektroniczna, kwalifikowany znacznik czasu, uwierzytelnianie witryn internetowych, środki identyfikacji elektronicznej.

Prawodawca unijny zdecydował się na wydanie jednej regulacji dotyczącej usług zaufania, niektóre z nich są uregulowane w sposób cząstkowy inne uregulowano obszerniej. Celem polskiego ustawodawcy jest ustanowienie przepisów w odniesieniu do zagadnień wskazanych przez eIDAS jako pozostających w kompetencji państw członkowskich oraz dokonanie koniecznych zmian w aktach rangi ustawowej dla prawidłowego zrealizowania rozporządzenia eIDAS. Prace prowadzone są etapowo ze względu na szczególne wymagania techniczne dla niektórych nowych usług zaufania. Celem ustawy jest zminimalizowanie ryzyka kolizji polskich przepisów z rozporządzeniem eIDAS. Prawodawca unijny pozostawia także w niektórych obszarach swobodę dla regulacji prawa krajowego. Część przepisów ustawy o usługach zaufania wejdzie w życie 29 września 2018 roku.

Ustawa o usługach zaufania oraz identyfikacji elektronicznej (dalej u.u.z) w art. 1 ust 1 określa: krajową infrastrukturę zaufania; działalność dostawców usług zaufania, w tym zawieszania certyfikatów podpisów elektronicznych i pieczęci elektronicznych; tryb notyfikacji krajowego systemu identyfikacji elektronicznej; nadzór nad dostawcami usług zaufania. Jednocześnie w art. 1 ust 2 wyraźnie wskazuje, że przepisów ustawy nie stosuje się do identyfikacji elektronicznej lub świadczenia usług zaufania wykorzystywanych wyłącznie w zamkniętych systemach wynikających z przepisów prawa, porozumień lub umów zawartych przez określoną grupę uczestników.

W celu zapewnienia ciągłości świadczonych usług zaufania polski ustawodawca uznaje, że bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu w rozumieniu ustawy o podpisie elektronicznym jest obecnie kwalifikowanym podpisem elektronicznym w rozumieniu ustawy o usługach zaufania i identyfikacji elektronicznej (art.131 u.u.z.). Natomiast usługę znakowania czasem, o której mowa w ustawie o podpisie elektronicznym, uznaje się za usługę elektronicznego znacznika czasu zgodnie z ustawą o usługach zaufania (art. 133 ust 1, 2 i 3). Również w celu zapewnienia ciągłości świadczeń ważność zachowują przez okres w nich wskazany, o ile nie zostaną unieważnione, zaświadczenia certyfikacyjne, poświadczenia elektroniczne i certyfikaty wydane zgodnie z ustawą o podpisie elektronicznym (art. 132 ust 1). Do wyżej wymienionych zaświadczeń, poświadczeń, certyfika-

tów, stosuje się odpowiednio przepisy dotyczące certyfikatów krajowych dostawców usług zaufania oraz narodowego centrum certyfikacji (art. 132 ust 2 u.u.z).

Krajowa infrastruktura zaufania

Zgodnie z art. 2 u.u.z. minister właściwy do spraw informatyzacji zapewnia funkcjonowanie krajowej infrastruktury zaufania, która obejmuje:

1. Rejestr dostawców usług zaufania – rejestr jest prowadzony w postaci elektronicznej, jest jawny, każdy ma prawo dostępu do danych zawartych w rejestrze. Do rejestru wpisuje się dostawców usług zaufania, którzy mają siedzibę lub oddział na terytorium Polski oraz usługi zaufania przez nich świadczone.
2. Zaufaną listę – prowadzi ją minister właściwy do spraw informatyzacji, jest ona publikowana na stronie Narodowego Centrum Certyfikacji. Zawiera informacje dotyczące kwalifikowanych dostawców usług zaufania wraz z informacjami dotyczącymi ich usług[6]. Zaufana lista jest ważnym elementem budowania zaufania na europejskim rynku usług zaufania, umożliwia ustalenie statusu kwalifikowanych dostawców usług zaufania[7].
3. Narodowe Centrum Certyfikacji – to system informatyczny Narodowego Banku Polskiego, zbudowany w celu realizacji zadań powierzonych NBP przez ministra właściwego do spraw informatyzacji, zgodnie z ustawą o usługach zaufania. Narodowe Centrum Certyfikacji tworzy i wydaje kwalifikowanym dostawcom usług zaufania certyfikaty służące do weryfikacji zaawansowanych podpisów elektronicznych lub pieczęci elektronicznych, publikuje certyfikaty, publikuje listy unieważnionych certyfikatów, tworzy dane do opatrywania pieczęcią elektroniczną certyfikatów oraz certyfikatów

[6] Zgodnie z art. 22 rozporządzenia eIDAS, każde państwo członkowskie prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za które jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nie usług zaufania. Państwa członkowskie sporządzają, prowadzą i publikują – w zabezpieczony sposób – elektronicznie podpisane lub opatrzone pieczęcią zaufane listy w postaci dostosowanej do automatycznego przetwarzania. Następnie państwa członkowskie przekazują Komisji informacje o podmiocie odpowiedzialnym za sporządzenie, publikowanie listy zaufania wraz z informacjami szczegółowymi dotyczącymi miejsca publikacji tych list. Decyzja wykonawcza Komisji UE 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady UE nr 10/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. (Dz. Urz. UE. L z dnia 9 września 2015 r., nr 235, s. 26).

[7] Szerzej M. Marucha-Jaworska, *op. cit.*, s. 158 i n.

do weryfikacji tych pieczęci. Narodowe Centrum Certyfikacji realizuje zadania zgodnie z polityką certyfikacji[8].

Identyfikacja elektroniczna

Zgodnie z art. 3 pkt. 1 rozporządzenia eIDAS, „identyfikacja elektroniczna" oznacza proces używania danych w postaci elektronicznej identyfikujących osobę, unikalnie reprezentujących osobę fizyczną lub prawną lub osobę fizyczną reprezentującą osobę prawną. Identyfikacja elektroniczna jest początkiem procesu „identyfikacja i uwierzytelnianie", jest to deklaracja tożsamości, zaprezentowanie unikalnej cechy identyfikującej osobę, czyli elektroniczne przedstawienie się[9]. Drugim etapem procesu identyfikacji i uwierzytelniania jest uwierzytelnienie, czyli potwierdzenie autentyczności zadeklarowanego wcześniej identyfikatora, potwierdzenie prawidłowości identyfikacji, a następnie tożsamości. Rozporządzenie eIADS stanowi, że „uwierzytelnienie" oznacza proces elektroniczny umożliwiający identyfikację elektroniczną osoby fizycznej lub prawnej lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej. Tylko pozytywny wynik uwierzytelniania pozwala na przejście do kolejnego etapu, czyli autoryzacji, która polega na określeniu, czy uwierzytelniona tożsamość jest uprawniona do korzystania z danego zasobu oraz w jakim zakresie. W ramach tych procesów konieczne są dane identyfikujące osobę oraz środki identyfikacji elektronicznej. „Dane identyfikujące osobę" oznaczają zestaw danych umożliwiających ustalenie tożsamości osoby fizycznej lub prawnej lub osoby fizycznej reprezentującej osobę prawną. Podstawowe dane identyfikujące to nazwisko i imię, w związku z tym, że często się powtarzają, należy podawać dodatkowo informacje szczegółowe, np. aktualny adres, datę urodzenia, miejsce urodzenia, płeć.

Środki identyfikacji elektronicznej oznaczają materialne lub niematerialne jednostki zawierające dane identyfikujące osobę i używane do celów uwierzytelniania dla usługi *on-line*. Nowością zawartą w rozporządzeniu jest zasada wzajemnego uznawania i akceptowania środków identyfikacji elektronicznej dla usług zaufania, w przypadkach gdy identyfikacja elektroniczna jest wymagana.

---

[8] Rozporządzenie ministra cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania (Dz.U. z 2016 r., poz. 1632).

[9] T. Mielnicki, F. Wołowski, M. Grajek, P. Popis, *Identyfikacja i uwierzytelnianie w usługach elektronicznych*, Warszawa 2013, s.106 i n.

Wzajemnie uznawane środki identyfikacji elektronicznej ułatwią transgraniczne świadczenie licznych usług na rynku wewnętrznym i umożliwią przedsiębiorstwom prowadzenie działalności za granicą bez konieczności zmagania się z przeszkodami w kontaktach z organami publicznymi. Dzięki identyfikacji elektronicznej sprawniej może następować realizacja usług *on-line*. Osoba posiadająca środek identyfikacji elektronicznej (strona ufająca) wydany w jednym państwie członkowskim może skorzystać z publicznych usług *on-line* w innych krajach. Wiele usług *on-line* nie musi wymagać podpisu elektronicznego, wystarczy, że osoba fizyczna posługująca się określonymi danymi identyfikującymi zostanie dobrze i bez wątpliwości rozpoznana przez system teleinformatyczny, będzie mogła skorzystać z wielu usług oferowanych w ramach systemu, bez podpisywania dokumentów elektronicznych, wydając jedynie określone dyspozycje.

System identyfikacji elektronicznej (czyli system, w ramach którego wydaje się środki identyfikacji elektronicznej osobom fizycznym i prawnym oraz osobom fizycznym je reprezentującym) identyfikując określoną osobę, musi zapewnić pewność tej identyfikacji. Zależy od tego bezpieczeństwo usług *on-line*. W zależności od rodzaju usług różny jest poziom bezpieczeństwa identyfikacji elektronicznej. Stosownie do art. 6 rozporządzenia eIDAS, żeby skorzystać z usług *on-line*, poziom bezpieczeństwa środka identyfikacji elektronicznej musi być równy lub wyższy od poziomu wymaganego na potrzeby dostępu do tej usługi. Oznacza to, że osoba korzystająca z niższego niż wymagany poziom bezpieczeństwa nie będzie mogła skorzystać z usługi wymagającej wyższego poziomu bezpieczeństwa. W art. 8 rozporządzenia eIDAS wskazano trzy poziomy bezpieczeństwa: niski, średni i wysoki, oraz kryteria, jakie muszą być spełnione. Wymienione stopnie bezpieczeństwa są określane w odniesieniu do technicznych specyfikacji, standardów, procedur powiązanych ze środkami identyfikacji elektronicznej, w tym zabezpieczeń technicznych, których celem jest zapobieganie fałszowaniu lub modyfikacji tożsamości[10].

Zgodnie z art. 12 „współpraca i interoperacyjność" rozporządzenia eIDAS, krajowe systemy identyfikacji elektronicznej notyfikowane na podstawie art. 9 ust. 1 muszą być interoperacyjne, w tym celu ustanowiono ramy interope-

[10] Rozporządzenie wykonawcze Komisji (UE) nr 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. (Dz. Urz. UE. L nr 235, s. 7; zm. Dz. Urz. UE. L 2016 r., nr 345, s. 42).

racyjności oraz ich kryteria. Szczegółowe ramy interoperacyjności ujęto w rozporządzeniu wykonawczym Komisji UE 2015/1501[11].

Współpraca między państwami członkowskimi w zakresie interoperacyjności i bezpieczeństwa systemów identyfikacji elektronicznej ma zasadnicze znaczenie dla zapewnienia wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka występującego w tych systemach. Współpraca między państwami wymaga uproszczonych procedur, interoperacyjności i bezpieczeństwa systemów identyfikacji elektronicznej, nie da się jej zapewnić dzięki procedurom prowadzonym w różnych językach. Używanie języka angielskiego powinno ułatwić osiągniecie tych celów. Poszczególnymi systemami identyfikacji elektronicznej zarządzają różne organy i podmioty w państwach członkowskich. Aby umożliwić skuteczną współpracę i uprościć procedury administracyjne, należy utworzyć w każdym państwie członkowskim jeden punkt, przez który będzie możliwy kontakt z odpowiednimi organami i podmiotami[12].

Identyfikacja elektroniczna w polskim ustawodawstwie

Identyfikacja elektroniczna jest nowym pojęciem w polskim porządku prawnym, jej regulacja zawarta w ustawie o usługach zaufania ma charakter bardzo ogólny. Ustawodawca jednoznacznie przesądza o potrzebie funkcjonowania krajowego węzła identyfikacji, czyli punktu przyłączenia umożliwiającego sprzężenie krajowej infrastruktury identyfikacji z infrastrukturami innych państw. Funkcjonowanie takiego węzła zapewnia minister właściwy do spraw informatyzacji. Określa on także warunki organizacyjno-techniczne udostępniania krajowego węzła identyfikacji, mając na uwadze potrzebę zapewnienia interoperacyjności systemów identyfikacji, wykorzystywanych do uwierzytelniania osób w usługach *on-line*.

Krajowy węzeł identyfikacji będzie pełnił podwójną rolę: 1) będzie pośredniczył w uwierzytelnianiu posiadaczy zagranicznych środków identyfika-

[11] Rozporządzenie wykonawcze Komisji UE 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na postawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L z dnia 9 września 2015 r., nr 235, s. 1).

[12] Decyzja wykonawcza Komisji UE 2015/296 z dnia 24 lutego 2015 r. ustanawiająca proceduralne warunki współpracy między państwami członkowskimi w zakresie identyfikacji elektronicznej na postawie art. 12 ust.7 rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. UE L z dnia 25 lutego 2015 r., nr 53, s. 14).

cji elektronicznej, które zostały wydane w ramach notyfikowanych systemów identyfikacji *on-line* oraz 2) będzie pośredniczył w uwierzytelnianiu posiadaczy krajowych środków identyfikacji elektronicznej w zagranicznych usługach *on-line*, w przypadku gdy system identyfikacji, w ramach którego te środki zostały wydane, będzie notyfikowany.

Wniosek o notyfikowanie krajowego systemu identyfikacji elektronicznej w Komisji Europejskiej składa podmiot odpowiedzialny za ten system do ministra właściwego do spraw informatyzacji. Minister ten zgłasza krajowy system identyfikacji do notyfikacji, biorąc pod uwagę wynik wzajemnej oceny, o której mowa w art. 12 ust. 7 rozporządzenia eIDAS (art. 24 u.u.z.).

Zmiany w przepisach obowiązujących mają przede wszystkim na celu dostosowanie do nowej terminologii, jaką posługuje się rozporządzenie eIDAS, w taki sposób, żeby zapewnić nie tylko spójność z eIDAS, ale również ciągłość działania istniejących usług elektronicznych wykorzystujących środki identyfikacji elektronicznej oraz usługi zaufania. Jak dotychczas brak wspólnej podstawy prawnej zobowiązującej państwa członkowskie UE do uznawania i akceptowania środków identyfikacji elektronicznej wydanych w innych państwach członkowskich w celu zapewnienia dostępu do usług elektronicznych wraz z niewłaściwą transgraniczną interoperacyjnością krajowych systemów identyfikacji elektronicznej, tworzył bariery, które nie pozwoliły na korzystanie w pełni z jednolitego rynku cyfrowego. Rozporządzenie eIDAS powinno umożliwić bezpieczne i płynne interakcje drogą elektroniczną, zwiększając skuteczność publicznych i prywatnych usług *on-line*, biznesu i handlu elektronicznego w Unii Europejskiej.

Literatura

ePodręcznik, e-usługi publiczne, https://epodrecznik.mac.gov.pl.

Gołaczyński J., Szostek D., *Czy pieczęć elektroniczna ma szansę usprawnić administrację?*, „Monitor Prawniczy" 2009, nr 5.

Marucha-Jaworska M., *Rozporządzenie eIDAS. Zagadnienia prawne i techniczne*, Warszawa 2017.

Mielnicki T., Wołowski F., Grajek M., Popis P., *Identyfikacja i uwierzytelnianie w usługach elektronicznych*, Warszawa 2013.

Szostek D., *Pieczęć elektroniczna i możliwości jej wykorzystania w polskim prawie*, w: *Media elektroniczne. Współczesne problemy prawne*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek, Legalis C.H. Beck 2016.

Akty prawne

Decyzja wykonawcza Komisji UE 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady UE nr 10/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, Dz. Urz. UE. L z dnia 9 września 2015 r., nr 235.

Decyzja wykonawcza Komisji UE 2015/296 z dnia 24 lutego 2015 r. ustanawiająca proceduralne warunki współpracy między państwami członkowskimi w zakresie identyfikacji elektronicznej na postawie art. 12 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, Dz. Urz. UE L z dnia 25 lutego 2015 r., nr 53.

Komunikat z dnia 30 czerwca 2016 r. Narodowego Centrum Certyfikacji (NCCert), Dz.U. z 2013 r., poz. 262 z późn. zm.

Rozporządzenie ministra cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania, Dz.U. z 2016 r., poz. 1632.

Rozporządzenie wykonawcze Komisji (UE) nr 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów bezpieczeństwa w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, Dz. Urz. UE. L nr 235, s. 7; zm. Dz. Urz. UE. L 2016 r., nr 345.

Rozporządzenie wykonawcze Komisji UE 2015/1501 z dnia 8 września 2015 r. w sprawie ram interoperacyjności na postawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym, Dz. Urz. UE L z dnia 9 września 2015 r., nr 235.

TRUST SERVICES AND ELECTRONIC IDENTIFICATION

Summary

The e-IDAS Regulation is a new European act that comprehensively regulates the issues concerned with trust services and electronic identification. The e-IDAS Regulation broadens the catalogue of trust services, introduces uniform terminology and new standards in all European Union's Member Countries, it introduces the obligation to recognize and accept the electronic signatures and seals in European Union's Member Countries. The main goal is to increase the security level of trust services and to increase the popularity of these services among citizens of the European Union.

Keywords: trust services, electronic identification, electronic signature, electronic seal