Wdrożenie rozporządzenia eIDAS w Polsce

RAPORT

Wersja 4.2

Praca wykonana na podstawie Umowy z Ministerstwem Gospodarki

Grudzień 2014

Autorzy:

- dr hab. inż. Jerzy Pejaś,

- mgr inż. Marcin Szulga,

- r.pr. mgr Mateusz Wagemann,

- mgr Ałła Stoliarowa-Myć,

- mgr inż. Patrycja Wiktorczyk.

Elektronicznie podpisany przez Jerzy Pejaś
DN: cn=Jerzy Pejaś, givenName=Jerzy, sn=Pejaś, serialNumber=PESEL:54020713277, c=PL
Data: 2015.05.18 14:15:57 +02'00'

Dokument podpisany przez Ałła Stoliarowa-Myć
Data: 2015.05.14 17:28:33 CEST
Położenie: Szczecin; PL

Dokument podpisany przez Patrycja Wiktorczyk
Data: 2015.05.15 15:21:58 CEST

Dokument podpisany przez Marcin Szulga
Data: 2015.05.18 08:24:32 CEST

Signature Not Verified
Dokument podpisany przez Mateusz Wagemann
Data: 2015.05.18 10:26:40 CEST

Spis treści

1. WSTĘP

W Dzienniku Urzędowym Unii Europejskiej z dnia 23 lipca 2014 r. opublikowane zostało Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (tzw. rozporządzenie eIDAS, [eIDAS]). Celem przedstawionego rozporządzenia jest zharmonizowanie rynku cyfrowego UE w oparciu o takie kluczowe elementy jak elektroniczna identyfikacja i usługi zaufania.

Zakończenie prac nad rozporządzeniem eIDAs jest wynikiem żmudnego procesu negocjacyjnego z udziałem państw członkowskich. Niewątpliwie do sukcesu tych prac przyczynił się także aktywny udział Polski reprezentowanej przez zespół Ministerstwa Gospodarki, w którego składzie uczestniczył przedstawiciel pionu gospodarczego Stałego Przedstawicielstwa RP w Brukseli (minister Anna Will), pracownicy Departamentu Gospodarki Elektronicznej (Marcin Fijałkowski – Radca Ministra) oraz Departamentu Spraw Europejskich (Martyna Perek). W pracach tych nie można pominąć udziału Ministerstwa Administracji i Cyfryzacji, Ministerstwa Sprawiedliwości, Narodowego Funduszu Zdrowia, innych przedstawicieli administracji centralnej oraz Instytutu Maszyn Matematycznych, którzy aktywnie wspierali proces negocjacyjny, m.in. poprzez udział w posiedzeniach Międzyinstytucjonalnego Zespołu Wykonawczego ds. Gospodarki Elektronicznej.

Sukcesem Polski w toku negocjacji było doprowadzenie do kompromisu w zakresie otwarcia katalogu usług zaufania na nowe innowacje i wprowadzenie mechanizmów przeglądowych. Co prawda rozporządzenie wprowadza zamknięty katalog kwalifikowanych usług zaufania na poziomie unijnym, ale dopuszcza otwarty katalog tzw. „zwykłych" usług zaufania (tj. o mniejszych wymaganiach i kosztach w zakresie ich świadczenia) na poziomie państw członkowskich. Umożliwi to wypracowanie nowych usług, które później - w ramach przeglądu rozporządzenia - będą mogły zostać uwzględnione. Staraniem Polski udało się nadać rozporządzeniu wysoką elastyczność, m.in. poprzez odesłania do krajowych uregulowań prawnych. Przykładowo, w odniesieniu do niezharmonizowanych usług zaufania dopuszczalne będzie określenie ich skutków przepisami krajowymi. Krajowymi przepisami mają zostać określone również kwestie odpowiedzialności cywilnej i ubezpieczenia usługodawców, a także nadzór oraz jego instrumentarium techniczne i prawne. Polska we współpracy z Niemcami doprowadziła również do racjonalnego ograniczenia rodzajów mechanizmów elektronicznej identyfikacji (eID), których uznawanie będzie niezbędne, oraz do zawężenia zakresu obligatoryjnego zastosowania eID i podpisów elektronicznych do systemów administracji publicznej. Znalazło to wyraz m.in. w Preambule (15) rozporządzenia eiDAS:

> Obowiązek uznawania środka identyfikacji elektronicznej powinien odnosić się wyłącznie do tych środków, których poziom bezpieczeństwa tożsamości jest równy poziomowi wymaganemu w odniesieniu do danej usługi online lub wyższy od tego poziomu. Ponadto obowiązek ten powinien mieć zastosowanie wyłącznie wtedy, gdy dany podmiot sektora publicznego używa „średniego" lub „wysokiego" poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi online. Państwa członkowskie powinny mieć nadal swobodę, zgodnie z prawem unijnym, w zakresie uznawania środków identyfikacji elektronicznej charakteryzujących się niższymi poziomami bezpieczeństwa.

Udało się również wprowadzić ważkie wyłączenia zakresu stosowania rozporządzenia eIDAS w odniesieniu do tzw. systemów zamkniętych (patrz Art. 2, ust.2). Aktywny udział Polski w negocjacjach pozwolił także na uniknięcie szeregu zapisów, które zagrażały niespójnością z naszym systemem prawa administracyjnego i cywilnego.

Dzięki szczegółowym uwagom zgłaszanym przez Polskę także na końcowym etapie negocjacji (m.in. konsekwentnym postulatom zapewnienia odpowiedniego okresu na dostosowanie się podmiotów z sektora publicznego i prywatnego do wymogów regulacji oraz sygnalizowaniu niuansów dotyczących zarówno technicznych, jak również praktycznych rozwiązań w dziedzinie podpisu elektrycznego oraz e-identyfikacji), przepisy rozporządzenia zaowocują wypracowaniem w pełni funkcjonalnych oraz interoperacyjnych rozwiązań we wszystkich państwach członkowskich, pozwalając na dostosowanie podmiotów z branży podpisu elektronicznego oraz samej administracji do postępu technologicznego.

Rozporządzenie unijne w sprawie identyfikacji elektronicznej i usług zaufania (eIDAS) ma na celu wprowadzenie nowych narzędzi prawnych i technicznych, umożliwiających rozwój usług zaufania oraz podniesienie poziomu ich bezpieczeństwa. Rozporządzenie eIDAS stanowi ważny krok w kierunku stworzenia paneuropejskiej przestrzeni zaufania oraz zapewnienia swobody przepływu usług zaufania i ich produktów.

Cele proponowanego rozporządzenia eIDAS to w szczególności:

(a) zapewnienie wzajemnego uznawania i transgranicznej akceptacji elektronicznej identyfikacji (eID);

(b) poprawa istniejących ram dla podpisu elektronicznego, w szczególności poprzez ujednolicenie ram prawnych świadczenia usług zaufania oraz nadzoru nad dostawcami usług w Europie;

(c) zapewnienie skutku prawnego lub uznania dla usług zaufania związanych z elektronicznymi transakcjami, tj. podpisami elektronicznymi pieczęciami elektronicznymi, znakowaniem czasem, dokumentami elektronicznymi, archiwizacją dokumentów elektronicznych, usługami przekazu elektronicznego oraz uwierzytelnianiem witryn internetowych.

Rozporządzenie składa się z preambuły, sześciu rozdziałów oraz czterech załączników. W preambule zawarto motywację i uzasadnienie zapisów zawartych w rozporządzeniu, a także określono intencje ustawodawcy, m.in. otwartość na innowacje, neutralność technologiczną, zachowanie porównywalnego poziomu bezpieczeństwa kwalifikowanych usług zaufania, zgłaszanie i obsługę incydentów związanych z bezpieczeństwem usług zaufania, zastosowanie pieczęci elektronicznej.

Rozdział pierwszy zawiera przepisy ogólne, w tym słownik pojęć - element istotny dla całości rozporządzenia. Określony w tym rozdziale przedmiot i zakres rozporządzenia obejmuje wzajemne rozpoznawanie i akceptację notyfikowanych środków elektronicznej identyfikacji osób fizycznych i prawnych, elektronicznych usług zaufania (podpisu elektronicznego, elektronicznej pieczęci, dokumentu elektronicznego, znaczników czasu, długookresowego przechowywania elektronicznego podpisu i elektronicznej pieczęci, zarządzania certyfikatami, elektronicznego dostarczania wiadomości oraz uwierzytelniania stron www). Używany w rozporządzeniu przymiotnik *kwalifikowany* należy rozumieć jako spełniający wymagania rozporządzenia. Dotyczy to zarówno zaświadczeń typu certyfikat, pieczęć, znacznik czasu, ale także usług zaufania i ich dostawców.

W rozdziale drugim przedstawiono problemy wzajemnego uznawania i akceptowania środków identyfikacji elektronicznej, określono warunki notyfikowania systemów identyfikacji elektronicznej oraz zapewnienia im interoperacyjności technicznej w ramach podejścia opartego na koordynacji, w tym za pomocą aktów delegowanych. Rozporządzenie nie nakłada na państwo członkowskie obowiązku wprowadzania lub notyfikowania systemów identyfikacji elektronicznej, lecz nakazuje uznawać i akceptować notyfikowane środki identyfikacji elektronicznej dla tych usług w przypadku, gdy zgodnie z prawem tego państwa dostęp do usługi elektronicznej wymaga identyfikacji elektronicznej.

Najbardziej obszerny rozdział trzeci dotyczy przede wszystkim wymagań nakładanych na dostawców usług zaufania oraz usługi zaufania, w tym w szczególności:

(a) zasad odpowiedzialności dostawców niekwalifikowanych i kwalifikowanych usług zaufania,

(b) zasad uznawania i akceptowania kwalifikowanych usług zaufania świadczonych przez dostawcę z siedzibą w państwie trzecim,

(c) zasad ochrony danych osobowych i minimalizowania konieczności ich udostępniania,

(d) obowiązku udostępnia usług zaufania osobom niepełnosprawnym,

(e) obowiązku powołania przez państwa członkowskie organów nadzorczych oraz zakresu ich kompetencji w odniesieniu do dostawców usług zaufania i dostawców kwalifikowanych usług zaufania,

(f) mechanizmu wzajemnej pomocy między organami nadzorczymi w państwach członkowskich w celu ułatwienia transgranicznego nadzoru nad dostawcami usług zaufania,

(g) obowiązku wdrożenia przez dostawców niekwalifikowanych i kwalifikowanych usług zaufania odpowiednich środków technicznych i organizacyjnych na potrzeby bezpieczeństwa ich działalności oraz raportowania incydentów związanych z bezpieczeństwem,

(h) warunków nadzorowania kwalifikowanych dostawców usług zaufania oraz usług świadczonych przez tych dostawców,

(i) działań organu nadzorczego podejmowanych na wniosek dostawcy usług zaufania, który zamierza uruchomić kwalifikowaną usługę zaufania, a także zasad sporządzania zaufanych list zawierających informacje o kwalifikowanych dostawcach usług zaufania objętych nadzorem oraz o oferowanych przez nich usługach,

(j) wymagań, które muszą być spełnione, aby dostawca mógł być uznany za kwalifikowanego dostawcę usług,

(k) skutków prawnych podpisów elektronicznych osób fizycznych, w tym zrównania podpisu kwalifikowanego z podpisem własnoręcznym,

(l) wymagań nakładanych na:

- kwalifikowany certyfikat podpisu elektronicznego,
- kwalifikowane urządzenia do składania podpisu (w tym ich certyfikacji w celu ustalenia ich zgodności z wymaganiami bezpieczeństwa ustanowionymi w załączniku II do rozporządzenia oraz umieszczania na liście kwalifikowanego urządzeń do składania podpisu elektronicznego),
- procedury i usługi weryfikacji kwalifikowanych podpisów elektronicznych mających na celu zwiększenie pewności prawnej w odniesieniu do takiej weryfikacji,
- usługi długoterminowego przechowywania kwalifikowanego podpisu elektronicznego,

(m) skutków prawnych pieczęci elektronicznych osób prawnych, w tym kwalifikowanych pieczęci elektronicznych, które przez prawne domniemanie gwarantują autentyczność i integralność dokumentów elektronicznych, z którymi jest ona powiązana,

(n) wymagań nakładanych na:

- kwalifikowany certyfikat pieczęci elektronicznej,
- kwalifikowanego urządzenia do składania pieczęci elektronicznej1
- procedury i usługi weryfikacji kwalifikowanych pieczęci elektronicznych mających na celu zwiększenie pewności prawa w odniesieniu do takiej weryfikacji2,
- usługi długoterminowego przechowywania kwalifikowanej pieczęci elektronicznej3,

(o) skutków prawnych elektronicznych znaczników czasu, które w przypadku kwalifikowanych elektronicznych znaczników czasu przez domniemanie prawne powinny być traktowane jako data pewna,

(p) wymagań nakładanych na kwalifikowane znaczniki elektroniczne,

(q) skutków prawnych i warunków akceptowania dokumentów elektronicznych, które w przypadku podpisania ich z pomocą podpisu kwalifikowanego lub opieczętowania za pomocą kwalifikowanej pieczęci elektronicznej przez domniemanie prawne są autentyczne4, tj. znane jest źródło pochodzenia dokumentu oraz zachowana jest jego integralność,

---

[1] Stosuje się odpowiednio wymagania nakładane na urządzenie do składania kwalifikowanego podpisu elektronicznego.

[2] Stosuje się odpowiednio wymagania nakładane na procedury i usługi weryfikacji kwalifikowanych podpisów elektronicznych.

[3] Stosuje się odpowiednio wymagania nakładane na procedury długoterminowego przechowywania kwalifikowanego podpisu elektronicznego.

[4] Warunkiem tego typu domniemania jest pozytywnie zakończona weryfikacja kwalifikowanego podpisu lub kwalifikowanej pieczęci na moment, w którym nastąpiło oznaczenie czasem.

(r) skutków prawnych danych wysyłanych i otrzymywanych przy użyciu usług rejestrowanego doręczania elektronicznego; w przypadku kwalifikowanych usług rejestrowanego doręczania elektronicznego prawnie domniemywa się o integralności danych, które są wysyłane lub otrzymywane, o zidentyfikowanych nadawcach i zidentyfikowanych adresatach danych oraz o dokładności czasu wysłania lub otrzymania danych,

(s) wymagań dotyczących kwalifikowanych usług rejestrowanego doręczania elektronicznego,

(t) wymagań dotyczących kwalifikowanych certyfikatów uwierzytelniania witryn internetowych.

Standardowe zapisy o możliwości skorzystania przez Komisję z aktów delegowania oraz aktów wykonawczych przedstawiono w rozdziale czwartym i piątym rozporządzenia.

1.1 Zastosowanie dokumentu

Niniejsza ekspertyza jest wynikiem pracy wykonanej na zlecenie Ministerstwa Gospodarki. Celem ekspertyzy jest przedstawienie różnych aspektów wdrożenia w krajowych uwarunkowaniach rozporządzenia eIDAS w aspekcie prawnym, organizacyjnym i technicznym w terminach wynikających z rozporządzenia. Ekspertyza została przygotowana przy założeniu, że podstawowym narzędziem wprowadzenia zmian będzie obowiązujące bezpośrednio w krajowym porządku prawnym rozporządzenie eIDAS wraz z systemem aktów delegowanych i implementujących oraz towarzysząca rozporządzeniu ustawa o usługach zaufania wraz z krajowymi aktami wykonawczymi.

Niestety w momencie tworzenia ekspertyzy brakuje jeszcze wielu aktów delegowanych i implementujących w zakresie usług zaufania i elektronicznej identyfikacji. Opracowanie aktów delegowanych i implementujących przez UE w znacznym stopniu zależeć będzie od dostępności standardów intensywnie opracowywanych przez ETSI (patrz harmonogram tych prac przedstawiony w rozdz. 4.2). Komisja Europejska zastrzega, że w odniesieniu do delegacji fakultatywnych nie ma obowiązku przygotowywania aktu i może być tak, że w wyjątkowych przypadkach akty takie powstaną dopiero po wielu latach obowiązywania eIDAS lub nie powstaną wcale.

Przedstawiona sytuacja stwarza niezbyt komfortowe warunki dla krajowego systemu prawnego, jak również dla podmiotów świadczących usługi zaufania lub usługi bazujące na elektronicznej identyfikacji. Rozwiązanie tej sytuacji wymaga zastąpienia w ustawie o usługach zaufania i towarzyszących jej rozporządzeniach tych aktów delegowanych i implementujących rozporządzenia eIDAS, które nie będą istniały w momencie prac nad ustawą lub rozporządzeniami, a których brak może być istotny dla rozwoju usług zaufania i identyfikacji elektronicznej w Polsce oraz ich interoperacyjności i transgraniczności w ramach wspólnego rynku UE.

1.2 Definicje i oznaczenia

L.p.	Nazwa, skrót, oznaczenie	Definicja
1.	jednostka oceniająca zgodność	(ang. conformity assessment body): oznacza jednostkę określoną w art. 2 pkt 13 rozporządzenia (WE) nr 765/2008, która jest akredytowana zgodnie z tym rozporządzeniem jako właściwa do przeprowadzania oceny zgodności kwalifikowanego dostawcy usługi zaufania i świadczonych przez niego kwalifikowanych usług zaufania
2.	Rozporządzenie eIDAS	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 dnia 23.07.2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym
3.	CAB	ang. Conformity Assessment Body – organ oceny zgodności
4.	SB	ang. Supervisory Body – jednostka odpowiedzialna za prowadzenie działań nadzorczych na mocy

		rozporządzenia eIDS
5.	ACAB	ang. Accreditation of Conformity Assessment Bodies) - akredytacja jednostek oceniających zgodność
6.	Ustawa o podpisie elektronicznym lub PodElU	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym
7.	MG	Ministerstwo Gospodarki
8.	MAiC	Ministerstwo Administracji i Cyfryzacji
9.	TSP	ang. Trust Service Provider - dostawca usług zaufania
10.	UoUZ	Ustawa o usługach zaufania: akt krajowy proponowany jako akt zastępujący Ustawę o podpisie elektronicznym i wdrażający niezbędne regulacje, wskazane w Rozporządzeniu 910/2014 (eIDAS) do uregulowania na poziomie krajów członkowskich.
11.	NCCert	Narodowe Centrum Certyfikacji
12.	NAB	ang. National accreditation body – narodowy organ akredytacyjny – w Polsce PCA – Polskie Centrum Akredytacji
13.	QSCD	ang. Qualified electronic signature creation device – kwalifikowane urządzenie do składania podpisu elektronicznego
14.	QC	ang. Qualified certificate – kwalifikowany certyfikat (może odnośic się do podpisu elektronicznego, pieczęci lub uwierzytelniania witryn internetowych)
15.	QeS	ang. Qualified electronic signature – kwalifikowany podpis elektroniczny
16.	QTS	ang. Qualified TS – kwalifikowana usługa zaufania
17.	QTSP	ang. Qualified TSP – kwalifikowany dostawca usług zaufania
18.	NQTSP	ang. Non-Qualified TSP – niekwalifikowany dostawca usług zaufania
19.	TS	ang. Electronic trust service – elektroniczna usługa zaufania
20.	TSP	ang. Trust service provider – dostawca usług zaufania
21.	TSL	ang. Trust Service List – lista usług zaufania
22.	TFUE	Traktat o funkcjonowaniu Unii Europejskiej
23.	electronic delivery (e-Delivery):	Rejestrowane doręczenie elektroniczne

24.	qualified electronic delivery service (QeDS)	Kwalifikowana Usługa rejestrowanego doręczenia elektronicznego, oznacza usługę, które spełnia wymagania Artykułu 36 R910/2014
25.	UPO	Urzędowe poświadczenie odbioru
26.	eDS	(ang. Electronic Delivery Service) Usługa rejestrowanego doręczenia elektronicznego
27.	eTS	(ang. Electronic Trust Service) elektroniczne usługi zaufania
28.	eID	(ang. Electronic Identification) elektroniczna identyfikacja
29.	LSP	(ang. Large Scale Project) projekty dużej skali

2. CZĘŚĆ PRAWNA

2.1 Uwagi wstępne

Część prawna niniejszej ekspertyzy dotyczy skutków prawnych dla polskiego systemu prawnego, które wywołuje uchwalenie przez Parlament Europejski i Radę (UE) rozporządzenia z dnia 23 lipca 2014 r. nr 910/2014 *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE* (Dz.Urz.UE L z dn. 28 sierpnia 2014 r.), zwane dalej rozporządzeniem eIDAS. Przy opracowaniu niniejszej ekspertyzy uwzględniono charakter i skutki prawne wywoływane przez rozporządzenie eIDAS oraz zasady prawa unijnego, w tym charakter prawny unijnego aktu prawnego jakim jest rozporządzenie eIDAS. Mając na względzie powyższe oraz proponując w niniejszej ekspertyzie rozwiązania o charakterze prawnym, czy prawotwórczym, przyjęto, że na poziomie prawa unijnego znaczna część przedmiotowej materii została już uregulowana, bądź zostanie uregulowana w aktach wykonawczych lub aktach delegowanych. Jednocześnie uwzględniono okoliczność, że rozporządzenie eIDAS pozostawia w niektórych materiach swobodę regulacyjną dla prawa krajowego, stąd też w ekspertyzie zaproponowano merytorykę tych rozwiązań, które nie są w sposób wyczerpujący regulowane na poziomie unijnym.

Prawodawca europejski zdecydował się uregulować kwestie dotyczące identyfikacji elektronicznej i usług zaufania w formie rozporządzenia. Rozporządzenie eIDAS ma na celu popularyzację usług elektronicznych w celu budowania zaufania dla transakcji elektronicznych wśród konsumentów, przedsiębiorstw i instytucji publicznych. Uznano, że zapewnienie jednolitej wspólnej podstawy prawnej dla transakcji elektronicznych na całym rynku wewnętrznym UE przyczyni się do powiększenia zaufania dla tego typu transakcji, co w konsekwencji ma sprzyjać rozwojowi społecznemu i gospodarczemu. Celem Unii Europejskiej stało się utworzenie jednolitego rynku cyfrowego. Uznano, że niewystarczające jest zapewnienie spójności rozwiązań stosowanych przez państwa członkowskie w omawianym zakresie poprzez dyrektywę nr 1999/93/WE. Uznano za niezbędne opracowanie rozporządzenia, które w sposób kompleksowy ureguluje warunki dla transakcji elektronicznych i usług zaufania. Celem nowego rozporządzenia jest także zapewnienie obywatelom UE możliwości uwierzytelniania się w każdym państwie członkowskim korzystając z dowolnego notyfikowanego systemu identyfikacji elektronicznej, co będzie możliwe dopiero po wprowadzeniu wzajemnego uznawania między państwami członkowskimi krajowych systemów identyfikacji elektronicznej. Prawodawca europejski obrał za cel zniesienie barier w transgranicznym stosowaniu środków identyfikacji elektronicznej stosowanych w państwach członkowskich dla usług publicznych. Z tego też względu rozporządzenie ustanawia warunki uznawania środków identyfikacji elektronicznej na poziomie europejskim między państwami członkowskimi,.

Projektując założenia do uregulowań krajowych nie sposób pominąć charakteru aktu prawnego wydanego na poziomie unijnym, który reguluje daną materię. W przypadku usług zaufania prawodawca europejski zdecydował się uchwalić rozporządzenie. Zgodnie z art. 288 Traktatu *o funkcjonowaniu Unii Europejskiej* rozporządzenie jest aktem prawnym o zasięgu ogólnym, wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Rozporządzenie unijne odnosi zatem bezpośredni skutek w każdym państwie członkowskim, a także jest w całości wiążące, co oznacza, że jego skuteczność nie zależy od żadnego aktu zewnętrznego. Państwa członkowskie są przy tym zobowiązane do pełnego i jednolitego stosowania rozporządzenia i nie mogą go stosować w sposób selektywny[5]. Ponadto rozporządzenie jest 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 krajowego[6].

[5] A. Wróbel [w]: Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom III, pod red. D. Kornobis-Romanowskiej i J. Łacny, Warszawa 2012, s. 646.

[6] Ibidem, s. 647.

W tym kontekście projektując przepisy prawa krajowego należy także uwzględniać zasadę pierwszeństwa prawa unijnego, wywodzącą się z szerokiego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. Zasada ta stanowi fundament funkcjonowania prawa europejskiego, albowiem przesądza ona o odrębności europejskiego porządku prawnego i jest niezbędna dla jego prawidłowego funkcjonowania. Istotą tej zasady jest pierwszeństwo zastosowania normy wywodzonej z prawa unijnego przed normą pochodzącą z prawa krajowego w przypadku kolizji tych dwóch porządków prawnych. Państwo członkowskie zobowiązane jest zatem powstrzymywać się przed stanowieniem przepisów, które byłyby niezgodne z prawem unijnym, bądź też zobowiązane jest tego typu przepisy zmienić lub uchylić[7].

Zasadą wyrażoną m.in. w orzecznictwie Trybunału Sprawiedliwości UE jest zakaz implementacji rozporządzeń[8]. Zakaz ten wynika z charakteru aktu prawnego jakim jest rozporządzenie, które wiąże w całości i jest stosowane bezpośrednio przez państwo członkowskie. Z tego względu nie tylko nie ma potrzeby dokonywania aktu implementacji rozporządzeń do krajowych porządków prawnych, ale tego typu działanie jest niedozwolone, albowiem groziłoby to uzależnieniem bezpośredniego skutku rozporządzeń od działania organów krajowych, co jest sprzeczne z charakterem rozporządzenia.

Państwo członkowskie zobowiązane jest z jednej strony przepisy rozporządzenia stosować, czego przejawem jest m.in. wprowadzanie w życie przepisów unijnych poprzez ich stosowanie w praktyce administracyjnej, czy sądowniczej. Z drugiej strony państwo członkowskie zobowiązane jest na mocy Traktatu o Unii Europejskiej (art. 4 ust. 3) do podejmowania wszelkich środków właściwych dla zapewnienia wykonania zobowiązań wynikających z Traktatów lub aktów instytucji Unii. Państwa Członkowskie ułatwiają wypełnianie przez Unię jej zadań i powstrzymują się od podejmowania wszelkich środków, które mogłyby zagrażać urzeczywistnieniu celów Unii. Z kolei Traktat o funkcjonowaniu Unii Europejskiej w art. 291 ust. 1 nakłada na państwa członkowskie obowiązek podejmowania wszelkich środków prawa krajowego niezbędnych do wprowadzenia w życie wiążących aktów Unii.

Mając powyższe na względzie należy traktować planowaną do wprowadzenia w polskim systemie prawnym **ustawę o usługach zaufania**, jako akt porządkujący polski system prawny w związku z wejściem w życie rozporządzenia eIDAS, a jednocześnie akt, który uzupełni rozporządzenie eIDAS w tych obszarach, gdzie rozporządzenie to wprost odsyła do prawa krajowego, a stosowanie rozporządzenia eIDAS wymaga jednocześnie wprowadzenia stosownej regulacji w prawie krajowym (np. wskazanie organu nadzoru). Ponadto ustawa ta winna uzupełniać regulacyjnie te obszary, które w rozporządzeniu eIDAS są uregulowane w sposób niepełny, bądź dla których rozporządzenie to pozostawia swobodę dla krajowych porządków prawnych.

Wyżej przytoczone zasady związane z funkcjonowaniem prawa Unii Europejskiej prowadzą do wniosku, że w związku z wejściem w życie rozporządzenia eIDAS niezbędne jest zreformowanie w polskim systemie prawnym wszystkich tych aktów prawnych, które mogłyby okazać się sprzeczne, bądź niezgodne z treścią normatywną rozporządzenia eIDAS. Skoro zatem rozporządzenie to w sposób kompleksowy reguluje problematykę funkcjonowania usług zaufania na rynku wewnętrznym, zasadna wydaje się rewizja obowiązujących aktualnie przepisów prawa polskiego w tym zakresie. Należy bowiem pamiętać, że niedopuszczalną w systemie prawa europejskiego jest sytuacja, w której po wejściu w życie rozporządzenia unijnego w państwie członkowskim obowiązują przepisy niezgodne lub sprzeczne z prawem unijnym. Tego typu sytuacja traktowana jest przez Komisję Europejską, a także Trybunał Sprawiedliwości UE jako naruszenie obowiązków traktatowych przez państwo członkowskie i podlega ona kontroli prowadzonej na podstawie opisanych dalej przepisów prawa pierwotnego UE.

W kontekście powyższego należy w szczególności uznać, że ustawa z dnia 18 września 2001 r. *o podpisie elektronicznym* w nowym porządku prawnym kształtowanym przez rozporządzenie eIDAS winna być uchylona. Podpis

[7] D. Miąsik [w]: System Prawa Administracyjnego. Tom 3. Europeizacja prawa administracyjnego, pod red. R. Hausera, Z. Niewiadomskiego, A. Wróbla, Warszawa 2014, s. 69.

[8] N. Półtorak [w]: Traktat o funkcjonowaniu Unii Europejskiej…, s. 263.

elektroniczny należy do usług zaufania, które zostały w całości zharmonizowane na poziomie prawa unijnego, jak też prawo unijne określa skutki prawne podpisu elektronicznego. Jednocześnie uregulowania wymaga obszar, który nie był dotychczas regulowany przepisami polskiego prawa, a który dotyczy usług zaufania wskazanych w rozporządzeniu eIDAS.

Opracowując niniejszą ekspertyzę przyjęto, że w polskim systemie prawnym zaistnieje konieczność wprowadzenia zmian dwojakiego rodzaju. Do pierwszej grupy należą te akty prawne (ustawy i rozporządzenia), które zawierają bezpośrednie odesłania do ustawy o podpisie elektronicznym. Akty te najczęściej zawierają pojęcia i terminy definiowane ustawą o podpisie elektronicznym. Z tego względu w oddzielnym zestawieniu wskazano wszystkie te akty prawne, jak też zaproponowano w stosunku do nich kierunek i sposób zmian ze wskazaniem jednostki redakcyjnej tekstu aktu prawnego, która winna ulec zmianie. Do drugiej grupy aktów prawnych należą wszystkie te, które korzystają z terminów i pojęć definiowanych ustawą o podpisie elektronicznym, lecz nie zawierają bezpośredniego odesłania do tej ustawy. Dla tych aktów zaproponowano reguły modyfikujące wskazujące, które pojęcia winny ulec zastąpieniu i jakie inne terminy powinny je zastępować.

Istnieje też grupa przepisów, które regulują różnego rodzaje zagadnienia wykorzystując w sposób pośredni instytucję podpisu elektronicznego, czy szerzej komunikacji elektronicznej. W odniesieniu do tych przepisów w niniejszej ekspertyzie zaproponowano *de lege ferenda* określone rozwiązania, czy też pożądane kierunki zmian, które w ocenie autorów ekspertyzy uzasadnione są oczekiwanym kierunkiem przemian mającym swój wyraz w treści rozporządzenia eIDAS. Do grupy przepisów, o których tu mowa należą przede wszystkim regulacje prawa cywilnego (Kodeks cywilny), procedury cywilnej (Kodeks postępowania cywilnego) oraz procedury administracyjnej (Kodeks postępowania administracyjnego).

W zakresie proponowanych rozwiązań, co do których rozporządzenie eIDAS pozostawia swobodę dla krajowego porządku prawnego, odniesiono się do zarówno do przepisów rozporządzenia, które odsyłają do prawodawstwa krajowego, jak i do motywów preambuły rozporządzenia, które wspominają o krajowym porządku prawnym. W odniesieniu do motywów preambuły uwzględniono fakt, że motywy te nie zawierają przepisów normatywnych, a stanowią raczej uzasadnienie regulacji[9], a zatem nie formułują powinności określonego działania lub zaniechania. Nie można z motywów preambuły dochodzić określonych praw czy obowiązków, albowiem to dopiero z treści normatywnej aktu prawnego wynikają prawa czy obowiązki. Niemniej jednak powołując się na prawo krajowe w motywach preambuły, prawodawca europejski daje wyraz swojej woli, wskazując jaki był cel danej regulacji i czemu ma ona służyć. Z tego względu proponując w niniejszej ekspertyzie określone rozwiązania, uwzględniono także treść określonych motywów preambuły rozporządzenia eIDAS.

Organy państwa polskiego będącego członkiem Unii Europejskiej winny uwzględniać w planowanych przez siebie działaniach spoczywający na każdym kraju członkowskim obowiązek podjęcia wszystkich tych środków na gruncie prawa krajowego, które są niezbędne, aby przepisy rozporządzenia eIDAS, będącego wiążącym aktem Unii, mogły skutecznie wejść w życie i funkcjonować w naszym kraju. Uchybienie temu obowiązkowi może prowadzić do wszczęcia przez Komisję Europejską procedury, o której mowa w art. 258 i nast. Traktatu o funkcjonowaniu Unii Europejskiej. Na mocy tych przepisów Komisja posiada kompetencję do wniesienia skargi do Trybunału Sprawiedliwości UE, po uprzednim wydaniu pisemnej opinii i uzyskaniu wyjaśnień ze strony państwa członkowskiego. Procedurę tę wszczyna się w przypadku, gdy Komisja uzna, że państwo członkowskie uchybiło jednemu z zobowiązań, które na nim ciążą na mocy Traktatów. Uchybienia te mogą być wielorakiego rodzaju i mogą przybierać dowolną formę. Naruszeniem jest utrzymywanie krajowych przepisów niezgodnych z prawem unijnym, zaniechanie niezbędnych zmian w prawie krajowym, brak implementacji dyrektywy, czy dokonanie implementacji rozporządzenia[10]. W toku postępowania Trybunał Sprawiedliwości może stwierdzić, że państwo członkowskie uchybiło któremuś z zobowiązań traktatowych. W takiej sytuacji państwo jest zobowiązane podjąć środków, które zapewnią wykonanie wyroku Trybunału, pod

[9] A. Malinowski, Teksty prawne Unii Europejskiej. Opracowanie treściowe i redakcyjne oraz zasady ich publikacji, Warszawa 2010, s. 85.
[10] N. Półtorak [w]: Traktat o funkcjonowaniu Unii Europejskiej…, s. 263.

rygorem wniesienia przez Komisje kolejnej skargi do Trybunału Sprawiedliwości (art. 260 ust. 1 i 2 TFUE). Wnosząc drugą skargę do Trybunału, Komisja wskazuje wysokość ryczałtu lub okresowej kary pieniężnej do zapłacenia przez państwo członkowskie, jaką uzna za odpowiednią do okoliczności. Wysokość tej kary nie jest sprecyzowana w żadnym z powszechnie obowiązujących aktów prawnych, niemniej jednak Komisja Europejska w 2005 r. wydała komunikat w sprawie stosowania art. 228 Traktatu o Wspólnocie Europejskiej. W komunikacie tym ustanowiono podstawę wykorzystywaną przez Komisję do obliczania kwot sankcji finansowych w postaci kar ryczałtowych i okresowych kar pieniężnych, o zastosowanie których Komisja zwraca się do Trybunału Sprawiedliwości wnosząc skargę do Trybunału na mocy art. 260 TFUE. Komunikat ten został zaktualizowany w 2010 oraz w 2014 roku. Komisja Europejska przyjęła zasadę, że w każdej sprawie wnioskuje do Trybunału Sprawiedliwości o nałożenie kar dwojakiego rodzaju. Po pierwsze Komisja wnioskuje o nałożenie ryczałtu za niewykonywanie orzeczenia Trybunału przed wszczęciem postępowania, a po drugie okresowej kary pieniężnej naliczanej za każdy dzień zwłoki. Kara okresowa naliczana jest za każdy dzień opóźnienia w wykonaniu wyroku Trybunału. Kwotę tej kary oblicza się uwzględniając kwoty ustalone przez Komisję Europejską w Komunikacie z dn. 17.09.2014 pn. „Aktualizacja danych wykorzystywanych do obliczania kar ryczałtowych oraz kar pieniężnych wskazywanych Trybunałowi Sprawiedliwości przez Komisję w ramach postępowań w sprawie uchybienia”[11]. Według tego komunikatu minimalna kara ryczałtowa dla Polski wynosi aktualnie 4 274 000 euro. Wysokość okresowej kary pieniężnej jest zaś uzależniona od wyniku mnożenia stawki bazowej wynoszącej 660 euro, współczynnika *n*, który dla Polski wynosi 7,75, oraz współczynnika wagi uchybienia, który może wynosić od 1 do 20, oraz współczynnika czasu trwania uchybienia, który może wynosić od 1 do 3[12].

Z powyższego wynika zatem, że kary za uchybienia związane z niedostosowaniem prawa krajowego do uwarunkowań unijnych aktów prawnych mogą być bardzo dotkliwe, przy czym każdorazowo wysokość kar pieniężnych uzależniona jest od ciężaru naruszenia, długości okresu naruszenia oraz konieczności zapewnienia skutku odstraszającego, co ma zapewnić zaniechanie w dokonywaniu przez państwa członkowskie kolejnych naruszeń[13]. Z tego też względu organy polskie winny podjąć wszelkie niezbędne działania zmierzające po pierwsze do wyeliminowania z polskiego porządku prawnego wszelkich tych przepisów, które są niezgodne z rozporządzeniem eIDAS, bądź uniemożliwiają stosowanie przepisów tego rozporządzenia, jak też powinny podjąć działania mające na celu umożliwienie skutecznego wejścia w życie rozporządzenia i korzystanie z jego rozwiązań przez wszystkie zainteresowane podmioty. Zaniechanie tego typu działań może wiązać się bowiem z nałożeniem na Polskę sankcji, które w konsekwencji postępowań wyżej opisanych mogą przybrać także charakter finansowy.

Mając na względzie powyższe należy uznać, że państwo członkowskie ma prawo doprecyzowania czy dookreślania 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 rozporządzenia. Zatem za niedopuszczalne należy uznać wprowadzanie takich przepisów krajowych, które uniemożliwią w praktyce zastosowanie jakichś rozwiązań proponowanych w rozporządzeniu eIDAS, natomiast możliwe (a nawet pożądane) byłoby wprowadzenie ram dookreślających niektóre zagadnienia. Przykładowo, gdy rozporządzenie eIDAS wskazuje w art. 24 ust. 2 lit. c) na wymogi odnoszące się do dostawcy kwalifikowanych usług zaufania podając, że dostawca taki powinien utrzymywać „dostateczne” zasoby finansowe lub dysponować „stosownym” ubezpieczeniem od odpowiedzialności, dopuszczalne – a nawet pożądane – byłoby doprecyzowanie w przepisach prawa krajowego jakiego rodzaju, czy jakiej wielkości zasoby uznaje się za „dostateczne”, jak też uzasadnione jest dookreślenie w prawie krajowym warunków ubezpieczenia odpowiedzialności cywilnej. Natomiast niedopuszczalnym byłoby wprowadzenie takich warunków dla dostawców kwalifikowanych usług zaufania, które – odnosząc te warunki do realiów danego państwa członkowskiego – byłyby *de facto* niemożliwe do spełnienia, co z kolei mogłoby prowadzić do uniemożliwienia działalności podmiotom kwalifikowanym w jakimś państwie, a zatem cel rozporządzenia eIDAS byłby w takim państwie nieosiągnięty. Należy też wskazać, że dookreślenie w prawie krajowym obszarów, które

[11] http://ec.europa.eu/atwork/applying-eu-law/docs/c_2014_6767_pl.pdf
[12] http://ec.europa.eu/atwork/applying-eu-law/docs/sec_2005_1658_pl.pdf

[13] N. Półtorak [w]: Traktat o funkcjonowaniu Unii Europejskiej…, s. 293.

prawodawca unijny pozostawił dla państw członkowskich winno odbywać się z poszanowaniem zasad ogólnych rozporządzenia eIDAS oraz mając na względzie cel rozporządzenia. W związku z tym należy wprowadzając określone regulacje w prawie krajowym mieć na uwadze promowane przez rozporządzenie eIDAS m.in. zasady interoperacyjności, czy transgraniczności świadczenia usług.

W związku z obowiązkiem notyfikacji przepisów technicznych nałożonym na państwa członkowskie w dyrektywie 98/34/WE Parlamentu Europejskiego i Rady z 22 czerwca 1998 r., która została zmieniona dyrektywą nr 98/48/WE Parlamentu Europejskiego i Rady z 20 lipca 1998 r. należy także zwrócić uwagę na konieczność notyfikacji projektowanej ustawy o usługach zaufania. Przepisami technicznymi podlegającymi notyfikacji w myśl ww. dyrektyw są specyfikacje techniczne i inne wymagania bądź zasady dotyczące usług. Poprzez usługę należy w myśl wspomnianych dyrektyw rozumieć każdą usługa społeczeństwa informacyjnego, to znaczy każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług. W ocenie autorów niniejszej ekspertyzy usługi zaufania jak chociażby usługa podpisu elektronicznego, czy usługa pieczęci elektronicznej winna być traktowana jako usługa w rozumieniu wymienionych wyżej dyrektyw. W związku z tym regulacje krajowe zawierające zasady dotyczące tych usług winny być traktowane jako przepisy techniczne, a zatem przepisy, które podlegają notyfikacji.

2.2 Analiza proponowanego zakresu regulacji ustawy o usługach zaufania

2.2.1 Cel regulacji

Wejście w życie rozporządzenia eIDAS implikuje nowy porządek prawny w obszarze usług zaufania, co rodzi konieczność dostosowania prawa krajowego do nowych uwarunkowań. Celem regulacji zawartych w ustawie o usługach zaufania powinna być regulacja uwarunkowań prawnych dla usług zaufania, które zostały dopuszczone na poziomie rozporządzenia eIDAS. W tym kontekście należy wskazać, że w prawie polskim dotychczas regulowana była w sposób pełny jedynie instytucja podpisu elektronicznego, podczas gdy w świetle regulacji rozporządzenia eIDAS zachodzi aktualnie potrzeba wprowadzenia stosownych regulacji dotyczących także pozostałych usług zaufania. Zasadniczym celem regulacji powinno usunięcie istniejących w krajowych przepisach odwołań do ustawy o podpisie elektronicznym, która zostanie uchylona, wprowadzenie niezbędnych odwołań do rozporządzenia eIDAS, a także stworzenie warunków prawnych dla funkcjonowania usług zaufania, o których mowa w rozporządzeniu eIDAS z zachowaniem zgodności z regulacjami tego rozporządzenia.

Regulacje zawarte w rozporządzeniu eIDAS dotyczące usług zaufania pozostawiają w kilku obszarach swobodę dla prawa krajowego. I tak niezbędnym jest utworzenie regulacji krajowych, które w pierwszej mierze określą skutki prawne dla usług zaufania w zakresie, w jakim skutki te nie są regulowane rozporządzeniem eIDAS. Ponadto niezbędne jest określenie na poziomie ustawy porządku instytucjonalnego w sposób określający role poszczególnych instytucji, których pełnienie jest przewidziane rozporządzeniem eIDAS. Rozporządzenie to odsyła do prawa krajowego także w zakresie zasad odpowiedzialności cywilnoprawnej dostawców usług zaufania, stąd wprowadzenie tej regulacji na poziomie krajowym jest wymagane. Za niezbędne należy także uznać określenie sposobu i środków sprawowania nadzoru, monitoringu oraz kontroli dostawców usług zaufania. Konsekwencją regulacji tej materii winno być także określenie czynów niedozwolonych z punktu widzenia zapewnienia bezpieczeństwa rynku usług zaufania, czego konsekwencją jest określenie sankcji administracyjnych i karnych.

Poza wskazanymi wyżej regulacjami rozporządzenie eIDAS powoduje wprowadzenie do porządku prawnego nowych usług zaufania, a przez to powstanie nowego katalogu pojęciowego. Zmiany wymaga zatem siatka pojęciowa funkcjonująca dotychczas w wielu aktach prawnych w Polsce, a także niezbędne jest wprowadzenie w polskim systemie prawnym szeregu zmian porządkujących oraz zapewniających spójność systemu prawa. Ponadto za niezbędne należy uznać uchylenie ustawy o podpisie elektronicznym i uregulowanie materii w niej poruszanej przepisami nowej ustawy o usługach zaufania.

2.2.2 Obowiązujące rozwiązania

W polskim porządku prawnym obowiązuje ustawa z dnia 18 września 2001 r. *o podpisie elektronicznym*. Ustawa ta reguluje bezpośrednio usługę podpisu elektronicznego oraz znacznik czasu. Tymczasem rozporządzenie eIDAS wprowadziło do europejskiego porządku prawnego szereg usług zaufania, których regulowanie w niektórych zakresach zostało pozostawione krajowym porządkom prawnym. Dzisiejsza ustawa o podpisie elektronicznym nie odpowiada uwarunkowaniom prawnym rozporządzenia eIDAS. Przede wszystkim należy zwrócić uwagę na fakt, że samo rozporządzenie wprowadziło skutek prawny kwalifikowanego podpisu elektronicznego wskazując, że jest on równoważny względem podpisu własnoręcznego. Istniejąca w Polsce ustawa o podpisie elektronicznym odbiega w swej nomenklaturze od pojęć używanych przez prawodawcę europejskiego. W rozporządzeniu eIDAS mowa jest bowiem o podpisie elektronicznym, zaawansowanym podpisie elektronicznym oraz kwalifikowanym podpisie elektronicznym, podczas gdy w ustawie o podpisie elektronicznym używane jest pojęcie zwykłego podpisu elektronicznego, bezpiecznego podpisu elektronicznego oraz bezpiecznego podpisu elektronicznego weryfikowanego za pomocą certyfikatu kwalifikowanego. Obowiązujące rozwiązania w polskim porządku prawnym nie przystają zatem do uwarunkowań rozporządzenia eIDAS, w związku z czym niezbędne jest po pierwsze uchylenie ustawy o podpisie elektronicznym, a po drugie unormowanie proponowanych na poziomie europejskim usług zaufania w jednym krajowym akcie prawnym.

Należy przy tym wspomnieć, że Polsce w praktyce na rynku funkcjonuje większa liczba usług zaufania niż te, które zostały uregulowane w przepisach ustawy o podpisie elektronicznym. Są to tzw. usługi nienazwane, które co prawda nie zostały szczegółowo uregulowane w przepisach, ale jednocześnie zostały one przez prawo dopuszczone. Uznano, że katalog usług zawarty w obowiązującej ustawie o podpisie elektronicznym ma charakter otwarty. W związku z tym w stosunku do niektórych z usług nienazwanych zastosowano procedurę z ustawy pozwalającą zakwalifikować je do usług kwalifikowanych.

Rozporządzenie eIDAS reguluje określony zamknięty katalog kwalifikowanych usług zaufania, dookreślając jednocześnie, że kwalifikowaną usługą zaufania jest usługa spełniająca wymaga określone w tym rozporządzeniu. Dostrzegając fakt, że katalog usług zaufania zawarty w rozporządzeniu eIDAS zawiera usługi niewymienione dotychczas w polskim ustawodawstwie w tym w ustawie o podpisie elektronicznym trzeba zauważyć, że to m.in. doświadczenie Polski związane z wprowadzaniem na rynek dzisiejszych usług nienazwanych pozwoliło wnieść wkład w tworzenie regulacji rozporządzenia eIDAS. Doświadczenia te stanowią jednocześnie dla autorów niniejszej ekspertyzy podstawę zaprezentowanego w niniejszym opracowaniu podejścia tak, aby polskiego dorobku w omawianym zakresie nie zniweczyć.

2.2.3 Rekomendowane rozwiązania

Rozporządzenie eIDAS zawiera regulacje dotyczące zarówno samego podpisu elektronicznego, jak też innych usług zaufania takich jak: pieczęć elektroniczna, elektroniczny znacznik czasu, usługa rejestrowanego doręczenia elektronicznego, uwierzytelnianie witryn internetowych. Prawodawca unijny zdecydował się na wydanie jednej regulacji, która obejmuje kilka rozwijających się usług zaufania. Z tego punktu widzenia krajowe regulacje prawne tyczące się omawianych zagadnień winny być możliwie skondensowane w jednym akcie prawnym. Tego typu rozwiązanie wpłynie niewątpliwie korzystnie na przejrzystość i spójność systemu prawnego, jak też będzie czytelniejsze dla odbiorcy. Dlatego też proponuje się uregulowanie w jednej ustawie o usługach zaufania wszystkich tych zagadnień, które rozporządzenie eIDAS pozostawia dla prawa krajowego. Ustawa winna stanowić także podstawę prawną dla wydania kilku aktów wykonawczych, które doregulują w sposób szczegółowy niektóre zagadnienia – podobnie jak miało to miejsce w przypadku ustawy o podpisie elektronicznym. Należy jednak zważyć na fakt, że rozporządzenie eIDAS odsyła w bardzo wielu kwestiach do obligatoryjnych, lub w większej ilości – fakultatywnych – aktów wykonawczych, które mają być wydane przez Komisję Europejską. Tyczy się to przede wszystkim określenia norm, formatów referencyjnych dotyczących poszczególnych usług zaufania, czy też określonych procedur. Z tego względu katalog krajowych aktów wykonawczych do ustawy o usługach zaufania winien zostać zawężony do zagadnień regulowanych w prawie krajowym.

2.2.4 Istota proponowanych rozwiązań

Ustawa o usługach zaufania powinna w pierwszej mierze dostosować krajowe przepisy do ram i uwarunkowań, które regulowane są rozporządzeniem eIDAS. Tego typu dostosowanie wymaga kilku rozstrzygnięć, jak też uchylenia lub zmiany szeregu przepisów obowiązujących aktualnie w polskim porządku prawnym. Przede wszystkim uchyleniu powinna ulec ustawa o podpisie elektronicznym. Po drugie należy dokonać zmiany bardzo wielu istniejących przepisów, które odsyłają do ustawy o podpisie elektronicznym, bądź posługują się nomenklaturą wprowadzoną tą właśnie ustawą. Terminologia rozporządzenia eIDAS została ujednolicona na poziomie europejskim i z tego względu krajowy porządek prawny winien być do niej dostosowany. Zmiany wymagają pojęcia, które nie będą dłużej funkcjonowały w krajowym systemie prawnym. Należy więc dokonać nowelizacji szeregu aktów prawnych, które zostały wymienione w dalszej części niniejszej ekspertyzy.

Ponadto istotne jest uregulowanie w nowych przepisach ustawy o usługach zaufania szeregu zagadnień, które nie są regulowane na poziomie rozporządzenia eIDAS. Należy przede wszystkim określić skutki prawne dla usług zaufania, dla których skutki te nie zostały określone w rozporządzeniu eIDAS. Należy bowiem podkreślić, że w porządku prawnym państw członkowskich UE pojawią się nowe usługi zaufania, które tylko częściowo zostały uregulowane na poziomie prawa unijnego. Zachodzi więc konieczność doprecyzowania w prawie krajowym jakie będą skutki prawne posługiwania się określonymi usługami zaufania. Ustawa o usługach zaufania winna określać zasady i przesłanki odpowiedzialności cywilnoprawnej podmiotów świadczących usługi zaufania, gdyż dotychczas stosowne przepisy dotyczyły tylko podmiotów świadczących usługi certyfikacyjne w rozumieniu ustawy o podpisie elektronicznym. Z tego też względu konieczne jest 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 certyfikatów.

W odniesieniu do obowiązków usługodawców niekwalifikowanych, które obecnie zawarte są w przepisach ustawy o podpisie elektronicznym, zasadne jest utrzymanie tych obowiązków jako niekolidujących z regulacjami prawa europejskiego. Państwo członkowskie ma prawo uregulować w prawie krajowym zasady świadczenia niekwalifikowanych usług zaufania. Zasadnym jest zwłaszcza uwzględnienie w przepisach ustawy o usługach zaufania następujących wymogów w odniesieniu do niekwalifikowanych usługodawców:

1) wymogi co do wiedzy, wykształcenia, niekaralności osób zatrudnionych przy świadczeniu usług zaufania;
2) obowiązek opracowania polityki certyfikacji;
3) obowiązek zachowania tajemnicy związanej ze świadczeniem usług zaufania;
4) obowiązek niszczenia danych po upływie określonego czasu, np. po utracie ważności certyfikatu;
5) obowiązki informacyjne związane z zawarciem umowy o świadczenie usług zaufania;
6) określenie formy umowy o świadczenie usług zaufania;
7) obowiązek publikacji listy zawieszonych i unieważnionych certyfikatów;
8) obowiązek poddania się czynnościom kontrolnym organu nadzorczego zgodnie z art. 17 ust. 3 lit. b) rozporządzenia eIDAS

Rozporządzenie eIDAS zostało skonstruowane w sposób wymagający określonej aktywności państwa członkowskiego w zakresie zagadnień związanych z usługami zaufania. Z tego względu ustawa o usługach zaufania winna wskazywać, który organ wykonuje w Polsce funkcje państwa członkowskiego wymienione w rozporządzeniu eIDAS. Proponuje się, aby organem tym był minister właściwy ds. gospodarki z racji doświadczeń w zakresie nadzoru nad świadczeniem usług związanych z podpisem elektronicznym. Regulacja taka wymaga wprowadzenia stosownej zmiany w ustawie o działach administracji rządowej.

Ustawa z dnia 4 września 1997 r. o działach administracji rządowej
Art. 9 ust. 2
Do ministra właściwego do spraw gospodarki należą w szczególności sprawy:
(...)

6) nadzoru nad świadczeniem usług związanych z podpisem elektronicznym w rozumieniu przepisów o podpisie elektronicznym;

Wraz z wejściem w życie ustawy o usługach zaufania proponuje się zastąpienie cytowanego wyżej przepisu art. 9 ust. 2 pkt 6 ustawy o działach administracji rządowej w ten sposób, że zostanie wskazane, iż do ministra właściwego ds. gospodarki należą sprawy nadzoru nad świadczeniem usług zaufania w rozumieniu przepisów o usługach zaufania.

Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym
Art. 30 ust. 1
Minister właściwy do spraw gospodarki sprawuje nadzór nad przestrzeganiem przepisów ustawy przez kwalifikowane podmioty, zapewniając ochronę interesów odbiorców usług certyfikacyjnych.

Uchylenie ustawy o podpisie elektronicznym zrodzi konieczność zawarcia w ustawie o usługach zaufania przepisu analogicznego do zacytowanego wyżej art. 30 ust. 1 ustawy o podpisie elektronicznym, który winien stanowić, że minister właściwy ds. gospodarki sprawuje nadzór na przestrzeganiem przepisów ustawy przez podmioty świadczące usługi zaufania zapewniając ochronę interesów odbiorców usług zaufania.

Podsumowując należy wskazać, że celem ustawy o usługach zaufania powinno być:

1) dostosowanie krajowego porządku prawnego do uwarunkowań rozporządzenia eIDAS poprzez wyeliminowanie wszelkich przepisów niezgodnych z rozporządzeniem eIDAS, np. wyeliminowanie pojęć i instytucji nieznanych rozporządzeniu eIDAS, dostosowanie terminologii w krajowych aktach do terminów występujących w rozporządzeniu eIDAS, tj. dokonanie swoistego „czyszczenia" systemu prawa; należy przy tym zaznaczyć, że ustawa o usługach zaufania może wprowadzić określone zmiany w innych ustawach, ale nie może wprowadzać zmian w aktach niższego rzędu w tym m.in. w rozporządzeniach; tymczasem jak wskazano w dalszej części niniejszego dokumentu zmian wymaga szereg przepisów występujących w rozmaitych rozporządzeniach, o czym należy pamiętać dokonując dostosowania przepisów polskich do rozporządzenia eIDAS;
2) uregulowanie tych obszarów, które niezbędne są do umożliwienia stosowania rozporządzenia eIDAS na gruncie prawa polskiego tj. m.in. przyporządkowanie ról odpowiednim organom w zakresie kompetencji nadzorczych;
3) uregulowanie obszarów pozostawionych do kompetencji państw członkowskich; w tym zakresie w ustawie zasadnym będzie uregulowanie procedur i zasad przygotowania w warunkach krajowych do notyfikacji środków identyfikacji elektronicznej z sektora prywatnego.

SKUTKI PRAWNE USŁUG ZAUFANIA

Skutki prawne podpisu elektronicznego zostały wyrażone w treści rozporządzenia eIDAS, które wskazuje w art. 25 ust. 2, że kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu. Zgodnie z intencją wyrażoną w motywie 49. rozporządzenia eIDAS w prawie krajowym należy zdefiniować skutek prawny podpisów elektronicznych z wyjątkiem wymogów przewidzianych w tym rozporządzeniu, zgodnie z którymi kwalifikowany podpis elektroniczny powinien mieć skutek prawny równoważny podpisowi własnoręcznemu. Nadto art. 25 ust. 1 rozporządzenia eIDAS wskazuje, że „Podpisowi elektronicznemu nie można odmówić skutku prawnego ani dopuszczalności jako dowodu w postępowaniu sądowym wyłącznie z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wymogów dla kwalifikowanych podpisów elektronicznych." Regulacje te obowiązują wprost i bezpośrednio także na gruncie krajowym a zatem nie ma potrzeby powtarzania tych rozwiązań w prawie krajowym. Zgodnie bowiem z regułami opisanymi w rozdziale 2.1 Uwagi wstępne, ponawianie czy przenoszenie bezpośrednio obowiązujących w państwie członkowskim regulacji rozporządzenia unijnego jest niedopuszczalne i niepotrzebne. Stąd też w planowanej ustawie o usługach zaufania nie ma potrzeby uwzględniania przepisów analogicznych do obecnego brzmienia przepisów art. 5 ust. 1 i 2 oraz art. 8 ustawy o podpisie elektronicznym.

Rozporządzenie eIDAS wprowadza instytucję pieczęci elektronicznej dla osób prawnych. Kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia tych danych, z którymi kwalifikowana pieczęć elektroniczna jest powiązana (art. 35 ust. 2 rozporządzenia eIDAS). Tak określony skutek prawny kwalifikowanej pieczęci elektronicznej wydaje się w sposób wystarczający definiować istotę tej usługi zaufania, a wskazany przepis winien być interpretowany w ten sposób, że kwalifikowana pieczęć elektroniczna stanowi dowód

tego, że dane, z którymi pieczęć ta jest powiązana pochodzą od podmiotu posługującego się pieczęcią oraz nie zostały zmienione. Jednakże na gruncie prawa krajowego nie jest zasadne ponawianie przepisów określających skutek prawny kwalifikowanej pieczęci elektronicznej, skoro został on już definiowany na poziomie prawa europejskiego.

W odniesieniu do elektronicznych znaczników czasu wedle art. 41 ust. 2 rozporządzenia eIDAS kwalifikowany znacznik czasu korzysta z domniemania dokładności daty i czasu, jakie wskazuje oraz integralności danych, z którymi wskazywane data i czas są połączone. W polskim porządku prawnym zasadne wydaje się wprowadzenie regulacji, zgodnie z którą dokument elektroniczny opatrzony elektronicznym znacznikiem czasu korzysta z waloru daty pewnej. Kwestię tę omówiono w części poświęconej zmianom Kodeksu cywilnego.

Skutki prawne dla usługi rejestrowanego doręczenia elektronicznego w rozporządzeniu eIDAS zostały opisane w ten sposób, że dane wysyłane 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 czasu wysłania i otrzymania wskazanych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego (art. 43 ust. 2 rozporządzenia eIDAS). W kontekście krajowego porządku prawnego proponuje się sprecyzowanie skutku prawnego opisanego w rozporządzeniu eIDAS poprzez wskazanie, że wysłanie oświadczenia woli przy użyciu kwalifikowanej usługi doręczenia elektronicznego stanowi dowód tego, że oświadczenie to zostało wysłane przez zidentyfikowanego nadawcę i dotarło do zidentyfikowanego adresata w czasie wysłania i otrzymania wskazanych przez kwalifikowaną usługę rejestrowanego doręczenia elektronicznego z zachowaniem integralności jego treści. Pożądanym byłoby z pewnością wykorzystanie usługi rejestrowanego doręczenia elektronicznego w krajowych postępowaniach sądowych i administracyjnych. Zasadnym jest rozszerzenie form dokonywania doręczeń w postępowaniach sądowych i administracyjnych o formę rejestrowanego doręczenia elektronicznego, które winno być traktowane pod względem skutków prawnych tak jak doręczenie za pośrednictwem operatora pocztowego, czy sądowej służby doręczeniowej.

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

ZASADY I PRZESŁANKI ODPOWIEDZIALNOŚCI CYWILNOPRAWNEJ DOSTAWCÓW USŁUG ZAUFANIA

Do prawa krajowego należy określenie zasad i przesłanek odpowiedzialności cywilnoprawnej podmiotów świadczących usługi zaufania. W związku z tym zasadne jest wskazanie w prawie krajowym, że dostawca usług zaufania odpowiada wobec odbiorców tych usług, a także wobec osób trzecich, za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług, chyba że niewykonanie tych obowiązków lub nienależyte wykonanie jest następstwem okoliczności, za które podmiot ten nie ponosi odpowiedzialności i którym nie mógł zapobiec pomimo dołożenia należytej staranności.

Zasadne jest ograniczenie odpowiedzialności podmiotów świadczących usługi zaufania polegające na wydawaniu certyfikatów dla podpisu elektronicznego oraz dla pieczęci elektronicznej w ten sposób, że podmioty te nie będą odpowiadać wobec odbiorców tych usług za szkody wynikające z użycia certyfikatu poza zakresem określonym w polityce certyfikacji, która została wskazana w certyfikacie, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie. Ponadto podmiot świadczący wskazane wyżej usługi nie powinien ponosić odpowiedzialności za szkodę wynikłą z nieprawdziwości danych podanych w certyfikacie w przypadku wpisania tych danych na wniosek osoby składającej podpis elektroniczny, bądź posługujących się pieczęcią elektroniczną.

W zakresie odpowiedzialności cywilnoprawnej należy także ustanowić w prawie krajowym obowiązek zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług zaufania. Ustawa o usługach zaufania powinna zawierać delegację dla właściwego ministra do wydania rozporządzenia, które ureguluje szczegółowy zakres ubezpieczenia, termin powstania obowiązku ubezpieczenia oraz minimalną sumę gwarancyjną.

W odniesieniu do innych usług certyfikacyjnych wpisanych zgodnie z ustawą o podpisie elektronicznym do rejestru kwalifikowanych usług certyfikacyjnych i zgodnie z motywem 25 preambuły rozporządzenia eIDAS:

> Preambuła (25). Państwa członkowskie powinny zachować swobodę określania innych rodzajów usług zaufania oprócz tych, które figurują w zamkniętym wykazie usług zaufania przewidzianym w niniejszym rozporządzeniu, do celów uznania ich na szczeblu krajowym jako kwalifikowanych usług zaufania.

proponujemy następujące uregulowanie co do skutków prawnych:

L.p.	Kwalifikowane usługi zarejestrowane w Rejestrze usług certyfikacyjnych lub innych w Polsce	Propozycja uregulowania po Rozporządzeniem 910/2014 (eIDAS)
1	kwalifikowanego urzędu certyfikacji QCA	Zgodnie z Art. 28
2	kwalifikowana usługa znacznika czasu QTSA	Zgodnie z Art. 41,42
3	kwalifikowanego urzędu weryfikacji statusu certyfikatu QOCSP	Zgodnie z Art. 32 ustęp 1 a), Art. 33
4	kwalifikowanego urzędu walidacji danych QDVCS	Zgodnie z Art. 32 ustęp 1, Art. 33
5	kwalifikowanego urzędu poświadczania odbioru i przedłożenia QDA	Zgodnie z Art. 43, Art.44
6	kwalifikowanego urzędu depozytów obiektów QODA	Zgodnie z Art. 44
7	kwalifikowanego urzędu rejestrów i repozytoriów QRRA	Zgodnie z Preambułą p.(25) powinny być określone zakres uznawania dowodów na szczeblu krajowym.
8	kwalifikowanego urzędu certyfikatów atrybutów QACA	Zgodnie z Art. 28 ustęp 3,

Przy czym w zakresie określenia konkretnych nazw i identyfikatorów usług zaufania należy spodziewać się konkretnych propozycji w akcie implementującym definiującym format i obsługę listy zaufania zgodnie z art. 22 rozporządzenia UE 910/2014. Może okazać się konieczność wprowadzenia znaczących zmian w zakresie nazw i typów usług. Przykładowo usługę „kwalifikowanego urzędu certyfikacji QCA" trzeba będzie zmienić na usługę „kwalifikowana usługa tworzenia kwalifikowanych certyfikatów podpisu" zgodnie z rozporządzeniem eIDAS. Na poziomie aktu implementacyjnego do rozporządzenia 910/2014 może zostać wprowadzona możliwość agregacji kilku usług do jednej, przykładowo w zakresie wydawania kwalifikowanych certyfikatów podpisu i certyfikatów pieczęci „kwalifikowana usługa tworzenia certyfikatów kwalifikowanego podpisu i certyfikatów kwalifikowanej pieczęci ". jeżeli taka agregacja nie pojawi się w odpowiednim akcie implementacyjnym, to przykładowa kwalifikowana usługa przytoczona powyżej powinna być sklasyfikowana jako „nieokreślona" odnośnie zapisów rozporządzenia eIDAS i jej skutek prawny wtedy należy określić w prawie krajowym.

SPOSOBY I ŚRODKI NADZORU, MONITORINGU I KONTROLI

Nadzór nad przestrzeganiem przepisów krajowych regulujących zasady świadczenia usług zaufania winien zostać powierzony ministrowi właściwemu ds. gospodarki. Nadzór ten winien być realizowany w pierwszej mierze poprzez prowadzenie listy, o której mowa w art. 22 rozporządzenia eIDAS oraz umieszczanie na tej liście podmiotów świadczących kwalifikowane usługi zaufania oraz wykreślanie z tej listy tych podmiotów w przypadkach przewidzianych przepisami ustawy. Ponadto minister winien być upoważniony do prowadzenia kontroli działalności podmiotów świadczących kwalifikowane usługi zaufania, jak też winien posiadać kompetencje do nakładania kar administracyjnych przewidzianych przepisami ustawy.

Przedmiotem kontroli prowadzonej przez właściwy organ winno być prowadzenie działalności w sposób zgodny z przepisami regulującymi zasady świadczenia tych usług, przy czym organ kontrolny winien mieć na uwadze także konieczność wspierania przez państwo członkowskie celów regulacji prawa unijnego, a zatem winien prowadzić kontrolę zarówno pod kątem przestrzegania przez podmiot świadczący usługi prawa krajowego, jak i unijnego.

Kontrola winna być prowadzona przez pracowników organu kontrolnego na podstawie pisemnego upoważnienia organu. Organ winien mieć uprawnienie do wszczynania kontroli z urzędu, jak i na wniosek innych organów państwa zwłaszcza sądów i prokuratur. Postępowanie kontrolne winno być zakończone protokołem pokontrolnym doręczanym podmiotowi kontrolowanemu, który winien posiadać uprawnienie do zgłoszenia zastrzeżeń w stosownym terminie. Organ winien ustosunkować się w formie pisemnej do zgłoszonych zastrzeżeń, a w przypadku ich nieprzyjęcia w całości lub w części organ ma prawo zobowiązać podmiot kontrolowany do usunięcia nieprawidłowości w terminie określonym ustawą o usługach zaufania. Ponadto w przypadku stwierdzenia przez organ kontrolny nieprawidłowości niedających się usunąć, bądź w przypadku nieusunięcia przez podmiot kontrolowany nieprawidłowości we wskazanym przez organ terminie, organ winien posiadać kompetencję do wydania decyzji administracyjnej w przedmiocie usunięcia podmiotu świadczącego kwalifikowane usługi zaufania z zaufanej listy, o której mowa w art. 22 rozporządzenia eIDAS.

Należy także rozważyć wprowadzenie dla organu kontrolnego uprawnienia do nakładania kar administracyjnych w kwotach nieprzekraczających limitu określonego przepisami ustawy o usługach zaufania. Kara administracyjna winna mieć zastosowanie zwłaszcza w przypadkach, w których naruszenia przez podmioty przepisów regulujących zasady działalności podmiotów świadczących kwalifikowanej usługi zaufania, mogła narazić odbiorców tych usług na poniesienie znacznej szkody.

W kontekście systemu nadzoru nad świadczeniem usług zaufania za istotne uznano omówienie zagadnień, które regulowane były dotychczas w ustawie o podpisie elektronicznym w jej art. 9. Zgodnie z tą regulacją prowadzenie działalności w zakresie świadczenia usług certyfikacyjnych nie wymagało uzyskania zezwolenia ani koncesji. Autorzy niniejszej ekspertyzy wskazują na zasadność uwzględnienia analogicznej regulacji w ustawie o usługach zaufania. Nie ulega wątpliwości, że usługi certyfikacyjne w Polsce były dotychczas świadczone na zasadach rynkowych, a więc podlegały zasadom konkurencji na zliberalizowanym, choć nadzorowanym rynku. Wydaje się, że dotychczasowy system właściwie spełnił swoją rolę, zaś elementy nadzoru stosowane na zasadach opisanych w ustawie o podpisie elektronicznym w sposób wystarczający zapewniały bezpieczeństwo użytkownikom tych usług. Nie zachodzi więc potrzeba większego ograniczenia wolności gospodarczej na rynku usług zaufania i z tego względu za zasadne uznano powtórzenie regulacji w ustawie o usługach zaufania, zgodnie z którą świadczenie usług zaufania nie będzie wymagało uzyskania zezwolenia, ani koncesji.

Kolejnym aspektem poruszanym w przepisie art. 9 ust. 2 ustawy o podpisie elektronicznym było wprowadzone tą regulacją ograniczenie możliwości świadczenia usług certyfikacyjnych przez organy władzy publicznej oraz Narodowy Bank Polski wyłącznie na użytek własny lub innych organów władzy publicznej. Jedynie jednostki samorządu terytorialnego mogły świadczyć usługi certyfikacyjne na zasadach niezarobkowych dla członków wspólnoty samorządowej (art. 9 ust. 3 ustawy o podpisie elektronicznym). W ocenie autorów niniejszej ekspertyzy działanie ustawodawcy, które dało swój wyraz w treści art. 9 ust. 2 ustawy o podpisie elektronicznym było uzasadnione i winno znaleźć swoją kontynuację w stosownych regulacjach ustawy o usługach zaufania. Z chwilą uchwalenia ustawy o podpisie elektronicznym ustawodawca zadecydował, że usługi certyfikacyjne zostaną pozostawione rynkowi, a ich świadczenie powierzone zostanie podmiotom komercyjnym. Konsekwencją takiego podejścia było słuszne ograniczenie możliwości konkurowania na tym rynku przez podmioty publiczne, albowiem państwo co do zasady powinno ograniczać swój aktywny udział w wolnorynkowej gospodarce (patrz także rozdz. 5.5.1).

Zagadnienia regulowane dotychczas w art. 9 ustawy o podpisie elektronicznym należy uznać za element nadzoru. Rozporządzenie eIDAS pozostawia państwom członkowskim prawo uregulowania zagadnień dotyczących systemu nadzoru, wskazując przy tym na obligatoryjność wykonywania określonych zadań o charakterze nadzorczym. Oznacza to, że państwo członkowskie ma możliwość wprowadzenia własnych regulacji w zakresie systemu nadzoru z uwzględnieniem regulacji rozporządzenia eIDAS w tym w szczególności sekcji 2 tego rozporządzenia pt. „Nadzór". W związku z tym proponuje się wprowadzenie do ustawy o usługach zaufania analogicznych rozwiązań jak miało to miejsce w art. 9 ustawy o podpisie elektronicznym. W tym zakresie proponuje się wprowadzenie ograniczenia możliwości świadczenia usług zaufania przez organy władzy publicznej wyłącznie na użytek własny lub na użytek innych organów władzy publicznej. Dotychczasowe doświadczenia związane z ograniczeniem możliwości aktywnego udziału w rynku usług certyfikacyjnych przez organy władzy publicznej wydają się być pozytywne, a przez to

zasługujące na kontynuację w warunkach ustawy o usługach zaufania. Dotychczasowe funkcjonowanie rynku usług certyfikacyjnych, na którym funkcjonowały w Polsce wyłącznie podmioty komercyjne uzasadnia postawienie tezy, że rynek ten odpowiedział na potrzeby jego uczestników, jak też zapewnił dostęp do usług certyfikacyjnych dla podmiotów, które były tym zainteresowane. Interwencja państwa w tym obszarze wydaje się nie znajdować w związku z tym uzasadnienia.

Analizując ewentualny udział organów władzy publicznej w rynku usług zaufania należy zwrócić uwagę na kilka aspektów. Przede wszystkim godzi się zauważyć, że organ władzy publicznej, który zamierzałby świadczyć tego typu usługi na zewnątrz, musiałby robić to na równych i konkurencyjnych zasadach z podmiotami komercyjnymi. Organ taki brałby udział w grze rynkowej, a zatem winien być traktowany w tym zakresie jak każdy inny podmiot gospodarczy. To z kolei rodzić może znaczne wątpliwości w zakresie dopuszczalności udzielania pomocy publicznej w zgodzie przede wszystkim z przepisami Traktatu o funkcjonowaniu Unii Europejskiej (dalej TFUE) - art. 107, 108 i 109. Kwestia ta wymagałaby odrębnej dogłębnej analizy, której nie sposób przeprowadzić w ograniczonych ramach niniejszej ekspertyzy. Niemniej jednak należy mieć na uwadze fakt, że zgodnie z art. 107 ust. 1 TFUE wszelka pomoc udzielana przez państwo lub z użyciem zasobów państwowych, która zakłóca lub grozi zakłóceniem konkurencji poprzez sprzyjanie niektórym przedsiębiorstwom lub produkcji niektórych towarów, jest niezgodna z rynkiem wewnętrznym w zakresie, w jakim wpływa na wymianę handlową między Państwami Członkowskimi. Istnieje przy tym, szereg warunków dopuszczalności pomocy publicznej, jednakże za niedopuszczalne (niezgodne z rynkiem wewnętrznym stanowiącym jeden z celów Unii Europejskiej) należałoby uznać konkurowanie przez organy państwowe z podmiotami komercyjnymi, z wykorzystaniem zasobów państwowych, bez żadnych ograniczeń.

Kolejną kwestią jest fakt, że organy władzy publicznej, które będą zainteresowane świadczeniem usług zaufania będą musiały być traktowane w taki sam sposób jak podmioty komercyjne w zakresie spełnienia wymogów świadczenia tych usług, jak też w zakresie sprawowania nad nimi nadzoru, zgłaszania zagrożeń itp. Zatem organy publiczne będą podlegały nadzorowi tak jak i inne podmioty świadczące usługi zaufania, zaś wszelkie zagrożenia i incydenty związane z bezpieczeństwem będą musiały być raportowane analogicznie jak będzie to miało miejsce w przypadku podmiotów komercyjnych (art. 19 ust. 2 rozporządzenia eIDAS). Organy świadczące usługi zaufania musiałyby nadto ponosić pełną odpowiedzialność za świadczone usługi wobec ich odbiorców, w tym także odpowiedzialność finansową. Sytuacja ta rodziłaby potencjalną odpowiedzialność Skarbu Państwa za działania jego organów w zakresie usług zaufania.

ZAWIESZENIE CERTYFIKATÓW, ROZPOCZĘCIE I ZAKOŃCZENIE DZIAŁALNOŚCI USŁUGODAWCÓW

Rozporządzenie eIDAS w art. 28 ust. 5 wprowadza możliwość, aby przepisy krajowe państwa członkowskiego uregulowały kwestię tymczasowego zawieszenia kwalifikowanego certyfikatu podpisu elektronicznego. Wydaje się zatem zasadnym wprowadzenie w ustawie o usługach zaufania instytucji zawieszenia kwalifikowanego certyfikatu podpisu elektronicznego. Należy przy tym zapewnić w ustawie przestrzeganie zasady wyrażonej w art. 28 ust. 5 lit. a) rozporządzenia eIDAS stanowiącej, że czasowo zawieszony kwalifikowany certyfikat podpisu elektronicznego traci ważność na okres zawieszenia. Należy też uregulować w ustawie przesłanki zawieszenia analogicznie jak miało to miejsce w ustawie o podpisie elektronicznym (art. 21 ust. 4 PodElU). Zawieszenie winno zatem być instrumentem natychmiastowego zawieszenia certyfikatu w przypadku wystąpienia podejrzenia zaistnienia przesłanek stanowiących podstawę unieważnienia certyfikatu. Należy przy tym zapewnić zgodność z art. 28 ust. 5 lit. b) eIDAS poprzez wprowadzenie obowiązku oznaczania w bazie danych certyfikatów statusu certyfikatu z wyraźnym oznaczeniem okresu zawieszenia. Analogiczne rozwiązania proponuje się zastosować w odniesieniu do pieczęci elektronicznej, powołując się na pozostawienie w rozporządzeniu eIDAS także i tej materii do swobodnej regulacji prawa krajowego (art. 38 ust. 5 rozporządzenia eIDAS).

Rozpoczęcie działalności usługodawców kwalifikowanych winno być poprzedzone wnioskiem takiego podmiotu o wpis na zaufaną listę, o której mowa w art. 22 eIDAS. Świadczenie kwalifikowanych usług zaufania nie może być prowadzone bez wpisu na listę, skoro rozporządzenie eIDAS nakłada na państwo członkowskie obowiązek prowadzenia i publikowania listy zawierającej informacje dotyczące kwalifikowanych dostawców usług zaufania. Z tego względu w prawodawstwie krajowym należy na tego dostawców kwalifikowanych usług nałożyć obowiązek uzyskania wpisu na zaufaną listę przed rozpoczęciem działalności. Z racji doświadczenia w zakresie prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, zasadnym jest powierzenie prowadzenia

zaufanej listy, o której mowa w art. 22 eIDAS ministrowi właściwemu ds. gospodarki. Minister ten winien być zobligowany do sporządzania, prowadzenia i publikowania listy zgodnie z właściwymi przepisami rozporządzenia eIDAS oraz aktem wykonawczym, który zostanie wydany przez Komisję Europejską na podstawie art. 22 ust. 5 eIDAS.

W związku z obowiązkiem określonym w art. 21 ust. 2 rozporządzenia eIDAS, wpis podmiotu na zaufaną listę winien być poprzedzony weryfikacją spełnienia przez podmiot ubiegający się o wpis warunków, o których mowa w art. 24 rozporządzenia eIDAS. Wpisanie podmiotu na listę podobnie jak odmowa wpisu podmiotu na listę winny mieć formę decyzji administracyjnej.

Zakończenie działalności usługodawców winno gwarantować odbiorcom usług zaufania bezpieczeństwo oraz minimalizować ryzyko wystąpienia szkody. Kwalifikowani dostawcy usług zaufania winni posiadać i w miarę potrzeby aktualizować plany zakończenia działalności, które w szczególności będą zapewniały realizację obowiązku udostępniania po zakończeniu działalności informacji dotyczących danych wydanych i otrzymanych przez tego dostawcę, zwłaszcza do celów przedstawiania dowodów w postępowaniach sądowych oraz do celów zapewnienia ciągłości usług.

PROPONOWANE AKTY WYKONAWCZE DO USTAWY

Rozporządzenie eIDAS daje podstawę prawną Komisji Europejskiej do wydania szeregu aktów wykonawczych. Jednocześnie rozporządzenie to w wielu miejscach odsyła do regulacji prawa krajowego. Z tego względu na potrzeby niniejszej ekspertyzy dokonano porównania delegacji do wydania aktów wykonawczych zawartych w rozporządzeniu eIDAS oraz delegacji do wydania rozporządzeń zawartych w obowiązującej dotychczas ustawie o podpisie elektroniczny. Zweryfikowano w ten sposób niezbędny zakres rozporządzeń, które powinny lub które potencjalnie mogą być wydane pod nową ustawą o usługach zaufania. Zidentyfikowano w ten sposób następujące obszary, które winny być regulowane w prawie krajowym w formie rozporządzeń:

1. Szczegółowy zakres ubezpieczenia obowiązkowego, termin powstania obowiązku ubezpieczenia oraz minimalną sumę gwarancyjną.

   Rozporządzenie eIDAS wskazuje na obowiązek posiadania ubezpieczenia odpowiedzialności cywilnej przez dostawców kwalifikowanych usług zaufania. Zakres tego ubezpieczenia winien być regulowany przez prawo krajowe.
2. Wzór i szczegółowy zakres wniosku podmiotu zamierzającego świadczyć kwalifikowane usługi zaufania o wpis na zaufaną listę, o której mowa w art. 22 eIDAS.
3. Sposób prowadzenia zaufanej listy kwalifikowanych podmiotów świadczących usługi zaufania, o której mowa w art. 22 rozporządzenia eIDAS, wzór tej listy oraz szczegółowy tryb postępowania w sprawach o wpis na listę.

   Rozporządzenie eIDAS nakłada na państwo członkowskie obowiązek prowadzenia zaufanej listy podmiotów świadczących kwalifikowane usługi zaufania. Niektóre kwestie techniczne zostaną określone w rozporządzeniu wykonawczym KE wydanym na podstawie art. 22 ust. 5 rozporządzenia eIDAS. Po wydaniu tego rozporządzenia należy zweryfikować, czy na potrzeby procedur krajowych zasadne jest doregulowanie niektórych zagadnień związanych z prowadzeniem listy na poziomie prawa krajowego, przy czym regulacja ta powinna zapewniać zachowanie wymogów dotyczących prowadzenia list wskazanych w art. 22 rozporządzenia eIDAS, a także nie może ona zawierać regulacji stanowiących powtórzenie zagadnień uregulowanych w rozporządzeniu wykonawczym KE.

W odniesieniu do istniejących aktualnie rozporządzeń wykonawczych do ustawy o podpisie elektronicznym dokonano analizy zasadności ponowienia tych aktów po wejściu w życie ustawy o usługach zaufania. W wyniku tej analizy wprowadzono następujące wnioski.

1) Rozporządzenie Ministra Gospodarki z dn. 9 sierpnia 2002 r., w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym (Dz.U. 2002 nr 128 poz. 1101).

   Proponuje się pozostawić tego typu rozporządzenie, przy czym należy dostosować je do rozporządzenia eIDAS, m.in. w miejsce zaświadczenia i poświadczenia certyfikacyjnego używać odpowiednio: kwalifikowany certyfikat pieczęci elektronicznej oraz zaawansowana pieczęć elektroniczna. Dotyczy to także formatów i procedur wydawania certyfikatów dostawcom usług zaufania. Należy przy tym pamiętać, że zgodnie z art. 21, ust. 4. eIDAS Komisja Europejska może w drodze aktów wykonawczych określić formaty i procedury na użytek

ust. 1 i 2 eIDAS. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2 eIDAS.

2) Rozporządzenie Ministra Gospodarki z dnia 6 sierpnia 2002 r. w sprawie sposobu prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzoru tego rejestru oraz szczegółowego trybu postępowania w sprawach o wpis do rejestru. (Dz.U.2002.128.1099)

   Rozporządzenie to proponuje się usunąć, ponieważ zgodnie z art. 22, ust. 5 eIDAS. *Do dnia 18 września 2015 r. Komisja w drodze aktów wykonawczych określi informacje, o których mowa w ust. 1, oraz techniczne specyfikacje i formaty dotyczące zaufanych list mające zastosowanie na użytek ust. 1–4* eIDAS. *Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2* eIDAS.

3) Rozporządzenie Ministra Gospodarki z dn. 6 sierpnia 2002 r. w sprawie wysokości opłaty za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym (Dz.U.2002.128.1098).

   Proponuje się pozostawić rozporządzenie lub alternatywnie połączyć z je z rozporządzeniami Dz.U.2002.128.1101, Dz.U.2002.128.1099 i Dz.U.2002.128.1097.

4) Rozporządzenie Ministra Gospodarki z dnia 6 sierpnia 2002 r w sprawie wzoru i szczegółowego zakresu wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym (Dz.U.2002.128.1097).

   Rozporządzenie proponuje się pozostawić, ale dostosować do eIDAS. Zgodnie z art. 21, ust. 4 eIDAS. *Komisja może w drodze aktów wykonawczych określić formaty i procedury na użytek ust. 1 i 2* eIDAS. *Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2* eIDAS.

5) Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia 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 (Dz.U. 2002 nr 128 poz. 1094).

   Rozporządzenie to dotyczy:

   - szczegółowych warunków technicznych, jakim powinny odpowiadać bezpieczne urządzenia do składania podpisów elektronicznych oraz bezpieczne urządzenia do weryfikacji podpisów elektronicznych;
   - podstawowych wymagań organizacyjnych i technicznych dotyczących polityk certyfikacji dla kwalifikowanych certyfikatów;
   - szczegółowych warunków technicznych i organizacyjnych, które muszą spełniać kwalifikowane podmioty świadczące usługi certyfikacyjne.

   Większość przepisów rozporządzenia pokrywa się z wymaganiami określonymi w rozporządzeniu eIDAS oraz będą opisane m.in. w następujących normach technicznych:

   (a) oprogramowanie do generowania i weryfikowania podpisów elektronicznych

   - ✓ CEN prEN 419103 *Conformity assessment for signature creation and validation applications*,

   (b) urządzenie do składania podpisu elektronicznego

   - ✓ CEN EN 419211-1: Protection profiles for secure signature creation device — Part1: Overview.
   - ✓ CEN EN 419211-2: Protection profiles for secure signature creation device — Part 2: Device with key generation.
   - ✓ CEN EN 419211-3: Protection profiles for secure signature creation device — Part 3: Device with key import.

- ✓ CEN EN 419211-4: Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application;
- ✓ prCEN/TR 419200: Business guidance for signature creation and other related devices

(c) wymagania organizacyjne i techniczne dotyczące polityk certyfikacji dla kwalifikowanych certyfikatów

- ✓ ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 1: Overview and common data structures."
- ✓ ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons".
- ✓ ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 3: Certificate Profile for certificates issued to legal persons".
- ✓ ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 4: Certificate Profile for TLS/SSL certificates issued to organisations".
- ✓ ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Qualified Certificate Statements for Qualified Certificate profiles".

(d) wymagania dotyczące warunków technicznych i organizacyjnych, które muszą spełniać kwalifikowane podmioty świadczące usługi certyfikacyjne

- ✓ ETSI EN 319 401 General Policy Requirements for Trust Service Providers supporting Electronic Signatures
- ✓ EN 319 411-2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates

Z tego powodu proponuje się wycofanie rozporządzenia, zaś zapisy nieuregulowane przez Rozporządzenie eIDAS lub niezbędne elementy rozporządzenia przenieść do ustawy o usługach zaufania. Dodatkowo, ponieważ zgodnie z art. 28 ust. 5 eIDAS państwa członkowskie mogą ustanawiać przepisy krajowe dotyczące tymczasowego zawieszenia kwalifikowanego certyfikatu podpisu elektronicznego, problem zawieszania certyfikatów powinien zostać uregulowany także w ustawie o usługach zaufania.

PROBLEMATYKA OCHRONY DANYCH OSOBOWYCH

Rozporządzenie eIDAS przywołuje w motywie 11 preambuły problematykę ochrony danych osobowych wskazując, że powinno być ono stosowane w pełnej zgodności z zasadami dotyczącymi ochrony danych osobowych przewidzianymi w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.. Rozporządzenie wskazuje, że uwierzytelnianie dla usługi online powinno dotyczyć przetwarzania tylko tych danych identyfikacyjnych, które są adekwatne, właściwe i nie wykraczają poza cele przyznania dostępu do tej usługi online. Ponadto dostawcy usług zaufania i organy nadzoru powinny przestrzegać wymogów na mocy dyrektywy 95/46/WE dotyczących poufności i bezpieczeństwa przetwarzania. Nie ulega więc wątpliwości, że zarówno po stronie państwa członkowskiego, jak i po stronie dostawców usług zaufania spoczywają obowiązki związane z przetwarzaniem danych osobowych w zgodzie z przytoczoną wyżej dyrektywą. W Polsce jej implementację zapewnia ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Mając na uwadze powyższe zachodzi więc konieczność uwzględniania w nowoprojektowanej ustawie o usługach zaufania obowiązków przestrzegania reguł wynikających z ustawy o ochronie danych osobowych. W dotychczasowej ustawie o podpisie elektronicznym problematyka ochrony danych osobowych była w zasadzie pominięta. Podmioty świadczące usługi certyfikacyjne zobowiązane były mocą tej ustawy do pozyskania od osoby ubiegającej się o

certyfikat pisemnej zgody na stosowanie danych służących do weryfikacji jej podpisu elektronicznego, które są zawarte w wydanym certyfikacie (art. 14 ust. 7 ustawy o podpisie elektronicznym). W literaturze wskazuje się jednak, że przepis ten nie odnosi się do problematyki ochrony danych osobowych, a jego celem jest wytworzenie dokumentu wiążącego wydany certyfikat z konkretną osobą[14]. Wydaje się zatem, że w kontekście obowiązków związanych z właściwym traktowaniem gromadzonych danych osobowych przez dostawców usług zaufania w ustawie o usługach zaufania zasadne będzie wprowadzenie szerszej niż dotychczas regulacji. Art. 5 ust. 1 rozporządzenia eIDAS wskazuje, że przetwarzanie danych osobowych prowadzone jest zgodnie z przepisami dyrektywy 95/46/WE. Analogiczny przepis mógłby znaleźć się w ustawie o usługach zaufania wskazując, że przetwarzanie przez dostawców usług zaufania danych osobowych odbiorców usług zaufania wino odbywać się na podstawie ustawy o ochronie danych osobowych. Tego typu odesłanie zapewni zgodność regulacji ustawy o usługach zaufania z wymogiem wyrażonym w rozporządzeniu eIDAS dotyczącym przestrzegania wymogów dyrektywy 95/46/WE, albowiem ustawa o ochronie danych osobowych implementuje na grunt prawa krajowego dyrektywę 95/46/WE.

2.3 Analiza zmian niezbędnych do wprowadzenia w krajowym systemie prawnym

Na potrzeby niniejszej ekspertyzy dokonano analizy krajowego porządku prawnego pod kątem wymaganych zmian w związku z wejściem w życie rozporządzenia eIDAS. Analiza ta doprowadziła do następujących wniosków. Po pierwsze w krajowym porządku prawnym funkcjonuje bardzo wiele aktów prawnych, których przepisy odsyłają do ustawy o podpisie elektronicznym. Są to najczęściej odesłania do pojęć stosowanych w tej ustawie. Niewątpliwie uchylenie ustawy o podpisie elektronicznym doprowadziłoby do pojawienia się w polskim porządku prawnym pustych odesłań i pustych definicji w bardzo wielu aktach prawnych dotyczących rozmaitych dziedzin. Tego typu sytuacja jest niezgodna z zasadami legislacji i jako taka niepożądana gdyż prowadzi ona do zachwiania bezpieczeństwa prawnego i utrudnia, a w wielu przypadkach może nawet uniemożliwiać stosowanie podpisu elektronicznego lub innych usług zaufania w kontaktach z organami administracji publicznej oraz w kontaktach między podmiotami niepublicznymi. W związku z tym analiza, którą uwzględniono w niniejszej ekspertyzie w pierwszej mierze zawiera wszystkie akty prawne pochodzące z krajowego porządku prawnego, które wymagają zmiany w związku z uchyleniem ustawy o podpisie elektronicznym. Dokonując przeglądu tych aktów zaproponowano także w wielu przypadkach rozszerzenie katalogu akceptowanych w danych dziedzinach czy obszarach innych niż podpis elektroniczny usług zaufania. Rekomendacje te należy traktować jako rozwiązania nieobligatoryjne, acz pożądane. Należy bowiem wskazać, że dotychczas w polskich aktach prawnych odsyłano w zasadzie wyłącznie do podpisu elektronicznego, podczas gdy rozporządzenie eIDAS wprowadza szereg innych usług zaufania, których stosowanie prawodawca europejski traktuje jako oczekiwane przez uczestników życia publicznego, społecznego, czy gospodarczego.

Drugą grupą aktów prawnych, które analizowano na potrzeby niniejszej ekspertyzy są akty, które zawierają w swej treści pojęcia odnoszące się do usług zaufania dotychczas występujące w polskim porządku prawnym. Jest to bardzo liczna grupa aktów prawnych, których wylistowanie uznano za niezasadne. W odniesieniu do tych aktów wskazano na reguły modyfikacyjne, które winny mieć w odniesieniu do tych aktów zastosowanie. Opisano pojęcia występujące w krajowych aktach prawnych wskazując na terminy, które powinny zastąpić dzisiejsze pojęcia.

Trzecią grupę przepisów stanowią akty stanowiące fundament niektórych gałęzi prawa. Uznano za niezbędne odniesienie się w sposób szerszy do Kodeksu cywilnego, a zwłaszcza przepisów traktujących o formach czynności prawnych. Ustosunkowano się także do procedury cywilnej uregulowanej w Kodeksie postępowania cywilnego oraz do procedury administracyjnej uregulowanej w Kodeksie postępowania administracyjnego.

W odniesieniu do pierwszej ze wskazanych grup przepisów autorzy niniejszej ekspertyzy opracowali poniższy katalog propozycji zmian istniejących przepisów prawa polskiego. W katalogu tym wskazano akty prawne pochodzące z polskiego systemu prawnego obowiązujące na dzień sporządzenia niniejszej ekspertyzy. W odniesieniu do

[14] tak R. Podpłoński w: R. Podpłoński, P. Popis, Podpis elektroniczny. Komentarz, Warszawa 2004, s. 271-272.

rozporządzeń przeanalizowano delegacje do ich wydania, przy czym nie zidentyfikowano w żadnym z przypadków konieczności zmiany tych delegacji.

2.4 Analiza proponowanych zmian terminologicznych

Dotychczasowa nomenklatura wywodząca się z regulacji ustawy o podpisie elektronicznym posługiwała się pojęciem podpisu elektronicznego, bezpiecznego podpisu elektronicznego oraz bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu. Tymczasem w nomenklaturze prawa unijnego występuje przede wszystkim pojęcie usług zaufania. Rozporządzenie eIDAS posługuje się pojęciami: podpis elektroniczny, zaawansowany podpis elektroniczny oraz kwalifikowany podpis elektroniczny. Uznaje się zatem za konieczne dostosowania obowiązujących przepisów prawa do nomenklatury prawa europejskiego. W związku z tym w krajowych przepisach prawnych należy usunąć pojęcie bezpiecznego podpisu elektronicznego oraz bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu. W miejsce tych pojęć należy wprowadzić pojęcie zaawansowanego podpisu elektronicznego oraz kwalifikowanego podpisu elektronicznego, którymi to pojęciami powinna posługiwać się także ustawa o usługach zaufania. Proponuje się wprowadzenie rozwiązania zgodnie, z którym ilekroć w aktach prawa występuje pojęcie bezpiecznego podpisu elektronicznego, należy przez to rozumieć zaawansowany podpis elektroniczny w rozumieniu art. 3 pkt 11 rozporządzenia eIDAS, a ilekroć w aktach prawa występuje pojęcie bezpiecznego podpisu elektronicznego weryfikowanego przy pomocy ważnego kwalifikowanego certyfikatu, należy przez to rozumieć kwalifikowany podpis elektroniczny w rozumieniu art. 3 pkt 12 rozporządzenia eIDAS. Stosując powyższą regułą należy wszakże dokonać weryfikacji, czy ustawodawca posługując się w określonych aktach prawnych pojęciem bezpiecznego podpisu elektronicznego bez wskazania że chodzi tu o podpis weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu, zrobił to w sposób zamierzony i czy w danych okolicznościach użycie zaawansowanego podpisu elektronicznego będzie wystarczające, czy też należałoby raczej używać w tego typu przypadkach pojęcia kwalifikowanego podpisu elektronicznego.

Należy też odejść w polskim ustawodawstwie od używania pojęcia kwalifikowanego podmiotu świadczącego usługi certyfikacyjne w zakresie podpisu elektronicznego. Ilekroć tego typu pojęcie występuje w aktach prawnych należy zastąpić je pojęciem kwalifikowanego dostawcy usług zaufania w rozumieniu art. 3 pkt 20 rozporządzenia eIDAS.

Wprowadzając omawiane zmiany należy mieć na uwadze termin wejścia w życie rozporządzenia eIDAS. Rozporządzenie to zostało opublikowane i weszło w życie, jednakże na podstawie art. 52 ust. 2 stosuje się je od 1 lipca 2016 r. W związku z tym należy przyjąć, że do czasu stosowania przepisów rozporządzenia eIDAS obowiązują przepisy aktualne, a zatem m.in. przepisy ustawy o podpisie elektronicznym. Wprowadzając zmiany w obowiązujących przepisach prawa polskiego należy mieć na uwadze datę rozpoczęcia stosowania przepisów rozporządzenia eIDAS, która to data winna być tożsama z datą wejścia w życie przepisów zmieniających określone pojęcia czy terminy występujące w przepisach prawa polskiego. Do czasu rozpoczęcia stosowania rozporządzenia eIDAS należy stosować przepisy – a zatem także pojęcia i terminy – obowiązujące aktualnie, tj. pojęcia z ustawy o podpisie elektronicznym. Dotyczy to wszakże terminologii, która jest znana aktualnemu prawodawstwu krajowemu. Rozporządzenie eIDAS wprowadza przy tym szereg pojęć, które dotychczas w przepisach polskich nie występowały. W związku z tym w odniesieniu do tych pojęć, które w prawie krajowym do tej pory nie występowały, zasadne jest wprowadzanie do przepisów krajowych definicji zgodnych z rozporządzeniem eIDAS – nawet przed datą 1 lipca 2016 r. Należy bowiem zaznaczyć, że rozporządzenie to zostało opublikowane i obowiązuje, zaś stosowanie jego przepisów zostało odłożone w czasie. W ocenie autorów niniejszej ekspertyzy można zatem już obecnie wprowadzać do prawa krajowego definicje zawarte w rozporządzeniu eIDAS, dążąc jednocześnie do pełnej unifikacji pojęć w przepisach prawa krajowego i europejskiego tak, aby z dniem 1 lipca 2016 r. możliwe było skuteczne stosowanie na gruncie krajowym przepisów rozporządzenia eIDAS.

W kontekście powyższego należy podkreślić, że Polska jako państwo członkowskie Unii Europejskiej powinna dostosować prawo krajowe do rozporządzenia eIDAS tak, by rozporządzenie to mogło być bez przeszkód stosowane w Polsce od 1 lipca 2016 roku. Oznacza to, że organy administracji centralnej odpowiedzialne za określone działy administracji rządowej, winny dokonać wszelkich wymaganych zmian i zapewnić wejście ich w życie najpóźniej z dniem 1 lipca 2016 r.

2.5 Analiza proponowanych zmian kodeksowych

Popularyzacja korzystania z usług zaufania w obrocie prawnym, zwłaszcza w kontaktach z administracją publiczną, choć nie tylko, prowadzi do konieczności podjęcia refleksji nad dotychczasowymi unormowaniami dotyczącymi form czynności prawnych zawartymi w przepisach Kodeksu cywilnego. Aktualne brzmienie art. 78 § 2 k.c. wprowadza równoważny skutek prawny między oświadczeniem woli składanym w postaci elektronicznej opatrzonym podpisem elektronicznym weryfikowanym przy pomocy ważnego kwalifikowanego certyfikatu oraz oświadczeniem woli składanym w formie pisemnej. Rozwiązanie to nie wpłynęło na rozwój czynności prawnych podejmowanych w postaci elektronicznej z użyciem wymienionego rodzaju podpisu elektronicznego, zaś w praktyce często wykorzystywane są inne formy uwierzytelniania służące zawarciu umów. W związku z tym zasadne jest rozważenie możliwości wprowadzenia do polskiego porządku prawnego formy elektronicznej jako autonomicznej formy czynności prawnych, która stanowić może formę odrębną, acz równoważną w stosunku do formy pisemnej. W kontekście tego postulatu jako pożądaną należy ocenić projektowaną zmianę Kodeksu cywilnego (druk sejmowy nr 2678) w zakresie dotyczącym formy elektronicznej[15]. Zachowanie formy elektronicznej poprzez złożenie oświadczenia w postaci elektronicznej i opatrzenie go podpisem elektronicznym umożliwiającym identyfikację osoby składającej oświadczenie jest rozwiązaniem właściwym z punktu widzenia z jednej strony usankcjonowania obecnych dziś na rynku rozwiązań, a z drugiej strony mając na względzie zamiar popularyzacji czynności prawnych dokonywanych w formie elektronicznej. Zmiany w tym zakresie, które są obecnie projektowane w Kodeksie cywilnym wydają się w sposób wyczerpujący uregulować omawianą materię, co oznacza, że projektowana ustawa o usługach zaufania nie wymaga regulacji odnoszących się do formy elektronicznej jako formy czynności prawnych.

Drugim zagadnieniem związanym z przepisami Kodeksu cywilnego wymagającym omówienia w niniejszej ekspertyzie jest instytucja daty pewnej. Rozporządzenie eIDAS w art. 41 wprowadza skutek prawny elektronicznych znaczników czasu wskazując, że kwalifikowany elektroniczny znacznik czasu korzysta z domniemania dokładności daty i czasu jakie wskazuje, oraz integralności danych, z którymi wskazywane data i czas są połączone. Z drugiej strony rozporządzenie nakazuje dopuścić jako dowód w postępowaniu sądowym elektroniczny znacznik czasu oraz zabrania kwestionować jego skutku prawnego tylko z powodu elektronicznej postaci znacznika, bądź niespełnienia wymogów znacznika kwalifikowanego. Rozporządzenie nakazuje też wzajemną uznawalność kwalifikowanych znaczników czasu wydanych we wszystkich państwach członkowskich. W związku z tym zasadnym wydaje się nadanie skutków daty pewnej także takiej czynności prawnej, gdy dokument w postaci elektronicznej został oznaczony czasem z wykorzystaniem kwalifikowanej usługi elektronicznego znacznika czasu w rozumieniu art. 3 pkt 33 rozporządzenia eIDAS - od daty znakowania czasem. Wydaje się, że tego typu rozwiązanie, mając na względzie wymogi co do kwalifikowanych elektronicznych znaczników czasu opisane w art. 42 rozporządzenia eIDAS, zapewni niezbędne dla zachowania waloru daty pewnej bezpieczeństwo integralności i nienaruszalności danych z którymi znacznik czasu jest powiązany, jak też zagwarantuje precyzyjne określenie daty i czasu.

W kontekście procedury cywilnej ustawodawca winien podjąć działania zmierzające do wprowadzenia prawnej i proceduralnej skuteczności pism wnoszonych w postępowaniu cywilnym w postaci elektronicznej. Chodzi tu o dopuszczenie do każdego postępowania cywilnego możliwości komunikowania się z sądem w postaci elektronicznej. W chwili obecnej istnieją jedynie fragmentaryczne rozwiązania polegające na umożliwieniu stronie postępowania cywilnego komunikacji z sądem w postaci elektronicznej, jak np. elektroniczne postępowanie upominawcze, czy możliwość zawarcia umowy spółki z ograniczoną odpowiedzialnością za pomocą elektronicznego wzorca. Postulowanym kierunkiem zmian jest objęcie wszystkich postępowań regulowanych Kodeksem postępowania

[15] patrz: druk sejmowy nr 2678, w którym wskazano: „Umieszczenie definicji formy elektronicznej w odrębnym przepisie jednoznacznie przesądzi o tym, że stanowi ona odrębny, choć równoważny w stosunku do formy pisemnej, typ formy szczególnej. Takie rozwiązanie pozwala na rozstrzygnięcie od lat prowadzonej dyskusji w zakresie potrzeby wyróżnienia formy elektronicznej jako odrębnej formy czynności prawnej."
http://orka.sejm.gov.pl/Druki7ka.nsf/0/875C0623FA3DA082C1257D410036BBCD/%24File/2678.pdf

cywilnego możliwością wykorzystywania formy elektronicznej. Wydaje się, że tego typu zmiany są konieczne, skoro inne przepisy prawa wskazują na równoważność formy elektronicznej oraz formy pisemnej. Niewątpliwie konieczne wydaje się wprowadzenie jednoznacznych regulacji, które usankcjonują podejmowanie przez strony czynności procesowych w formie elektronicznej, skoro strony te będą mogły dokonywać skutecznych czynności prawnych w formie elektronicznej. Ponadto koniecznym będzie dostosowanie funkcjonujących w Polsce systemów dla publicznych usług on-line do wzajemnej uznawalności środków identyfikacji elektronicznej wydanych w pozostałych państwach członkowskich, o czym mowa jest w art. 6 rozporządzenia eIDAS. Tyczy się to także funkcjonujących już dziś w procedurze cywilnej systemów, jak choćby elektroniczne postępowanie upominawcze.

Nie ulega też wątpliwości, że wprowadzenie elektronicznej komunikacji stron z sądem w sprawach cywilnych wpłynie korzystnie na ograniczenie czynności o charakterze biurokratycznym podejmowanych w związku z prowadzeniem tego typu postępowań, co z kolei przyczyni się do znacznego ograniczenia czasu trwania postępowań.
Mając na względzie powyższe postulatem godnym wyartykułowania jest wprowadzenie w Kodeksie postępowania cywilnego prawnej skuteczności i dopuszczalności pism procesowych wnoszonych w postaci elektronicznej opatrzonych kwalifikowanym podpisem elektronicznym lub wnoszonych w postaci elektronicznej poprzez kwalifikowaną usługę rejestrowanych doręczeń elektronicznych.. Jednocześnie zasadnym byłoby wykorzystanie po stronie sądu usługi pieczęci elektronicznej jako poświadczenia wniesienia przez stronę określonego pisma procesowego w postaci elektronicznej.

Istotnym zagadnieniem zasługującym na szerszą analizę w kontekście wejścia w życie rozporządzenia eIDAS jest postępowanie administracyjne. 11 maja 2014 r. w życie weszły zmiany Kodeksu postępowania administracyjnego, które w swych założeniach miały wprowadzić obowiązek zapewnienia możliwości prowadzenia postępowania administracyjnego z użyciem kwalifikowanego podpisu elektronicznego bądź profilu zaufanego. W kontekście rozporządzenia eIDAS nowelizację tę należy jednak uznać za niewystarczającą. Wprowadzone w art. 39^1 k.p.a. mechanizmy doręczania pism w postępowaniu administracyjnym drogą elektroniczną oraz warunki użycia tego trybu winny uwzględniać wymagania rozporządzenia eIDAS. O ile bowiem za słuszne należy uznać rozwiązanie zgodnie z którym organ administracji publicznej zobowiązany jest doręczać uczestnikowi postępowania pisma w formie elektronicznej, jeżeli uczestnik postępowania wniesie pismo drogą elektroniczną, bądź o taką formę doręczeń wystąpi, o tyle należy pamiętać, że państwa członkowskie zobowiązane są do akceptowania i wzajemnego uznawania notyfikowanych w Komisji Europejskiej środków identyfikacji elektronicznej (art. 6 rozporządzenia eIDAS). Wiąże się z tym zagadnieniem regulacja art. 63 k.p.a., który to przepis winien zapewniać i dopuszczać możliwość uwierzytelnienia nie tylko z użyciem mechanizmów wskazanych w art. 20a ust. 1 i 2 ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*, ale także z użyciem wszystkich notyfikowanych systemów identyfikacji elektronicznej. Skoro bowiem organ administracji zapewnia dostęp do usługi online, powinien on jednocześnie zapewnić możliwość identyfikacji zgodnie z wyrażoną w art. 6 rozporządzenia eIDAS zasadą wzajemnego uznawania. Należy tu też zwrócić uwagę na fakt, że przepisy k.p.a. winny jednocześnie dopuszczać możliwość zgłoszenia przez uczestnika postępowania żądania, o którym mowa w art. 39^1 k.p.a. także za pomocą każdego notyfikowanego środka identyfikacji elektronicznej spełniającego warunki art. 6 ust. 1 lit. a-c rozporządzenia eIDAS. Jeśli bowiem strona postępowania ma prawo zgodnie ze znowelizowanym k.p.a. zgłosić żądanie otrzymywania pism w formie elektronicznej, a organ administracji ma obowiązek spełnić zadość takiemu żądaniu, to zgłoszenie żądania otrzymywania pism w formie elektronicznej nie może odbywać się tylko z użyciem tych środków identyfikacji elektronicznej, które stosowane są obecnie, ale także winno być możliwe zgodnie z zasadą wzajemnego uznawania przy użyciu każdego notyfikowanego środka identyfikacji elektronicznej z zachowaniem warunków art. 6 rozporządzenia eIDAS, a więc m.in. zgodnie z przyjętym poziomem bezpieczeństwa środka identyfikacji elektronicznej.

Analogiczne rozwiązanie tyczy się także uregulowanego w art. 33 § 2a k.p.a. zagadnienia uwierzytelniania pełnomocnictwa w formie dokumentu elektronicznego. Nie jest bowiem wystarczające także i w tym przypadku odesłanie do art. 20a ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*, albowiem przepis ten nie daje możliwości wykorzystania do uwierzytelniania środków identyfikacji notyfikowanych w myśl art. 6 i nast. rozporządzenia eIDAS. Wskazany przepis winien umożliwiać uwierzytelnianie pełnomocnictw, które posiadają formę dokumentu elektronicznego z użyciem każdego notyfikowanego środka identyfikacji elektronicznej (zarówno

krajowego, jak i pochodzącego z innych państw członkowskich UE), z zachowaniem warunków art. 6 rozporządzenia eIDAS (w tym także dot. poziomu bezpieczeństwa).

Uwagi wymaga także niewątpliwie kwestia doręczania przez organ pism w formie dokumentu elektronicznego, o czym mowa jest w art. 46 § 4 k.p.a. Przepis ten opisuje sposób doręczania tego typu pism powołując się przy tym – wzorem innych przepisów k.p.a. - na uwierzytelnianie uczestnika postępowania w celu odbioru pisma za pomocą środków o których mowa w art. 20a ustawy *o informatyzacji działalności podmiotów realizujących zadania publiczne*. Jak wyżej wskazano tego typu rozwiązanie jest niewystarczające w myśl rozporządzenia eIDAS. Należy bowiem także i przy czynnościach związanych z odbiorem pisma w formie elektronicznej dopuścić wszystkie te środki identyfikacji elektronicznej, o których mowa w art. 6 rozporządzenia eIDAS.

Rozważenia godne jest także rozwiązanie, w którym doręczanie pism w postępowaniu administracyjnym odbywałoby się z użyciem kwalifikowanej usługi rejestrowanego doręczenia elektronicznego i należy w ocenie autorów niniejszej ekspertyzy rozważyć wprowadzenie do k.p.a. dopuszczalności doręczania przy użyciu tej usługi. Tego typu rozwiązanie mogłoby być korzystne dla tych organów administracji publicznej, które z uwagi na niewielki zakres i ilość prowadzonych postępowań miałyby trudności w budowie własnych systemów doręczania pism w formie elektronicznej, a zakup na rynku usługi rejestrowanego doręczenia elektronicznego byłby dla nich rozwiązaniem tańszym, a jednocześnie gwarantowałby zapewnienie bezpieczeństwa uczestnikom postępowania. Kwalifikowana usługa rejestrowanego doręczenia elektronicznego jest bowiem obwarowana szeregiem wymogów wskazanych w art. 44 rozporządzenia eIDAS. Należy wziąć też pod uwagę fakt, że dopuszczenie możliwości wykorzystania w/w usługi mogłoby przyczynić się także do popularyzacji wykorzystania metod komunikacji elektronicznej w kontakcie uczestników postępowań z organami administracji.

Kodeks postępowania administracyjnego wymaga także nowelizacji w zakresie stosowanej nomenklatury. Ilekroć w k.p.a. mowa jest o opatrywaniu pism bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu (art. 54 § 2, art. 107 § 1, art. 124 § 1, art. 217 § 4, art. 238 § 1) należy pojęcie to zastąpić pojęciem kwalifikowanego podpisu elektronicznego w rozumieniu art. 3 pkt 12 rozporządzenia eIDAS.

2.6 Inne zagadnienia prawne

Analizując materię rozporządzenia eIDAS i jego wpływu na krajowy porządek prawny zidentyfikowano kilka zagadnień prawnych, których omówienie wydaje się w niniejszej ekspertyzie uzasadnione. Jednocześnie brak odpowiedniego miejsca na poruszenie opisanych niżej problemów w innych częściach niniejszej ekspertyzy. Z tego względu niniejszy podrozdział porusza kilka istotnych zagadnień o charakterze prawnym.

Pierwszą kwestię, którą uznano za zasługującą na odrębne omówienie jest zasada niedyskryminacji usług kwalifikowanych. Rozporządzenie eIDAS w odniesieniu do niektórych usług zaufania wprowadza zasadę wzajemnego uznawania usług kwalifikowanych w państwach członkowskich. Tak jest na przykład w odniesieniu do kwalifikowanego podpisu elektronicznego, bowiem w art. 25 ust. 3 rozporządzenia eIDAS wskazano, iż kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich. Podobna regulacja została zawarta w odniesieniu do pieczęci elektronicznej. Wedle art. 35 ust. 3 rozporządzenia eIDAS kwalifikowana pieczęć elektroniczna oparta na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawana za kwalifikowaną pieczęć elektroniczną we wszystkich pozostałych państwach członkowskich. Wzajemne uznawanie powyższych kwalifikowanych usług oznacza, że każde państwo członkowskie musi uznać skutek prawny kwalifikowanej usługi wydanej w innym państwie członkowskim. Odnosząc powyższe do podpisu elektronicznego należy uznać, że kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim odnosi skutek podpisu własnoręcznego w każdym innym państwie członkowskim. W tym stanie rzeczy, choć rozporządzenie eIDAS nie konstytuuje wprost tego typu zasady, zasadne wydaje się wprowadzenie w krajowym porządku prawnym zasady niedyskryminacji usług kwalifikowanych. Powinna ona polegać na tym, że strona ufająca korzystająca z usługi kwalifikowanej nie może być dyskryminowana z tego powodu, że korzystając z określonego systemu w kontakcie z administracją publiczną używa kwalifikowanej usługi zaufania, podczas gdy organ wykorzystujący dany system dopuszcza, czy preferuje usługę niekwalifikowaną. Tylko bowiem wprowadzając tego typu

zasadę w polskim porządku prawnym możliwe będzie pełne wdrożenie regulacji rozporządzenia eIDAS. Skoro bowiem rozporządzenie to określa skutek prawny, zwłaszcza w odniesieniu do kwalifikowanego podpisu elektronicznego, wskazując że ma on skutek równoważny podpisowi własnoręcznemu, to skutek ten powinien być zawsze uznawany w kontaktach z wszelkimi organami administracji publicznej. Organ wykorzystujący określony system, który preferuje usługę niekwalifikowaną, nie może więc odmówić dostępu do tego systemu stronie, która korzysta z usługi kwalifikowanej. Ma to istotne znaczenie zwłaszcza w odniesieniu do podpisu elektronicznego, którego skutek prawny został określony w rozporządzeniu eIDAS, niemniej w ocenie autorów niniejszej ekspertyzy zasadę niedyskryminacji usług zaufania należy rozciągnąć także na inne niż podpis elektroniczny usługi zaufania. Usługi kwalifikowane winny być bowiem preferowane jako niosące za sobą największy stopień bezpieczeństwa dla strony ufającej.

W dalszej części niniejszej ekspertyzy omówiono kwestie organizacyjne i techniczne wskazując na pozytywne doświadczenia związane z funkcjonowaniem Narodowego Centrum Certyfikacji pełniącego funkcję głównego urzędu certyfikacji dla infrastruktury bezpiecznego podpisu elektronicznego w Polsce powierzoną Narodowemu Bankowi Polskiemu. Rozważa się możliwość powierzenia pod rządami nowej ustawy o usługach zaufania bankowi centralnemu funkcji NCCert, nad którym nadzór sprawować miałby minister właściwy ds. gospodarki. W związku z tym należy zapewnić możliwość sprawowania nadzoru przez organ nadzorczy będący organem władzy wykonawczej nad niezależnym i konstytucyjnie wyodrębnionym organem tj. Narodowym Bankiem Polskim. W ocenie autorów niniejszej ekspertyzy dopuszczalny jest nadzór na wykonywaniem określonych funkcji sprawowany przez ministra w odniesieniu do Narodowego Banku Polskiego. Należy bowiem zwrócić uwagę na fakt, że wykonywanie funkcji NCCert odbywałoby się w drodze powierzenia zadań przez ministra właściwego ds. gospodarki. Zatem organ, któremu powierza się realizację tego typu funkcji nie może uniknąć funkcjonalnego i merytorycznego nadzoru w zakresie powierzonych do wykonania zadań. Ponadto w krajowej infrastrukturze usług zaufania NBP występuje nie jako konstytucyjny bank centralny, ale jako główny urząd certyfikacji. Konstytucyjną niezależność NBP należy raczej odnosić do jego zadań związanych z pełnieniem funkcji banku centralnego. Nie jest jurydycznie uzasadnionym przypisanie atrybutu niezależności banku centralnego tym zadaniom, które bank ten przyjmuje w związku z wykonywaniem funkcji innych niż te które dotyczą jego roli banku centralnego. Ponadto należy zważyć na fakt, że rozporządzenie eIDAS w art. 17 przewiduje obowiązek wyznaczenia organu nadzoru. Istnienie organu nadzoru jest więc obowiązkowe, stąd dopuszczalna jest taka konstrukcja krajowej infrastruktury usług zaufania, w której właściwy minister jako organ nadzoru sprawowałby funkcje nadzorcze także nad zadaniami realizowanymi przez Narodowy Bank Polski w zakresie funkcji NCCert.

Rozporządzenie eIDAS wprowadziło m.in. instytucję pieczęci elektronicznej. Zgodnie z definicją zawartą w art. 3 pkt 25 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. W motywie 59 preambuły rozporządzenia wskazano, że pieczęcie elektroniczne powinny służyć jako dowód wydania danego dokumentu elektronicznego przez daną osobę prawną, dając pewność co do pochodzenia i integralności dokumentu. Zgodnie z kolei z definicją w art. 3 pkt 24 rozporządzenia podmiotem składającym pieczęć jest osoba prawna, która składa pieczęć elektroniczną. 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. Niewątpliwie zaś pojawi się problem dopuszczalności wykorzystywania pieczęci elektronicznych przez jednostki organizacyjne nieposiadające osobowości prawne, którym ustawa nadaje zdolność prawną, o których mowa w art. 33^1 § 1 k.c. Przepis ten wskazuje, że do tego typu jednostek stosuje się odpowiednio przepisy o osobach prawnych. 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 autorów niniejszej ekspertyzy zasadne jest stworzenie takiej możliwości także tzw. ułomnym osobom prawnym, których dotyczy przepis art. 33^1 § 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.

Uzupełniając powyższe rozważania w odniesieniu do instytucji pieczęci elektronicznej należy wskazać, że tak jak przepisy rozporządzenia eIDAS nie naruszają wynikających z prawa krajowego zasad dotyczących reprezentacji osób prawnych, tak nie ma potrzeby, aby projektowane nowe uregulowania krajowe dotyczące pieczęci elektronicznej dokonywały jakiejkolwiek modyfikacji w zakresie istniejących zasad reprezentacji osób prawnych. 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 reprezentacji osoby prawnej, pieczęć elektroniczna powinna służyć przede wszystkim potwierdzeniu autentyczności pochodzenia i zapewnieniu integralności danych, nie zaś reprezentacji podmiotu.

Analizując zagadnienia związane z usługami zaufania należy zwrócić szczególną uwagę na definicję usług zaufania i usług w ogólności, wywodzącą się z prawa europejskiego. Rozporządzenie eIDAS przytaczając definicją usług zaufania wskazuje, że jest to usługa świadczona zazwyczaj za wynagrodzeniem. Konstrukcja ta wywodzi się z pierwotnego prawa europejskiego, albowiem sam Traktat o funkcjonowaniu Unii Europejskiej w art. 57 definiuje usługi jako świadczenia wykonywane zwykle za wynagrodzeniem. Zatem usługą w rozumieniu Traktatu, a także w konsekwencji usługą zaufania w rozumieniu rozporządzenia eIDAS będzie tylko taka usługa, która posiada element odpłatności. Jest to usługa, której świadczenie uzależnione jest od odpłatności uiszczanej na rzecz świadczeniodawcy. Musi więc istnieć gospodarczy związek między usługą a świadczeniem wzajemnym odbiorcy usług. Usługami nie są świadczenia, za które nie jest pobierane wynagrodzenie. Jednakże brak odpłatności w konkretnym przypadku nie oznacza, że dane świadczenie nie będzie usługą. Fakt, że określony podmiot w określonych okolicznościach rezygnuje z wynagrodzenia, nie prowadzi do automatycznego wniosku, że jego świadczenie nie jest usługą, albowiem należy zwrócić uwagę na fakt, że prawo europejskie wskazuje w definicji usługi, że jest to świadczone **zazwyczaj** za wynagrodzeniem, a zatem niekoniecznie zawsze za wynagrodzeniem. Należałoby zatem dane świadczenie oceniać w kontekście tego, czy stanowi ono usługę, czy nie, rozpatrując szerokie okoliczności, w tym zwłaszcza fakt, czy istnieje rynek danych świadczeń i czy na rynku świadczenia określone są świadczone co do zasady odpłatnie, czy też nie. Należy też zwrócić uwagę na fakt, że nie jest wymaganym elementem definicji usługi, aby koszt danego świadczenia zawsze ponosił bezpośrednio jej odbiorca. Usługą będzie bowiem też takie świadczenie, którego koszt ponoszony jest przez podmiot inny niż odbiorca – konsument[16].

[16] E. Skrzydło-Tefelska [w]: Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I, pod red. D. Miąsika i N. Półtorak, Warszawa 2012, s. 965

3. LISTA PROPOZYCJI UREGULOWANIA ZAGADNIEŃ DLA KTÓRYCH EIDAS PRZEWIDUJE WYKORZYSTANIE PRAWA KRAJOWEGO

Rozporządzenie eIDAS przewiduje wykorzystanie prawa krajowego w następujących przypadkach: motywy preambuły nr 13, 14, 15, 17, 18, 19, 20, 21, 22, 24, 25, 30, 33, 34, 37, 49, 50, 54, 66, 75 oraz artykuły 2, 5, 11, 16, 17, 18, 19, 22, 24, 27, 36, 37. Poniżej załączona jest lista wyszczególnionych pozycji wraz z propozycją uregulowania.

3.1 Rozporządzenie eIDAS - motyw 13 preambuły

3.1.1 Rozporządzenie eIDAS - treść przepisu

Państwa członkowskie powinny zachować swobodę w stosowaniu lub wprowadzaniu środków dostępu do usług online do celów identyfikacji elektronicznej. Powinny również mieć możliwość podjęcia decyzji, czy w dostarczanie tych środków należy zaangażować sektor prywatny. Państwa członkowskie nie powinny być zobowiązane do notyfikowania Komisji swoich systemów identyfikacji elektronicznej. Do państw członkowskich należy wybór tego, czy notyfikować Komisji wszystkie, niektóre lub żaden z systemów identyfikacji elektronicznej używanych na szczeblu krajowym dla uzyskiwania dostępu przynajmniej do publicznych usług online lub szczególnych usług.

3.1.2 Propozycje uregulowania.

Po uzyskaniu notyfikacji systemu identyfikacji elektronicznej należy przewidzieć środki informowania obywateli o tym fakcie. Rozwiązaniem może być prowadzony Rejestr krajowych notyfikowanych środków identyfikacji elektronicznej. Powinna zostać uregulowana kwestia Organu odpowiedniego do prowadzenia takiego rejestru. Równolegle w celu określenia swobody przepływu usług w systemach informatycznych administracji i sektora prywatnego należy dystrybuować przez krajowy organ nadzoru Wykaz Artykułu 9 Notyfikacja punkt 2, które systemy identyfikacji elektronicznej z innych krajów UE są notyfikowane. Na poziomie krajowym powinien zostać określony termin co do dostosowania krajowych systemów administracji publicznej w zakresie dostosowania tych systemów do uznawania notyfikowanych systemów identyfikacji elektronicznej z innych krajów UE. Termin ten nie może być dłuższy niż określony w Artykule 6 Wzajemne uznawanie punkt 1 "Takiego uznania dokonuje się nie później niż 12 miesięcy po opublikowaniu przez Komisję wykazu, o którym mowa w akapicie pierwszym lit. a)."

3.2 Rozporządzenie eIDAS - motyw 14 preambuły

3.2.1 Rozporządzenie eIDAS – treść przepisu

W niniejszym rozporządzeniu należy ustanowić pewne warunki dotyczące tego, które środki identyfikacji elektronicznej muszą być uznawane i w jaki sposób należy notyfikować systemy identyfikacji elektronicznej. Warunki te powinny pomóc państwom członkowskim w zbudowaniu niezbędnego wzajemnego zaufania do stosowanych przez nie systemów identyfikacji elektronicznej oraz we wzajemnym uznawaniu środków identyfikacji elektronicznej objętych notyfikowanymi systemami. Zasada wzajemnego uznawania powinna mieć zastosowanie, jeżeli system identyfikacji elektronicznej notyfikującego państwa członkowskiego spełnił warunki notyfikacji i notyfikacja ta została opublikowana w Dzienniku Urzędowym Unii Europejskiej. Jednak zasada wzajemnego uznawania powinna odnosić się wyłącznie do uwierzytelniania dla usługi online. Dostęp do tych usług online i ich ostateczne wykonanie na rzecz wnioskodawcy powinny być ściśle powiązane z prawem do korzystania z takich usług na warunkach określonych w przepisach krajowych

3.2.2 Propozycje uregulowania.

W krajowych przepisach dotyczących dostępu do różnego rodzaju usług online należy zapewnić dostępność tych usług dla użytkowników wszystkich systemów identyfikacji elektronicznej, które zostały notyfikowane na poziomie UE i które spełniają warunki art. 6 ust. 1 lit. a-c rozporządzenia eIDAS. Należy zapobiegać sytuacjom, w których dostęp do usługi

online byłby dostępny wyłącznie dla użytkowników krajowych systemów identyfikacji elektronicznej bez zapewnienia tej dostępności użytkownikom innych notyfikowanych systemów zachowujących warunki art. 6 rozporządzenia eIDAS.

3.3 Rozporządzenie eIDAS - motyw 15 preambuły

3.3.1 Rozporządzenie eIDAS - treść przepisu

Obowiązek uznawania środka identyfikacji elektronicznej powinien odnosić się wyłącznie do tych środków, których poziom bezpieczeństwa tożsamości jest równy poziomowi wymaganemu w odniesieniu do danej usługi online lub wyższy od tego poziomu. Ponadto obowiązek ten powinien mieć zastosowanie wyłącznie wtedy, gdy dany podmiot sektora publicznego używa "średniego" lub "wysokiego" poziomu bezpieczeństwa w odniesieniu do dostępu do tej usługi online. Państwa członkowskie powinny mieć nadal swobodę, zgodnie z prawem unijnym, w zakresie uznawania środków identyfikacji elektronicznej charakteryzujących się niższymi poziomami bezpieczeństwa.

3.3.2 Propozycje uregulowania.

Na poziomie krajowym niezbędne jest rozstrzygnięcie kwestii konieczności określenia w stosunku do obecnych środków identyfikacji elektronicznej obowiązkowego ich poziomu bezpieczeństwa. Wymóg ten wynika z Artykułu 8 Poziomy bezpieczeństwa systemów identyfikacji elektronicznej.

3.4 Rozporządzenie eIDAS - motyw 17 preambuły

3.4.1 Rozporządzenie eIDAS - treść przepisu

Państwa członkowskie powinny zachęcać sektor prywatny do dobrowolnego korzystania ze środków identyfikacji elektronicznej w ramach notyfikowanego systemu do celów identyfikacji, gdy jest ona potrzebna do celów usług online lub transakcji elektronicznych. Możliwość korzystania z takich środków identyfikacji elektronicznej sprawiłaby, że sektor prywatny mógłby polegać na elektronicznej identyfikacji i uwierzytelnianiu stosowanych już powszechnie w wielu państwach członkowskich przynajmniej w odniesieniu do usług publicznych, a przedsiębiorstwom i obywatelom ułatwiłaby transgraniczny dostęp do ich usług online. Aby ułatwić transgraniczne korzystanie z takich środków identyfikacji elektronicznej przez sektor prywatny, możliwość uwierzytelniania zapewniona przez jakiekolwiek państwo członkowskie powinna być dostępna dla stron ufających z sektora prywatnego mających siedzibę poza terytorium tego państwa członkowskiego na tych samych warunkach co warunki stosowane do stron ufających z sektora prywatnego mających siedzibę na terytorium tego państwa członkowskiego. W rezultacie, jeżeli chodzi o strony ufające z sektora prywatnego, notyfikujące państwo członkowskie może określić warunki dostępu do środków uwierzytelniania. W takich warunkach dostępu można podawać, czy środki uwierzytelniania powiązane z notyfikowanym systemem są obecnie dostępne dla stron ufających z sektora prywatnego.

3.4.2 Propozycje uregulowania.

Na poziomie krajowym niezbędne jest rozstrzygnięcie kwestii konieczności określenia w stosunku do obecnych środków identyfikacji elektronicznej obowiązkowego ich poziomu bezpieczeństwa. Wymóg ten wynika z Artykułu 8 Poziomy bezpieczeństwa systemów identyfikacji elektronicznej.

3.5 Rozporządzenie eIDAS - motyw 18 preambuły

3.5.1 Rozporządzenie eIDAS - treść przepisu

Niniejsze rozporządzenie powinno przewidywać, że notyfikujące państwo członkowskie, strona wydająca środek identyfikacji elektronicznej oraz strona przeprowadzająca procedury uwierzytelniania przyjmują odpowiedzialność za niewypełnienie odpowiednich obowiązków na mocy niniejszego rozporządzenia. Niniejsze rozporządzenie powinno być jednak stosowane zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności. Nie narusza ono zatem tych przepisów krajowych, na przykład dotyczących definicji odszkodowania lub odpowiednich obowiązujących przepisów proceduralnych, w tym przepisów krajowych dotyczących ciężaru dowodu.

3.5.2 Propozycje uregulowania.

W związku z brakiem kolizji między regulacjami eIDAS w zakresie odpowiedzialności, a krajowymi przepisami dotyczącymi odpowiedzialności, definicji odszkodowania, przepisów proceduralnych, proponuje się pozostawienie bez zmian istniejących dziś przepisów krajowego prawa cywilnego dotyczących odpowiedzialności deliktowej i kontraktowej z jednoczesnym określeniem zasad odpowiedzialności w ustawie o usługach zaufania.

3.6 Rozporządzenie eIDAS - motyw 19 preambuły

3.6.1 Rozporządzenie eIDAS - treść przepisu

Bezpieczeństwo systemów identyfikacji elektronicznej ma kluczowe znaczenie dla wiarygodnego transgranicznego wzajemnego uznawania środków identyfikacji elektronicznej. W tym kontekście państwa członkowskie powinny współpracować w odniesieniu do bezpieczeństwa i interoperacyjności systemów identyfikacji elektronicznej na szczeblu unijnym. W każdym przypadku, gdy systemy identyfikacji elektronicznej nakładają wymóg korzystania przez strony ufające na szczeblu krajowym z konkretnego sprzętu lub oprogramowania, transgraniczna interoperacyjność oznacza wymóg nienakładania przez te państwa członkowskie takich wymogów i powiązanych kosztów na strony ufające mające siedzibę poza ich terytorium. W takim przypadku należy w zakresie ram interoperacyjności omówić i opracować odpowiednie rozwiązania. Niemniej jednak nieuniknione są wymogi techniczne wynikające ze specyfikacji właściwych krajowym środkom identyfikacji elektronicznej i mogące wpływać na posiadaczy takich środków elektronicznych (np. kart elektronicznych).

3.6.2 Propozycje uregulowania.

Rozstrzygnięcia wymaga kwestia czy istnieją obecnie środki identyfikacji elektronicznej nakładające wymóg korzystania przez strony ufające na szczeblu krajowym z konkretnego sprzętu lub oprogramowania(typu aplikacja ZRODLO) i nałożenia wymogu uzupełnienia (o ile zachodzi taka potrzeba) do takich systemów identyfikacji elektronicznej o akceptowanie środków identyfikacji elektronicznej na odpowiednim poziomie zgodnie z Artykułem 8 Poziomy bezpieczeństwa systemów identyfikacji elektronicznej

3.7 Rozporządzenie eIDAS - motyw 20 preambuły

3.7.1 Rozporządzenie eIDAS - treść przepisu

Współpraca między państwami członkowskimi powinna ułatwiać techniczną interoperacyjność notyfikowanych systemów identyfikacji elektronicznej w celu uzyskania wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka. We współpracy tej pomóc powinna wymiana informacji i najlepszych praktyk między państwami członkowskimi mająca na celu wzajemne uznawanie ich systemów.

3.7.2 Propozycje uregulowania.

Konieczność uznawania jest wprowadzona w rozporządzeniu eIDAS w artykule 6 Wzajemne uznawanie punkt 1 "Takiego uznania dokonuje się nie później niż 12 miesięcy po opublikowaniu przez Komisję wykazu, o którym mowa w akapicie pierwszym lit. a)." Powinien być określony ogólny proces dochodzenia do uznawania notyfikowanego systemu ID. w szczególności czy takie dostosowanie wymaga dodatkowego Rozporządzenia, jakie systemy administracji publicznej muszą być dostosowane, w jakim czasie (<12 miesięcy) i jakim kosztem.

3.8 Rozporządzenie eIDAS - motyw 21 preambuły

3.8.1 Rozporządzenie eIDAS - treść przepisu

W niniejszym rozporządzeniu należy również ustanowić ogólne ramy prawne dotyczące korzystania z usług zaufania. Nie należy jednak wprowadzać ogólnego obowiązku korzystania z nich ani instalowania punktu dostępu dla wszystkich istniejących usług zaufania. W szczególności niniejsze rozporządzenie nie powinno obejmować świadczenia usług wykorzystywanych wyłącznie w obrębie systemów zamkniętych przez określoną grupę uczestników i niemających skutków dla stron trzecich. Wymogom niniejszego rozporządzenia nie powinny na przykład podlegać systemy utworzone w przedsiębiorstwach lub administracjach publicznych w celu zarządzania procedurami wewnętrznymi przy

użyciu usług zaufania. Wymogi określone w rozporządzeniu powinny spełniać jedynie usługi zaufania świadczone na rzecz społeczeństwa, mające skutki dla stron trzecich. Niniejsze rozporządzenie nie powinno również obejmować aspektów związanych z zawieraniem i ważnością umów lub innych obowiązków prawnych, w przypadku gdy istnieją wymogi dotyczące formy wprowadzone na mocy prawa krajowego lub unijnego. Dodatkowo nie powinno ono mieć wpływu na krajowe wymogi w zakresie formy dotyczące rejestrów publicznych, w szczególności rejestrów handlowych i rejestrów gruntów.

3.8.2 Propozycje uregulowania.

W zakresie przepisów dotyczących form czynności prawnych proponuję się zmianę art. 78 § 2 Kodeksu cywilnego (opisaną w innej części niniejszej ekspertyzy), jak też rozważenie zmian Kodeksu cywilnego w zakresie autonomiczności formy elektronicznej jako formy czynności prawnej. W zakresie przepisów prawa administracyjnego regulujących kwestie prowadzenia i dostępu do publicznych rejestrów proponuje się zapewnienie dostępności do tych rejestrów podmiotom posługującym się podpisem elektronicznym w rozumieniu przepisów o usługach zaufania.

Odnośnie: "Wymogi określone w rozporządzeniu powinny spełniać jedynie usługi zaufania świadczone na rzecz społeczeństwa, mające skutki dla stron trzecich." Należy wprowadzić odpowiednie wymogi (określić szczegółowo jakie) do tak zwanych publicznych niekwalifikowanych usług zaufania.

3.9 Rozporządzenie eIDAS - motyw 22 preambuły

3.9.1 Rozporządzenie eIDAS - treść przepisu

Aby wspierać ogólne transgraniczne korzystanie z usług zaufania, należy zapewnić możliwość używania tych usług jako dowodu w postępowaniach sądowych we wszystkich państwach członkowskich. W prawie krajowym należy określić skutki prawne usług zaufania, o ile w niniejszym rozporządzeniu nie postanowiono inaczej.

3.9.2 Propozycje uregulowania.

Ustawa o usługach zaufania winna określać skutki prawne dla usług zaufania z zachowaniem regulacji rozporządzenia eIDAS.

3.10Rozporządzenie eIDAS - motyw 24 preambuły

3.10.1 Rozporządzenie eIDAS - treść przepisu

Państwa członkowskie mogą utrzymać lub wprowadzić przepisy krajowe, zgodne z prawem unijnym, odnoszące się do usług zaufania, o ile usługi te nie są w pełni zharmonizowane w drodze niniejszego rozporządzenia. Jednak usługi zaufania spełniające wymogi niniejszego rozporządzenia powinny podlegać swobodnemu obrotowi na rynku wewnętrznym.

3.10.2 Propozycje uregulowania.

Przepisy dotyczące usług zaufania znajdą się w nowej ustawie o usługach zaufania. Ustawa ta powinna dopuszczać swobodę świadczenia tych usług przez podmioty tym zainteresowane.

3.11Rozporządzenie eIDAS - motyw 25 preambuły

3.11.1 Rozporządzenie eIDAS - treść przepisu

Państwa członkowskie powinny zachować swobodę określania innych rodzajów usług zaufania oprócz tych, które figurują w zamkniętym wykazie usług zaufania przewidzianym w niniejszym rozporządzeniu, do celów uznania ich na szczeblu krajowym jako kwalifikowanych usług zaufania.

3.11.2 Propozycje uregulowania.

Przepisy dotyczące usług zaufania znajdą się w nowej ustawie o usługach zaufania. Ustawa ta powinna dopuszczać swobodę świadczenia tych usług przez podmioty tym zainteresowane.

3.12Rozporządzenie eIDAS - motyw 30 preambuły

3.12.1 Rozporządzenie eIDAS - treść przepisu

Państwa członkowskie powinny wyznaczyć organ nadzoru lub organy nadzoru do celów prowadzenia działań nadzorczych na mocy niniejszego rozporządzenia. Państwa członkowskie powinny także mieć możliwość podjęcia decyzji, za obopólnym porozumieniem z innym państwem członkowskim, w sprawie wyznaczenia organu nadzoru na terytorium tego innego państwa członkowskiego.

3.12.2 Propozycje uregulowania.

Kwestie organu nadzoru oraz rozwiązania instytucjonalne opisano w części organizacyjnej niniejszej ekspertyzy.

3.13Rozporządzenie eIDAS - motyw 33 preambuły

3.13.1 Rozporządzenie eIDAS - treść przepisu

Przepisy dotyczące używania pseudonimów w certyfikatach nie powinny uniemożliwiać państwom członkowskim wymogu identyfikacji osób zgodnie z prawem unijnym lub prawem krajowym.

3.13.2 Propozycje uregulowania.

Instytucja "pseudonimu" była obecna w PodEU od 2001 r. Proponujemy w zachować analogiczne rozwiązania o ile nie będą sprzeczne z innym standardami lub regulacjami UE, tzn. zachować w aktach wykonawczych do Ustawy o usługach zaufania (UoUZ) przepisów z § 9 punkt 3.

3.14Rozporządzenie eIDAS - motyw 34 preambuły

3.14.1 Rozporządzenie eIDAS - treść przepisu

W celu zapewnienia porównywalnego poziomu bezpieczeństwa kwalifikowanych usług zaufania wszystkie państwa członkowskie powinny stosować wspólne podstawowe wymogi dotyczące nadzoru. Aby ułatwić spełnianie tych wymogów w jednolity sposób w całej Unii, państwa członkowskie powinny przyjąć porównywalne procedury i powinny wymieniać się informacjami na temat swoich działań nadzorczych oraz najlepszymi praktykami stosowanymi w tej dziedzinie.

3.14.2 Propozycje uregulowania.

Proponuje się powierzenie organowi nadzoru zadania wymiany wiedzy, doświadczeń i informacji w zakresie sprawowania nadzoru nad usługami zaufania z innymi państwami członkowskimi.

3.15Rozporządzenie eIDAS - motyw 37 preambuły

3.15.1 Rozporządzenie eIDAS - treść przepisu

Niniejsze rozporządzenie powinno przewidywać odpowiedzialność wszystkich dostawców usług zaufania. W szczególności ustanawia system odpowiedzialności, w ramach, którego wszyscy dostawcy usług zaufania powinni być odpowiedzialni za szkody wyrządzone osobie fizycznej lub osobie prawnej w związku z niewypełnieniem obowiązków na mocy niniejszego rozporządzenia. Aby ułatwić ocenę ryzyka finansowego, które dostawcy usług zaufania mogą być zmuszeni ponosić lub które powinni pokryć za pomocą polis ubezpieczeniowych, niniejsze rozporządzenie umożliwia dostawcom usług zaufania ustalanie, pod pewnymi warunkami, ograniczeń w zakresie korzystania ze świadczonych przez nich usług i zwalnia ich z odpowiedzialności za szkody wynikające z korzystania z usług wykraczających poza takie ograniczenia. Klienci powinni być z góry należycie informowani o tych ograniczeniach. Te ograniczenia powinny być uznawalne przez stronę trzecią, na przykład poprzez zawieranie informacji o nich w warunkach świadczonej usługi lub za pomocą innych uznawalnych środków. Do celów nadania tym zasadom mocy obowiązującej niniejsze rozporządzenie powinno być stosowane zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności. Niniejsze

rozporządzenie nie wpływa zatem na przepisy krajowe dotyczące, na przykład, definicji szkód, zamiaru, zaniedbania lub odpowiednich obowiązujących zasad proceduralnych.

3.15.2 Propozycje uregulowania.

Proponuję się pozostawienie bez zmian przepisów krajowego prawa cywilnego dotyczących definicji szkody, zamiaru, zaniedbania oraz przepisów proceduralnych. Skoro rozporządzenie eIDAS nie koliduje z przepisami krajowymi w tym zakresie, zasadne jest pozostawienie regulacji krajowych bez zmian. Rozwiązanie takie wpłynie na spójność i trwałość systemu prawnego albowiem usługi zaufania będą podlegały reżimowi odpowiedzialności deliktowej i kontraktowej analogicznie jak usługi, bądź czynności innego rodzaju. W ustawie o usługach zaufania należy doprecyzować zasady odpowiedzialności, a dodatkowo do ustawy tej proponuje się przenieść z obecnego systemu: Rozporządzenie Ministra Finansów w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.

3.16Rozporządzenie eIDAS - motyw 49 preambuły

3.16.1 Rozporządzenie eIDAS - treść przepisu

Niniejsze rozporządzenie powinno wprowadzić zasadę, że nie należy kwestionować skutku prawnego podpisu elektronicznego z tego powodu, że podpis ten ma postać elektroniczną lub że nie spełnia wszystkich wymogów kwalifikowanego podpisu elektronicznego. Jednakże to w prawie krajowym należy zdefiniować skutek prawny podpisów elektronicznych, z wyjątkiem wymogów przewidzianych w niniejszym rozporządzeniu, zgodnie z którymi kwalifikowany podpis elektroniczny powinien mieć skutek prawny równoważny podpisowi własnoręcznemu.

3.16.2 Propozycje uregulowania.

W ustawie o usługach zaufania należy wskazać, że kwalifikowany podpis elektroniczny wywołuje skutki określone ustawą oraz rozporządzeniem eIDAS, przywołując tym samym zasadę wyrażoną w tym rozporządzeniu, zgodnie z którą oświadczenie woli złożone w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym jest równoważne z oświadczeniem woli złożonym w formie pisemnej.

3.17Rozporządzenie eIDAS - motyw 50 preambuły

3.17.1 Rozporządzenie eIDAS - treść przepisu

Ponieważ właściwe organy w państwach członkowskich używają obecnie różnych formatów zaawansowanych podpisów elektronicznych do elektronicznego podpisywania swoich dokumentów, państwa członkowskie powinny zapewnić możliwość obsługi pod względem technicznym co najmniej kilku formatów zaawansowanego podpisu elektronicznego przy odbiorze dokumentów podpisanych elektronicznie. Podobnie, kiedy właściwe organy w państwach członkowskich używają zaawansowanych pieczęci elektronicznych, należałoby zapewnić możliwość obsługi co najmniej kilku formatów zaawansowanej pieczęci elektronicznej.

3.17.2 Propozycje uregulowania.

Należy zapewnić w krajowych systemach możliwość obsługi pod względem technicznym co najmniej kilku formatów zaawansowanego podpisu elektronicznego przy odbiorze dokumentów podpisanych elektronicznie. Podobnie, kiedy organy krajowe używają zaawansowanych pieczęci elektronicznych, należałoby zapewnić możliwość obsługi co najmniej kilku formatów zaawansowanej pieczęci elektronicznej. Jednocześnie należy zapewnić pełną uznawalność formatów, które zostaną określone w aktach wykonawczych do rozporządzenia eIDAS.

3.18Rozporządzenie eIDAS - motyw 54 preambuły

3.18.1 Rozporządzenie eIDAS - treść przepisu

Transgraniczna interoperacyjność i transgraniczne uznawanie kwalifikowanych certyfikatów stanowią warunek wstępny transgranicznego uznawania kwalifikowanych podpisów elektronicznych. Dlatego kwalifikowane certyfikaty nie powinny podlegać żadnym obowiązkowym wymogom przekraczającym wymogi określone w niniejszym

rozporządzeniu. Jednak na szczeblu krajowym należy dopuścić zawieranie w kwalifikowanych certyfikatach szczególnych atrybutów, takich jak unikalne identyfikatory, pod warunkiem że takie szczególne atrybuty nie utrudniają transgranicznej interoperacyjności i transgranicznego uznawania kwalifikowanych certyfikatów i podpisów elektronicznych.

3.18.2 Propozycje uregulowania.

Należy zapewnić w systemach kwalifikowanych usługodawców dostosowanie profili certyfikatów do nowych standardów dotyczących certyfikatów kwalifikowanych oraz w systemach informatycznych administracji publicznej prawidłowe rozpoznawanie zmienionej struktury certyfikatów kwalifikowanych zgodnie z propozycjami standardów w tym zakresie.

- ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
- ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate Profile for certificates issued to natural persons".
- ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate Profile for certificates issued to legal persons".
- ETSI EN 319 412-5 “Electronic Signatures and Infrastructures (ESI); Certificate Profiles;Part 5: QCStatements”
- ETSI TS 101 862: "Qualified Certificate profile".

W szczególności dotyczy to zmian identyfikatorów osoby fizycznej i prawnej, oraz do wskazania zgodności z regulacjami UE, przykładowo takich jak:

- esi4-qcStatement-1 QCStatement (claiming that the certificate is a EU qualified Certificate,) - to pole jest obowiązkowe i oznacza, że certyfikat został wydany zgodnie z Dyrektywa UE z 1999 r o podpisie elektronicznym lub Aneksem 1 Rozporządzenia UE nr. 910/2014
- esi4-qcStatement-4 QCStatement (claiming that the private key related to the certified public key resides in a QSCD) oznacza, że klucz prywatny związany z tym certyfikatem klucza publicznego jest umieszczony na QSCD
- oraz identyfikatorów dotyczących wyróżnienia certyfikatów osoby fizycznej lub prawnej: id-etsi-qcs-semanticsId-Natural OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-identifiers 1 }
- id-etsi-qcs-SemanticsId-Legal OBJECT IDENTIFIER ::= { id-etsi-qcs-semantics-identifiers 2 }

Zmiana powinna być wprowadzona poprzez usunięcie w aktach normatywnych krajowych zapisów niezgodnych z wprowadzanymi standardami. Zmiany wyżej przytoczone można spodziewać się, że wejdą w porządek prawny krajowy jako akta delegowane lub wykonawcze do rozporządzenia eIDAS.

3.19Rozporządzenie eIDAS - motyw 66 preambuły

3.19.1 Rozporządzenie eIDAS - treść przepisu

Istotne jest ustanowienie ram prawnych służących ułatwieniu transgranicznego uznawania między istniejącymi krajowymi systemami prawnymi, związanego z usługami rejestrowanego doręczenia elektronicznego. Ramy te mogłyby stworzyć także nowe możliwości rynkowe dla unijnych dostawców usług zaufania w odniesieniu do oferowania nowych ogólnoeuropejskich usług rejestrowanego doręczenia elektronicznego.

3.19.2 Propozycje uregulowania.

W prawie krajowym jest częściową uregulowana kwestia doręczeń dokumentów drogą elektroniczną do administracji publicznej lub sądownictwa, jednak przepisy te nie mogą wykluczać doręczeń dokonanych poprzez kwalifikowane usługi rejestrowanego doręczenie elektronicznego również należy przepisy krajowe uzupełnić o taką możliwość.

3.20 Rozporządzenie eIDAS - motyw 75 preambuły

3.20.1 Rozporządzenie eIDAS - treść przepisu

Daty rozpoczęcia stosowania określone w niniejszym rozporządzeniu nie wpływają na istniejące obowiązki, które już dotyczą państw członkowskich na mocy prawa Unii, w szczególności na mocy dyrektywy 2006/123/WE.

3.20.2 Propozycje uregulowania.

Obecnie obowiązują w zakresie usług certyfikacyjnych : decyzja C(2013) 6542 z dnia 14 października 2013 r. zmieniającą decyzję 2009/767/WE oraz Decyzja 2014/148/UE bezpośrednio stosowane w Polsce i w gestii aktów delegowanych lub wykonawczych do R910/2014 jest zastąpienie wskazanych decyzji.

3.21Rozporządzenie eIDAS - art. 2

3.21.1 Rozporządzenie eIDAS - treść przepisu

Zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do systemów identyfikacji elektronicznej, które zostały notyfikowane przez państwo członkowskie, oraz do dostawców usług zaufania mających siedzibę w Unii.

2. Niniejsze rozporządzenie nie ma zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników.

3. Niniejsze rozporządzenie nie ma wpływu na prawo krajowe ani unijne związane z zawieraniem i ważnością umów lub innych zobowiązań prawnych lub proceduralnych, dotyczące ich formy.

3.21.2 Propozycje uregulowania.

W zakresie przepisów dotyczących form czynności prawnych proponuje się zmianę art. 78 § 2 Kodeksu cywilnego (opisaną w innej części niniejszej ekspertyzy), jak też rozważenie zmian Kodeksu cywilnego w zakresie autonomiczności formy elektronicznej jako formy czynności prawnej.

3.22Rozporządzenie eIDAS - art. 5

3.22.1 Rozporządzenie eIDAS - treść przepisu

Przetwarzanie i ochrona danych

1. Przetwarzanie danych osobowych prowadzone jest zgodnie z przepisami dyrektywy 95/46/WE.

2. Bez uszczerbku dla skutku prawnego, jaki prawo krajowe przyznaje pseudonimom, nie zakazuje się używania pseudonimów w transakcjach elektronicznych.

3.22.2 Propozycje uregulowania.

Proponuje się zachować analogiczne rozwiązania w odniesieniu do instytucji pseudonimu, jak miało to miejsce w przypadku ustawy o podpisie elektronicznym.

Wskazana dyrektywa została implementowana do prawa krajowego w ustawie o ochronie danych osobowych i w związku z tym jej przestrzeganie jest na poziomie krajowym gwarantowane.

3.23Rozporządzenie eIDAS - art. 11

3.23.1 Rozporządzenie eIDAS - treść przepisu

Odpowiedzialność

1. Notyfikujące państwo członkowskie jest odpowiedzialne za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niewypełnieniem swoich obowiązków na mocy art. 7 lit. d) i f), w ramach transgranicznej transakcji.

2. Strona wydająca środek identyfikacji elektronicznej jest odpowiedzialna za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązku, o którym mowa w art. 7 lit. e), w ramach transgranicznej transakcji.

3. Strona przeprowadzająca procedurę uwierzytelniania jest odpowiedzialna za szkody wyrządzone, w sposób zamierzony lub z powodu zaniedbania, osobie fizycznej lub prawnej w związku z niezapewnieniem poprawnego przebiegu uwierzytelniania, o którym mowa w art. 7 lit. f), w ramach transgranicznej transakcji.

4. Ust. 1, 2 i 3 mają zastosowanie zgodnie z krajowymi przepisami dotyczącymi odpowiedzialności.

5. Ust. 1, 2 i 3 pozostają bez uszczerbku dla odpowiedzialności, na mocy prawa krajowego właściwego dla stron transakcji, na potrzeby której zastosowano środki identyfikacji elektronicznej objęte systemem identyfikacji elektronicznej notyfikowanym na podstawie art. 9 ust. 1.

3.23.2 Propozycje uregulowania.

Proponuje się pozostawienie bez zmian istniejących dziś przepisów krajowego prawa cywilnego dotyczących odpowiedzialności deliktowej i kontraktowej. W ustawie o usługach zaufania należy doprecyzować zasady odpowiedzialności, a dodatkowo do ustawy tej proponuje się przenieść z obecnego systemu: Rozporządzenie Ministra Finansów w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi certyfikacyjne.

3.24Rozporządzenie eIDAS - art. 16

3.24.1 Rozporządzenie eIDAS - treść przepisu

Sankcje

Państwa członkowskie ustanawiają przepisy o sankcjach mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia. Przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające.

3.24.2 Propozycje uregulowania

Niezbędne jest uwzględnienie w ustawie o usługach zaufania przepisów zawierających sankcje o charakterze administracyjnym oraz karnym za naruszenia rozporządzenia eIDAS krajowych przepisów o usługach zaufania. W tym zakresie proponuje się określenie zasad odpowiedzialności karnej za następujące czyny:

1) świadczenie usług zaufania, jako kwalifikowany dostawca usług zaufania bez uprzedniego zawarcia umowy ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom tych usług;

2) składanie kwalifikowanego i zaawansowanego podpisu elektronicznego lub posługiwanie się pieczęcią elektroniczną za pomocą danych, które zostały przyporządkowane do innej osoby;

3) kopiowanie lub przechowywanie przez podmioty świadczące usługi zaufania danych służących do składania kwalifikowanego lub zaawansowanego podpisu elektronicznego lub posługiwania się pieczęcią elektroniczną;

4) wydawanie przez podmiot świadczący usługi zaufania certyfikatu zawierającego nieprawdziwe dane, jak też umożliwianie wydania takiego certyfikatu w imieniu podmiotu świadczącego usługi oraz posługiwanie się takim certyfikatem;

5) zaniechanie przez podmiot świadczący usługi zaufania unieważnienia certyfikatu w okolicznościach, w których prawo do tego zobowiązuje;

6) umożliwianie oznaczania danych czasem innym niż z chwili wykonania usługi elektronicznego znakowania czasem przez podmiot świadczący takie usługi;

7) ujawnianie lub wykorzystywanie wbrew warunkom ustawowym tajemnicy związanej ze świadczeniem usług zaufania;

8) niepoinformowanie przez podmiot świadczący usługi zaufania osoby ubiegającej się o certyfikat i warunkach uzyskania i używania certyfikatu;

9) porzucenie działalności w zakresie świadczenia kwalifikowanych usług zaufania bez realizacji planu zakończenia działalności lub bez zapewnienia ciągłości świadczenia tych usług przez inny podmiot.

Dodatkowo proponuje się przeniesienie do UoUZ przepisów pochodzących z ustawy o podpisie (art.45 do art. 53) rozciągając sankcje na inne usługi certyfikacyjne.

Sankcje karne grożące za popełnienie czynów wymienionych powyżej w punktach 1-9 winny być przede wszystkim sankcjami o charakterze pieniężnym (grzywny), a także – przynajmniej w odniesieniu do punktów 1, 3, 4, 5, 6, 7, 8 i 9 – należy wprowadzić środek karny w postaci zakazu prowadzenia działalności i wykonywania zawodu polegających na świadczeniu kwalifikowanych i niekwalifikowanych usług zaufania.

3.25Rozporządzenie eIDAS - art. 17

3.25.1 Rozporządzenie eIDAS - treść przepisu

Organ nadzoru

1. Państwa członkowskie wyznaczają organ nadzoru z siedzibą na swoim terytorium lub, za obopólnym porozumieniem z innym państwem członkowskim, organ nadzoru z siedzibą w tym innym państwie członkowskim. Organ ten jest odpowiedzialny za zadania nadzoru w wyznaczającym państwie członkowskim.

Organom nadzoru przyznaje się uprawnienia i odpowiednie zasoby niezbędne do wykonywania ich zadań.

2. Państwa członkowskie notyfikują Komisji nazwy i adresy wyznaczonych przez siebie organów nadzoru.

3. Organ nadzoru odgrywa następującą rolę:

a) sprawuje nadzór nad kwalifikowanymi dostawcami usług zaufania mającymi siedzibę na terytorium wyznaczającego państwa członkowskiego w celu zapewnienia - za pomocą działań nadzorczych ex ante i ex post - aby kwalifikowani dostawcy usług zaufania i świadczone przez nich kwalifikowane usługi zaufania spełniały wymogi określone w niniejszym rozporządzeniu;

b) podejmuje, w razie konieczności, działania w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego - za pomocą działań nadzorczych ex post - gdy dowiaduje się, że niekwalifikowani dostawcy usług zaufania lub świadczone przez nich usługi zaufania rzekomo nie spełniają wymogów określonych w niniejszym rozporządzeniu.

4. Do celów ust. 3 i z zastrzeżeniem ograniczeń w nim określonych, zadania organu nadzoru obejmują w szczególności:

a) współpracę z innymi organami nadzoru i udzielanie im pomocy zgodnie z art. 18;

b) analizowanie raportów z oceny zgodności, o których mowa w art. 20 ust. 1 i art. 21 ust. 1;

c) informowanie innych organów nadzoru i społeczeństwa o naruszeniach bezpieczeństwa lub utracie integralności zgodnie z art. 19 ust. 2;

d) składanie sprawozdań Komisji na temat jego głównych działań zgodnie z ust. 6 niniejszego artykułu;

e) przeprowadzanie audytów lub zwracanie się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności kwalifikowanych dostawców usług zaufania zgodnie z art. 20 ust. 2;

f) współpracę z organami ochrony danych, w szczególności przez informowanie ich, bez zbędnej zwłoki, o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy, jak się wydaje, doszło do naruszenia przepisów dotyczących ochrony danych osobowych;

g) przyznawanie dostawcom usług zaufania i świadczonym przez nich usługom statusu kwalifikowanego dostawcy usług zaufania i kwalifikowanych usług, a także odebranie tego statusu zgodnie z art. 20 i 21;

h) informowanie organu odpowiedzialnego za krajową zaufaną listę, o której mowa w art. 22 ust. 3, o swoich decyzjach o przyznaniu lub odebranie statusu kwalifikowanego, chyba że ten organ jest również organem nadzoru;

i) weryfikacja istnienia i prawidłowego stosowania przepisów dotyczących planów zakończenia działalności, w przypadkach gdy kwalifikowany dostawca usług zaufania zaprzestaje swojej działalności, w tym tego, w jaki sposób zapewnia się dalszą dostępność informacji zgodnie z art. 24 ust. 2 lit. h);

j) wymaganie, aby dostawcy usług zaufania eliminowali wszelkie przypadki niespełnienia wymogów określonych w niniejszym rozporządzeniu.

5. Państwa członkowskie mogą wymagać, by organ nadzoru utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z warunkami określonymi w prawie krajowym.

6. Do dnia 31 marca każdego roku każdy organ nadzoru przekazuje Komisji sprawozdanie z jego głównych działań w poprzednim roku kalendarzowym wraz z zestawieniem notyfikacji dotyczących naruszeń otrzymanych od dostawców usług zaufania zgodnie z art. 19 ust. 2.

7. Komisja udostępnia państwom członkowskim roczne sprawozdanie, o którym mowa w ust. 6.

8. Komisja może w drodze aktów wykonawczych określić formaty i procedury dotyczące sprawozdania, o którym mowa w ust. 6. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

3.25.2 Propozycje uregulowania.

Ustawa o usługach zaufania winna wskazywać kto będzie pełnił funkcję organu nadzoru w rozumieniu rozporządzenia eIDAS, jak też regulować kwestię organu który będzie wykonywał funkcje państwa członkowskiego określone w tym rozporządzeniu.

Propozycja jest rozważenia umiejscowienie nadzoru MG - usługi zaufania; MAIC - EID. Trzeba to rozważyć i określić w Ustawie o usługach zaufania. Dodatkowo w zakresie "podejmuje (...) działania w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego - za pomocą działań nadzorczych ex post - gdy dowiaduje się, że niekwalifikowani dostawcy usług zaufania lub świadczone przez nich usługi zaufania rzekomo nie spełniają wymogów określonych w niniejszym rozporządzeniu." Wymaga wprowadzenie dodatkowych mechanizmów, co do ewidencji niekwalifikowanych usługodawców świadczących publicznie niekwalifikowanie usługi zaufania. Jako minimalne rozwiązanie w tym zakresie należy zaproponować procedurę rejestracji niekwalifikowanych TSP i prowadzenie Rejestru najlepiej w postaci list TSL, co do takich usługowców i usług. Obowiązki te będą wymagały znacząco zwiększenie planowanych koszów na Nadzór oraz zaangażowania odpowiedzialnych za nadzór. W ramach UoUZ należy w postaci Rozporządzenia uregulować ogólne zasady co do nadzoru usług niekwalifikowanych i obowiązków stron, tzn. usługodawców i nadzoru.

3.26Rozporządzenie eIDAS - art. 18

3.26.1 Rozporządzenie eIDAS - treść przepisu

Wzajemna pomoc

1. Organy nadzoru prowadzą współpracę, w ramach której wymieniają się dobrymi praktykami.

Organ nadzoru, na uzasadniony wniosek innego organu nadzoru, udziela temu organowi pomocy, tak aby działania organów nadzoru były prowadzone w spójny sposób. Wzajemna pomoc może obejmować w szczególności wnioski o informacje i środki nadzorcze, takie jak wnioski o przeprowadzenie inspekcji związanych z raportami z oceny zgodności, o których mowa w art. 20 i 21.

2. Organ nadzoru, do którego kierowany jest wniosek o pomoc, może odrzucić ten wniosek z któregokolwiek z poniższych względów:

a) organ nadzoru nie jest właściwy do udzielenia pomocy, której dotyczy wniosek;

b) pomoc, której dotyczy wniosek, nie jest proporcjonalna do działań nadzorczych organu nadzoru prowadzonych zgodnie z art. 17;

c) udzielenie pomocy, której dotyczy wniosek, byłoby niezgodne z niniejszym rozporządzeniem.

3. W stosownych przypadkach państwa członkowskie mogą upoważnić swoje odpowiednie organy nadzoru do prowadzenia wspólnych dochodzeń, w których biorą udział pracownicy z organów nadzoru innych państw członkowskich. Ustalenia i procedury dotyczące takich wspólnych działań są uzgadniane i określane przez zainteresowane państwa członkowskie zgodnie z ich prawem krajowym.

3.26.2 Propozycje uregulowania.

Wykonanie powyżej wymienionych czynności powinno być zawarte w ocenie skutków regulacji, gdyż zakres regulacji zwiększa zaangażowanie osobowe i czasowe przedstawicieli nadzoru w zakresie wykonania dodatkowych czynności w stosunku do obecnie wykonywanych. Co do "wniosków o informacje" oraz „procedur wspólnych działań" należy dążyć do uregulowania na szczeblu UE zakresu zawartości informacji do niezbędnych, a procedur do ujednolicenia w ramach UE (patrz rozdz. 4.3).

3.27Rozporządzenie eIDAS - art. 19

3.27.1 Rozporządzenie eIDAS - treść przepisu

Wymogi w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania

1. Kwalifikowani i niekwalifikowani dostawcy usług zaufania przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania. Przy uwzględnieniu najnowszych osiągnięć w dziedzinie technologii środki te zapewniają poziom bezpieczeństwa współmierny ze stopniem ryzyka. W szczególności należy podjąć środki zapobiegające incydentom związanym z bezpieczeństwem lub minimalizujące ich wpływ oraz należy informować zainteresowane strony o negatywnych skutkach wszelkich takich incydentów.

2. Kwalifikowani i niekwalifikowani dostawcy usług zaufania, bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia, zawiadamiają organ nadzoru i, w stosownych przypadkach, inne właściwe podmioty, takie jak właściwy krajowy organ ds. bezpieczeństwa informacji lub organ ochrony danych, o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe..

W przypadku, gdy prawdopodobne jest, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną, na rzecz, której świadczona była usługa zaufania, dostawca usług zaufania bez zbędnej zwłoki zawiadamia także tę osobę fizyczną lub prawną o tym naruszeniu bezpieczeństwa lub utracie integralności.

W stosownych przypadkach, w szczególności, jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej liczby państw członkowskich, zawiadomiony organ nadzoru powiadamia organy nadzoru w pozostałych zainteresowanych państwach członkowskich oraz ENISA.

Zawiadomiony organ nadzoru podaje zaistniałe fakty do wiadomości publicznej lub nakłada taki obowiązek na dostawcę usług zaufania, w przypadku, gdy uzna, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym.

3. Raz do roku organ nadzoru przekazuje ENISA zestawienie zawiadomień o naruszeniach bezpieczeństwa lub utraty integralności otrzymanych od dostawców usług zaufania.

Obowiązuje od dnia: 2014.09.17.

4. Komisja może w drodze aktów wykonawczych:

a) określić bardziej szczegółowo środki, o których mowa w ust. 1; oraz

b) określić formaty i procedury, w tym również terminy, mające zastosowanie na użytek ust. 2.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

3.27.2 Propozycje uregulowania.

Ad.1 Obecnie Rozdział 4 Rozporządzenie Rady Ministrów w sprawie określenia 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 (Dz.U.2002.128.1094) Opisuje ochronę

fizyczną, przed dostępem nieuprawnionym itd. Naruszenie tych wymagań ewidencjonowane, jako incydenty. Rozporządzenie obecnie nie dotyczy niekwalifikowanych usługodawców świadczących usługi publiczne - należy przynajmniej częściowo rozszerzyć wymagania na niekwalifikowane TSP. AD 2. Docelowym rozwiązaniem jest powołane się w porządku krajowym na akta i procedury wydane do tego artykułu przez KE. Niema przesłanek, ze przed momentem obowiązywania odpowiedzenie akty zostaną przygotowane, chociażby z tego względu, że nie jest określony termin ich wydania. na okres przejściowy powinny zostać opracowane procedury krajowe do realizacji wymagań artykułu 19 punkt 2. i wydane jako rozporządzenie pod UoUZ, określające co najmniej organy które się zawiadamia; przypadki szczegółowe do zawiadomienia innych organów ze wskazaniem których środków komunikacji w jaki sposób się zawiadamia; określenia przykładowych przypadków kiedy jest wymagany przekazanie informacji do wiadomości publicznej i w jaki sposób takie informacje podawane do wiadomości publicznej, aby uniknąć przypadków nierzetelnego wykonana obowiązku, na przykład podawanie do wiadomości publicznej jako wydruku na tablicy ogłoszeń.

3.28Rozporządzenie eIDAS - art. 22

3.28.1 Rozporządzenie eIDAS - treść przepisu

Zaufane listy.

1. Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za których jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania.

2. Państwa członkowskie sporządzają, prowadzą i publikują - w zabezpieczony sposób - elektronicznie podpisane lub opatrzone pieczęcią elektroniczną zaufane listy, o których mowa w ust. 1, w postaci dostosowanej do automatycznego przetwarzania.

3. Bez zbędnej zwłoki państwa członkowskie przekazują Komisji informacje o podmiocie odpowiedzialnym za sporządzenie, prowadzenie i publikowanie krajowych zaufanych list wraz ze szczegółowymi informacjami dotyczącymi miejsca publikacji tych list, certyfikatów użytych do podpisania lub opatrzenia pieczęcią zaufanych list i wszelkich zmian, jakie są do nich wprowadzane.

4. Komisja udostępnia publicznie informacje, o których mowa w ust. 3, w elektronicznie podpisanej lub opatrzonej pieczęcią elektroniczną postaci dostosowanej do automatycznego przetwarzania, używając w tym celu zabezpieczonego kanału komunikacji.

Obowiązuje od dnia: 2014.09.17.

5. Do dnia 18 września 2015 r. Komisja w drodze aktów wykonawczych określi informacje, o których mowa w ust. 1, oraz techniczne specyfikacje i formaty dotyczące zaufanych list mające zastosowanie na użytek ust. 1-4. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

3.28.2 Propozycje uregulowania.

Prawo krajowe winno określić sposób prowadzenia i upubliczniania zaufanych list zawierających informacje dotyczące kwalifikowanych dostawców usług zaufania w Polsce. Przepisy winny wskazywać podmiot odpowiedzialny za prowadzenie w/w listy, jak też regulować kwestie związane z wpisem podmiotu na listę, jak też jego wykreśleniem z listy - analogicznie jak miało to miejsce w ustawie o podpisie elektronicznym dla rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Listy winny być publikowane w formie elektronicznej z zachowaniem wymogów wskazanych w art. 23 ust. 2 rozporządzenia eIDAS w biuletynie informacji publicznej podmiotu prowadzącego listę.

3.29Rozporządzenie eIDAS - art. 24

3.29.1 Rozporządzenie eIDAS - treść przepisu

Wymogi dla kwalifikowanych dostawców usług zaufania

1. Wydając kwalifikowany certyfikat dla usługi zaufania, kwalifikowany dostawca usług zaufania weryfikuje, za pomocą odpowiednich środków i zgodnie z prawem krajowym, tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której wydaje kwalifikowany certyfikat.

Informacje, o których mowa w akapicie pierwszym, są weryfikowane przez kwalifikowanego dostawcę usług zaufania albo bezpośrednio, albo polegając na stronie trzeciej zgodnie z prawem krajowym:

a) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej; lub

b) zdalnie, przy użyciu środka identyfikacji elektronicznej, w przypadku którego przed wydaniem kwalifikowanego certyfikatu zapewniono fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej i który spełnia wymogi określone w art. 8 w odniesieniu do średniego lub wysokiego poziomu bezpieczeństwa; lub

c) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a) lub b); lub

d) przy użyciu innych metod identyfikacji uznanych na szczeblu krajowym, które zapewniają pewność równoważną, pod względem wiarygodności, fizycznej obecności. Równoważna pewność musi być potwierdzona przez jednostkę oceniającą zgodność.

2. Dostawca kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania:

a) informuje organ nadzoru o wszelkich zmianach w świadczeniu kwalifikowanych usług zaufania oraz o zamiarze zaprzestania swej działalności;

b) zatrudnia pracowników i, w stosownym przypadku, podwykonawców, którzy posiadają niezbędną wiedzę fachową, wiarygodność, doświadczenie i kwalifikacje i którzy przeszli odpowiednie szkolenia na temat przepisów dotyczących bezpieczeństwa i ochrony danych osobowych oraz którzy stosują procedury administracyjne i zarządcze odpowiadające europejskim lub międzynarodowym standardom;

c) w odniesieniu do ryzyka związanego z odpowiedzialnością za szkody zgodnie z art. 13 utrzymuje dostateczne zasoby finansowe lub dysponuje stosownym ubezpieczeniem od odpowiedzialności zgodnie z prawem krajowym;

d) przed wejściem w stosunek umowny informuje, w jasny i szczegółowy sposób, wszystkie osoby pragnące skorzystać z kwalifikowanej usługi zaufania o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej;

e) używa wiarygodnych systemów i produktów, które są chronione przed modyfikacją i zapewniają techniczne bezpieczeństwo i wiarygodność procesów przez niego obsługiwanych;

f) używa wiarygodnych systemów do przechowywania przekazanych mu danych w sprawdzalnej postaci, tak aby:

g) dane były publicznie dostępne do wyszukiwania dopiero po uzyskaniu zgody osoby, do której dane się odnoszą;

h) tylko upoważnione osoby mogły wprowadzać dane i zmiany w przechowywanych danych;

i) można było sprawdzać autentyczność danych;

j) podejmuje odpowiednie środki zapobiegające fałszowaniu i kradzieży danych;

k) rejestruje i udostępnia przez odpowiedni okres, w tym po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, w szczególności do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług. Rejestracja może odbywać się drogą elektroniczną;

l) ma aktualny plan zakończenia działalności, aby zapewnić ciągłość usług zgodnie z przepisami zweryfikowanymi przez organ nadzoru na mocy art. 17 ust. 4 lit. i);

m) zapewnia zgodne z prawem przetwarzanie danych osobowych zgodnie z dyrektywą 95/46/WE;

n) w przypadku kwalifikowanych dostawców usług zaufania wydających kwalifikowane certyfikaty - tworzy i aktualizuje bazę danych dotyczącą certyfikatów.

3. Jeżeli kwalifikowany dostawca usług zaufania wydający kwalifikowane certyfikaty postanowi unieważnić certyfikat, rejestruje on takie unieważnienie w swojej bazie danych dotyczącej certyfikatów i publikuje informację o statusie unieważnienia certyfikatu w odpowiednim czasie, ale w każdym razie w ciągu 24 godzin po otrzymaniu wniosku. Unieważnienie staje się skuteczne natychmiast po jego opublikowaniu.

4. W odniesieniu do ust. 3 kwalifikowani dostawcy usług zaufania wydający kwalifikowane certyfikaty dostarczają każdej stronie ufającej informacje o statusie ważności lub unieważnienia wydanych przez siebie kwalifikowanych certyfikatów. Informacje te są dostępne co najmniej na poziomie certyfikatu w automatyczny sposób, który jest wiarygodny, nieodpłatny i wydajny, w każdym momencie, także po upływie okresu ważności certyfikatu.

5. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących wiarygodnych systemów i produktów, które spełniają wymogi określone w ust. 2 lit. e) i f) niniejszego artykułu. W przypadku, gdy wiarygodne systemy i produkty spełniają te standardy, domniemywa się zgodność z wymogami określonymi w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

3.29.2 Propozycje uregulowania.

W prawie krajowym należy określić obowiązki kwalifikowanych dostawców usług zaufania.

Należy w pierwszej kolejności wskazać, że obowiązkiem kwalifikowanego dostawcy usług przy wydawania kwalifikowanego certyfikatu dla usługi zaufania jest weryfikacja tożsamości osoby ubiegającej się o certyfikat w oparciu o dokumenty stanowiące podstawę ustalenia tożsamości osoby zgodnie z prawem polskim. Weryfikacja tożsamości winna odbywać się bezpośrednio przez kwalifikowanego dostawę usług zaufania. W przypadku obecności pełnomocnika (upoważnionego przedstawiciela) osoby fizycznej za zasadne uznaje się wprowadzenie w polskim prawie krajowym wymogu dysponowania pełnomocnictwem w formie pisemnej z podpisem urzędowo poświadczonym, bądź pełnomocnictwa w formie elektronicznej podpisanego kwalifikowanym podpisem elektronicznym.

Obowiązkiem kwalifikowanych dostawców usług zaufania wyrażonym w prawie krajowym winno być ponadto w szczególności:

1) posiadanie ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone w związku ze świadczeniem usług. Ustawa o usługach zaufania winna zawierać delegację dla właściwego ministra do wydania rozporządzenia regulującego szczegółowy zakres tego ubezpieczenia oraz minimalną sumę gwarancyjną.

2) przechowywanie danych, o których mowa w art. 24 ust. 2 lit. h). Ustawa o usługach zaufania winna określać obowiązkowy okres przechowywania danych, o których mowa w art. 24 ust. 2 lit. h), a także winna zawierać delegację dla właściwego ministra do określenia w drodze rozporządzenia sposobu przechowywania i udostępniania tych danych.

3) zakres przechowywania danych, tzn. „wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych", o których mowa w art. 24 ust. 2 lit. h). Ustawa o usługach zaufania winna określać minimalny zakres przechowywania danych, o których mowa w art. 24 ust. 2 lit. h), a także winna zawierać delegację dla właściwego ministra do określenia w drodze rozporządzenia zakresu przechowywania danych.

4) przetwarzania danych osobowych z zachowaniem zasad wyrażonych w ustawie z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

W zakresie obowiązku o którym mowa w art. 24 ust. 3 „publikuje informację o statusie unieważnienia certyfikatu w odpowiednim czasie, ale w każdym razie w ciągu 24 godzin" proponujemy zachowanie w przepisach krajowych okresu 1h dla wykonania publikacji o unieważnieniach kwalifikowanego certyfikatu.

3.30 Rozporządzenie eIDAS - art. 27

3.30.1 Rozporządzenie eIDAS - treść przepisu Podpisy elektroniczne w usługach publicznych

1. Jeżeli państwo członkowskie wymaga zaawansowanego podpisu elektronicznego do korzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane podpisy elektroniczne, zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie podpisów elektronicznych oraz kwalifikowane podpisy elektroniczne, co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

2. Jeżeli państwo członkowskie wymaga zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie do skorzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie i

kwalifikowane podpisy elektroniczne, co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

3. W przypadku transgranicznego użycia w usłudze online oferowanej przez podmiot sektora publicznego państwa członkowskie nie wymagają podpisu elektronicznego o wyższym poziomie bezpieczeństwa niż kwalifikowany podpis elektroniczny.

Obowiązuje od dnia: 2014.09.17

4. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych podpisów elektronicznych. W przypadku gdy zaawansowany podpis elektroniczny spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych podpisów elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 26. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Obowiązuje od dnia: 2014.09.17

5. Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i unijnych aktów prawnych Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych podpisów elektronicznych lub metody referencyjne, w przypadku, gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

3.30.2 Propozycje uregulowania.

Ustawa o usługach zaufania winna normować zasadę, zgodnie, z którą w polskim systemie prawnym uznawane są wszelkie zaawansowane podpisy elektroniczne, zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie podpisów elektronicznych oraz kwalifikowane podpisy elektroniczne w formatach lub wykorzystujące metody określone w aktach wykonawczych wydanych przez Komisję na podstawie art. 27 ust. 4 i 5 rozporządzenia eIDAS, wymagane do korzystania z usługi online oferowanej przez podmiot sektora publicznego. Analogicznie ustawa winna zawierać normę, zgodnie, z którą w polskim systemie prawnym uznawane są wszelkie zaawansowane podpisy elektroniczne oparte na kwalifikowanym certyfikacie oraz kwalifikowane podpisy elektroniczne w formatach lub wykorzystujące metody określone w aktach wykonawczych wydanych przez Komisję na podstawie art. 27 ust. 4 i 5 rozporządzenia eIDAS, w przypadkach, gdy krajowe przepisy wymagają zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie do skorzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu.

3.31Rozporządzenie eIDAS - art. 36

3.31.1 Rozporządzenie eIDAS - treść przepisu

Wymogi dla zaawansowanych pieczęci elektronicznych

Zaawansowana pieczęć elektroniczna musi spełniać następujące wymogi:

a) jest unikalnie przyporządkowana podmiotowi składającemu pieczęć;

b) umożliwia ustalenie tożsamości podmiotu składającego pieczęć;

c) 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

d) jest powiązana z danymi, do których się odnosi, w taki sposób, że każda późniejsza zmiana danych jest rozpoznawalna.

3.31.2 Propozycje uregulowania.

Należy określić procedury wydawania CPE, w szczególności QCPE, unieważnienia i odpowiedzialności w zakresie "opieczętowanego dokumentu „, szczególnie wskazanych byłoby określenia "przykładowych / zalecanych przypadków użycia CPE". Można zastosować w tym przypadku/regule materiały informacyjne takie jak akty normatywne, zarządzenie, faktury mogą być opatrywane pieczęcią. Dokumenty, za którymi idzie odpowiedzialność prawna i finansowa (opinie rozstające konkretnego urzędnika państwowego należy podpisać certyfikatem kwalifikowanym reprezentując urząd).

3.32Rozporządzenie eIDAS - art. 37

3.32.1 Rozporządzenie eIDAS - treść przepisu

Pieczęcie elektroniczne w usługach publicznych

1. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej do skorzystania z usługi online 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, o których mowa w ust. 5.

2. Jeżeli państwo członkowskie wymaga zaawansowanej pieczęci elektronicznej opartej na kwalifikowanym certyfikacie do skorzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu, to państwo członkowskie uznaje zaawansowane pieczęcie elektroniczne oparte na kwalifikowanym certyfikacie i kwalifikowane pieczęcie elektroniczne co najmniej w formatach lub wykorzystujące metody określone w aktach wykonawczych, o których mowa w ust. 5.

3. W przypadku transgranicznego użycia w usłudze online oferowanej przez podmiot sektora publicznego państwa członkowskie nie wymagają pieczęci elektronicznej o wyższym poziomie bezpieczeństwa niż kwalifikowana pieczęć elektroniczna.

Obowiązuje od dnia: 2014.09.17

4. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych pieczęci elektronicznych. W przypadku, gdy zaawansowana pieczęć elektroniczna spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych pieczęci elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 36. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Obowiązuje od dnia: 2014.09.17

5. Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i aktów prawnych Unii Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych pieczęci elektronicznych lub metody referencyjne, w przypadku gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

3.32.2 Propozycje uregulowania.

Ustawa o usługach zaufania winna normować zasadę, zgodnie z którą w polskim systemie prawnym uznawane są wszelkie zaawansowane pieczęci elektroniczne, zaawansowane pieczęci elektroniczne oparte na kwalifikowanym certyfikacie pieczęci elektronicznych oraz kwalifikowane pieczęci elektroniczne w formatach lub wykorzystujące metody określone w aktach wykonawczych wydanych przez Komisję na podstawie art. 37 ust. 4 i 5 rozporządzenia eIDAS, wymagane do korzystania z usługi online oferowanej przez podmiot sektora publicznego. Analogicznie ustawa winna zawierać normę, zgodnie, z którą w polskim systemie prawnym uznawane są wszelkie zaawansowane pieczęci elektroniczne oparte na kwalifikowanym certyfikacie oraz kwalifikowane pieczęcie elektroniczne w formatach lub wykorzystujące metody określone w aktach wykonawczych wydanych przez Komisję na podstawie art. 37 ust. 4 i 5 rozporządzenia eIDAS, w przypadkach, gdy krajowe przepisy wymagają zaawansowanej pieczęci elektronicznej opartej na kwalifikowanym certyfikacie do skorzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu.

4. ASPEKTY ORGANIZACYJNE I EKONOMICZNE

4.1 Zalecany harmonogram wdrożenia eIDAS

L.p.	Zadanie	Data rozpoczęcia	Data zakończenia
1.	**eIDAS**		
1.1	Publikacja przez Komisję Europejską propozycji Rozporządzenia w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym COM(2012) 238 final.	2012-06-04	2012-06-04
1.2	Przyjęcie Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Data publikacji w Dzienniku Urzędowym UE: 2014-08-28 - od tej daty liczony jest termin wejścia w życie i stosowania.	2014-07-23	2014-07-23
1.3	Publikacja w Dzienniku Urzędowym UE Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. **Data wejścia w życie eIDAS.**	2014-08-28	2014-08-28
1.4	Określenie przez KE, w drodze aktów wykonawczych, niezbędnych proceduralnych warunków ułatwiania współpracy między państwami członkowskimi, w celu zapewnienia wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka.	2014-08-28	2015-03-18
1.5	Określenie przez KE, w drodze aktów wykonawczych, specyfikacji dot. wzoru znaku zaufania UE dla kwalifikowanych usług zaufania.	2014-08-28	2015-07-01
1.6	Określenie przez KE, w drodze aktów wykonawczych, formatów referencyjnych zaawansowanych pieczęci elektronicznych lub metod referencyjnych, w przypadku, gdy używane są formaty alternatywne.	2014-08-28	2015-09-18
1.7	[AW.INTEROP] Określenie przez KE, w drodze aktów wykonawczych, dotyczących ram interoperacyjności.	2014-08-28	2015-09-18
1.8	Określenie przez KE, w drodze aktów wykonawczych, dla środków identyfikacji elektronicznej minimalnych technicznych specyfikacji, standardów i procedur w odniesieniu, do których określone zostaną niski, średni i wysoki poziom bezpieczeństwa.	2014-08-28	2015-09-18
1.7	[AW.ID] Określenie przez KE, w drodze aktów wykonawczych, w których zostaną określone niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej.	2014-08-28	2015-09-18
1.8	Określenie przez KE, w drodze aktów wykonawczych, specyfikacji i formatów dot. zaufanych list zawierających informacje o kwalifikowanych dostawcach usług zaufania.	2014-08-28	2015-09-18
2.	**Ustawa o usługach zaufania**		
2.1	Złożenie ustawy o usługach zaufania do sejmu	2015-10-01	2015-10-31
2.2	Uchwalenie ustawy o usługach zaufania	2016-02-01	2016-02-01
2.3	Wydanie rozporządzeń do ustawy o usługach zaufania, w szczególności: a) Rozporządzenia w sprawie krajowej infrastruktury klucza publicznego (regulującego „root" w NBP); b) Rozporządzenia w sprawie rejestru Ministra Gospodarki i zaświadczeń certyfikacyjnych – certyfikat najwyższego poziomu (rootCA) i certyfikaty CA.	2016-02-01	2016-02-01
2.4	Nowelizacja aktów prawnych w Polsce, w których występuje odniesienie do usług zaufania	2016-04-01	2016-04-01

2.5	Wejście w życie ustawy o usługach zaufania – miesięczne *vacatio legis* do 01.07.2016.	2016-05-01	2016-06-01
2.6	Wejście w życie rozporządzeń do ustawy o usługach zaufania – miesięczne *vacatio legis* do 01.07.2016.	2016-05-01	2016-06-01
2.7	Wejście w życie znowelizowanych aktów prawnych w Polsce, w których występuje odniesienie do usług zaufania	2016-07-01	2016-07-01
2.8	Uchylenie Dyrektywy 1999/93/WE z dnia 13 grudnia 1999r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.	2016-07-01	2016-07-01
2.9	Uchylenie ustawy o podpisie elektronicznym z dnia 18 września 2001r. oraz wydanych na jej podstawie aktów wykonawczych.	2016-07-01	2016-07-01
3.	**Nadzór, Ocena zgodności (harmonogram działań uwzględnia plan przedstawiony przez PCA w piśmie AJ-ER-535-35/14)**		
3.1	Przygotowanie krajowych jednostek akredytujących i jednostek oceny zgodności. Zgodnie z [PCA.AJ-ER-535-35/14]: *"Przygotowanie szczegółowego planu wdrożenia.* *Przygotowanie do akredytacji, w tym:* *a) uzupełnienie bazy PCA o kompetentnych auditorów/ekspertów;* *b) szkolenie personelu wewnętrznego i zewnętrznego;* *c) uzgodnienie z organem nadzoru (w rozumieniu przedmiotowego rozporządzenia) sposobu formułowania zakresu akredytacji;* d) *ogłoszenie komunikatu o uruchomieniu akredytacji do celów Rozporządzenia eIDAS;"*	2014-11-01	2015-05-31
3.2	Akredytacja jednostek oceny zgodności. Zgodnie z [PCA.AJ-ER-535-35/14]: *"Oceny akredytacyjne CABs do celów Rozporządzenia eIDAS, zgodnie z PN-EN ISO/IEC 17065 + ETSI TS 119 403 (realizacja złożonych wniosków".*	2015-06-01	2016-06-30[17] 2016-07-31[18]
3.3	Zgodnie z [PCA.AJ-ER-535-35/14]: *"Opublikowanie komunikatu PCA w związku z publikacją EN 319 403"*	2016-03-01	2016-03-31[10]
3.4	Zgodnie z [PCA.AJ-ER-535-35/14]: *"Przyjmowanie wniosków CABs o zmianę dokumentu akredytacyjnego z TS 119 403 na EN 319 403"*	2016-07-01	2016-07-31[10]
3.5	Audyty zgodnie z EN 319 403 & EN 319 4X1	2016-07-01	2016-06-30[9] 2016-07-31[10]
3.6	Zgodnie z [PCA.AJ-ER-535-35/14]: *"Zmiana dokumentu akredytacyjnego w udzielonych akredytacjach na podstawie przeglądu dokumentacji (przy braku istotnych różnic między TS 119 403 a EN 319 403) bez potrzeby oceny w siedzibie i uruchamiania obserwacji."*	2016-09-01	2016-09-30
3.7	Audyty zgodnie z EN XXX	2017-07-01	Proces ciągły
3.8	[DUUE.ID.NOT] Opublikowanie przez KE w Dzienniku Urzędowym Unii Europejskiej wykazu systemów identyfikacji elektronicznej, które zostały notyfikowane na mocy art. 9, pkt. 2 eIDAS.	Rok od daty stosowania aktów wykonawczych [AW.ID] i	Rok od daty stosowania aktów wykonawczych [AW.ID] i

[17] Zgodnie z ETSI TSP Standards Time-Scale

[18] Zgodnie z [PCA.AJ-ER-535-35/14]

		[AW.INTEROP] 2016-09-18	[AW.INTEROP]
3.9	Termin przedłożenia przez istniejących TSP raportów z oceny zgodności do organów nadzoru.	2014-07-23	2017-07-01
3.10	Wprowadzenie obowiązku uznawania notyfikowanych zagranicznych środków identyfikacji elektronicznej.	Rok od daty ogłoszenia wykazu systemów identyfikacji [DUUE.ID.NOT] 2017-09-18	2018-07-01

Należy zwrócić uwagę na fakt, że dostosowanie do dnia 1 lipca 2016 polskiego systemu prawnego oraz krajowej infrastruktury klucza publicznego do rozporządzenia eIDAS i utworzenie systemu zgodności powinno mieć nadany najwyższy priorytet ze względu na ryzyko nałożenia przez KE kar za ew. niewdrożenie w terminie nowego reżimu unijnego lub utrzymanie w mocy przepisów krajowych niespójnych z rozporządzeniem unijnym.

4.2 Harmonogram publikacji standardów odnoszących się do aktów prawnych niższego poziomu

Poniższa tabela opracowana została przez Instytut Maszyn Matematycznych19 i *"przywołuje wszystkie artykuły dotyczące usług zaufania, z rozporządzenia eIDAS, które zawierają odwołania do aktów prawnych niższego poziomu. Dla każdego z wymienionych artykułów zostały wskazane odpowiednie standardy (włączając w to standardy ISO) wraz z datami publikacji ogłoszonymi (w niektórych przypadkach wyłącznie wstępnie) przez CEN lub ETSI."*

Act of art.	Art. uzupełniający	Krótki opis artykułu	Główny standard(y) mające odniesienie	Szacowana data dostępności:
17.8	17.6	***Coroczny raport nadzoru*** Akt implementujący uszczegóławiający format (np. szablon) corocznego raportu dotyczącego aktywności organu nadzoru i procedura składania raportu do Komisji Europejskiej (EC) (i Państw Członkowskich - MS).	N/A	N/A
19.4	19.1	***Bezpieczeństwo przez dochowanie należytej staranności przez dostawców usług zaufania (TSP)*** Akt implementujący uszczegóławiający środki organizacyjne i techniczne, które powinny być zaimplementowane przez (kwalifikowanych I niekwalifikowanych) dostawców usług zaufania (TSP) w celu zarządzania ryzykami dotyczącymi bezpieczeństwa usług zaufania, które świadczą, włączając w to redukowanie ryzyka i informację dla osób kluczowych.	Zalecenia ENISA	2015
			N/A	N/A
19.4	19.2	***Notyfikowanie o incydentach bezpieczeństwa przez***	Zalecenia ENISA	2015

[19] *Opracowanie: Daniel Wachnik, IMM. Kompletny dokument stanowi Załącznik nr 1 do niniejszej ekspertyzy.*

Act of art.	Art. uzupełniający	Krótki opis artykułu	Główny standard(y) mające odniesienie	Szacowana data dostępności:
		TSP Akt implementujący uszczegóławiający format i procedurę notyfikacji o incydentach bezpieczeństwa przez QTSP i NQTSP do SB i innych odpowiednich stron.	EN 319 401	30.4.2016
20.4	20.1	***CAB standardy akredytacji I audytu*** Akt(y) implementujący wymieniający standard(y) dotyczące:		
		(a) Akredytacji jednostek oceniających zgodność(ang. Conformity Assessment Bodies – CAB zgodnie z Rozporządzeniem UE 765/2008 (Akredytacja CAB przez NAB)	ISO 17065 ISO 17020	Dostępny Dostępny
			ISO 27006	Dostępny
		(b) Raport zgodności (działalność TSP); (raport nie jest zestandaryzowany)	EN 319 403	30.3.2016
			EN 319 411 N/A	30.4.2016
21.4	21.1	***Inicjacja działalności QTSP*** Akt implementujący definiujący: • Formaty I procedury inicjacji działalności QTSP (notyfikacja do SB) • Wstępny raport oceny zgodności wydany przez CAB.	Patrz wyżej	Patrz wyżej
21.4	21.2	***Kwalifikacja QTSP*** Akt implementujący definiujący:		
		(a) Format i procedury uruchamiane przez SB w celu poinformowania TSP o tym, że usługi, które zamierza świadczyć uzyskały status kwalifikowany, lub że kwalifikowany status nie został przyznany kwalifikowanej usłudze, którą zamierza świadczyć (albo, że przedłużono termin nadania statusu – informacja wraz z uzasadnieniem),	N/A	N/A
		(b) Formaty i procedury dla SB w celu zarządzania od kraju członkowskiego(MS) aktualizacji listy zaufania(Trusted List).	N/A	N/A
22.5	22.1 to 22.4	***Lista zaufania (Trusted List)*** Akt implementujący definiujący format i obsługę listy zaufania.	EN 319 612	31.5.2015
23.3	23.1	***Znak zaufania QTS (Trustmark)*** Akt implementujacy specyfikujący formę (sposób prezentacji, układ, rozmiar i projekt) znaku zaufania EU dla usług kwalifikowanych.	N/A	N/A

Act of art.	Art. uzupełniający	Krótki opis artykułu	Główny standard(y) mające odniesienie	Szacowana data dostępności:
24.5	24.2.e	***Standardy dotyczące wyposażenia QTSP*** Akt implementujący wymieniający standardy(np. profile zabezpieczeń – ang. protection profiles) dla zaufanych produktów i systemów (ang. "trustworthy systems and products") używanych przez QTSP: CEN 419 221 (ex. CWA 14167) Akt zastąpi profile zabezpieczeń dla urządzeń HSM wymienione w Decyzji 2003/511/EC w odniesieniu do Załącznika II.f Dyrektywy 1999/93/EC.	EN 419 221 (1 to 4)	24-miesięczny projekt (1Q2017)
24.5	24.2.f	***Standardy dla zaufanych systemów i produktów do składowania danych*** Akt implementujący wymieniający standardy dla zaufanych systemów i produktów do składowania danych, w formie umożliwiającej weryfikację, tak, aby: - Były one publiczne dostępne do pobranie tylko w przypadku, gdy osoba, do której odnoszą się dane wyraziła zgodę, - Wyłącznie autoryzowane osoby mogą wprowadzać dane i zmiany do składowanych danych, - Dane mogą być zweryfikowane pod kątem autentyczności.	ISO 27000	Available
27.4	26 27.1, 27.2	***Standardy dotyczące zaawansowanych podpisów elektronicznych*** Akt implementujący wymieniający dla zaawansowanych podpisów elektronicznych. ETSI iCEN wciąż analizują czy pieczęci elektroniczne(ang. eSeals) mogą być objęte standardami dotyczącymi podpisów, lub czy powinny ich dotyczyć wyłącznie specyficzne wymagania.	EN 319 172	25 months project (1Q2017)
			TS 119 312	15.11.2014
			EN 419 221-5	Niezdefiniowana
			Standary walidacji – patrz art. 32.3 i 40	30.4.2017
			Formaty standardów podpisu - patrz art 27.5 i 37.5	30.4.2016
27.5 + 37.5	27.1, 27.2 + 37.1, 37.2	***Formaty dla zaawansowanego e-podpisu i e-pieczęci*** Akt implementujący wymieniający standardy dla formatów e-podpiu i profili, które będą obsługiwane przez usługi administracji publicznej(np. XAdES, PAdES, CAdES, ASiC).	EN 319 122 EN 319 132 EN 319 142 EN 319 152	30.3.2015 (wersja ostateczna: 30.4.2016)
28.6	Annex I	***QC dla e-podpisu*** Akt implementujący wymieniający standardy uszczegóławiające pola certyfikatu kwalifikowanego dla e-podpisu,	EN 319 412-2 EN 319 412-5	30.4.2016

Act of art.	Art. uzupełniający	Krótki opis artykułu	Główny standard(y) mające odniesienie	Szacowana data dostępności:
29.2	Annex II	***Profile zabezpieczeń dla QCSD***	N/A	N/A
30.3.	30.3.a	***Ocena bezpieczeństwa QSCD*** Akt implementujący wymieniający standardy dotyczące certyfikacji (zgodności z normą) produktów ICT. Zastąpi profile zabezpieczeń dla rządzeń QSCD wymienione w Decyzji 2003/511/EC.	ISO 15408	Dostępny
			ISO 18045	Dostępny
			EN 419 211 EN 419 241	24-miesięczny projekt (około 1Q 2017)
30.4	30.1	***Organy oceniające zgodność QSCD*** *("Designated Bodies")* Akt delegowany ustanawiający kryteria, które powinny spełniać organy certyfikujące (na zgodność z normą) urządzenia QSCD (tzw. Designated Bodies). Akt może zaktualizować Decyzję 2000/709/EC.	N/A	N/A
31.3	31.1	***Notyfikacja QSCD*** Akt implementujący uszczegóławiający format i procedurę notyfikacji certyfikowanych urządzeń QSCD przez Kraje Członkowskie(MS) i Komisję Europejską(EC).	N/A	N/A
32.3	32.1	***Walidacja QeS*** Akt implementujący wymieniający standardy wskazujące, w jaki sposób może być walidowany podpis kwalifikowany (QeS) zgodnie z art. 25.1	EN 319 101	30.4.2017
			EN 319 102	30.4.2016
			EN 419 103	30.3.2016
			EN 419 111	Niezdefiniowana
33.2	33.1	***QTSP walidujący QeS*** Akt wymieniający standardy wskazujące minimalne wymagania, które powinien spełniać QTSP świadczący usługi walidacji QeS	EN 319 441	46-miesięczny projekt (1Q2019)
34.2	34.1	***Konserwacja kwalifikowanych e-podpisów*** Akt implementujący wymieniający standardy wskazujące możliwe procedury i techniki bezpieczeństwa dotyczące konserwacji QeS.	EN 319 521	37-miesięczny projekt (1Q2018)
38.6	Annex III	***QC dla pieczęci elektronicznych*** Akt implementujący wymieniający standardy uszczegóławiające pola certyfikatu kwalifikowanego dla pieczęci elektronicznych EN 319 412-3 i EN 319 412-5	EN 319 412-3 EN 319 412-5	30.4.2016

Act of art.	Art. uzupełniający	Krótki opis artykułu	Główny standard(y) mające odniesienie	Szacowana data dostępności:
37.4	36, 37.1, 37.2,	***Standardy zaawansowanej pieczęci elektronicznej*** Akty implementujące wymieniające standardy dla zaawansowanych pieczęci elektronicznych.	Patrz art. 27.4	Patrz art.27.4
37.5	37.1, 37.2	***Formaty elektronicznych pieczęci***	Patrz art.27.5	Patrz art.27.5
39.1	39.1	***Profile zabezpieczeń dla urządzeń do składania zaawansowanych pieczęci elektronicznych.***	Patrz art.29.2	Patrz Art.29.2
39.2	39.2	***Common criteria dla oceny kwalifikowanych urządzeń do składania pieczęci elektronicznych.***	Patrz art. 30.3.a	Patrz Art.30.3.a
39.2	39.2	***Organy oceniające zgodność kwalifikowanych urządzeń do składania pieczęci elektronicznych*** ("Designated Bodies")	Patrz art.30.4	Patrz Art.30.4
39.3	39.3	***Notyfikacja kwalifikowanych urządzeń do składania pieczęci elektronicznych.***	Patrz.art.31.3	Patrz art.31.3
40	40	***Walidacja kwalifikowanych pieczęci elektronicznych***	Patrz art. 32.3	Patrz art.32.3
40	40	***QTSP świadczące walidację kwalifikowanych pieczęci elektronicznych***	Patrz art. 33.2	Patrz art.33.2
40	40	**Konserwacja kwalifikowanych pieczęci elektronicznych**	Patrz art.34.2	Patrz art.34.2
42.2	42.1	***Świadczenie i bezpieczeństwo kwalifikowanego znakowania czasem*** Akt implementujący wymieniający standardy dotyczące: 1. Powiązania daty i daty z danymi i 2. Dokładnych źródeł czasu (zaufane świadczenie usługi znakowania czasem i systemy).	EN 319 422	30.4.2016
			EN 319 421	30.4.2016
			EN 419 231	30.3.2016
44.2	44.1	***Kwalifikowane usługi rejestrowanych e-doręczeń.*** Akt implementujący wymieniając standardy wskazujące jak kwalifikowane usługi rejestrowanych e-doręczeń mogą być uznane za zgodne z wymaganiami art. 36.1.	ETSI - REM	Dostępny
			UPU - PREM	Dostępny
			EN 319 511	Niezdefiniowana
			SR 019 530	30.10.2014
45.2	Załącznik IV	***QC do uwierzytelnienia strony internetowej*** Akt implementujący wymieniający standardy uszczegóławiające pola certyfikatu kwalifikowanego dla uwierzytelnienia witryny internetowej.	EN 319 412-4	30.4.2016

4.3 System nadzoru i oceny zgodności w ramach eIDAS

Celem wdrożenia rozporządzenia eIDAS jest zwiększenie zaufania do transakcji elektronicznych na rynku wewnętrznym poprzez zapewnienie wspólnej podstawy bezpiecznej interakcji elektronicznej między obywatelami, przedsiębiorstwami i organami publicznymi, co pozwoli podnieść efektywność publicznych i prywatnych usług online, e-biznesu i e-handlu w Unii [eIDAS, preambuła, ust. 2].

Jednym z warunków koniecznych do zapewnienia zwiększenia zaufania pomiędzy uczestnikami transakcji elektronicznych jest silna reprezentacja interesów obywateli i przedsiębiorstw przez instytucje państwowe działające w ich imieniu oraz bezpośrednio przez obywateli i przedsiębiorstwa, posiadające zasoby do sprawowania "społecznego nadzoru" nad usługami identyfikacji i usługami zaufania.

4.3.1 Podział kompetencji nadzoru w Polsce

Zgodnie z Art. 30 ustawy o podpisie elektronicznym *"Minister właściwy do spraw gospodarki sprawuje nadzór nad przestrzeganiem przepisów ustawy przez kwalifikowane podmioty, zapewniając ochronę interesów odbiorców usług certyfikacyjnych"*[20] [21]. Przepis ten oddaje w pełni potrzebę sprawowania nadzoru nad przestrzeganiem obowiązujących przepisów związanych ze świadczeniem usług certyfikacyjnych. **Wydaje się, że naturalnym rozwinięciem tych obowiązków po wejściu w życie eIDAS będzie sprawowanie nadzoru przez ministra właściwego do spraw gospodarki nad wszystkimi usługami zaufania.** Pod nadzór MG, w dacie wejścia rozporządzenia, przesunięte zostaną nowe usługi zaufania, takie jak np. usługa rejestrowanego doręczenia elektronicznego, konserwacja elektronicznych podpisów i pieczęci (lub certyfikatów powiązanych z tymi usługami), pieczęć elektroniczna i uwierzytelnienie witryn internetowych.

Z uwagi na występowanie w regulacji eIDAS także usług elektronicznej identyfikacji, będących w kompetencji ministra właściwego do spraw administracji publicznej i informatyzacji[22], **wydaje się być naturalnym sprawowanie nadzoru**

---

[20] Dz.U. 2001 Nr 130 poz. 1450, Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym
Rozdział VII
Nadzór nad działalnością kwalifikowanych podmiotów świadczących usługi certyfikacyjne
Art. 30.
1. Minister właściwy do spraw gospodarki sprawuje nadzór nad przestrzeganiem przepisów ustawy przez kwalifikowane podmioty, zapewniając ochronę interesów odbiorców usług certyfikacyjnych.
2. Zadanie, o którym mowa w ust. 1, minister właściwy do spraw gospodarki realizuje w szczególności poprzez:
1) prowadzenie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne;
2) wydawanie i unieważnianie zaświadczeń certyfikacyjnych, o których mowa w art. 23 ust. 2;
3) kontrolę działalności podmiotów świadczących usługi certyfikacyjne pod względem zgodności z ustawą;
4) nakładanie kar przewidzianych w ustawie.
3. Prowadzenie rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne minister właściwy do spraw gospodarki może powierzyć podmiotom, o których mowa w art. 23 ust. 4 i 5, które spełniają wymagania ustawy dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne w zakresie bezpieczeństwa, wydawania, przechowywania i unieważniania certyfikatów i nie świadczą usług certyfikacyjnych polegających na wydawaniu certyfikatów.

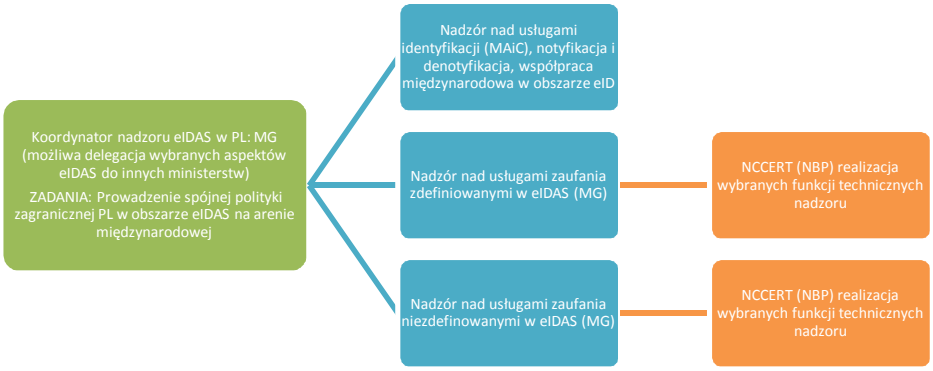
[21] Dz.U. 2007 nr 65 poz. 437, Ustawa z dnia 4 września 1997 r. o działach administracji rządowej
Art. 9. *(przyp. aut. dotyczy MG)*
1. Dział gospodarka obejmuje sprawy gospodarki, w tym konkurencyjności gospodarki, współpracy gospodarczej z zagranicą, energetyki, oceny zgodności, miar i probiernictwa, własności przemysłowej, innowacyjności, działalności gospodarczej, promocji gospodarki polskiej w kraju i za granicą, umów offsetowych oraz współpracy z organizacjami samorządu gospodarczego. Do ministra właściwego do spraw gospodarki należą w szczególności sprawy:
(…)
6) nadzoru nad świadczeniem usług związanych z podpisem elektronicznym w rozumieniu przepisów o podpisie elektronicznym

[22] Dz.U. 2007 nr 65 poz. 437, Ustawa z dnia 4 września 1997 r. o działach administracji rządowej
(…)
12a. *(przyp. aut. dotyczy MAiC)*
Dział informatyzacja obejmuje sprawy:
1) informatyzacji administracji publicznej;
2) systemów i sieci teleinformatycznych administracji publicznej;
3) technologii i technik informacyjnych;
4) standardów informatycznych;

nad środkami identyfikacji elektronicznej przez Ministerstwo Administracji i Cyfryzacji. W kompetencjach MAiC, w tym obszarze, pozostawałby nadzór ze strony państwa, wraz z instrumentami technicznymi i prawnymi, w tym także systemem kar.

MAiC powinien odpowiadać za notyfikację i denotyfikację systemów eID, w tym także systemów z sektora prywatnego. Powinien również opracować procedurę administracyjną dla realizacji obu tych zadań, tak aby nie był to przedmiot arbitralnych decyzji państwa. Trzeba też podkreślić, że eIDAS odróżnia nadzór usług zaufania od nadzoru elektronicznej identyfikacji. Nadzór usług zaufania jest regulowany w art. 17. Wymóg ustanowienia nadzoru usług zaufania jest wymogiem unijnym. Art. 17 nakazuje państwom członkowskim zapewnienie uprawnień i odpowiednich zasobów niezbędnych do wykonywania zadań. Na poziomie krajowym konieczne jest odpowiednie opracowanie narzędzi prawnych i technicznych.

Rozporządzenie eIDAS nie nakłada na poziomie unijnym obowiązku ustanowienia organu nadzoru dla eID - brak jest w tym zakresie odpowiednika art. 17. Niemniej w art. 9.1 (b) mowa jest o systemie nadzoru (supervisory regime) nad eID, który trzeba notyfikować, co oznacza, że implicite zakłada się istnienie tego rodzaju nadzoru na poziomie państw członkowskich. Wstępnie należy zakładać, że nadzór usług zaufania i nadzór eID są to merytorycznie różne nadzory, realizowane w oparciu o różne podstawy prawne i w różnym zakresie regulowane w eIDAS. Biorąc pod uwagę, iż w rozporządzeniu eIDAS zdecydowanie większa część uregulowań przypisana jest usługom zaufania, **podmiotem koordynującym** nie tylko wdrożenie rozporządzenia eIDAS, ale także, po wdrożeniu, kompleksowy **nadzór nad zgodnością wszystkich objętych rozporządzeniem usług powinno być Ministerstwo Gospodarki**.



Rys. 4.1 Proponowana struktura organizacyjna sprawowania nadzoru nad usługami zdefiniowanymi w eIDAS.

Centralizacja koordynacji nadzoru nad wszystkimi usługami w ramach MG ma na celu:

a) Optymalizację kosztów nadzoru związanych z pozyskiwaniem i utrzymywaniem kompetencji niezbędnych do prowadzenia nadzoru (zarówno w części eID jak i TS), zarządzaniem procesami nadzoru, kontaktami z innymi instytucjami nadzoru (w szczególności prowadzenia spójnej polityki zagranicznej);
b) Wykorzystanie efektów synergii w realizacji nadzoru dostawców usług zaufania oferujących szeroki portfel takich usług. Tacy dostawcy preferować będą z pewnością jedno źródło nadzoru (pojedynczy punkt kontaktowy nadzoru). Komercyjni dostawcy usług identyfikacji świadczący jednocześnie usługi zaufania

5) wspierania inwestycji w dziedzinie informatyki;
6) zastosowań technologii informatycznych w społeczeństwie informacyjnym;
7) rozwoju społeczeństwa informacyjnego;
7a) przeciwdziałania wykluczeniu cyfrowemu;
7b) rozwoju usług świadczonych drogą elektroniczną oraz usług na żądanie;
8) realizacji zobowiązań międzynarodowych Rzeczypospolitej Polskiej w dziedzinie informatyzacji;
9) koordynacji interoperacyjności.

spodziewać się będą nie dublowania czynności realizowanych przez audytorów eID i audytorów TS (z wyjątkiem czynności kontrolnych specyficznych dla danego typu usługi, które nie są realizowane dla innej usługi). Wymaga to wprowadzenia koordynacji nadzoru organów odpowiedzialnych za eID i TS;

c) Uzyskanie jak najwyższej transparentności usług nadzoru dla instytucji "społecznego nadzoru" (np. mediów).

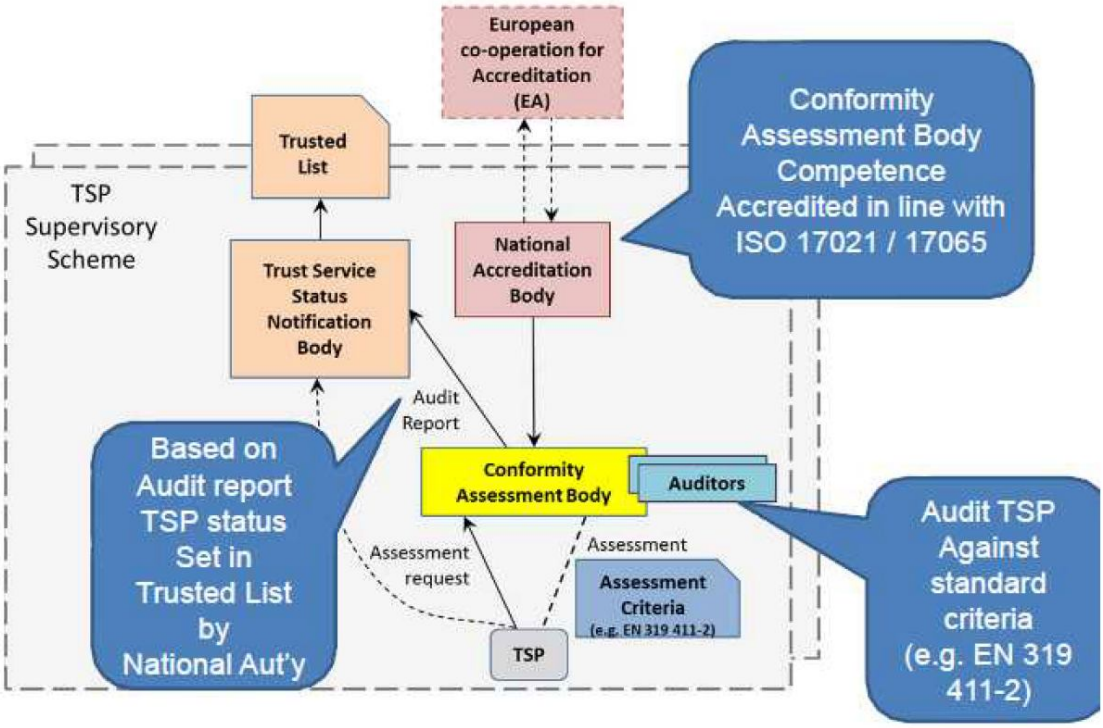
W państwach członkowskich EU nadzór nad usługami zaufania przypisany jest do różnych organów. Poniższe zestawienie autorstwa FESA[23] może być źródłem informacji, w jakich kompetencjach umiejscowiony jest nadzór nad TSP:

AL: National Authority for Electronic Certification
AT: Austrian Regulatory Authority for Broadcasting and Telecommunications
BE: FPS Economy, SMEs, Self-employed and Energy - Quality and Security - Information Management
CH: Federal Office of Communications
CZ: Ministry of Informatics
DE: Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway
DK: The Danish Agency for Digitisation
ES: State Secretariat for Telecommunications and for the Information Society (SETSI). Ministry of Industry, Energy and Tourism (MINETUR).
FI: Finnish Communications Regulatory Authority (FICORA)
FR: Central Directorate for Information and Network Security
FR: Ministry of Economics, Finance and Industry
GB: Department for Business, Innovation & Skills
GR: National Telecommunications and Post Commission (EETT)
HU: National Media and Infocommunications Authority
IS: The Consumer Agency
LT: Communications Regulatory Authority of the Republic of Lithuania
LU: Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services (ILNAS) - Digital trust department
ME: Secretariat for Development
MT: Malta Communications Authority
NL: Authority for Consumers & Markets
NO: Norwegian Post and Telecommunications Authority
PL: Ministry of Economy
RS: Ministry of Telecommunication and Information Society
SE: National Post and Telecom Agency
SE: SWEDAC, Swedish Board for Accreditation and Conformity Assessment
SK: National Security Authority
TR: Turkish Telecommunications Authority

4.3.2 Model nadzoru i oceny zgodności z eIDAS dla dostawców usług zaufania

Model oceny zgodności dostawców usług zaufania stanowiący element modelu nadzoru opublikowany jest w drafcie standardu ETSI EN 319 403, Załącznik B (patrz [EN319403]).

[23] http://www.fesa.eu/members.html



Rys. 4.2 Model oceny zgodności dostawców usług zaufania jako część schematu nadzoru. Źródło: EN 319 403.

W ramach wdrażanego w Polsce nowego modelu nadzoru obejmującego wszystkie usługi zaufania, zaprezentowane na powyższym diagramie podmioty mogłyby zostać odwzorowane na następujące instytucje:

1. **European co-operation for Accreditation (EA)** - związek organizacji akredytujących w PCz Europy, które są oficjalnie uznawane przez rządy PCz jako podmioty uprawnione do oceny i weryfikacji (w odniesieniu do standardów międzynarodowych) organizacji, które realizują usługi oceny takie jak certyfikacja, weryfikacja, inspekcja, testowanie i kalibracja - powszechnie znane jako usługi potwierdzania zgodności. EA akredytuje narodowe organy akredytacji w PCz w tym Polskie Centrum Akredytacji. EA utworzono na mocy Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 765/2008 z dnia 9 lipca 2008 r.

2. **National Accreditation Body (NAB)** - Krajowa jednostka akredytująca - w Polsce funkcję tę realizuje Polskie Centrum Akredytacji. Jest to centralny organ administracji nadzorowany przez Ministerstwo Gospodarki i działający w oparciu o ustawę z dnia 30 sierpnia 2002r. o systemie oceny zgodności. Działalność PCA polega na akredytowaniu jednostek certyfikujących lub kontrolujących, laboratoriów lub innych podmiotów przeprowadzających oceny zgodności lub weryfikacji oraz nadzorze w zakresie przestrzegania przez te jednostki warunków akredytacji.

   Proponowane zmiany

   PCA akredytować będzie jednostki oceny zgodności tzw. CAB (Conformity Assessment Bodies) wg kryteriów:

   a) Określonych w ISO/IEC 17065 (Wewnętrzne i Zewnętrzne Usługi):
      - z kompetencjami do oceny zgodności z ISO/IEC 17021;
      - z kompetencjami do oceny zgodności z ISO/IEC 27006;

   b) Określonych w standardach danego sektora, w szczególności, w kontekście eIDAS, w stosunku do usług zaufania i dostawców usług zaufania w odniesieniu do wymagań wyspecyfikowanych w standardzie ETSI EN 319 403 *"Wymagania dla organów oceny zgodności oceniających dostawców usług zaufania"* i na podstawie decyzji krajowej jednostki akredytującej, weryfikującej znajomość wymagań dla danego typu usługi zaufania np. EN 319 411-1 (dla jednostek audytujących TSP wydających certyfikaty).

W okresie przejściowym jako tymczasowy dokument zawierający wymagania akredytacyjne może zostać użyta specyfikacja techniczna ETSI TS 119 403 (V2.1.1 z listopada 2014r.). Specyfikacja zostanie zastąpiona normą EN 319 403 w planowanym terminie jej wydania - marcu 2016r.
Zgodnie z [PCA.AJ-ER-535-35/14] Rozpoczęcie audytów potwierdzających spełnienie wymagań zdefiniowanych w Rozporządzeniu eIDAS planowane jest na 01 lipca 2016r.

3. **Conformity Assessment Body (CAB)** - Jednostka oceny zgodności przeprowadzająca audyty zgodności z wymaganiami. W Polsce, w zakresie usług kwalifikowanych, funkcję tę pełni Ministerstwo Gospodarki, zaś w przypadku usług niekwalifikowanych np. dotyczących zgodności z wymaganiami WebTrust dla certyfikatów SSL funkcję tę realizują firmy doradcze tzw. wielkiej czwórki (E&Y, PwC, Deloitte, KPMG).
   Proponowane zmiany
   Patrz rozdział 4.3.8.

4. **Trust Service Provider (TSP)** - Dostawca usług zaufania np. usługi wydawania kwalifikowanych certyfikatów uwierzytelniania witryn internetowych.

5. **Trust Service Status Notification Body** - Organizacja dokonująca notyfikacji statusu usługi zaufania. W przypadku usług kwalifikowanych, wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym realizuje Ministerstwo Gospodarki.
   Proponowane zmiany dla kwalifikowanych usług zaufania
   Ministerstwo Gospodarki prowadzić będzie rejestry i dokonywać wpisów dla wszystkich zdefiniowanych w eIDAS kwalifikowanych usług zaufania. Ponadto NCCERT (NBP) prowadzić będzie listy TSL oraz wydawać będzie zaświadczenia certyfikacyjne dla QTSP.
   Proponowane zmiany dla niekwalifikowanych usług zaufania:
   Ministerstwo Gospodarki prowadzić będzie rejestry i dokonywać wpisów dla wszystkich zdefiniowanych w eIDAS niekwalifikowanych usług zaufania. Zgłoszenie do rejestru powinno być dobrowolne. Wpisanie do rejestru usług niekwalifikowanych powinno dawać usługodawcy korzyść w postaci obecności na niekwalifikowanych listach TSL w Polsce zarządzanych przez NCCERT (NBP), umożliwiających automatyczne przetwarzanie M2M.

6. **Trusted List (Trusted Service Status List)** - Listy zaufania - obecnie zaufana lista nadzorowanych podmiotów świadczących usługi certyfikacyjne. Po wdrożeniu eIDAS powstanie lista nadzorowanych podmiotów świadczących usługi zaufania.

4.3.3 Przedmiot i formy nadzoru

Przedmiot nadzoru zdefiniowany jest w art. 17 ust. 3 rozporządzenia eIDAS:

"Organ nadzoru odgrywa następującą rolę:

a) sprawuje nadzór nad kwalifikowanymi dostawcami usług zaufania mającymi siedzibę na terytorium wyznaczającego państwa członkowskiego w celu zapewnienia – za pomocą działań nadzorczych ex ante i ex post – aby kwalifikowani dostawcy usług zaufania i świadczone przez nich kwalifikowane usługi zaufania spełniały wymogi określone w niniejszym rozporządzeniu;

b) podejmuje, w razie konieczności, działania w odniesieniu do niekwalifikowanych dostawców usług zaufania mających siedzibę na terytorium wyznaczającego państwa członkowskiego – za pomocą działań nadzorczych ex post – gdy dowiaduje się, że niekwalifikowani dostawcy usług zaufania lub świadczone przez nich usługi zaufania rzekomo nie spełniają wymogów określonych w niniejszym rozporządzeniu."

W związku z tym, w zgodzie z eIDAS nadzór w pełnym zakresie będzie dotyczył tylko usługodawców kwalifikowanych, zaś w odniesieniu do usługodawców niekwalifikowanych nadzór będzie realizowany ad-hoc.

Na podstawie art. 17 ust. 4 zadania organu nadzoru obejmują w szczególności:

"

a) ***współpracę z innymi organami nadzoru*** *i udzielanie im pomocy (...);*
b) ***analizowanie raportów z oceny zgodności*** *(...);*
c) *informowanie innych organów nadzoru i społeczeństwa o naruszeniach bezpieczeństwa lub utracie integralności (...);*
d) *składanie sprawozdań Komisji na temat jego głównych działań (...);*
e) *przeprowadzanie audytów lub zwracanie się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności kwalifikowanych dostawców usług zaufania (...);*
f) *współpracę z organami ochrony danych, w szczególności przez informowanie ich, bez zbędnej zwłoki, o wynikach audytów kwalifikowanych dostawców usług zaufania, w przypadku gdy, jak się wydaje, doszło do naruszenia przepisów dotyczących ochrony danych osobowych;*
g) *przyznawanie dostawcom usług zaufania i świadczonym przez nich usługom statusu kwalifikowanego dostawcy usług zaufania i kwalifikowanych usług, a także odebranie tego statusu (...);*
h) *informowanie organu odpowiedzialnego za krajową zaufaną listę (...) o swoich decyzjach o przyznaniu lub odebraniu statusu kwalifikowanego, chyba że ten organ jest również organem nadzoru;*
i) *weryfikacja istnienia i prawidłowego stosowania przepisów dotyczących planów zakończenia działalności, w przypadkach gdy kwalifikowany dostawca usług zaufania zaprzestaje swojej działalności, w tym tego, w jaki sposób zapewnia się dalszą dostępność informacji (...);*
j) *wymaganie, aby dostawcy usług zaufania eliminowali wszelkie przypadki niespełnienia wymogów określonych w niniejszym rozporządzeniu."*

Formy i środki nadzoru powinny, przynajmniej w okresie wdrożenia eIDAS pozostać niezmienione tzn. odwzorowane na postawie obecnej ustawy o podpisie elektronicznym. Są one dobrze znane przez aktualnych dostawców kwalifikowanych usług zaufania i przez nich akceptowane. Poprzez stosowanie zasad dobrego nadzoru, wymienionych w dalszej części dokumentu, formy te będą w sposób elastyczny dostosowywane do zmieniających się w trakcie wdrożenia eIDAS wymagań interesariuszy (dostawców i odbiorców usług zaufania).

Na postawie *„Rozporządzenia Ministra Gospodarki z dnia 6 sierpnia 2002 r. w sprawie wysokości opłaty za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym": "…za rozpatrzenie wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne pobiera się jednorazową opłatę w wysokości równowartości w złotych 10 000 euro."* W związku z przeniesieniem ciężaru finansowego przygotowania raportu oceny zgodności na QTSP proponuje się ograniczenie wielkości opłaty za dokonanie wpisu do kwoty adekwatnej do czynności związanych z „rozpatrzeniem wniosku".

Warto odnotować, że wstępna autoryzacja była zakazana w dyrektywie unijnej o podpisie elektronicznym, a jest nakazana w art. 17 eIDAS. Jest to istotna zmiana w zakresie usług kwalifikowanych i wyjątek od ogólnej zasady w prawie polskim, że zasadniczo nie jest wymagane przejście wstępnej kontroli (merytorycznej on-site, a nie tylko formalnej kontroli dokumentów) do rozpoczęcia działalności gospodarczej.

4.3.4 Infrastruktura nadzoru

Zgodnie z art. 17 ust. 5 rozporządzenia eIDAS *"Państwa członkowskie mogą wymagać, by organ nadzoru utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z warunkami określonymi w prawie krajowym"*. W aktualnym porządku prawnym zgodnie z art. 23 ust. 3, 4, 5 ustawy o podpisie elektronicznym *"Minister właściwy do spraw gospodarki publikuje, w postaci elektronicznej, listę wydanych zaświadczeń certyfikacyjnych (...) oraz dane służące do weryfikacji wydanych przez siebie zaświadczeń certyfikacyjnych"*. Wytwarzanie i wydawanie zaświadczeń certyfikacyjnych może być powierzone w trybie zamówień publicznych podmiotowi świadczącemu usługi certyfikacyjne, lub - na wniosek prezesa NBP - Narodowemu Bankowi Polskiemu lub podmiotowi zależnemu od NBP.

Utrzymywanie infrastruktury nadzoru w rozumieniu eIDAS na mocy art. 17 ust. 5 może opierać się w Polsce na:

a) utrzymywaniu krajowej listy TSL;
b) generowaniu i unieważnianiu tzw. zaświadczeń certyfikacyjnych (certyfikatów CA) kwalifikowanych dostawców usług zaufania;
c) utrzymywaniu krajowego rejestru QTSP;

Listy TSL

Zgodnie z art. 22, rozporządzenia eIDAS, pkt 1. *"Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za których jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania"*.

pkt. 2. *"Państwa członkowskie sporządzają, prowadzą i publikują – w zabezpieczony sposób – elektronicznie podpisane lub opatrzone pieczęcią elektroniczną zaufane listy, o których mowa w ust. 1, w postaci dostosowanej do automatycznego przetwarzania"*.

pkt. 3. *"Bez zbędnej zwłoki państwa członkowskie przekazują Komisji informacje o podmiocie odpowiedzialnym za sporządzenie, prowadzenie i publikowanie krajowych zaufanych list wraz ze szczegółowymi informacjami dotyczącymi miejsca publikacji tych list, certyfikatów użytych do podpisania lub opatrzenia pieczęcią zaufanych list i wszelkich zmian, jakie są do nich wprowadzane"*.

Ze względu na długoletnią, owocną współpracę dostawców usług zaufania z NBP, proponuje się aby zarządzanie krajowymi listami TSL (kwalifikowaną i niekwalifikowaną) powierzyć NCCERT niezależnie od tego czy "Root Krajowy" zostanie utrzymany czy zlikwidowany. Odpowiedzialność NCCERT ograniczona powinna być wyłącznie do zabezpieczenia infrastruktury teleinformatycznej oraz wydanym dzięki nim listom TSL lub zaświadczeniom certyfikacyjnym (wraz z listą CRL). Odpowiedzialność za zarządzanie listami w ujęciu biznesowym (nie technicznym) spoczywać powinna na ministrze właściwym do spraw gospodarki reprezentowanym przez organ nadzoru.

NBP będzie zatem pełnił, zgodnie z EN 319 403 wyłacznie rolę "Trust Service Status Notification Body". Dostawcy usług zaufania oraz usługi które przejdą pozytywnie audyt jednej z krajowych jednostek oceny zgodności, będą mogły zostać zamieszczone na listę TSL.

Zaświadczenia certyfikacyjne i Root PKI dla usług zaufania

Na chwilę obecną model wydawania zaświadczeń certyfikacyjnych przez Narodowe Centrum Certyfikacji dla kwalifikowanych usług zaufania (zdefiniowanych i niezdefiniowanych w eIDAS):

a) wydawania kwalifikowanych certyfikatów (w tym certyfikatów atrybutów),
b) znakowania czasem,
c) walidacji danych,
d) weryfikowania statusu certyfikatów w trybie on-line,
e) poświadczania odbioru i przedłożenia,
f) poświadczenia depozytowego,
g) poświadczenia rejestrowego i repozytoryjnego

funkcjonuje w ocenie komercyjnych dostawców kwalifikowanych usług zaufania prawidłowo.

Utrzymanie infrastruktury zaświadczeń certyfikacyjnych (certyfikatów CA) w Polsce umożliwia skuteczną egzekucję sankcji nałożonych przez organy nadzoru na dostawców usług zaufania poprzez unieważnienie certyfikatów "Root CA" dla wskazanych QTSP. Z drugiej strony kompromitacja roota krajowego może oznaczać kompromitacje rootów CA, co może wywołać poważne konsekwencje w funkcjonowaniu polskich TSP. Prawdopodobieństwo zaistnienia takiego scenariusza jest jednak bardzo niewielkie, ponieważ infrastruktura, którą zarządza NBP funkcjonuje w modelu *offline*.

Klasyczny scentralizowany model budowania zaufania, oparty na certyfikacie "Krajowego Root'a" stosowany jest od lat także ze względu na prostą i sprawdzoną od lat implementację funkcjonalności walidacji podpisu elektronicznego i certyfikatów w oprogramowaniu, w oparciu o budowę tzw. ścieżki certyfikacji.

W przypadku list TSL zawierających tzw. autocertyfikaty (certyfikaty "self-signed") QTSP, unieważnienie certyfikatu "Root CA" należącego do QTSP następuje nie poprzez wygenerowanie nowej listy CRL, a poprzez zmianę statusu na liście TSL. Oprogramowanie wykorzystujące klasyczne metody walidacji oparte tylko i wyłącznie na listach CRL nie może stwierdzić czy certyfikat "Root CA" typu "self-signed" został unieważniony, o ile QTSP nie zamieści go na własnej liście CRL, co może być bardzo trudne w egzekucji przez organy nadzoru. Chcąc skutecznie wdrożyć listy TSL przez krajowych dostawców oprogramowania organ nadzoru w Polsce powinien użyć narzędzi opisanych w rozdziale "Zasady dobrego nadzoru" (np. promowanie dostawców usług prawidłowo implementujących listy TSL poprzez np. nadawanie krajowego znaku jakości).

W miarę jak twórcy aplikacji w UE (w tym w Polsce) zaczną implementować poprawnie krajowe listy TSL, będzie można zacząć rozważać wariant rezygnacji z infrastruktury nadzoru opartej na "Krajowym Roocie" i pozostawienia wyłącznie list TSL. Do dnia, w którym przeprowadzone w kraju testy interoperacyjności usług walidacji nie wykażą prawidłowej implementacji list TSL, zaleca się pozostawienie bez zmian aktualnego systemu budowania zaufania opartego na "Krajowym Roocie". Komisja Europejska do 18 września 2015r. w drodze aktów wykonawczych doprecyzuje specyfikacje i formaty dotyczące list TSL. Prawidłowa implementacja list TSL w oprogramowaniu nie nastąpi wcześniej niż w pierwszej połowie 2016r. W tym okresie powinna zostać wykonana analiza i podjęta ewentualna decyzja o rezygnacji lub pozostawieniu "Krajowego Roota" jako rozwiązania zastępczego (redundantnego i zwiększającego odporność na awarie) dla list TSL.

Dostawcy usług zaufania działający globalnie zadają pytanie jak zarejestrowany w Polsce dostawca usług zaufania, którego certyfikat "Root CA" został podpisany przez NCCERT mógłby zmienić siedzibę działalności na inne PCz UE oraz jak zarejestrowany w innym kraju UE TSP mógłby przenieść swoją działalność do Polski?. Czy przeniesienie rejestracji TSP poza Polskę oznaczać będzie automatyczne unieważnienie zaświadczenia certyfikacyjnego w Polsce? Co z dostawcami usług zaufania z innych PCz, których "Root CA" jest tzw. certyfikatem "self sign" umieszczonym na liście TSL w innym PCz, a którzy z chęcią przenieśliby swoją działalność do Polski? Tacy QTSP, po przeniesieniu działalności do Polski musieliby wydać nową politykę certyfikacji, a ich certyfikaty "root CA" wydane na mocy tej polityki byłyby "kontrolowane" przez NCCERT. Rozwiązaniem o wiele bardziej "elastycznym", umożliwiającym swobodną migrację TSP pomiędzy PCz jest lista TSL.

W przypadku certyfikatów uwierzytelniania witryn internetowych root krajowy prawdopodobnie nie będzie wykorzystywany. Stosowane przez twórców przeglądarek internetowych kryteria uznawania certyfikatów jako "kwalifikowane" odwzorowane są w wymaganiach opisanych w "SSL Baseline Requirements" wskazanych przez CAB Forum[24]. Opracowane przez WebTrust kryteria audytów dostawców certyfikatów SSL oraz norma EN 319 411 (zastępująca TS 102 042) zawierają "SSL Baseline Requirements" jednak nie ma gwarancji, że kryteria WebTrust, ETSI i CAB Forum będą w przyszłości zbieżne (pomimo deklaracji woli wszystkich stron). Dostawcy usług spełniający wymagania WebTrust i ETSI wprowadzani są do magazynów certyfikatów w przeglądarkach internetowych. We współczesnych przeglądarkach internetowych odwzorowane są dwa poziomy bezpieczeństwa: poziom podstawowy dla certyfikatów DV i OV oraz wysoki poziom bezpieczeństwa dla certyfikatów EV. Nie istnieje jednak porozumienie pomiędzy Komisją Europejską lub ETSI i CAB Forum, na mocy którego producenci przeglądarek zobowiązują się uznawać certyfikaty uwierzytelniania witryn internetowych spełniające wymagania załącznika nr 4 Rozporządzenia eIDAS jako kwalifikowane w rozumieniu eIDAS. Co więcej może okazać się, że spełnienie wymagań określonych w załączniku 4 eIDAS nie zagwarantuje uznawania certyfikatu jako zaufanego w przeglądarkach. O możliwości zaistnienia takiego scenariusza świadczyć mogą wymagania twórców przeglądarek w stosunku do certyfikatów SSL EV

[24] *Źródło: https://cabforum.org/wp-content/uploads/BRv1.2.3.pdf*

wykraczające poza eIDAS np. wymagania dot. *Certificate Transparency*[25] zdefiniowane przez producenta przeglądarki posiadającej ponad 50% udziałów w rynku - Google Chrome. W tym kontekście przewaga konkurencyjna na rynku globalnym budowana jest nie poprzez zgodność z odpowiednimi regulacjami prawnymi i standardami w UE lecz na bazie potencjału technologicznego i ekonomicznego mierzonego udziałami w rynku przeglądarek WWW i możliwością definiowania przez to własnych, specyficznych wymagań.

Proces uznawania certyfikatów SSL jako kwalifikowanych w rozumieniu eIDAS rodzi ryzyko wykluczenia podmiotów z państw trzecich co jest sprzeczne z wymogiem 67 preambuły eIDAS:

"Dodatkowo niniejsze rozporządzenie nie powinno 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. Jednak usługi uwierzytelniania witryny internetowej świadczone przez dostawcę z państwa trzeciego można uznać za kwalifikowane, zgodnie z niniejszym rozporządzeniem, wyłącznie wtedy, gdy zawarta została umowa międzynarodowa między Unią a krajem siedziby tego dostawcy."

W przypadku zawarcia np. porozumienia pomiędzy UE a USA potraktowanie rozszerzonego audytu WebTrust jako wiarygodnego do uznawania certyfikatów uwierzytelniania witryn jako kwalifikowanych, powinno być konsekwentnie stosowane dla wszystkich dostawców certyfikatów stosujących kryteria WebTrust wewnątrz UE. Dla takich dostawców nie istnieje "rootWebTrust". Można by przyjąć "kosmetyczną" regulację, że uzyskanie pozytywnego wyniku z rozszerzonego audytu WebTrust powoduje automatyczne wydanie zaświadczenia certyfikacyjnego przez NCC dla dostawcy kwalifikowanych certyfikatów SSL w Polsce.

Jeśli organ nadzoru w Polsce podejmie decyzję o utrzymaniu krajowego root'a wówczas obowiązkowym celem do zrealizowania przez Narodowe Centrum Certyfikacji jest modernizacja "root'a" tak by wykorzystywał algorytm funkcji skrótu SHA-2.

4.3.5 Zasady dobrego nadzoru

Komisja Europejska określiła w preambule zasady dobrego nadzoru. Zostało to doprecyzowane w kontekście oceny zgodności ad-hoc jednakże zasady te dotyczą także codziennych prac organów nadzoru.

Motyw 43 preambuły eIDAS stanowi, że *"W każdym przypadku, gdy organ nadzoru nakłada na kwalifikowanego dostawcę usług zaufania wymóg przekazywania raportów z oceny zgodności ad hoc, organ nadzoru powinien przestrzegać w szczególności zasad*

- ***dobrego zarządzania**, w tym*
- ***obowiązku uzasadniania swoich decyzji**, a także*
- ***zasady proporcjonalności**.*

Organ nadzoru powinien zatem należycie uzasadnić swą decyzję ustanawiającą wymóg przeprowadzenia oceny zgodności ad hoc."

Odnosząc się do zasady dobrego zarządzania i proporcjonalności, organy nadzoru powinny przestrzegać zasady unikania podwójnego finansowania wykonywanych przez siebie prac. W związku z tym jeśli dostawca usług zaufania udostępniać będzie wiele usług zaufania, wówczas należy unikać realizowania czynności, które zostały już wykonane w ramach audytów innych dostarczanych usług zaufania. Przykładowo usługi kwalifikowanego znacznika czasu i rejestrowanych doręczeń elektronicznych mogą wykorzystywać te same elementy infrastruktury teleinformatycznej dostawcy usług. Wielokrotne analizowanie tychże elementów przez audytorów kolejnych usług narusza zasady dobrego nadzoru.

[25] *Źródła: http://www.certificate-transparency.org, http://tools.ietf.org/html/rfc6962*

Organy nadzoru powinny także brać pod uwagę, iż w wyniku wdrożenia rozporządzenia eIDAS pojawi się "rynek nadzoru". Brak przestrzegania zasad dobrego nadzoru rodzi ryzyko odpływu poza granice Polski lub braku przypływu przedsiębiorców świadczących usługi zaufania do Polski. **Bardzo istotnym wydaje się być w tym kontekście obserwowanie rynku nadzoru szczególnie w pierwszych miesiącach funkcjonowania rozporządzenia eIDAS i dostosowanie reguł nadzoru w Polsce do dobrych praktyk tworzących się w Unii Europejskiej.**

Aby poprawić "ofertę" usług nadzoru w Polsce należy zastanowić się nad wprowadzeniem licznych wartości dodanych do tej usługi nieprzewidzianych w rozporządzeniu eIDAS. Zgodnie z regułą marketingową "4P" należy wspierać:

a) Rozwój produktu nadzoru i oceny zgodności (w aspekcie poprawy jakości i użyteczności);
b) Rozwój modeli cenowych (dostosowanie modelu do zmian rynku europejskiego);
c) Relacje z rynkiem usług zaufania (podmiotami nadzorowanymi i klientami usług zaufania);
d) Działania promocyjno-edukacyjne.

Przykładowe cele:

a) Ciągłe analizowanie rynku podmiotów wykonujących ocenę zgodności w celu ochrony interesów TSP i klientów usług zaufania;
b) Nieustanne znoszenie barier i optymalizacja procedur, procesów i środków technicznych nadzoru tak, aby były możliwie najbardziej przyjazne dla biznesu krajowego i międzynarodowego;
c) Wspieranie organizacji biznesowych realizujących usługi zaufania poprzez dążenie do minimalizacji kosztów jakie ponoszą te organizacje w związku z nadzorem, poprzez tworzenie modeli cenowych (opłat za usługi) dostosowanych do wielkości (skali) prowadzonej działalności;
d) Konsultowanie zmian w procesach nadzoru z interesariuszami i unikanie zmian nieprzewidywalnych przez uczestników rynku usług zaufania, które mogłyby podważyć zasadę pewności inwestowania;
e) Wspieranie edukacji dotyczącej realizacji (świadczenia) usług zaufania i środków identyfikacji elektronicznej;
f) Prowadzenie działalności promocyjnej organów nadzoru mających popularyzować polski system nadzoru usług zaufania w krajach UE (na wzór działań podejmowanych przez TUV-IT w Niemczech, skierowanych na kraje Europy środkowo-wschodniej) oraz polskich dostawców usług zaufania i dostawców usług wykorzystujących usługi zaufania (i np. dobrze implementujących listy TSL), którzy świadczą je z wysoką starannością - w celu pokazania, że system nadzoru pozytywnie oddziałuje na krajowy rynek.

W kontekście realizacji zasady dobrego zarządzania nieodzownym wydaje się utworzenie transparentnego dla opinii publicznej modelu biznesowego realizacji nadzoru w Polsce np. na bazie *Business Model Canvas*.

4.3.6 Współpraca organów nadzoru z innymi nadzorami

Współpraca organu nadzoru z podmiotami zagranicznymi dotyczyć będzie:

a) współpracy z Komisją Europejską (art. 17 ust. 6) w zakresie przekazywania do dnia 31 marca każdego roku sprawozdania z głównych działań organu nadzoru wraz z zestawieniem notyfikacji dotyczących naruszeń otrzymanych od dostawców usług zaufania;
b) współpracy z ENISA w zakresie przekazywania raz w roku zestawienia zawiadomień o naruszeniach bezpieczeństwa lub utraty integralności od dostawców usług zaufania (art. 19 ust. 3). W przypadku jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej ilości państw członkowskich krajowy organ nadzoru może zweryfikować w ENISA czy została poinformowana o incydencie bezpieczeństwa;
c) ewentualnej współpracy z innymi organami nadzoru w PCz UE w sytuacji udzielania bądź otrzymywania wzajemnej pomocy regulowanej art. 18 ust. 1 rozporządzenia eIDAS;
d) prowadzenia wspólnych dochodzeń wg. ustaleń uzgodnionych i określonych zgodnie z prawem krajowym PCz (art. 18 ust. 3);

Współpraca organu nadzoru z podmiotami krajowymi realizującymi funkcje nadzoru dotyczyć będzie współpracy z:

a) właściwymi organami ds. bezpieczeństwa teleinformatycznego (ABW, UKE, etc.), na mocy art. 19;
b) organem ochrony danych (GIODO) na mocy art. 19 i art. 20 ust. 2;
c) UOKIK, np. w sprawach dotyczących ochrony konsumentów w związku z naruszeniem ich praw przez dostawców usług zaufania.

Zasady współpracy z innymi krajowymi organami nadzoru powinny być uzgodnione przez MG z tymi organami w drodze wspólnych ustaleń. Istnieje potrzeba doprecyzowania zakresu informacji (raportów) wymienianych pomiędzy organami nadzoru w Polsce oraz na potrzeby komunikacji organów nadzoru w ramach UE (postulat zgłoszony przez członków FESA[26]).

Warto też nadmienić, że. eIDAS jest wyłączony z systemu założonego przez NIS (Network and Information Security), co przemawia za wyłączeniem systemu zgłaszania naruszeń z rozporządzenia eIDAS z działań instytucji takich jak CERT. Jednocześnie w perspektywie eIDAS organem nadzoru nie są organy ścigania (np. Policja, Prokuratura) co wyklucza te podmioty z zakresu współpracy w ramach nadzoru (podmioty biorące udział w obrocie usługami identyfikacji i zaufania mogą nadal korzystać ze standardowych metod współpracy z organami ścigania).

Organów wymiaru sprawiedliwości nie należy utożsamiać z organami nadzoru w rozumieniu eIDAS. Niemniej jednak należy pamiętać, że obowiązek współpracy z organami wymiaru sprawiedliwości przez organy administracji publicznej może wynikać z odrębnych krajowych przepisów np. obowiązek zawiadamiania o podejrzeniu popełnienia przestępstwa.

4.3.7 Wzmocnienie organów nadzoru w Polsce

Zgodnie z art. 17 ust. 1 rozporządzenia eIDAS *"Organom nadzoru przyznaje się uprawnienia i odpowiednie zasoby niezbędne do wykonywania ich zadań"*. Na chwile obecną zasoby te wydają się odpowiednie do realizacji tylko podstawowych funkcji nadzoru i to przy założeniu, że ocena zgodności realizowana będzie przez podmioty komercyjne, nie zaś instytucje państwowe.

Zapewnienie przez PCz odpowiednich zasobów jest obowiązkiem nałożonym unijnym prawem. Krajowa administracja ma swobodę w określeniu ilościowym i jakościowym pod warunkiem spełnienia obowiązków wynikających z art. 17 ust. 1. Podkreślić należy, że w większości państw członkowskich nadzory przypisane do usługi e-podpisu były dotychczas mało liczne i dysponowały ograniczonymi budżetami. Rozporządzenie Parlamentu i Rady naświetla ten problem w najbardziej jaskrawy sposób poprzez podniesienie obowiązku państw członkowskich w tym zakresie do rangi przepisu, którego naruszenie może być przedmiotem **nałożenia kary**.

W miarę rozwoju rynku usług zaufania (mierzonego ilością podmiotów rejestrowanych na listach TSL) istotne będzie także "skalowanie" zasobów organów nadzoru. W kontekście nieznanej obecnie dynamiki wzrostu ilości TSP należy opracować procesy i procedury zarządzania zasobami w odpowiedzi na zmiany rynku. Przy najprostszym skalowaniu liniowym, podwojenie ilości TSP w stosunku do ilości podmiotów nadzorowanych obecnie przez MG powinno skutkować podwojeniem zasobów organów nadzoru.

Zwiększenie zasobów organu nadzoru powinno być uzasadnione, szczególnie w początkowym okresie wdrożenia eIDAS w Polsce, nie tylko realizacją zadań nadzorczych, lecz przede wszystkim wdrażaniem zasad dobrego nadzoru. Do tych celów wystarczy zaplanowanie w miarę stabilnych w czasie zasobów ludzkich odpowiedzialnych za zarządzanie operacyjne usługą nadzoru w aspekcie biznesowym.

[26] FESA - ang. Forum of European Supervisory Authorities for Electronic Signatures.

Bardzo istotny jest aspekt zarządzania zasobami ludzkimi odpowiedzialnymi za nadzór. Jednym z kluczowych aspektów tego obszaru jest zarządzanie kompetencjami pracowników nadzoru i prowadzenie nieustannych szkoleń podnoszących poziom wiedzy np. z zakresu:

- Znajomości standardów w zakresie podlegającym nadzorowi (mandat m460). Szkolenie powinny być przeprowadzane regularnie ze względu na dynamiczny rozwój tej dziedziny. Wzrost liczby usług podlegających nadzorowi o np. e-doręczenia, e-konserwację, e-uwierzytelnianie wymusza konieczność szkolenia w każdym z nowych obszarów podlegających kontroli urzędów państwowych. Po nabyciu kompetencji (min. przez zespoły DGE, DHU, BKA w Ministerstwie Gospodarki) należy wdrożyć systemowy program utrzymania kompetencji np. dzięki regularnym, corocznym szkoleniom lub warsztatom;
- Tworzenia i zarządzania zespołami obsługi incydentów (np. na wzór szkoleń NASK dotyczącego tworzenia i utrzymania zespołów CERT – po dostosowaniu do specyfiki nadzoru i obsługi incydentów usług zaufania);
- Współpracy z ENISA w zakresie wykorzystania europejskiego systemu obsługi incydentów bezpieczeństwa;
- Współpracy z krajowymi CAB w zakresie analizy dostarczanych przez nich wyników audytów;
- Znajomości języków obcych w celu skutecznej reprezentacji na arenie międzynarodowej np. w zakresie współpracy międzynarodowej, udziale w zagranicznych zespołach kontrolnych. Szkolenia powinny być ukierunkowane na znajomość dziedzinową języka w zakresie zdefiniowanym w eIDAS, aktach wykonawczych i normach technicznych;

W odpowiedzi na zapytania kierowane przez organy administracji centralnej (np. ZUS) istnieje także potrzeba przeprowadzenia regularnych szkoleń dla szerokiego grona beneficjentów.

Ważne jest także utrzymanie wysokiej aktywności przedstawicieli Polski w warsztatach międzynarodowych, na których wymieniane są dobre praktyki dot. nadzoru np. *CA Conformity Assessment Workshops* w Berlinie. Wykwalifikowane zasoby ludzkie będzie można utrzymać w ramach organu nadzoru tylko wówczas, gdy wynagrodzenie za ich pracę będzie porównywalne z wynagrodzeniem w państwach UE. W przeciwnym wypadku istnieje wysokie ryzyko migracji wykwalifikowanej kadry sektora publicznego do instytucji zajmujących się oceną zgodności w sektorze biznesowym lub do organów nadzoru w innych instytucjach UE.

4.3.8 Ocena zgodności dostawców usług zaufania z wymaganiami eIDAS/EN

Ze względu na wysokie prawdopodobieństwo zwiększania się ilości podmiotów świadczących kwalifikowane usługi zaufania (TSP), jednak nie znaną jeszcze dynamikę tego wzrostu proponuje się przyjąć następujący kompleksowy schemat oceny zgodności zgodny z art. 21 ust. 1 i 2 rozporządzenia eIDAS:

Część I - Obejmuje kwalifikowanych i niekwalifikowanych (dobrowolnie) dostawców usług zaufania

Zgodność technologiczną i organizacyjną rozumianą jako zgodność z normami EN 319 XXX, przeprowadzaną w ramach oceny opisanej w EN 319 403 oraz zgodność z wymaganiami eIDAS weryfikować będą podmioty komercyjnie świadczące usługi audytów zgodności (np. Ernst & Young Polska, TUV Niemcy etc.). W etapie 1 usługa i usługodawca oceniani są na podstawie dostarczonej audytorom dokumentacji. Następie w etapie 2 odbywa się audyt w miejscu realizacji usługi. W etapie 3 sporządzany jest raport z audytu.

Podejście takie jest uzasadnione sprawdzonym przez wiele lat modelem audytów takich (nowych w kontekście eIDAS) usług zaufania jak np. certyfikaty uwierzytelniania witryn internetowych (audyty WebTrust), w których specjalizują się od lat wykwalifikowane przedsiębiorstwa posiadające zasoby do realizacji audytów (np. E&Y). Zgodnie z EN 319 403, rozdział 6.1 jednostka certyfikująca musi posiadać bardzo wysokie kompetencje, których utrzymywanie w trybie ciągłym jest kosztowne. W związku z tym, w początkowym okresie po wdrożeniu rozporządzenia eIDAS, prawdopodobnie nie będzie znane wystarczające uzasadnienie biznesowe do budowania kompetencji w ramach urzędów administracji publicznej.

Problemem w realizacji oceny zgodności w okresie wdrożenia eIDAS może być trwający nadal proces definiowania standardów dotyczących zasad audytów, zgodnie z którymi jednostki oceniające zgodność będą przeprowadzać oceny kwalifikowanych dostawców usług zaufania.

Wprawdzie opublikowano już ETSI TS 119 403 V2.1.1 (2014-11), ale nie ma jeszcze kompletu standardów dla poszczególnych usług zaufania, które są konieczne w procesie oceny kompetencji wymaganych do świadczenia usług. Ze względu na fakt, iż przy akredytacji NIK wymaga, aby PCA opierało się o dokumenty opracowane w języku polskim, istnieje ważna potrzeba tłumaczenia przez PKN standardów z mandatu m460 na język polski.

Na dzień dzisiejszy jednostkami, które mogłyby w Polsce przeprowadzać ocenę zgodności są firmy konsultingowe wykonujące audyty WebTrust (E&Y) oraz audyty zgodności z normami ISO 9001:2008 i 27001. Do wykonywania oceny zgodności powinna być dopuszczona każda jednostka spełniająca wymagania zdefiniowane w standardzie EN 319 403. Potencjałem do wykonania ocen zgodności dysponują zarówno jednostki publiczne jak i prywatne np. Instytut Maszyn Matematycznych, PwC, Trusted Information Consulting, Galach Consulting.

Wybór jednostki przeprowadzającej audyt zgodnościowy powinien należeć do dostawców usług zaufania.

Część II - Obejmuje tylko kwalifikowanych dostawców usług zaufania

Zgodnie z preambułą eIDAS (motyw 43) *"Aby zapewnić przestrzeganie przez kwalifikowanych dostawców usług zaufania wymogów określonych w niniejszym rozporządzeniu i zgodność świadczonych przez nich usług z tymi wymogami, jednostka oceniająca zgodność powinna przeprowadzać ocenę zgodności, a będące jej wynikiem raporty z oceny zgodności powinny być przekazywane przez kwalifikowanych dostawców usług zaufania organowi nadzoru."*. Postulat ten odwzorowany jest np. w art. 20 rozporządzenia eIDAS na mocy którego kwalifikowani dostawcy usług zaufania przedkładają raporty z oceny zgodności organowi nadzoru. Na mocy art. 21 ust.2 rozporządzenia eIDAS organ nadzoru weryfikuje (ponadto) czy dostawca usługi zaufania i świadczone przez niego usługi zaufania spełniają wymogi określone w rozporządzeniu.

Zatwierdzenie oceny zgodności, w szczególności z wymaganiami prawnymi eIDAS wykona organ nadzoru czyli właściwe ministerstwo. Do jej przeprowadzenia wymagane będzie przedstawienie raportu z oceny zgodności technologicznej i organizacyjnej. W przypadku, gdy audytowany TSP nie uzyskał raportu z oceny zgodności wg. EN 319 403 i wymagań prawnych eIDAS lub wyniki raportu pozostawiają wątpliwości ministerstwo może zgodnie z art. 17 ust. 4 lit. e) przeprowadzić całkowity audyt we własnym zakresie. Proponuje się wyznaczyć termin, w którym jeśli zatwierdzenie zgodności nie zostanie ogłoszone przez organ nadzoru *explicite*, wówczas przez domniemanie zostanie przyjęty raport z oceny zgodności.

Rys. 4.3 Kompleksowy schemat oceny zgodności kwalifikowanych dostawców usług zaufania.

4.3.9 Częstotliwość przeprowadzania audytów

Zgodnie z rozporządzeniem eIDAS (art. 20 ust. 1) kwalifikowani dostawcy usług zaufania podlegają audytowi na ich własny koszt co najmniej raz na 24 miesiące lub, na żądanie organu nadzoru, w dowolnym momencie. Regulator europejski prawdopodobnie wycenił ryzyko działalności TSP i zestawił je z kosztami audytu, które ponoszą

przedsiębiorcy i ocenił że audyt realizowany co 2 lata jest wystarczający. Zgodnie z zaleceniami standardu EN 319 403 kompleksowe audyty recertyfikujące powinny odbywać się nie rzadziej niż co trzy lata, zaś audyty kontrolne nie rzadziej niż raz w roku. Biorąc pod uwagę powyższe sugestie, z punktu widzenia podmiotów realizujących usługi zaufania., najbardziej korzystnym scenariuszem realizacji audytów będzie schemat zaproponowany w eIDAS.

4.3.10 Kryteria oceny zgodności

W ramach tego schematu może być przeprowadzana ocena zgodności w odniesieniu do ustandaryzowanych wymagań zdefiniowanych dla usług zaufania w:

a) normach ETSI, np.:
   - EN 319 401 (ogólne wymagania dla TSP),
   - EN 319 411-1 (wymagania dla TSP wydających certyfikaty),
   - EN 319 411-2 (wymagania dla TSP wydających certyfikaty kwalifikowane),
   - EN 319 412 (wymagania zgodności z profilem certyfikatów X.509 i RFC 3161),
   - EN 319 421 (wymagania dot. wydawania kwalifikowanych znaczników czasu);
   - EN 419 221 (profile zabezpieczeń dla modułów kryptograficznych);
   - EN 419 261 (wymagania bezpieczeństwa dla zaufanych systemów);
b) artykułach eIDAS:
   - głównych wymaganiach dla TSP (Art. 15, Art. 19, Art. 20, Art. 24);
   - wymaganiach dla TSP wydających certyfikaty kwalifikowane (Art. 28, Załącznik 1);
   - wymaganiach dla kwalifikowanych urządzeń do składania podpisu elektronicznego (Art. 29);
   - wymaganiach dotyczących pieczęci elektronicznych (Art. 38, Załącznik 3);
   - wymaganiach dla usług walidacji (Art. 32, 33, 40);
   - wymaganiach dla usług konserwacji kwalifikowanych podpisów elektronicznych (Art. 34);
   - wymaganiach dla usług rejestrowanego doręczenia elektronicznego (Art. 44);
   - wymaganiach dla usług wydawania certyfikatów uwierzytelniania witryn internetowych (Art. 45, Załącznik 4);

Główne obszary wymagań rozporządzenia eIDAS dla kwalifikowanych dostawców usług zaufania (Art. 24 eIDAS) związane są z:

a) wymaganiami organizacyjnymi:
   - dot. identyfikacji osoby fizycznej lub prawnej, której wydawany jest certyfikat;
   - dot. zaprzestania działalności;
   - dot. kompetencji pracowników i podwykonawców;
   - dot. utrzymywania zasobów finansowych lub stosownych ubezpieczeń od odpowiedzialności;
b) wymaganiami technicznymi:
   - dot. używania wiarygodnych systemów i produktów, które są chronione przed modyfikacją i zapewniają techniczne bezpieczeństwo i wiarygodność procesów;
   - dot. używania wiarygodnych systemów do przechowywania przekazanych TSP danych;
   - dot. podejmowania odpowiednich środków zapobiegających fałszowaniu i kradzieży danych;
c) wymaganiami funkcjonalnymi:
   - dot. rejestracji (logowania) i udostępniania wszelkich odpowiednich informacji dotyczących danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, w szczególności do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług;
   - dot. przetwarzania danych osobowych zgodnie z dyrektywą 95/46/WE;
   - dot. zarządzania bazą danych certyfikatów;
   - dot. unieważniania certyfikatów i informowania o ich statusie;

4.3.11 System kar

System kar zdefiniowany w obecnej ustawie o podpisie elektronicznym, w szczególności rozdział VII, art. 31 - 33 i rozdział VIII, skonstruowane są w odczuciu usługodawców w sposób prawidłowy. System ten powinien być zaktualizowany na podstawie incydentów, które miały miejsce w ostatnich latach oraz na podstawie opinii obecnych usługodawców, którzy dostrzegają praktyki związane z nieuczciwą konkurencją ze strony podmiotów (biznesowych i publicznych) wchodzących na rynek. Proponuje się wprowadzenie uzupełnienia systemu kar o następujące elementy:

L.p.	Działanie podlegające karze	Sankcje
1.	Porzucenie działalności przez TSP,	Środki karne: Zakaz świadczenia usług zaufania przez okres 5 lat. Grzywny: Dla podmiotów świadczących usługi odpłatnie dla klienta końcowego - równowartość przychodów ze sprzedaży usług zaufania w okresie ostatnich 3 lat. Dla podmiotów świadczących usługi nieodpłatnie dla klienta końcowego - równowartość poniesionych kosztów związanych z prowadzeniem usługi w okresie ostatnich 3 lat.
2.	Brak zapewnienia ciągłości działania TS przez TSP. Incydent zgłoszony, co najmniej 3 razy w roku.	Grzywny: Dla podmiotów świadczących usługi odpłatnie dla klienta końcowego - równowartość 30% przychodów ze sprzedaży usługi zaufania w okresie, w którym nastąpiła rejestracja incydentów. Dla podmiotów świadczących usługi nieodpłatnie dla klienta końcowego - równowartość 30% kosztów związanych z prowadzeniem usługi zaufania w okresie, w którym nastąpiła rejestracja incydentów.
3.	Nieprawidłowe zakwalifikowanie usługi - jako zamkniętej, podczas gdy jest ona świadczona, jako otwarta w rozumieniu postulatu 21 Preambuły eIDAS (patrz rozdział: „Otwarte i zamknięte usługi zaufania").	Środki karne: Zakaz świadczenia usług zaufania przez okres 5 lat. Grzywny: Dla podmiotów świadczących usługi odpłatnie dla klienta końcowego - równowartość przychodów ze sprzedaży usług zaufania w okresie ostatnich 3 lat. Dla podmiotów świadczących usługi nieodpłatnie dla klienta końcowego - równowartość poniesionych kosztów związanych z prowadzeniem usługi w okresie ostatnich 3 lat.
4.	Brak usunięcia potwierdzonej niezgodności z obowiązującymi standardami ujętymi bezpośrednio lub pośrednio w Aktach delegowanych lub wykonawczych w okresie 6 m-cy od decyzji organu nadzoru.	Grzywny: Dla podmiotów świadczących usługi odpłatnie dla klienta końcowego - równowartość 30% przychodów ze sprzedaży usługi zaufania w okresie, w którym nastąpiła rejestracja incydentów. Dla podmiotów świadczących usługi nieodpłatnie dla klienta końcowego - równowartość 30% kosztów związanych z prowadzeniem usługi zaufania w okresie, w którym nastąpiła rejestracja incydentów.

4.3.12 Ocena zgodności przez jednostki akredytowane w innych państwach

Rozporządzenie eIDAS otwiera nie tylko rynek usług zaufania, ale także oceny zgodności realizacji usług z wymaganiami prawnymi, organizacyjnymi i technicznymi. Dzięki temu TSP będą mogli skorzystać z usług oceny zgodności świadczonych przez jednostki akredytowane w innych państwach (np. audyt zgodności z wymaganiami ETSI realizowany przez TUV-IT w Niemczech). Realizacja oceny zgodności przez jednostki zagraniczne pozwoli na wprowadzenie większej konkurencji na rynku audytów i z pewnością zostanie przyjęta z aprobatą przez TSP działających obecnie na rynku globalnym.

Z punktu widzenia organów nadzoru istotnym wydaje się być zapewnienie właściwej komunikacji z jednostkami akredytowanymi w innych państwach i nałożenie na nie wymogu raportowania w języku polskim oraz wskazania osób kontaktowych posługujących się językiem polskim.

W związku z tym, że istnieją już zagraniczne podmioty oferujące usługę oceny zgodności, brak funkcjonowania krajowego systemu zgodności w obszarze usług zaufania, w początkowym okresie po wdrożeniu eIDAS, nie będzie powodować negatywnych skutków dla dostawców usług zaufania. W dłuższym horyzoncie czasu organy nadzoru w Polsce powinny monitorować ceny usług audytów na rynku europejskim i ewentualne problemy zgłaszane przez TSP. Jeśli europejski rynek oceny zgodności będzie miał tendencję do centralizacji w ramach wybranych państw UE i tym samym ograniczona zostanie jego konkurencyjność oraz zwiększone ryzyko uzależnienia się od dostawców usług audytów (tzw. *vendor lock-in*), wówczas należy podjąć niezwłocznie działania mające na celu wykreowanie krajowego rynku oceny zgodności, włącznie z wprowadzeniem regulacji prawnych preferujących krajowych usługodawców (nie tylko pod kątem posługiwania się językiem polskim) z zachowaniem reguł traktatowych dotyczących m.in. swobody przepływu usług.

4.3.13 Model nadzoru i oceny zgodności z eIDAS dla środków identyfikacji elektronicznej

W przypadku środków identyfikacji elektronicznej będących pod nadzorem MAiC istotne jest doprecyzowanie wymagań (i całego systemu nadzoru) dla strony:

a) wydającej środki identyfikacji elektronicznej;
b) przeprowadzającej procedurę uwierzytelniania;

zgodnie z art. 9 ust. 1 lit. b) rozporządzenia eIDAS. Wymagania będą dotyczyć niskiego, średniego i wysokiego poziomu bezpieczeństwa (zgodnie z art. 8 ust. 2 rozporządzania eIDAS).

Wymagania dla dostawców środków identyfikacji elektronicznej będą mogły zostać opracowane po ogłoszeniu odpowiednich standardów międzynarodowych i określeniu przez Komisję Europejską w drodze aktów wykonawczych minimalnych technicznych specyfikacji, standardów i procedur, w odniesieniu do których określone zostaną niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej (zgodnie z art. 8 ust. 3 rozporządzenia eIDAS). Nastąpi to do dnia 18 września 2015r.

Obszary nadzoru określone są w art. 8 ust. 3 rozporządzenia eIDAS:

"Te minimalne techniczne specyfikacje, standardy i procedury są określane przez odniesienie do wiarygodności i jakości następujących elementów:

a) procedury wykazującej i weryfikującej tożsamość osób fizycznych lub prawnych wnioskujących o wydanie środka identyfikacji elektronicznej;
b) procedury wydawania wnioskowanego środka identyfikacji elektronicznej;
c) mechanizmu uwierzytelniania, w którym osoba fizyczna lub prawna używa środka identyfikacji elektronicznej do potwierdzenia swojej tożsamości wobec strony ufającej;
d) jednostki wydającej środek identyfikacji elektronicznej;

e) każdego innego organu zaangażowanego w ramach wniosku o wydanie środka identyfikacji elektronicznej;

f) specyfikacji technicznych i specyfikacji bezpieczeństwa wydanego środka identyfikacji elektronicznej."

W modelu nadzoru dla środków identyfikacji elektronicznej klarownym wydaje się być odpowiedzialność za dokonywanie wpisów do rejestru notyfikowanych środków identyfikacji elektronicznej w Komisji Europejskiej przez MAiC. Zgodnie z art. 7 rozporządzenia eIDAS MAiC będzie mogło nie tylko wydawać środki identyfikacji elektronicznej, upoważniać do wydawania środków identyfikacji elektronicznej ale, co istotne dla podmiotów komercyjnych, uznawać środki identyfikacji przez nie wytworzone. Dlatego też istotne będzie opracowanie wymagań, na podstawie których środki identyfikacji elektronicznej będą uznawane.

Ponadto MAiC będzie odpowiedzialne za informowanie PCz co najmniej 6 miesięcy przed notyfikacją poprzez przekazanie opisu systemu zgodnie z art. 7 lit. g) rozporządzenia eIDAS.

4.3.14 Certyfikacja kwalifikowanych urządzeń do składania podpisu elektronicznego

Zgodnie z art. 29 rozporządzenia eIDAS kwalifikowane urządzenia do składania podpisu elektronicznego muszą spełniać wymagania załącznika nr II do rozporządzenia. Zgodnie z definicją z art. 3 pkt 22 "urządzenie do składania podpisu elektronicznego" oznacza **skonfigurowane oprogramowanie lub skonfigurowany sprzęt**, które wykorzystuje się do składania podpisu elektronicznego, natomiast "kwalifikowane urządzenie do składania podpisu elektronicznego" oznacza "urządzenie do składania podpisu elektronicznego", które spełnia wymogi określone w załączniku II do rozporządzenia. W związku z powyższym staje się jasne, iż certyfikacja dotyczyć powinna zarówno oprogramowania jak i sprzętu. W rozumieniu zespołów pracujących przy opracowaniu eIDAS, oprogramowanie jest rozumiane jako oprogramowanie wbudowane w bezpieczne urządzenie np. aplety zainstalowane na kartach kryptograficznych, systemy operacyjne kart lub modułów HSM. Nie podlega certyfikacji oprogramowanie zewnętrzne w stosunku do urządzenia czyli np. system operacyjny, na którym zainstalowana jest aplikacja do podpisu, oprogramowanie wbudowane w stację roboczą (np. BIOS), czy wreszcie aplikacja składania podpisu elektronicznego.

Certyfikacja kwalifikowanych urządzeń do składania podpisu elektronicznego może odbywać się w oparciu o dwie równoważne procedury (Art. 30 ust. 3 eIDAS):

a) "*procedurze oceny bezpieczeństwa, przeprowadzonej zgodnie z jedną z norm dotyczących oceny bezpieczeństwa produktów informatycznych (...)."* Normy te nie zostały jeszcze określone przez Komisję Europejską w związku z czym jedyną procedurą obowiązującą w okresie przejściowym jest procedura opisana w punkcie b).

b) "procedurze innej niż procedura, o której mowa w lit. a), pod warunkiem że w procedurze tej stosuje się porównywalne poziomy bezpieczeństwa i podmiot publiczny lub prywatny, o którym mowa w ust. 1, zgłosi tę procedurę Komisji. Procedura ta może zostać zastosowana wyłącznie w razie braku norm, o których mowa w lit. a), lub gdy procedura oceny bezpieczeństwa, o której mowa w lit. a), wciąż trwa."

Na mocy art. 30 zgodność kwalifikowanych urządzeń do składania podpisu elektronicznego jest certyfikowana przez odpowiednie publiczne lub prywatne podmioty wyznaczone przez PCz. W Polsce takimi podmiotami mogłyby być np. Instytut Maszyn Matematycznych, NCK, SKW, ABW lub inne podmioty wyznaczone przez Ministerstwo Gospodarki (np. w zakresie badań tempestowych SILTEC i WAT). Na wstępie należy dokonać analizy ilości urządzeń do składania podpisu elektronicznego, dla których w obowiązującym obecnie porządku prawnym wydana została "deklaracja zgodności". Dopiero wyniki tej analizy wskażą czy zasadnym jest budowanie nowego organu certyfikującego, czy też rozszerzenie zakresu działalności obecnie funkcjonujących jednostek certyfikujących.

Możliwe jest także podjęcie decyzji, w późniejszym terminie, na postawie analizy listy certyfikowanych w UE urządzeń do składania podpisu elektronicznego, jednakże taki scenariusz oznaczać będzie konieczność kompletnej certyfikacji wykorzystywanych w Polsce urządzeń do składania podpisu elektronicznego w pierwszym okresie funkcjonowania

eIDAS poza granicami kraju. Większość z nich jest certyfikowana obecnie poza granicą (np. za zgodność z normą FIPS 140-2), jednakże konieczne będzie także dokonanie dodatkowej oceny np. dedykowanych apletów uruchamianych na kartach kryptograficznych, które są wytwarzane przez lokalnych dostawców.

Niezwykle istotnym dla dostawców usług zaufania jest aspekt biznesowy realizacji usługi certyfikacji. W tym kontekście usługi zagranicznych podmiotów certyfikujących mogą okazać się na tyle kosztowne, że polskie podmioty świadczące usługi zaufania utracą źródła przewagi konkurencyjnej. W związku z tym należy rozważać realnie wariant budowy polskiej jednostki certyfikacyjnej, która będzie świadczyła usługi po minimalnej możliwej do zaakceptowania przez biznes cenie i z krótkim czasem dostarczenia usługi, co pozwoli lokalnym TSP konkurować z zagranicznymi TSP.

4.3.15 System zarządzania usługodawcami niekwalifikowanymi – monitoring i rejestracja incydentów

W przypadku usługodawców niekwalifikowanych, z uwagi na ograniczenia czasowe wdrażania eIDAS w Polsce, zarządzanie niekwalifikowanymi usługodawcami proponuje się ograniczyć wyłącznie do:

a) Zarządzania listą zaufanych usługodawców niekwalifikowanych (TSL niekwalifikowanych TSP). Rejestracja na liście powinna być dobrowolna. W zamian za rejestrację usługodawca otrzymuje identyfikację na rynku i możliwość uczestniczenia w procesach automatycznej walidacji dzięki obecności na liście TSL.
b) Udostępnienia w ramach infrastruktury organów nadzoru środki techniczne do zgłaszania niezgodności z eIDAS przez odbiorców usług zaufania np. **system zarządzania ryzykiem dla krajowych usług zaufania**, w ramach, którego może np. funkcjonować portal do zgłaszania niezgodności. System powinien wyłącznie reagować na zdarzenia rejestrowane przez "rynek". Może obejmować także kwalifikowanych dostawców usług zaufania (ze zwiększonym zakresem monitorowanych i analizowanych zagrożeń).

4.4 Publiczne usługi zaufania w Polsce

4.4.1 Nieodpłatne publiczne centrum walidacji - nieodpłatne publiczne usługi zaufania

Utworzenie nieodpłatnego centrum walidacji wydaje się być nadmierną ingerencją administracji publicznej w rynek usług zaufania. Usługi takie dostępne są na rynku nieodpłatnie np. usługa WebNotarius PCC Certum do użytku niekomercyjnego lub w modelu "Premium" do zastosowań komercyjnych. Zbudowanie usługi walidacji w ramach administracji publicznej powinno zostać poprzedzone analizą biznesową uzasadniającą nie tylko koszty rozwoju krajowego centrum walidacji, ale także jego utrzymania. Należy także przeanalizować czy wdrożenie usługi walidacji w ramach administracji publicznej nie spowoduje obniżenia popytu na usługi komercyjne i przez to eliminację polskich TSP z rynku usług walidacji.

Wymienione powyżej aspekty wydają się być niedoceniane nie tylko na rynku krajowym, lecz także w działaniach Komisji Europejskiej, która udostępnia bezpłatnie narzędzia ("SD-DSS" - bibliotekę do tworzenia i walidacji podpisu[27]). KE nie ponosi odpowiedzialności prawnej i finansowej związanej ze świadczeniem usługi - dostarcza jedynie biblioteki programistyczne. W związku z tym transferuje wysokie ryzyko operacyjne i finansowe na podmioty bezkrytycznie wykorzystujące bibliotekę. Ryzyko to związane jest np. z:

a) Utrzymaniem kodu źródłowego w całym cyklu życia systemu, który korzysta z bibliotek DSS. Nie istnieje długoterminowa gwarancja wsparcia dla bibliotek oprogramowania lub długoterminowa gwarancja funkcjonowania podmiotu dostarczającego biblioteki. KE nie przedstawia użytkownikom bibliotek dowodów zawarcia ubezpieczeń od odpowiedzialności cywilnej gdyż nie ponosi takiej odpowiedzialności;

[27] *Źródło: http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-9action_en.htm*

b) Obsługą sytuacji kryzysowych związanych z błędami w bibliotekach (zarówno niekrytycznymi, jak i błędami krytycznymi wpływającymi w sposób zagrażający funkcjonowaniu kluczowych procesów biznesowych, w szczególności błędami bezpieczeństwa);
c) Uzależnieniem się od jednego dostawcy (tzw. *„vendor lock-in”*) oferującego pozornie darmowe biblioteki programistyczne;
d) Finansowaniem wypłaty kar umownych przez podmioty budujące usługi zaufania wykorzystujące biblioteki. Kary mogą wynikać z niedotrzymania parametrów SLA (np. parametrów związanych z dostępnością, wydajnością, bezpieczeństwem, ilością powtarzalnych defektów oprogramowania). Dostawca usługi wykorzystującej biblioteki nie może przenieść kar na dostawcę biblioteki (DSS);

Taką odpowiedzialność ponoszą komercyjni dostawcy usług walidacji, a jej zakres jest na tyle wysoki, że realizacja usługi walidacji w ramach administracji publicznej byłaby wysoce kosztowna, a biorąc pod uwagę poziom wynagrodzeń w sektorze publicznym, wielce ryzykowna we wdrożeniu i utrzymaniu.

Administracja publiczna krajów UE nie licząc TCO[28] dla inwestycji w nowe usługi zaufania, traktuje z pozoru darmowe narzędzia, jako bezpieczną z punktu wydawania środków publicznych alternatywę. Doświadczenia komercyjnych dostawców usług zaufania pokazują, że dla usług o wysokiej dostępności, odporności na awarie i wysokim poziomie bezpieczeństwa koszt opracowania logiki biznesowej usługi, (czyli np. logiki biznesowej usługi walidacji) może, w przypadku, gdy logika nie jest skomplikowana, stanowić nawet kilka procent całkowitego kosztu inwestycji. W związku z tym z pozoru nieodpłatne rozwiązania dla administracji publicznej okazują się być bardziej kosztowne od komercyjnych udostępnianych w modelu SaaS[29], których koszty rozwoju i utrzymania transferowane są przez usługodawców nie tylko na administrację, ale także klientów biznesowych.

Bardzo istotne z punktu widzenia interesu ekonomicznego kraju jest liczenie i podawanie do publicznej wiadomości całkowitych kosztów tworzenia "bezpłatnych" usług zaufania świadczonych przez administrację publiczną przy wysokim poziomie dostępności, bezpieczeństwa i zestawienie - w szczególności kosztów jednostkowych (w przeliczeniu na pojedynczego użytkownika usługi). Koszty te powinny być zestawiane z kosztami jednostkowymi rozwiązań komercyjnych, a ewentualne różnice uzasadniane obywatelom, którzy finansują budowę systemów administracji publicznej.

Aby uniknąć nieuczciwej konkurencji pomiędzy dostawcami usług zaufania sektora prywatnego i publicznego wszystkie usługi powinny być świadczone odpłatnie, zaś cena usługi nie powinna być ustalona poniżej kosztów wytworzenia. W przypadku podmiotów publicznych opłata może być transferowana na obywateli poprzez wskazanie rozliczenia podatkowego stwierdzającego, wprost jaka średnia kwota podatku (wyrażona w PLN) ponoszonego przez statystycznego użytkownika usługi jest przez niego odprowadzana, aby zasilić budżet rozwoju i utrzymania usługi.

Na krajowym rynku dostawców usług zaufania, obecne są opinie, że utworzenie konkurencyjnej dla biznesu usługi walidacji przez administrację publiczną wykreuje świadomość ważności usługi na rynku polskim, a klienci - po początkowym zapoznaniu się z podstawowymi usługami walidacji - zdecydują się na wybór usług komercyjnych w wariancie "premium" - o wyższej jakości i dostępności, co przełoży się na obniżenie ryzyka działalności na rynkach elektronicznych.

W związku z tym, że trudno oszacować okres zwrotu z inwestycji w krajowe centrum walidacji rozsądnym wydaje się być zastosowanie przez administrację publiczną konwersji CAPEX na OPEX i utworzenie centrum walidacji w modelu usługowym poprzez zakupienie usługi od istniejących dostawców (prywatnych lub publicznych).

28 ang. Total Cost of Ownership

[29] SaaS - ang. Software as a Service

Usługa taka realizowana powinna być przez kompetentnych pracowników z wieloletnim doświadczeniem w dziedzinie walidacji podpisów i certyfikatów. Wykorzystanie infrastruktury teleinformatycznej gwarantującej wysoki poziom dostępności i odporności na awarie krytyczne daje podstawy do ponoszenia wysokiej odpowiedzialności za świadczenie usługi walidacji. Udział doświadczonych pracowników w procesie rozwoju i świadczenia (utrzymania) usługi gwarantuje spełnienie wysokich parametrów SLA oczekiwanych od dostawców usług zaufania oraz wysokiego poziomu wsparcia technicznego dla usługobiorców.

4.4.2 Outsourcing usług zaufania

Administracja publiczna może budować własne usługi zaufania (insourcing) lub skorzystać z oferty komercyjnych dostawców usług. Samodzielne świadczenie usług zaufania w ramach sektora publicznego powinno spełniać pryncypium "nie nadzorowania samego siebie" czyli unikania świadczenia usług przez podmiot zajmujący się nadzorem (w szczególności MG).

Bazując na wieloletnich doświadczeniach we wdrażaniu rozwiązań teleinformatycznych w ramach administracji publicznej (np. systemu ePUAP) istotnym wydaje się być zbudowanie platformy usług zaufania w administracji publicznej, do której będzie podłączonych **możliwie jak najwięcej usług dostarczanych przez jednostki wewnętrzne administracji publicznej oraz podmioty komercyjne**. Platforma taka mogłaby powstać na wzór platformy identyfikacji i uwierzytelniania obywateli udostępnionej przez rząd Szwecji[30].

Konsument usługi zaufania (w tym przypadku: administracja publiczna) mógłby zdecydować o wyborze usługi na platformie usług online. Operator platformy rozliczałby się z dostawcami usług na podstawie dwustronnych umów cywilnoprawnych. Rozliczenie z dostawcą usługi następować mogłoby na podstawie raportów z wykorzystania usługi przez organy administracji publicznej. Dzięki temu usługi bardziej popularne (o wyższej jakości i poziomie bezpieczeństwa) uzyskiwałby finansowanie. Jeśli rozwiązanie zapewniające konkurencję dostawców usług zaufania w formie platformy online byłoby trudne do wdrożenia, należy zaimplementować w administracji publicznej rozwiązanie organizacyjne umożliwiające **dostarczanie zunifikowanych (dzięki eIDAS) usług zaufania do sektora publicznego przez więcej niż jednego TSP**. Jest to podyktowane nie tylko zasadą konkurencji rynkowej (unikanie monopoli i w konsekwencji wzrostu cen, uzależnienia się od dostawcy /tzw. vendor lock-in/), ale także ograniczenia skutków wystąpienia ryzyka nie przejścia audytu zgodności realizowanego przez CAB lub kompromitacji TSP podczas realizacji usługi.

Wytypowanie krajowych podmiotów publicznych, które ewentualnie mogłyby świadczyć poszczególne rodzaje usług zaufania w ramach administracji publicznej, powinno zostać poprzedzone zapytaniem do potencjalnych kandydatów czy są zainteresowani świadczeniem usług zaufania. Odpowiedź na to pytanie pozwoli ocenić sytuację rynkową i zaproponować dalsze działania.

4.5 Skutki ekonomiczne wdrożenia rozporządzenia eIDAS i ustawy o usługach zaufania w Polsce

Oszacowanie skutków ekonomicznych wdrożenia eIDAS jest w obecnym momencie obarczone ryzykiem popełnienia dużego błędu. Jest to spowodowane chwilowym niedoprecyzowaniem i ciągłym ustalaniem przez KE, ETSI oraz organy w Polsce aspektów:

a) Prawnych - np. opublikowanie przez KE aktów wykonawczych i delegowanych, przygotowanie ustawy o usługach zaufania;
b) Organizacyjnych - np. ustalenie procesów oceny zgodności i nadzoru; ustalenie zasad korzystania komercyjnych z usług zaufania przez administrację publiczną w Polsce i strategii budowy własnych usług zaufania;

[30] *Źródło: http://aaa-sec.com/projects/eid20/index.html*

c) Technologicznych - np. publikacja przez ETSI specyfikacji technicznych, które podlegać będą konwersji do norm europejskich EN;

Z punktu widzenia podmiotów biznesowych wdrożenie eIDAS pociągać będzie za sobą konieczność dostosowania się do wymagań zdefiniowanych w normach EN oraz do wymagań zdefiniowanych w rozporządzeniu. Większość z tych wymagań tworzonych było na bazie dobrych praktyk, zatem są one najczęściej już realizowane przez TSP. Przy ostrożnym szacowaniu ryzyk wpływających na poziom kosztów świadczenia usług, można założyć, że w najbliższych 3 latach rentowność sprzedaży (*ROS = zysk ze sprzedaży / sprzedaż*) spadnie o ok. 20%.

Szacuje się, że reorganizacja procesów produkcyjnych, zarządzania jakością i obsługi prawnej spowoduje prawdopodobnie obniżenie wskaźników sprawności zarządzania aktywami w przedsiębiorstwach mierzonej wskaźnikiem TAT (*TAT = sprzedaż / aktywa ogółem*) o ok. 20%.

Przy stosunkowo wysokim ryzyku realizacji usług zaufania, związanym z transformacją europejskiego rynku, ciężej będzie finansować aktywa TSP z kapitału obcego ze względu na niższą zdolność kredytową i wyższy koszt kapitału. W związku z tym szacuje się, że w najbliższych latach TSP w zwiększonym zakresie będą musieli finansować swoją działalność z kapitału własnego, co spowoduje, że mnożnik kapitałowy czyli wskaźnik EM (EM = aktywa ogółem / kapitał własny) spadnie także o ok. 20%.

Po uwzględnieniu powyższych założeń, korzystając z modelu *Du Ponta,* można ocenić, że przy założeniu niezmienności sprzedaży zmiana zyskowności przedsiębiorstw będzie wynosić:

$$ROE_{eIDAS} = ROS_{eIDAS} * TAT_{eIDAS} * EM_{eIDAS} =$$

$$= 80\% * ROS_{aktualne} * 80\% * TAT_{aktualne} * 80\% * EM_{aktualne} =$$

$$= 80\% * 80\% * 80\% \, ROE_{aktualne} = 51{,}2\% \, ROE_{aktualne}$$

W bardzo dużym uproszczeniu rentowność kapitału własnego przy nie zmienionym poziomie sprzedaży spadnie do poziomu 51,2% obecnej rentowności. Jeśli TSP nie zwiększą zaangażowania kapitału własnego, pozostawią niezmienny poziom aktywów (np. kapitału ludzkiego i infrastruktury) wówczas prawdopodobnie oczekiwać będą od rynku poprawy sprzedaży i kompensacji spadku zysku netto związanego z dostosowaniem do eIDAS. Z drugiej strony obniżenie ROE może być kompensowane przez instrumenty wsparcia udostępniane przez KE w formie bezzwrotnych dotacji np. funduszy CEF[31], które aby były skuteczne powinny oferować adekwatnie do powyższych założeń poziom dofinansowania ok. 50%.

Długoterminowo wartość ROE powinna zwiększać się pod wpływem rosnącej sprzedaży powodowanej ujednolicaniem się europejskiego rynku usług zaufania, poprawą sprawności działania TSP i zwiększeniem zaangażowania kapitału obcego spowodowanego obniżeniem poziomu ryzyka prowadzenia działalności gospodarczej.

Niebagatelną rolę w utrzymaniu się na transformującym rynku usług zaufania ma poziom zamówień składanych przez jednostki administracji publicznej do TSP. Przy spadku TAT do 80% wartości obecnej i EM do 80% wartości obecnej zwiększenie rentowności sprzedaży dla administracji publicznej do 156,25% wartości obecnej pozwoli utrzymać ROE na niezmienionym poziomie. W tym kontekście zapowiedzi o realizacji strategii insourcingu usług zaufania przez polską administrację publiczną mogą oznaczać eliminację niektórych polskich TSP z rynku w okresie transformacji.

Długoterminowo, popularyzacja usług zaufania w segmencie administracji publicznej prawdopodobnie przełoży się na zwiększone zainteresowanie tymi usługami w sektorze biznesowym, co zwiększy sprzedaż. Dynamika wzrostu sprzedaży usług zaufania uzależniona będzie od wielu czynników jednak najważniejszymi, z punktu widzenia istniejących usług udostępnianych online jest:

a) Na rynku masowym B2C, G2C - tzw. "traffic" czyli zainteresowanie klientów tzw. "contentem" usługi biznesowej zabezpieczanej przez usługę zaufania. Usługi zaufania będą tak popularne jak bardzo pożądane dla użytkowników będą chronione przez nich zasoby;
b) Na rynku biznesowym B2B - dodatkowym istotnym parametrem wycenianym przez interesariuszy jest ryzyko związane z realizacją usługi - im będzie ono większe tym większe będzie zainteresowanie usługami zaufania.

[31] Connecting Europe Facility

Biorąc pod uwagę wieloletnie doświadczenie autorów ekspertyzy w realizacji usług zaufania na rynku polskim i międzynarodowym można założyć, że dominującym "driverem" w sprzedaży usług zaufania w najbliższym czasie będzie rosnące ryzyko teleinformatyczne zawierania transakcji elektronicznych, które może zostać zmitygowane tylko przez usługi zaufania o wysokim poziomie bezpieczeństwa, dostępności i niezawodności. Założyć można tu ok 20% wzrost sprzedaży rok do roku, szczególnie dzięki sprzyjającym uregulowaniom prawnym dotyczącym możliwości realizacji usług zaufania w modelu serwerowym (SaaS).

Długoterminowo na europejskim rynku usług zaufania, po zakończeniu procesu transformacji i ustabilizowaniu się fluktuacji kosztów i przychodów, największą rolę odgrywać będą podmioty prywatne i publiczne o wysokim wskaźniku TAT i EM czyli te, które osiągną największą sprawność operacyjną z posiadanych aktywów oraz wykorzystają jednocześnie najlepiej efekt dźwigni finansowej. W kontekście ograniczeń jakie w świadczeniu usług zaufania nałożone są na administrację publiczną wydaje się, iż najbardziej korzystne dla polskiej gospodarki powinno być wspieranie kwalifikowanych, krajowych dostawców usług zaufania, którzy mogą:

a) finansować działalność z wykorzystaniem kapitału obcego (najlepiej krajowego ze względu na tzw. efekt mnożnikowy) oraz
b) pozyskiwać najbardziej wykwalifikowany dostępny na krajowym rynku personel.

Dodatkowo biznesowi TSP mogą wykorzystywać w maksymalnym możliwym zakresie **ekonomię skali**, która jest podstawowym czynnikiem decydującym o rentowności usług i budowaniu globalnej przewagi konkurencyjnej, w szczególności poprzez świadczenie usług dla klientów zagranicznych. Realizacja takiej strategii możliwa jest obecnie tylko w segmencie biznesowych TSP.

Skutki ekonomiczne wdrożenia eIDAS dla administracji publicznej w Polsce zależeć będą od przyjętego modelu świadczenia i korzystania z usług zaufania. Jeśli zbudowana zostanie platforma zapewniająca integrację systemów administracji publicznej z istniejącymi już usługami zaufania (publicznymi i prywatnymi) wówczas koszt wdrożenia eIDAS będzie zdecydowanie niższy niż w wariancie, w którym poszczególne jednostki administracji publicznej zdecydowałyby się na samodzielną budowę niezależnych usług. Najbardziej racjonalnym wydaje się **odwzorowanie strategii projektu e-SENS w skali kraju** z silną pozycją nadzorczą i decyzyjną jednostek publicznych, a także wykorzystaniem wypracowanego przez dziesiątki lat potencjału technologicznego i organizacyjnego biznesowych dostawców usług zaufania.

W kontekście globalnym coraz bardziej umacnia się trend budowania przewag konkurencyjnych wykorzystujących innowacyjną technologię i ekonomię. Strategię tę realizują w szczególności podmioty spoza EU, a skuteczność ich działań, skłania ku refleksji, że regulacje prawne powinny katalizować budowę nowoczesnych usług bazujących na najbardziej efektywnych modelach biznesowych (wykorzystujących technologie mobilne i usługi w tzw. chmurze).

5. ASPEKTY TECHNICZNE

W niniejszym rozdziale określono zmiany, które należy dokonać w infrastrukturze oraz dokumentacji centrów certyfikacji w związku z wejściem rozporządzenia eIDAS. Informacje te może wykorzystać organ nadzoru w celu poinformowania centrów o zakresie dostosowania regulaminów świadczenia usług lub polityk certyfikacji. W opracowaniu odniesiono się także do wpływu nowych przepisów rozporządzenia eIDAS na aplikacje do składania podpisu oraz sposób podpisywania lub znakowania czasem. Krótko przedstawiono także najważniejsze problemy techniczne związane z usługami walidacji, wydawania pieczęci elektronicznej, rejestrowanego doręczania informacji oraz konserwacji podpisu elektronicznego i pieczęci elektronicznej.

5.1 Usługi zaufania: walidacja, pieczęć elektroniczna, rejestrowane doręczenia oraz inne przewidziane unijnym rozporządzeniem, od strony technicznej

5.1.1 Usługi zaufania zdefiniowane w Rozporządzeniu eIDAS

Zgodnie z definicją zawartą w Art. 3 rozporządzenia eIDAS można określić bezpośrednio następującą listę usług zaufania:

> Artykuł 3 **Definicje**
> 16) „usługa zaufania" oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:
> a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
> b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub
> c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami;

Zakres zastosowania zdefiniowanych usług przedstawiono w Tab. 5.1.

Tab. 5.1. Usługi zaufania zdefiniowane w Rozporządzeniu 910/2014 (kolorem niebieskim zaznaczono poszczególne obiekty związane z usługą rejestrowanego doręczenia elektronicznego)

Usługi zaufania		**Usługi**			
		tworzenie	weryfikacja	walidacja	konserwacja
Obiekty	podpis elektroniczny	X	X	X	X
	pieczęć elektroniczna	X	X	X	X
	elektroniczny znacznik czasu	X	X	X	
	usługa rejestrowanego doręczenia elektronicznego	X	X	X	X
	dowód nadania wystawiony przez usługę rejestrowanego doręczenia elektronicznego	X	X	X	X
	dowód odbioru wystawiony przez usługę rejestrowanego doręczenia	X	X	X	X

	elektronicznego				
	Inne dowody powstałe w ramach usługi rejestrowanego doręczenia elektronicznego	X	X	X	X
	certyfikaty dot. usług zaufania	X	X	X	X
	certyfikaty uwierzytelniania witryn internetowych	X	X	X	

Analogiczne podejścia do określenia usług zaufania zastosowano jest w dokumencie *Trusted e-ID Infrastructures and services in EU. Recommendations for Trusted Provision of e-Government services* [ENISA2013]. Każda z wyżej wymienionych usług może być usługą kwalifikowaną lub niekwalifikowaną, przy czym w opinii autorów, nie ma zależności w zakresie tworzenia usług kwalifikowanych i takich samych odpowiednich usług niekwalifikowanych, tzn. niektóre z kwalifikowanych usług mogą nie mieć odpowiednika w postaci usługi niekwalifikowanej i na odwrót. Najbardziej wyrazistym przykładem takiego stanu są obecnie certyfikaty uwierzytelniania witryn internetowych, gdzie powszechnie stosowane są usługi niekwalifikowane.

Dodatkowo należy wskazać kwalifikowane usługi, które posiadają skutek prawny w Rozporządzaniu eIDAS przedstawiony w poniżej wymienionych artykułach dla usług i dodatkowo dokumentu elektronicznego:

a) artykuł 25 Skutki prawne podpisów elektronicznych;
b) artykuł 35 Skutki prawne pieczęci elektronicznych;
c) artykuł 41 Skutki prawne elektronicznych znaczników czasu;
d) artykuł 43 Skutek prawny usługi rejestrowanego doręczenia elektronicznego;
e) artykuł 46 Skutki prawne dokumentów elektronicznych.

Dla pozostałych usług skutek prawny nie został zdefiniowany i należy ewentualnie dookreślić go w ramach Ustawy o usługach zaufania.

W pkt. 17 artykułu 3 rozporządzenie eIDAS podaje definicję kwalifikowanej usługi zaufania:

> Art. 3, pkt. (17) „kwalifikowana usługa zaufania” oznacza usługę zaufania, która spełnia stosowne wymogi określone w niniejszym rozporządzeniu

Definicja ta wydaje się być jednak mało precyzyjna. O ile bez trudu w rozporządzeniu eIDAS można odszukać wymagania dla następujących usług zaufania:

- kwalifikowana usługa tworzenia kwalifikowanych certyfikatów podpisów elektronicznych (art.28, załącznik I),
- kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych (art. 32 i 33),
- kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych (art. 34),

- kwalifikowana usługa tworzenia kwalifikowanych certyfikatów pieczęci elektronicznych (art. 38, załącznik III),
- kwalifikowana usługa tworzenia kwalifikowanych pieczęci elektronicznych (art. 39, załącznik II)
- kwalifikowana usługa walidacji kwalifikowanych pieczęci elektronicznych (40),
- kwalifikowana usługa konserwacji kwalifikowanych pieczęci elektronicznych (art. 40),

- kwalifikowana usługa wydawania kwalifikowanych elektronicznych znaczników czasu (art.42)

- kwalifikowana usługa rejestrowanego doręczenia elektronicznego (art. 44),
- kwalifikowana usługa tworzenia kwalifikowanych certyfikatów uwierzytelniania witryn internetowych (art. 45, załącznik IV),

to pewnym problemem może być precyzyjne określenie, na podstawie zapisów w rozporządzeniu eIDAS, wymagań dla kwalifikowanych usług weryfikacji i walidacji certyfikatów podpisów/pieczęci elektronicznych, certyfikatów uwierzytelniania witryn internetowych, elektronicznych znaczników czasu. Najprawdopodobniej kwestie te mogą być wyjaśnione przez przygotowywane stosowne akty delegowane, wykonawcze i standardy.

Dodatkowo ciężko jest znaleźć argumenty przemawiające za koniecznością świadczenia tak dużej ilości rozdzielnych usług. Po pierwsze wymagania dla poszczególnych usług często pokrywają się. Po drugie zbyt duża ilość wyspecjalizowanych usług zaufania będzie zbyt trudna do użycia dla stron ufających, co z kolei nie będzie zgodne z postulatem przytoczonym np. w 57 punkcie Preambuły rozporządzenia, odnoszącym się do łatwości i wygodny walidacji kwalifikowanych podpisów elektronicznych dla wszystkich stron.

W celu zilustrowania problemu dużej ilości wyspecjalizowanych usług zaufania, załóżymy, że to osoba, do której trafi podpis czy pieczęć elektroniczna ma sama zdecydować czy informacji na temat podpisu/pieczęci udzieli jej kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych czy może kwalifikowana usługa walidacji kwalifikowanych pieczęci elektronicznych a może usługa weryfikacji podpisów elektronicznych?

Poniżej zebrano propozycję agregacji usług zdefiniowanych w rozporządzeniu eIDAS dla kwalifikowanych usług zaufania dookreślonych w krajowym ustawodawstwie.

Propozycja krajowej kwalifikowanej usługi zaufania	Usługa zaufania zdefiniowana w rozporządzeniu eIDAS
Kwalifikowana usługa wydawaniu certyfikatów kwalifikowanych	kwalifikowana usługa tworzenia kwalifikowanych certyfikatów podpisów elektronicznych
	kwalifikowana usługa weryfikacji kwalifikowanych certyfikatów podpisów elektronicznych
	kwalifikowana usługa walidacji kwalifikowanych certyfikatów podpisów elektronicznych
	kwalifikowana usługa tworzenia kwalifikowanych certyfikatów pieczęci elektronicznych
	kwalifikowana usługa weryfikacji kwalifikowanych certyfikatów pieczęci elektronicznych
	kwalifikowana usługa walidacji kwalifikowanych certyfikatów pieczęci elektronicznych
	kwalifikowana usługa tworzenia kwalifikowanych certyfikatów uwierzytelniania witryn internetowych
	kwalifikowana usługa weryfikacji kwalifikowanych certyfikatów uwierzytelniania witryn internetowych
	kwalifikowana usługa walidacji kwalifikowanych certyfikatów uwierzytelniania witryn internetowych
Kwalifikowana usługa elektronicznego znakowania	kwalifikowana usługa tworzenia elektronicznych

czasem	kwalifikowanych znaczników czasu
	kwalifikowana usługa weryfikacji elektronicznych kwalifikowanych znaczników czasu
	kwalifikowana usługa walidacji elektronicznych kwalifikowanych znaczników czasu
Kwalifikowana usługa konserwacji kwalifikowanych podpisów i pieczęci elektronicznych	Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych
	Kwalifikowana usługa konserwacji kwalifikowanych pieczęci elektronicznych
Kwalifikowana usługa rejestrowanego doręczenia elektronicznego	Kwalifikowana usługa tworzenia rejestrowanego doręczenia elektronicznego
	Kwalifikowana usługa weryfikacji rejestrowanego doręczenia
	Kwalifikowana usługa walidacji rejestrowanego doręczenia elektronicznego
Kwalifikowana usługa walidacji kwalifikowanych podpisów i pieczęci elektronicznych	Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych
	Kwalifikowana usługa walidacji kwalifikowanych pieczęci elektronicznych
Kwalifikowana usługa tworzenia kwalifikowanych podpisów i pieczęci elektronicznych	Kwalifikowana usługa tworzenia kwalifikowanych podpisów elektronicznych
	Kwalifikowana usługa tworzenia kwalifikowanych pieczęci elektronicznych
Kwalifikowana usługa zarządzania danymi służącymi do składania podpisów i pieczęci elektronicznych	Kwalifikowana usługa zarządzania danymi służącymi do składania podpisów elektronicznych
	Kwalifikowana usługa zarządzania danymi służącymi do składania pieczęci elektronicznych
Kwalifikowana usługa weryfikacji i walidacji kwalifikowanych obiektów	kwalifikowana usługa weryfikacji kwalifikowanych certyfikatów podpisów elektronicznych
	kwalifikowana usługa walidacji kwalifikowanych certyfikatów podpisów elektronicznych
	kwalifikowana usługa weryfikacji kwalifikowanych certyfikatów pieczęci elektronicznych
	kwalifikowana usługa walidacji kwalifikowanych certyfikatów pieczęci elektronicznych
	kwalifikowana usługa weryfikacji kwalifikowanych

	certyfikatów uwierzytelniania witryn internetowych
	kwalifikowana usługa walidacji kwalifikowanych certyfikatów uwierzytelniania witryn internetowych
	kwalifikowana usługa weryfikacji elektronicznych kwalifikowanych znaczników czasu
	kwalifikowana usługa walidacji elektronicznych kwalifikowanych znaczników czasu
	Kwalifikowana usługa weryfikacji rejestrowanego doręczenia
	Kwalifikowana usługa walidacji rejestrowanego doręczenia elektronicznego
	Kwalifikowana usługa weryfikacji kwalifikowanych podpisów elektronicznych
	Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych
	Kwalifikowana usługa weryfikacji kwalifikowanych pieczęci elektronicznych
	Kwalifikowana usługa walidacji kwalifikowanych pieczęci elektronicznych

5.1.2 Walidacja podpisów i pieczęci elektronicznych

Wymogi dla kwalifikowanej usługi walidacji podpisów elektronicznych definiuje art. 32 i 33 rozporządzenia eIDAS. Wymagania te są takie same w przypadku pieczęci elektronicznych (art. 40).

Artykuł 32 **Wymogi dla walidacji kwalifikowanych podpisów elektronicznych**

1. Proces walidacji kwalifikowanego podpisu elektronicznego potwierdza ważność kwalifikowanego podpisu elektronicznego, pod warunkiem, że:

a) certyfikat, który towarzyszy podpisowi, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I;
b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;
c) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;
d) unikalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;
e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;
f) podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego;
g) integralność podpisanych danych nie została naruszona;
h) wymogi przewidziane w art. 26 zostały spełnione w momencie składania podpisu.

2. System wykorzystany do walidacji kwalifikowanego podpisu elektronicznego zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia stronie ufającej wykrycie wszelkich problemów związanych z

bezpieczeństwem.

3. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących walidacji kwalifikowanych podpisów elektronicznych. Jeżeli walidacja kwalifikowanych podpisów elektronicznych spełnia te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 33 **Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych**

1. Kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych może świadczyć wyłącznie kwalifikowany dostawca usług zaufania, który:

a) zapewnia walidację zgodnie z art. 32 ust. 1; oraz

b) umożliwia stronom ufającym otrzymanie wyniku procesu walidacji w automatyczny, wiarygodny i skuteczny sposób oraz przy użyciu zaawansowanego podpisu elektronicznego lub zaawansowanej pieczęci elektronicznej dostawcy kwalifikowanej usługi walidacji.

2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej usługi walidacji, o której mowa w ust. 1. W przypadku, gdy usługa walidacji kwalifikowanych podpisów elektronicznych spełnia te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Standardy przygotowywane w tej chwili przez ETSI, które mogą być wskazane w pkt. 3 artykułu 32 i pkt. 2 artykułu 33 to:

Norma	Nazwa	Data publikacji
EN 319 101	General policy and security requirement issues for signature creation and validation	30.4.2017
EN 319 102	Procedures for signature creation and verification	30.4.2016
EN 419 103	Conformity assessment for signature creation and validation applications	30.3.2016
EN 419 111	Protection profiles for signature creation and validation applications	Niezdefiniowana
EN 319 441	Akt wymieniający standardy wskazujące minimalne wymagania, które powinien spełniać QTSP świadczący usługi walidacji QeS	46-miesięczny projekt (1Q2019)

Zgodnie z powyższą tabelą, w przeciągu 2 lat zostaną opublikowane standardy dotyczące walidacji podpisu elektronicznego. Standardu opisującego zaufaną usługę walidacji kwalifikowanych podpisów elektronicznych i pieczęci elektronicznych możemy się spodziewać najwcześniej za 4 lata – w pierwszym kwartale 2019 roku.

Walidacja podpisów elektronicznych jest zadaniem ekstremalnie skomplikowanym. Wyzwania przed jakimi stoją twórcy standardów to m.in.:

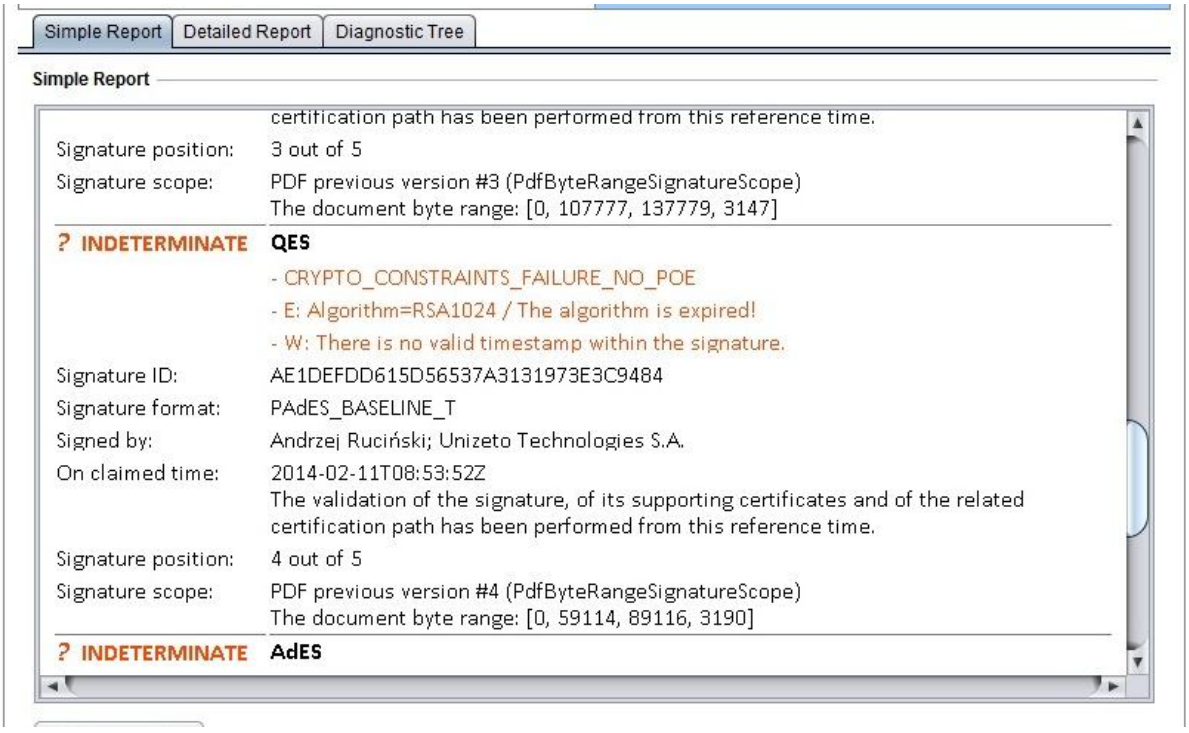
- minimalizacja ryzyka negatywnej walidacji poprawnych czy akceptacji nieważnych podpisów/ pieczęci elektronicznych;
- rozstrzygnięcie kwestii użytych w podpisie/ pieczęci algorytmów kryptograficznych: czy jeżeli są zbyt słabe to decyzja o akceptacji podpisu powinna być wyborem strony przyjmującej czy może zbyt słaby algorytm powinien zawsze wskazywać na niezgodność z wymaganiami rozporządzenia?
- rozstrzygnięcie czy algorytm walidacji certyfikatu podpisującego powinien zakładać walidację pełnej ścieżki certyfikacji aż do root'a czy może w pewnym szczególnych warunkach będzie można poprzestać tylko na walidacji certyfikatu podpisującego?

- czy należy dopuścić jako dowód, w jakim momencie podpis został złożony, tylko i wyłącznie zaufany znacznik czasu czy może również deklarację własną podpisującego bądź walidującego? Może kwestia ta powinna być zagadnieniem polityki walidacji?

Z jednej strony nie jest rzeczą skomplikowaną opracowanie algorytmu walidacji dla jednego typu podpisów elektronicznych, składanych z tą samą polityką podpisu. Przy próbie stworzenia algorytmu obejmującego szersze spektrum podpisów elektronicznych zawsze ciężar podjęcia ostatecznej decyzji można przełożyć na stronę żądającą walidacji. Wtedy jednak często zaprzeczamy już idei deklarowanej m.in. w 57 punkcie preambuły - „walidacja kwalifikowanych podpisów elektronicznych powinna być łatwa i wygodna dla wszystkich stron".

> Preambuła (57). Aby zagwarantować pewność prawa w odniesieniu do ważności podpisu, niezbędne jest wyszczególnienie elementów kwalifikowanego podpisu elektronicznego, które powinny być ocenione przez stronę ufającą dokonującą walidacji. Ponadto wyszczególnienie wymogów dla kwalifikowanych dostawców usług zaufania mogących świadczyć kwalifikowane usługi walidacji na rzecz stron ufających, które same nie chcą lub nie są w stanie dokonać walidacji kwalifikowanych podpisów elektronicznych, powinno zachęcić sektory prywatny i publiczny do inwestowania w takie usługi. Dzięki tym obu elementom walidacja kwalifikowanych podpisów elektronicznych powinna być łatwa i wygodna dla wszystkich stron na poziomie Unii.

Jako przykład ilustrujący przełożenie ostatecznej decyzji o wyniku weryfikacji na stronę pytającą, niech posłuży poniższy rysunek, przedstawiający część wyniku walidacji podpisu elektronicznego, wygenerowanego przez aplikację DSS w wersji 4.2.0 (https://joinup.ec.europa.eu/asset/sd-dss/asset_release/sd-dss-420-rc).



Rysunek 1 Rezultat walidacji kwalifikowanego podpisu elektronicznego prezentowany przez aplikację DSS w wersji 4.2.0

Ponadto w punkcie 7 preambuły rozporządzenia eIDAS mowa jest o konieczności stworzenia bramki europejskich urzędów walidacji.

Preambuła (7). Parlament Europejski w rezolucji z dnia 21 września 2010 r. dotyczącej ostatecznego utworzenia wewnętrznego rynku handlu elektronicznego (1) podkreślił znaczenie bezpieczeństwa usług elektronicznych, zwłaszcza podpisów elektronicznych, i potrzebę stworzenia infrastruktury klucza publicznego na poziomie ogólnoeuropejskim, a także wezwał Komisję do stworzenia bramki europejskich urzędów walidacyjnych w celu zapewnienia transgranicznej interoperacyjności podpisów elektronicznych i podniesienia bezpieczeństwa transakcji przeprowadzanych przy użyciu Internetu.

Próba taka została podjęta w projekcie LSP PEPPOL – http://www.peppol.eu/peppol_elements/esignature. W ramach pilotażu stworzono sieć urzędów walidacji, które wzajemnie przekierowywały do siebie żądania walidacji certyfikatów elektronicznych. Stworzono również protokół obsługujący walidację podpisów elektronicznych, wraz z obsługą przekierowywania żądań pomiędzy usługami. Został on zaimplementowany i przetestowany przez usługi w ramach projektu PEPPOL, w tym usługę WebNotarius. Obecnie te protokoły są produkcyjnie przez tę usługę wykorzystywane.

5.1.3 Usługa tworzenia podpisu i pieczęci elektronicznych

Preambuła (51). Podpisującemu należy umożliwić powierzanie kwalifikowanych urządzeń do składania podpisu elektronicznego stronie trzeciej pod warunkiem wdrożenia odpowiednich mechanizmów i procedur zapewniających, aby podpisujący miał wyłączną kontrolę nad używaniem swoich danych służących do składania podpisu elektronicznego i aby urządzenie użytkowane było ze spełnieniem wymogów dotyczących kwalifikowanego podpisu elektronicznego.

Preambuła (52). Coraz powszechniejsze będzie składanie podpisu elektronicznego na odległość, w przypadku którego środowiskiem składania podpisu elektronicznego zarządza dostawca usług zaufania w imieniu podpisującego, gdyż wiąże się ono z licznymi korzyściami gospodarczymi. Jednakże w celu zapewnienia, aby takie podpisy elektroniczne były prawnie uznawane na równi z podpisami elektronicznymi składanymi w środowisku, nad którym całkowicie panuje użytkownik, dostawcy usługi składania podpisu elektronicznego na odległość powinni stosować szczególne procedury zarządzania i szczególne administracyjne procedury bezpieczeństwa, używać wiarygodnych systemów i produktów, w tym bezpiecznych kanałów komunikacji elektronicznej, aby zagwarantować niezawodność środowiska składania podpisu elektronicznego oraz korzystanie z tego środowiska pod wyłączną kontrolą podpisującego. W przypadku kwalifikowanego podpisu elektronicznego składanego za pomocą urządzenia do składania podpisu elektronicznego na odległość należy stosować wymogi mające zastosowanie do kwalifikowanych dostawców usług zaufania, określone w niniejszym rozporządzeniu.

Preambuła (55). Certyfikacja bezpieczeństwa informatycznego oparta na normach międzynarodowych, takich jak ISO 15408 i powiązane metody oceny i ustalenia dotyczące wzajemnego uznawania, jest ważnym narzędziem weryfikacji bezpieczeństwa kwalifikowanych urządzeń do składania podpisu elektronicznego i należy ją propagować. Jednakże innowacyjne rozwiązania i usługi, takie jak mobilny podpis i podpisywanie w chmurze, polegają na technicznych i organizacyjnych rozwiązaniach, jakimi są kwalifikowane urządzenia do składania podpisu elektronicznego, w odniesieniu do których mogą jeszcze nie być dostępne normy bezpieczeństwa lub pierwsza certyfikacja bezpieczeństwa informatycznego jeszcze trwa. Poziom bezpieczeństwa takich kwalifikowanych urządzeń do składania podpisu elektronicznego można by poddawać ocenie przy użyciu alternatywnych procedur tylko w przypadku, gdy takie normy bezpieczeństwa nie są dostępne lub gdy pierwsza certyfikacja bezpieczeństwa informatycznego jeszcze trwa. Procedury te powinny być porównywalne z normami certyfikacji bezpieczeństwa informatycznego w zakresie, w jakim ich poziomy bezpieczeństwa są równoważne. Procedury te mogłaby ułatwić wzajemna ocena.

5.1.4 Rejestrowane doręczenia – ujęcie w projektach UE: LSP STORK, PEPPOL, e-CODEX, E-SENS

Z raportu *eDocuments and e-Delivery in the context of the services directive* [ED2009] wynika, że większość krajów członkowskich UE na różny sposób wdrożyła w wybranych obszarach systemy doręczeń dokumentów do krajowej administracji publicznej oraz systemy doręczenia wysyłanych przez administracje publiczną dokumentów do obywateli lub firm. Takie dokumenty są z reguły podpisywane elektroniczne, a dowody doręczenia dokumentów tworzą systemy informatyczne administracji.

W wielu ogólnoeuropejskich projektach dużej skali (ang. Large Scale Project, LSP) były opracowywane moduły związane z usługami typu *e-delivery*.

LSP STORK

W dokumencie: ”D6.4.1 eDelivery – Funkcjonał Specyfication” jako przypadek użycia rozpatrzono zagadnienia dostarczenia wiarygodnych danych identyfikujących podmiotu z jednego kraju do drugiego kraju w celu udostępniania usług systemów informatycznych administracji publicznej drugiego kraju w oparciu o krajowe centra doręczania.

Polska: udział w projekcie - Nie

LSP SPOCS (http://www.eu-spocs-starterkit.eu/building-blocks/edelivery).

Blok projektowy *e-delivery* na podstawie komunikacji pomiędzy sobą zaufanych usług krajowych (informacje pobierane z listy TSL) słuzy do wymiany danych we wszystkich obszarach komunikacji obywatel, biznes lub administracja do wszystkich pozostałych. Techniczna warstwa transportowa: SMTP/MIME, Web Services (WS-*).

Polska: udział w projekcie - Tak.

Organizacja uczestnicząca: Instytut Logistyki i Magazynowania(ILIM).

Osoba kontaktowa: Tomasz Kawecki (tomasz.Kawecki@ilim.poznan.pl)

LSP epSOS (http://www.epsos.eu/home.html).

W projekcie zaplanowano możliwość komunikacji obywateli z instytucjami służbyi opieki zdrowotnej oraz odwrotnie. System doręczeń może być wykorzystywany także w przypadku kontaktu obywatela innego kraju z instytucją opieki zdrowotnej w innym kraju. Węzłami kontaktującymi się w zakresie identyfikacji pacjenta, świadczeń, zwolnień lekarskich dla pacjenta są krajowe punkty kontaktowe w zakresie opieki zdrowotnej

Techniczna warstwa transportowa pomiędzy punktami krajowymi: Web Services (WS-*).

Polska: udział w projekcie - Tak.

Organizacja uczestnicząca: NARODOWY FUNDUSZ ZDROWIA (NFZ)

Organizacja uczestnicząca: Instytut Logistyki i Magazynowania(ILIM).

LSP PEPPOL (http://www.peppol.eu/).

Wprojekcie została zrealizowana komunikacja pomiędzy podmiotami realizującymi publiczne zamówienia online. W krajach biorących udział w projekcie zbudowany został punkt dostępowy. Podmioty świadczące usługę zamówień publicznych są podłączeni do punktu dostępowego, a użytkownicy końcowi przy pomocy własnych systemów do usługodawcy świadczącego usługę zamówień. Poprzez warstwę transportową realizowana jest wymiana dokumentów dotyczących przetargów, ale może ona służyć także do innych celów. W warstwie transportowej komunikacja jest określana poprzez metadane Adresata i Publikującego/Nadawcy w celu określenia drogi komunikacji. Oznacza to, że w ramach projektu została zbudowana transgraniczna usługa *e-delivery* realizująca bezpieczne i poś5.1.5aidczane (np. potwierdzenie odbioru) przekazywanie dokumentów pomiędzy punktami dostępowymi Infrastruktury transportowej PEPPOL.

Polska: udział w projekcie - Nie

e-CODEX (http://www.e-codex.eu/home.html).

W projekcie została zrealizowana komunikacja pomiędzy systemami sądownictwa poszczególnych krajów członkowskich. W krajach biorących udział w projekcie zbudowany został MS Gateway w celu realizacji wymiany dokumentów.

System sądownictwa określonego kraju może zostać podłączony do MS Gateway, przy czym projekt nie ingerował w poszczególne krajowe systemy sądownictwa. Dokument przekazywany do innego kraju opatrywany jest podpisem elektronicznym zgodnie z wymogami krajowymi w ramach krajowego systemu sądownictwa, a następnie przekazywany do MS Gateway nadawcy, który waliduję podpis i generuje raport walidacji. Całość, tj. dokument oraz raport są podpisywane przez MS Gateway nadawcy zgodnie z formatem ASIG. Po otrzymaniu przesyłki MS Gateway odbiorcy waliduje podpis MS Gateway nadawcy i w przypadku pozytywnego wyniku przekazuje przesyłkę do systemu Sądownictwa kraju odbiorcy.

Podsumowując usługa e-Delivery: realizowana jest poprzez system krajowych bram dostępowych w celu zagwarantowania integralności przekazywanych danych. Usługa jest realizowana zgodnie z wymaganiami określonymi w normie ETSI TS 102 640.

Polska: udział w projekcie - Tak.

Organizacja uczestnicząca: Instytut Logistyki i Magazynowania(ILIM).

5.1.6 Rejestrowane doręczenia – uznawanie i standaryzacja

Zgodnie z rozporządzaniem eIDAS:

Artykuł 3 punkt 16): „usługa zaufania" oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:

a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub
c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami;

Z powyższej definicji możemy wywnioskować, że świadczone mogą być usługi:

- „tworzenia rejestrowanego doręczania 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;
- „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.

Z kolei wg art. 3, pkt. 36):

> Artykuł 3, punkt 36):
>
> „usługa rejestrowanego doręczenia elektronicznego" oznacza 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 jakiejkolwiek nieupoważnionej zmiany;

Na działanie powyższej usługi składają się następujące działania:

a) przesyłanie danych;
b) wystawianie dowodów powstałe na skutek posługiwania się tymi danymi (tzn. różne dowody - nie tylko dowody wysłania i otrzymania);
c) tworzenie dowodów wysłania;
d) tworzenie dowodów odbioru;
e) zabezpieczanie danych przez cały okres przesyłania.

Jaki jest obecnie stan w zakresie norm i standardów pozwalających na zdefiniowanie powyższych czynności?

Zgodnie z tabelą przedstawioną w rozdz. 4.2 obecnie dostępne są następujące normy, które powinny być podstawą do uregulowania wymagania określonego w art. 44, ust. 2 rozporządzenia eIDAS:

- ETSI TS 102 640-1: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture.
- ETSI TS 102 640-2: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM.
- ETSI TS 102 640-3: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains.
- ETSI TS 102 640-4:Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Conformance Profiles.
- ETSI TS 102 640-5: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles.
- ETSI TS 102 640-6.1: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.1: REM-MD UPU PReM interoperability Profile .
- ETSI TS 102 640-6.2.: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.2: REM-MD BUSDOX Interoperability Profile .
- ETSI TS 102 640-6.3: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.3: REM-MD SOAP Binding Profile.
- EN 319 511 Policy and security requirements for registered electronic mail (REM) service providers
- EN 319 512 Registered electronic mail (REM) services
- EN 319 513 Conformity assessment for REM service providers

- TS 119 514 Testing compliance and interoperability of REM service providers.

Zgodnie z dokumentem *Rationalised Framework for e-signatures standards (Dec. 2014, Mandate M/460)* dostępnym pod adresem http://www.e-signatures-standards.eu/layout/set/print/activities nie jest obecnie określony termin opracowania norm EN 319 511 , EN 319 512, EN 319 513 TS 119 514 .

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

- potwierdzenie dostarczenia danych do usługi,
- potwierdzenie dostarczenia przez usługę do odbiorczy 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 oraz mogą powstawać
- inne dowody wymagane przez procesy biznesowe lub postępowaniatypu administacyjne lub sądowe (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").

Dla wszystkich tych dowodów minimalnym wymaganiem powinno być opatrzenie ich podpisem elektronicznym lub pieczęcią elektroniczną świadczącego usługę rejestrowanych doręczeń elektronicznych, dołączenie niezaprzeczalnych informacji o danych przekazywanych, o odpowiednich datach poszczególnych czynności oraz o danych identyfikujących nadawców i odbiorców. W przypadku braku określenia szczegółowych standardów mogą powstawać „wyspowe" dedykowane dla konkretnych przypadków lub grup nadawców i odbiorców usługi rejestrowanych doręczeń elektronicznych.

Dowody powstające w ramach świadczenia usługi rejestrowanego doręczenia mogą powstawać wielokrotnie, na przykład podczas przekazywania danych od jednej usługi do drugiej, przy czym użytkownik usługi może zdecydować, czy należy prezentować nadawcy i odbiorcy końcowemu wszystkie powstałe dowody w ramach realizacji pojedynczego przekazu danych. Dla użytkownika końcowego ważne są ostateczne dowody dostarczenia otrzymane od usługi, do której się zwrócił. Pozostałe dowody, tzn. dowody „tranzytowe" dowody należy zachować na przykład na wypadek ewentualnych roszczeń sądowych lub w zakresie dotrzymania odpowiedniego SLA (Service Level Agreement).

Dowody powstające wskutek korzystania z usługi rejestrowanych doręczeń elektronicznych muszą zawsze spełniać wymagania określone w art. 44, ust. 1 rozporządzenia eIDAS:

> Art. 44, ust. 1. Kwalifikowane usługi rejestrowanego doręczenia elektronicznego muszą spełniają następujące wymogi:
>
> a) są świadczone przez co najmniej jednego kwalifikowanego dostawcę usług zaufania;
> b) z dużą dozą pewności zapewniają identyfikację nadawcy;
> c) zapewniają identyfikację adresata przed dostarczeniem danych;
> d) 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;

e) każda zmiana danych niezbędna do celów wysłania lub otrzymania danych jest wyraźnie wskazana nadawcy i adresatowi danych;
f) data i czas wysłania, otrzymania i wszelkiej zmiany danych są wskazane za pomocą kwalifikowanego elektronicznego znacznika czasu.

W przypadku przesyłania danych między co najmniej dwoma kwalifikowanymi dostawcami usług zaufania wymogi określone w lit. a)–f) mają zastosowanie do wszystkich kwalifikowanych dostawców usług zaufania.

Dodatkowo usługa taka będzie musiała być często zintegrowana w ten lub inny sposób z systemami płatności internetowych lub płatnościami za pośrednictwem usługi świadczonych przez operatorów telekomunikacyjnych.

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 liczę odbiorców i nadawców z możliwością przekazywania zarówno zdefiniowanych dokumentów, jak również dowolnych danych (e-listy, e-obrazy, …); w tym przypadku mogą powstawać wielostopniowe łańcuchy dowodów nadania i odbioru; jeżeli dla nadawcy docelowym odbiorcą jest pojedyncza elektroniczna skrzynka podawcza, to w wyniku skorzystania z usługi tworzone są dowody nadania i odbioru; podobne dowody tworzy także docelowy odbiorca przesyłki.
- elektroniczna usługa rejestrowanych doręczeń posiadająca określoną liczę 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 mogą powstawać wielostopniowe łańcuchy dowodów nadania i odbioru, wystawianych przez poszczególne usługi doręczeń, a potem do odbiorcy docelowego.

W obecnie obowiązujący polskim ustawodawstwie z zakresu doręczeń przyjęta jest zasada, że to obywatel lub podmiot mający odpowiedni obowiązek wnosi bezpośrednio dokumenty do systemów administracji i jest przy tej czynności odpowiednio identyfikowany i uwierzytelniany. Stąd konieczne jest doprecyzowanie, że za pośrednictwem kwalifikowanej elektronicznej usługi rejestrowanych doręczeń można wnosić dokumenty do odpowiednich podmiotów administracji publicznych. Jeżeli przy takim wnoszeniu dokumentów wymagane sa 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 powinien móc za pośrednictwem kwalifikowanej usługi doręczeń (zarówno krajowej, jak również świadczonej przez inne kraje UE) wnieść dane, np. pismo, e-fakturę do każdej publicznie dostępnej skrzynki mailowej administracji publicznej, i tak wniesione dane muszą być rozpatrzone na podstawie skutków prawnych określonych w rt. 43 rozporządzenia eIDAS:

Artykuł 43 **Skutek prawny usługi rejestrowanego doręczenia elektronicznego**

1. Nie jest kwestionowany skutek prawny danych wysłanych i otrzymanych 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.

2. 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.

Do rozstrzygnięcia również jest kwestia przechowywania przesyłanych danych i czy jest konieczna regulacja w tym zakresie, tzn. czy dane po przekazaniu do odbiorczy są dalej przechowywane przez usługodawcę, czy jest to kwestia opcjonalna i decyduje o tym nadawca i odbiorca, czy usługowca przechowuje wyłącznie dowody w zakresie tej usługi wyłącznie dowody powstałe w wyniku świadczenia usługi. Usługodawca ma taki obowiązek zgodnie z art.24 ust.2:

Art. 24, ust. 2, lit. h). Wymogi dla kwalifikowanych dostawców usług zaufania

h) rejestruje i udostępnia przez odpowiedni okres, w tym po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, w szczególności do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług. Rejestracja może odbywać się drogą elektroniczną;

Odpowiedź na powyższe pytanie nie jest prosta. Wydaje się, że usługodawca nie powinien przechowywać dodatkowo dane przesyłane, ale większość społeczeństwa ma konta mailowe u darmowych usługodawców poczty elektronicznej i woli przechowywać kompletne maile, a nie tylko dowody ich nadania lub otrzymania. W różny sposób można rozumieć „*wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych*". Wszystkie informacje związane z danymi, czy też dane w tym zawarte w mailu/ Informacji o zasadach przechowywania danych powinny być umieszczone w co najmniej w Regulaminie świadczenia usługi, zgodnie z:

Art. 24, ust. 2, lit. d). Wymogi dla kwalifikowanych dostawców usług zaufania

d) przed wejściem w stosunek umowny informuje, w jasny i szczegółowy sposób, wszystkie osoby pragnące skorzystać z kwalifikowanej usługi zaufania o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej;

Obecnie obowiązujące w Polsce przepisy w zakresie doręczeń do administracji publicznej lub sądownictwa pozwalają przede wszystkim na doręczanie dokumentów drogą komunikacji elektronicznej za pośrednictwem usług, które nie są świadczone przez kwalifikowanych usługodawców. Usługi te nie są jednak świadczone jako usługi zgodne z rozporządzeniem eIDAS (dokładniej, nie są zgodne z przedstawionymi powyżej normami). W związku z powyższym dowody z obecne świadczonych usług nie będą miały bezpośredniego skutku prawnego w innych krajach UE (wynika to z definicji usługi rejestrowanego doręczenia elektronicznego oraz Artykułu 43 rozporządzenia eIDAS). Jeżeli urzędowe potwierdzenie odbioru (UPO) będzie zawierało podpis kwalifikowany lub podpis przy użyciu pieczęci kwalifikowanej, to skutek prawny w UE będzie analogiczny ze skutkiem prawnym jak w przypadku usług podpisu elektronicznego.

W związku z powyższym wymagane jest przejrzenie wszystkich aktów prawnych (w szczególności dotyczących procedur postępowań administracyjnych i sądowych) w celu uzupełnienia o wykorzystanie możliwości doręczenia pism kierowanych do odpowiednich instytucji i przekazywanych przez te instytucje za pośrednictwem usług kwalifikowanych doręczeń elektronicznych, o których mowa w rozporządzeniu eIDAS. Dodatkowo, w przypadku doręczenia korespondencji do osoby fizycznej niezbędne jest zapisanie wymogu udostępnienia narzędzi do przeglądania, weryfikacja i walidacji dowodów usług rejestrowanego doręczenia elektronicznego.

5.1.7 Konserwacja podpisów elektronicznych.

Analiza zrealizowanych lub realizowanych obecnie w ranach UE projektów dużej skali (LSP) pokazuje, że w projekcie:

- LSP PEPPOL konserwacja podpisów elektronicznych nie została zaimplementowania;
- LSP e-CODEX konserwacja podpisów elektronicznych nie została zaimplementowana;
- LSP epSOS konserwacja podpisów elektronicznych została zrealizowana tylko dla przypadku ponownego dostępu do danych pacjenta; dane są podpisywane i ponownie znakowane czasem oraz przechowywane przykładowo przez 10 lat, przy czym do znakowania czasem wykorzystywany jest własny znacznik czasu, nie korzysta się z zewnętrznych dostawców niekwalifikowanych lub kwalifikowanych usług zaufania.

Odnośniki w rozporządzaniu eIDAS do usługi konserwacji podpisów można znaleźć w następujących punktach i artykułach:

Preambuła (61). 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.

Artykuł 3, pkt. 16)

16) „usługa zaufania" oznacza usługę elektroniczną zazwyczaj świadczoną za wynagrodzeniem i obejmującą:
a) tworzenie, weryfikację i walidację podpisów elektronicznych, pieczęci elektronicznych lub elektronicznych znaczników czasu, usług rejestrowanego doręczenia elektronicznego oraz certyfikatów powiązanych z tymi usługami; lub
b) tworzenie, weryfikację i walidację certyfikatów uwierzytelniania witryn internetowych; lub
c) konserwację elektronicznych podpisów, pieczęci lub certyfikatów powiązanych z tymi usługami;

Artykuł 34. Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych

1. 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 ważności.

2. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych. W przypadku, gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych spełniają te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Artykuł 40. Walidacja i konserwacja kwalifikowanych pieczęci elektronicznych

Art. 32, 33 i 34 stosuje się odpowiednio do walidacji i konserwacji kwalifikowanych pieczęci elektronicznych.

Należy zauważyć, że w przypadku usługi konserwacji podpisów/pieczęci elektronicznych nie jest określony dokładny termin wydania aktów delegowanych i wykonawczych.

Do usługi konserwacji podpisów elektronicznych nie są określone w rozporządzeniu eIDAS skutki prawne usługi konserwacji pieczęci/podpisu elektronicznego. Taka sytuacja będzie wymagała uregulowania skutków prawnych na poziomie krajowym (patrz Preambuła (22)), co na poziomie UE może doprowadzić do powstawania różnic pomiędzy różnymi krajami członkowskimi.

> Preambuła (22). Aby wspierać ogólne transgraniczne korzystanie z usług zaufania, należy zapewnić możliwość używania tych usług jako dowodu w postępowaniach sądowych we wszystkich państwach członkowskich. W prawie krajowym należy określić skutki prawne usług zaufania, o ile w niniejszym rozporządzeniu nie postanowiono inaczej.

W zakresie standardów należy zwrócić uwagę na dokumenty:

- ETSI TS 101 533-1 V1.3.1 (2012-04) Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management.
- document BSI TR-ESOR – 03125 TR-ESOR Preservation of Evidence of Cryptographically Signed Documents przygotowany przez Federal Office for Information Security, Germany,2011;
- ISO/TR 18492:2005 Long-term preservation of electronic document-based information, który odnosi się do wszystkich rodzajów informacji tworzonej przez systemy informatyczne;
- Preservation of Trust in Long-Term Records Management Systems. A State of Art Overview for the LongRec Project, Autorzy: Arne-Kristian Groven, Jon Ølnes, Habtamu Abie, Truls Fretland, 2008.- zawiera ogólną analizę zagadnienia oraz można znaleźć „dobre praktyki" w tym zakresie.

Z kolei w dokumencie *Rationalised Framework for e-signatures standards* (Dec. 2014, Mandate M/460) zasygnalizowano, że nieznane są jeszcze daty publikacji następujących dedykowanych norm dotyczących usług konserwacji:

- EN 319 521 Policy and security requirements for data preservation service providers;
- EN 319 522 Data preservation services through signing;
- EN 319 523 Conformity assessment of data preservation service providers.

Stan taki prowadzi do sytuacji, w której usługa konserwacji kwalifikowanych podpisów i pieczęci elektronicznych jest jedną z najmniej doprecyzowanych w dokumentach standaryzacyjnych i niewątpliwie wymaga dużego doprecyzowania w pracach standaryzacyjnych ETSI i legislacyjnych oraz przywołania ich przez UE w postaci aktów delegowanych i wykonawczych do rozporządzenia eIDAS.

5.2 Zmiany infrastruktury centrów certyfikacji oraz infrastruktura dostawców usług zaufania, w tym infrastruktura jaką powinny dysponować podmioty, aby realizować wymienione w katalogu eIDAS usługi

5.2.1 Wymagania nakładane na usługi zaufania wg rozporządzenia eIDAS

Rozdział III „Obowiązki podmiotów świadczących usługi certyfikacyjne" ustawy o podpisie elektronicznym oraz Rozdział 4 „Szczegółowe warunki techniczne i organizacyjne, które muszą spełniać kwalifikowane podmioty świadczące usługi certyfikacyjne " Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o 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 określają wymagania do infrastruktury centrów certyfikacji świadczących kwalifikowane usługi w zakresie zapewnienia odpowiednich środków organizacyjnych, personalnych, infrastruktury systemowej i technicznej, bezpieczeństwa oraz dostępu fizycznego. Wymagania określanie w wymienionych Ustawie i Rozporządzeniu odnoszą się do „kwalifikowanego podmiotu świadczącego usługi certyfikacyjne". Rozporządzenie R910/2014(eIDAS) poszerza zasięg stosowania na podmioty określane jako „kwalifikowany dostawca usług zaufania." W związku z powyższym zdefiniowana zostanie poszerzona lista wymagań dotycząca wszystkich lub poszczególnych świadczonych usług.

W Tab. 5.1 przedstawiono zebrano te wymagania zawarte w rozporządzeniu eIDAS, które mogą wpływać na krajową (obecną lub przyszłą) infrastrukturę zaufania. Dodatkowe wymagania te nawet w zakresie organizacyjnym, wymogów dotyczących bezpieczeństwa lub bezpośrednio wymogów technicznych będą często miały duży wpływ na infrastrukturę dostawców usług zaufania.

Tab. 5.1 Zapisy w rozporządzeniu eIDAS mające wpływ na krajową infrastrukturę zaufania

Numer w R910/2014(eIDAS)	Treść	Propozycja uregulowania
Preambuła punkt (16)	Poziomy bezpieczeństwa powinny oznaczać stopień, w jakim można mieć zaufanie do środka identyfikacji elektronicznej przy ustalaniu tożsamości danej osoby, dając tym samym pewność, że osoba podająca daną tożsamość jest faktycznie osobą, której przypisano tę tożsamość. Poziom bezpieczeństwa zależy od stopnia zaufania, jaki ten środek identyfikacji elektronicznej zapewnia co do podawanej lub zgłaszanej tożsamości danej osoby, przy uwzględnieniu procesów (na przykład potwierdzanie i weryfikacja tożsamości oraz uwierzytelnianie), działań zarządczych (na przykład jednostka wydająca środek identyfikacji elektronicznej i procedura wydawania takiego środka) oraz stosowanych zabezpieczeń technicznych. W wyniku wielkoskalowych projektów pilotażowych finansowanych na szczeblu unijnym, standaryzacji i działań międzynarodowych istnieją różne techniczne definicje i opisy poziomów bezpieczeństwa. W szczególności wielkoskalowy projekt pilotażowy STORK i ISO 29115 odnoszą się między innymi do poziomów 2, 3 i 4, które powinny być szczególnie brane pod uwagę przy ustalaniu minimalnych technicznych wymogów, standardów i procedur dotyczących niskiego, średniego i wysokiego poziomu bezpieczeństwa w rozumieniu niniejszego rozporządzenia, przy zapewnieniu spójnego stosowania niniejszego rozporządzenia, w szczególności w odniesieniu do wysokiego poziomu bezpieczeństwa związanego z potwierdzeniem tożsamości do celów wydania kwalifikowanych certyfikatów. Ustanowione wymogi powinny być neutralne pod względem technologicznym. Spełnienie niezbędnych wymogów bezpieczeństwa powinno być możliwe za pomocą różnych technologii.	
(26)	Ze względu na tempo zmian technologicznych w niniejszym rozporządzeniu należy przyjąć podejście otwarte na innowacje.	Oznacza to, że w przypadku postępu technicznego wskazane jest korzystanie z certyfikowanych nowszych rozwiązań w stosunku infrastruktury technicznej w tym kart kryptograficznych, nowych standardów np. uwzględniających rozwiązania mobilne.
(62)	Aby zapewnić bezpieczeństwo kwalifikowanych elektronicznych znaczników czasu, niniejsze rozporządzenie powinno wprowadzić wymóg używania zaawansowanej pieczęci elektronicznej lub zaawansowanego podpisu elektronicznego lub innych równoważnych metod. Można przewidzieć, że dzięki innowacjom mogą powstać nowe technologie, które mogą zapewnić znacznikom czasu równoważny poziom bezpieczeństwa. W każdym przypadku, gdy używana jest metoda inna niż zaawansowana pieczęć elektroniczna lub zaawansowany podpis elektroniczny, do kwalifikowanego dostawcy usługi zaufania powinno należeć wykazanie w raporcie z oceny zgodności, że taka	j.w.

Numer w R910/2014(eIDAS)	Treść	Propozycja uregulowania
	metoda zapewnia równoważny poziom bezpieczeństwa i spełnia obowiązki określone w niniejszym rozporządzeniu.	
Artykuł 19 Wymogi w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania	1. Kwalifikowani i niekwalifikowani dostawcy usług zaufania przyjmują odpowiednie środki techniczne i organizacyjne w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych przez nich usług zaufania. Przy uwzględnieniu najnowszych osiągnięć w dziedzinie technologii środki te zapewniają poziom bezpieczeństwa współmierny ze stopniem ryzyka. W szczególności należy podjąć środki zapobiegające incydentom związanym z bezpieczeństwem lub minimalizujące ich wpływ oraz należy informować zainteresowane strony o negatywnych skutkach wszelkich takich incydentów. 2. Kwalifikowani i niekwalifikowani dostawcy usług zaufania, bez zbędnej zwłoki, a w każdym razie nie później niż 24 godziny od otrzymania informacji o wystąpieniu zdarzenia, zawiadamiają organ nadzoru i, w stosownych przypadkach, inne właściwe podmioty, takie jak właściwy krajowy organ ds. bezpieczeństwa informacji lub organ ochrony danych, o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe.. W przypadku, gdy prawdopodobne jest, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną, na rzecz której świadczona była usługa zaufania, dostawca usług zaufania bez zbędnej zwłoki zawiadamia także tę osobę fizyczną lub prawną o tym naruszeniu bezpieczeństwa lub utracie integralności. W stosownych przypadkach, w szczególności, jeżeli naruszenie bezpieczeństwa lub utrata integralności dotyczą dwóch lub większej liczby państw członkowskich, zawiadomiony organ nadzoru powiadamia organy nadzoru w pozostałych zainteresowanych państwach członkowskich oraz ENISA. Zawiadomiony organ nadzoru podaje zaistniałe fakty do wiadomości publicznej lub nakłada taki obowiązek na dostawcę usług zaufania, w przypadku, gdy uzna, że ujawnienie naruszenia bezpieczeństwa lub utraty integralności leży w interesie publicznym. 3. Raz do roku organ nadzoru przekazuje ENISA zestawienie zawiadomień o naruszeniach bezpieczeństwa lub utraty integralności otrzymanych od dostawców usług zaufania. 4. Komisja może w drodze aktów wykonawczych: a) określić bardziej szczegółowo środki, o których mowa w ust. 1; oraz b) określić formaty i procedury, w tym również terminy, mające zastosowanie na użytek ust. 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Docelowym rozwiązaniem jest powołanie się w porządku krajowym na akta i procedury wydane do tego artykułu przez KE. Nie ma przesłanek , ze przed momentem obowiązywania odpowiedzenie akty zostaną przygotowane, chociażby z tego względu, że nie jest określony termin ich wydania. na okres przejściowy powinny zostać opracowane procedury krajowe do realizacji wymagań artykułu 19 punkt 1 jako „odpowiednie środki techniczne" i wydane jako rozporządzenie pod UoUZ odpowiednich w tym zakresie zapisów z " Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne,…." Oraz rozszerzenie zakresu stosowania tych zapisów do stosowania przez „kwalifikowanych dostawców usług zaufania"
Artykuł 24 Wymogi dla kwalifikowanych dostawców usług zaufania	1. Wydając kwalifikowany certyfikat dla usługi zaufania, kwalifikowany dostawca usług zaufania weryfikuje, za pomocą odpowiednich środków i zgodnie z prawem krajowym, tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której wydaje kwalifikowany certyfikat. Informacje, o których mowa w akapicie pierwszym, są	Docelowym rozwiązaniem jest powołanie się w porządku krajowym na akta i procedury wydane do tego artykułu przez KE. Nie ma przesłanek, ze przed momentem obowiązywania odpowiedzenie akty zostaną

Numer w R910/2014(eIDAS)	Treść	Propozycja uregulowania
	weryfikowane przez kwalifikowanego dostawcę usług zaufania albo bezpośrednio, albo polegając na stronie trzeciej zgodnie z prawem krajowym: a) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej; lub b) zdalnie, przy użyciu środka identyfikacji elektronicznej, w przypadku którego przed wydaniem kwalifikowanego certyfikatu zapewniono fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej i który spełnia wymogi określone w art. 8 w odniesieniu do średniego lub wysokiego poziomu bezpieczeństwa; lub c) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a) lub b); lub d) przy użyciu innych metod identyfikacji uznanych na szczeblu krajowym, które zapewniają pewność równoważną, pod względem wiarygodności, fizycznej obecności. Równoważna pewność musi być potwierdzona przez jednostkę oceniającą zgodność. 2. Dostawca kwalifikowanych usług zaufania świadczący kwalifikowane usługi zaufania: a) informuje organ nadzoru o wszelkich zmianach w świadczeniu kwalifikowanych usług zaufania oraz o zamiarze zaprzestania swej działalności; b) zatrudnia pracowników i, w stosownym przypadku, podwykonawców, którzy posiadają niezbędną wiedzę fachową, wiarygodność, doświadczenie i kwalifikacje i którzy przeszli odpowiednie szkolenia na temat przepisów dotyczących bezpieczeństwa i ochrony danych osobowych oraz którzy stosują procedury administracyjne i zarządcze odpowiadające europejskim lub międzynarodowym standardom; c) w odniesieniu do ryzyka związanego z odpowiedzialnością za szkody zgodnie z art. 13 utrzymuje dostateczne zasoby finansowe lub dysponuje stosownym ubezpieczeniem od odpowiedzialności zgodnie z prawem krajowym; d) przed wejściem w stosunek umowny informuje, w jasny i szczegółowy sposób, wszystkie osoby pragnące skorzystać z kwalifikowanej usługi zaufania o dokładnych warunkach korzystania z tej usługi, w tym o wszelkich ograniczeniach korzystania z niej; e) używa wiarygodnych systemów i produktów, które są chronione przed modyfikacją i zapewniają techniczne bezpieczeństwo i wiarygodność procesów przez niego obsługiwanych; f) używa wiarygodnych systemów do przechowywania przekazanych mu danych w sprawdzalnej postaci, tak aby: (i) dane były publicznie dostępne do wyszukiwania dopiero po uzyskaniu zgody osoby, do której dane się odnoszą; (ii) tylko upoważnione osoby mogły wprowadzać dane i zmiany w przechowywanych danych;	przygotowane, chociażby z tego względu, że nie jest określony termin ich wydania. na okres przejściowy powinny zostać opracowane procedury krajowe do realizacji wymagań artykułu 24, w szczególności punkt 2 litery e), f), g),h), j),k) , punkty 3 i 4 w zakresie **wymagań do infrastruktury** wydane jako rozporządzenie pod UoUZ odpowiednich w tym zakresie zapisów z ”Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne” Oraz rozszerzenie zakresu stosowania tych zapisów do stosowania przez „kwalifikowanych dostawców usług zaufania”

Numer w R910/2014(eIDAS)	Treść	Propozycja uregulowania
	(iii)można było sprawdzać autentyczność danych; g) podejmuje odpowiednie środki zapobiegające fałszowaniu i kradzieży danych; h) rejestruje i udostępnia przez odpowiedni okres, w tym po zaprzestaniu działalności przez kwalifikowanego dostawcę usług zaufania, wszelkie odpowiednie informacje dotyczące danych wydanych i otrzymanych przez kwalifikowanego dostawcę usług zaufania, w szczególności do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług. Rejestracja może odbywać się drogą elektroniczną; i) ma aktualny plan zakończenia działalności, aby zapewnić ciągłość usług zgodnie z przepisami zweryfikowanymi przez organ nadzoru na mocy art. 17 ust. 4 lit. i); j) zapewnia zgodne z prawem przetwarzanie danych osobowych zgodnie z dyrektywą 95/46/WE; k) w przypadku kwalifikowanych dostawców usług zaufania wydających kwalifikowane certyfikaty – tworzy i aktualizuje bazę danych dotyczącą certyfikatów. 3. Jeżeli kwalifikowany dostawca usług zaufania wydający kwalifikowane certyfikaty postanowi unieważnić certyfikat, rejestruje on takie unieważnienie w swojej bazie danych dotyczącej certyfikatów i publikuje informację o statusie unieważnienia certyfikatu w odpowiednim czasie, ale w każdym razie w ciągu 24 godzin po otrzymaniu wniosku. Unieważnienie staje się skuteczne natychmiast po jego opublikowaniu. 4. W odniesieniu do ust. 3 kwalifikowani dostawcy usług zaufania wydający kwalifikowane certyfikaty dostarczają każdej stronie ufającej informacje o statusie ważności lub unieważnienia wydanych przez siebie kwalifikowanych certyfikatów. Informacje te są dostępne co najmniej na poziomie certyfikatu w automatyczny sposób, który jest wiarygodny, nieodpłatny i wydajny, w każdym momencie, także po upływie okresu ważności certyfikatu. 5. Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących wiarygodnych systemów i produktów, które spełniają wymogi określone w ust. 2 lit. e) i f) niniejszego artykułu. W przypadku gdy wiarygodne systemy i produkty spełniają te standardy, domniemywa się zgodność z wymogami określonymi w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	
ZAŁĄCZNIK I	WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW PODPISÓW ELEKTRONICZNYCH	
ZAŁĄCZNIK II	WYMOGI DLA KWALIFIKOWANYCH URZĄDZEŃ DO SKŁADANIA PODPISU ELEKTRONICZNEGO	
ZAŁĄCZNIK III	WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW PIECZĘCI ELEKTRONICZNYCH	
ZAŁĄCZNIK IV	WYMOGI DLA KWALIFIKOWANYCH CERTYFIKATÓW UWIERZYTELNIANIA WITRYN INTERNETOWYCH	

Przedstawione poniżej (patrz tab. 5.2) akty delegowane będą miały z kolei wpływ na infrastrukturę dostawców usług zaufania.

Tab. 5.2. Wyszczególnienie aktów delegowanych i wykonawczych przyjmowanych zgodnie z rozporządzeniem eIDAS mających wpływ na infrastrukturę dostawców usług zaufania.

Rozporządzenie eIDAS		**Nazwa artykułu**	**Data wydania**
art. 8 ust. 3	Do dnia 18 września 2015 r., przy uwzględnieniu odpowiednich standardów międzynarodowych i z zastrzeżeniem ust. 2, Komisja określi w drodze aktów wykonawczych minimalne techniczne specyfikacje, standardy i procedury, w odniesieniu do których określone zostaną niski, średni i wysoki poziom bezpieczeństwa dla środka identyfikacji elektronicznej do celów ust. 1. Te minimalne techniczne specyfikacje, standardy i procedury są określane przez odniesienie do wiarygodności i jakości następujących elementów: a) procedury wykazującej i weryfikującej tożsamość osób fizycznych lub prawnych wnioskujących o wydanie środka identyfikacji elektronicznej; b) procedury wydawania wnioskowanego środka identyfikacji elektronicznej; c) mechanizmu uwierzytelniania, w którym osoba fizyczna lub prawna używa środka identyfikacji elektronicznej do potwierdzenia swojej tożsamości wobec strony ufającej; d) jednostki wydającej środek identyfikacji elektronicznej; e) każdego innego organu zaangażowanego w ramach wniosku o wydanie środka identyfikacji elektronicznej; oraz f) specyfikacji technicznych i specyfikacji bezpieczeństwa wydanego środka identyfikacji elektronicznej. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Poziomy bezpieczeństwa systemów identyfikacji elektronicznej	18-09-2015
art. 12 ust. 7	Do dnia 18 marca 2015 r. Komisja ustanowi w drodze aktów wykonawczych niezbędne proceduralne warunki ułatwiania współpracy między państwami członkowskimi, o której mowa w ust. 5 i 6, w celu zapewnienia wysokiego poziomu zaufania i bezpieczeństwa, stosownie do poziomu ryzyka.	Współpraca i interoperacyjność	18-03-2015
Art.17 ust.5	Państwa członkowskie mogą wymagać, by organ nadzoru utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z warunkami określonymi w prawie krajowym.	Organ nadzoru	
art. 19 ust. 4	Komisja może w drodze aktów wykonawczych: a) określić bardziej szczegółowo środki, o których mowa w ust. 1; oraz b) określić formaty i procedury, w tym również terminy, mające zastosowanie na użytek ust. 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Wymogi w zakresie bezpieczeństwa mające zastosowanie do dostawców usług zaufania	Termin nieokreślony

Rozporządzenie eIDAS		Nazwa artykułu	Data wydania
art. 20 ust. 4	Komisja może w drodze aktów wykonawczych podać numery referencyjne następujących norm: a) norm dotyczących akredytacji jednostek oceniających zgodność i dotyczących raportu z oceny zgodności, o którym mowa w ust. 1; b) norm dotyczących zasad audytów, zgodnie z którymi jednostki oceniające zgodność będą przeprowadzać oceny zgodności kwalifikowanych dostawców usług zaufania, o których mowa w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Nadzór nad kwalifikowanymi dostawcami usług zaufania	Termin nieokreślony
art. 21 ust. 4	Komisja może w drodze aktów wykonawczych określić formaty i procedury na użytek ust. 1 i 2. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Inicjowanie kwalifikowanej usługi zaufania	Termin nieokreślony
art. 24 ust. 5	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących wiarygodnych systemów i produktów, które spełniają wymogi określone w ust. 2 lit. e) i f) niniejszego artykułu. W przypadku gdy wiarygodne systemy i produkty spełniają te standardy, domniemywa się zgodność z wymogami określonymi w niniejszym artykule. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Wymogi dla kwalifikowanych dostawców usług zaufania	Termin nieokreślony
art. 27 ust. 4	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych podpisów elektronicznych. W przypadku gdy zaawansowany podpis elektroniczny spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych podpisów elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 26. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Podpisy elektroniczne w usługach publicznych	Termin nieokreślony
art. 27 ust. 5	Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i unijnych aktów prawnych Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych podpisów elektronicznych lub metody referencyjne, w przypadku gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Podpisy elektroniczne w usługach publicznych	18-09-2015
art. 28 ust. 6	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów podpisów elektronicznych. W przypadku gdy kwalifikowany certyfikat podpisu elektronicznego spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku I. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Kwalifikowane certyfikaty podpisów elektronicznych	Termin nieokreślony
art. 29 ust. 2	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych urządzeń do składania podpisu elektronicznego. Jeżeli kwalifikowane urządzenie do składania podpisu elektronicznego spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku II. Te akty wykonawcze przyjmuje się zgodnie z procedurą	Wymogi dla kwalifikowanych urządzeń do składania podpisu elektronicznego	Termin nieokreślony

Rozporządzenie eIDAS		Nazwa artykułu	Data wydania
	sprawdzającą, o której mowa w art. 48 ust. 2.		
art. 30 ust. 3	3. Certyfikacja, o której mowa w ust. 1, opiera się na następujących elementach: a) procedurze oceny bezpieczeństwa, przeprowadzanej zgodnie z jedną z norm dotyczących oceny bezpieczeństwa produktów informatycznych uwzględnionych na liście sporządzonej zgodnie z akapitem drugim; lub b) procedurze innej niż procedura, o której mowa w lit. a), pod warunkiem że w procedurze tej stosuje się porównywalne poziomy bezpieczeństwa i podmiot publiczny lub prywatny, o którym mowa w ust. 1, zgłosi tę procedurę Komisji. Procedura ta może zostać zastosowana wyłącznie w razie braku norm, o których mowa w lit. a), lub gdy procedura oceny bezpieczeństwa, o której mowa w lit. a), wciąż trwa. Komisja sporządza w drodze aktów wykonawczych listę norm dotyczących oceny bezpieczeństwa produktów informatycznych, o których mowa w lit. a). Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2	Certyfikacja kwalifikowanych urządzeń do składania podpisu elektronicznego	Termin nieokreślony
art. 30 ust. 4	Komisja jest uprawniona do przyjmowania aktów delegowanych, zgodnie z art. 47, dotyczących ustanowienia specjalnych kryteriów, które muszą spełniać wyznaczone podmioty, o których mowa w ust. 1 niniejszego artykułu.	Certyfikacja kwalifikowanych urządzeń do składania podpisu elektronicznego	Termin nieokreślony
art. 31 ust. 3	Komisja może w drodze aktów wykonawczych określić formaty i procedury mające zastosowanie na użytek ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Publikacja listy certyfikowanych kwalifikowanych urządzeń do składania podpisu elektronicznego	Termin nieokreślony
art. 32 ust. 3	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących walidacji kwalifikowanych podpisów elektronicznych. Jeżeli walidacja kwalifikowanych podpisów elektronicznych spełnia te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Wymogi dla walidacji kwalifikowanych podpisów elektronicznych	Termin nieokreślony
art. 33 ust. 2	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej usługi walidacji, o której mowa w ust. 1. W przypadku gdy usługa walidacji kwalifikowanych podpisów elektronicznych spełnia te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych	Termin nieokreślony

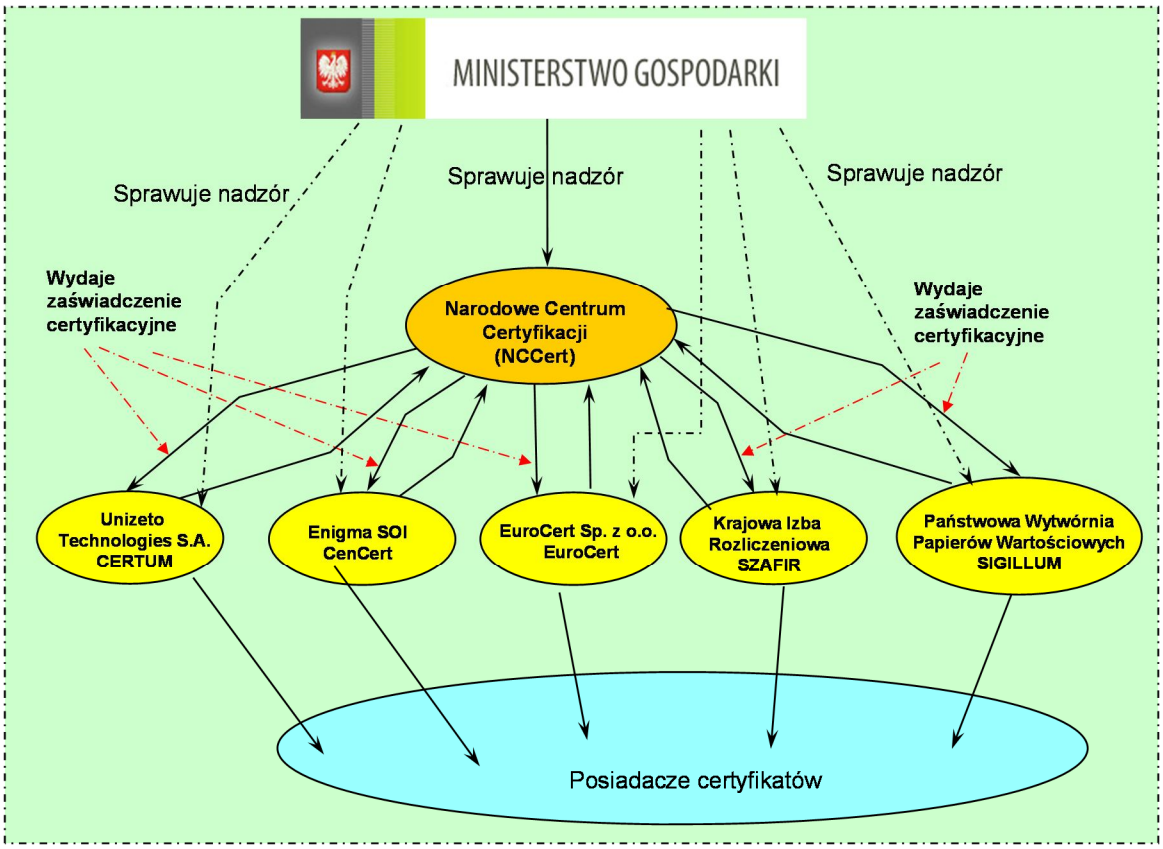
Rozporządzenie eIDAS		Nazwa artykułu	Data wydania
art. 34 ust. 2	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych. W przypadku gdy ustalenia w zakresie kwalifikowanej usługi konserwacji kwalifikowanych podpisów elektronicznych spełniają te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych	Termin nieokreślony
art. 37 ust. 4	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących zaawansowanych pieczęci elektronicznych. W przypadku gdy zaawansowana pieczęć elektroniczna spełnia te normy, domniemywa się zgodność z wymogami dotyczącymi zaawansowanych pieczęci elektronicznych, o których mowa w ust. 1 i 2 niniejszego artykułu i w art. 36. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Pieczęcie elektroniczne w usługach publicznych	Termin nieokreślony
art. 37 ust. 5	Do dnia 18 września 2015 r. i przy uwzględnieniu istniejących praktyk, standardów i aktów prawnych Unii Komisja określa w drodze aktów wykonawczych formaty referencyjne zaawansowanych pieczęci elektronicznych lub metody referencyjne, w przypadku gdy używane są formaty alternatywne. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Pieczęcie elektroniczne w usługach publicznych	18-09-2015
art. 38 ust. 6	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów pieczęci elektronicznych. W przypadku gdy kwalifikowany certyfikat pieczęci elektronicznej spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku III. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Kwalifikowane certyfikaty pieczęci elektronicznej	Termin nieokreślony
art. 42 ust. 2	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących powiązania daty i czasu z danymi oraz precyzyjnych źródeł czasu. W przypadku gdy powiązanie daty i czasu z danymi i precyzyjne źródło czasu spełniają te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Wymogi dla kwalifikowanych elektronicznych znaczników czasu	Termin nieokreślony
art. 44 ust. 2	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących procedur wysyłania i otrzymywania danych. W przypadku gdy proces wysyłania i otrzymywania danych spełnia te normy, domniemywa się zgodność z wymogami określonymi w ust. 1. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.	Wymogi dla kwalifikowanych usług rejestrowanego doręczenia elektronicznego	Termin nieokreślony
art. 45 ust. 2	Komisja może w drodze aktów wykonawczych podać numery referencyjne norm dotyczących kwalifikowanych certyfikatów uwierzytelniania witryn internetowych. W przypadku gdy kwalifikowany certyfikat uwierzytelniania witryn internetowych spełnia te normy, domniemywa się zgodność z wymogami określonymi w załączniku IV. Te	Wymogi dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych	Termin nieokreślony

Rozporządzenie eIDAS		Nazwa artykułu	Data wydania
	akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.		

5.2.2 Zmiany w krajowej infrastrukturze centrów certyfikacji

W skład funkcjonującej obecnie w Polsce infrastruktury zaufania wchodzi urząd główny NCCert oraz podporządkowane mu kwalifikowane urzędy certyfikacji. Urzędy te tworzą dwupoziomową infrastrukturę zaufania, w której na poziomie pierwszym znajduje się urząd główny, zaś na poziomie drugim kwalifikowane urzędy certyfikacji (patrz rys. 5.1). Kwalifikowane podmioty świadczące usługi certyfikacyjne wydają certyfikaty kwalifikowane posiadaczom certyfikatów (subskrybentom lub jeszcze inaczej – użytkownikom końcowym).

Dwupoziomowa hierarchiczna infrastruktura zaufania wynika z przepisów zawartych w Rozporządzeniu Ministra Gospodarki w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem (Dz.U.2002.128.1101 z dnia 9 sierpnia 2002 r.). Zgodnie z tym rozporządzeniem urząd główny NCCert, działający z upoważnienia w imieniu ministra właściwego do spraw gospodarki, wystawia sobie zaświadczenie (nazywane autozaświadczeniem), którego autentyczność jest potwierdzona za pomocą poświadczenia złożonego przez NCCert. Od tego momentu NCCert na każde żądanie ministra właściwego do spraw gospodarki wydaje zaświadczenie certyfikacyjne kwalifikowanemu urzędowi certyfikacji, znajdującemu się na drugim poziomie hierarchicznej infrastruktury zaufania. Zaświadczenie to jest tworzone i poświadczane przez NCCert niezwłocznie po uprzednim dokonaniu przez ministra właściwego do spraw gospodarki wpisu podmiotu odpowiedzialnego za funkcjonowanie kwalifikowanego urzędu certyfikacji do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Dodatkowo, w momencie aktualizacji zaświadczenia certyfikacyjnego kwalifikowanego podmiotu świadczącego usługi certyfikacyjne, ustawodawca przewidział także konieczność wydawania przez ten podmiot dwóch zaświadczeń certyfikacyjnych (idea tego typu aktualizacji jest zgodna z wymaganiem opisanym w specyfikacji technicznej [RFC4210].



Rys. 5.1 Kwalifikowana infrastruktura zaufania w Polsce (stan na dzień 15 grudnia 2014 r.)

W obecnej krajowej infrastrukturze zaufania zarówno główny urząd certyfikacji NCCert, jak również kwalifikowane urzędy certyfikacji urzędy są osobami prawnymi. W rozporządzeniu eIDAS w art.3 pkt. 20 wprowadzono pojęcie kwalifikowanego dostawcy usług zaufania, które zdefiniowano następująco:

> **kwalifikowany dostawca usług zaufania** oznacza dostawcę usług zaufania, który świadczy przynajmniej jedną kwalifikowaną usługę zaufania i któremu status kwalifikowany nadał organ nadzoru;

przy czym:

> **dostawca usług zaufania** oznacza osobę fizyczną lub prawną, która świadczy przynajmniej jedną usługę zaufania, jako kwalifikowany lub niekwalifikowany dostawca usług zaufania.

Z definicji tych wynika, że rolę głównego lub podrzędnego urzędu certyfikacji może pełnić osoba prawna lub fizyczna. Jest to zgodne także wymogami określonymi w rozporządzeniu eIDAS dla kwalifikowanych certyfikatów podpisów elektronicznych (Załącznik I), dla kwalifikowanych certyfikatów pieczęci elektronicznych (III) oraz dla kwalifikowanych certyfikatów uwierzytelniania witryn internetowych (Załącznik IV). Zgodnie z tymi wymaganiami wymienione kwalifikowane certyfikaty powinny zawierać m.in. zaawansowany podpis elektroniczny lub zaawansowaną pieczęć elektroniczną wydającego kwalifikowanego dostawcy usług zaufania.

W związku z przedstawionymi powyżej uwagami należy zauważyć, że:

- rolę zaświadczeń wydawanych kwalifikowanym dostawcom usług zaufania będą pełnić certyfikaty pieczęci elektronicznej (w przypadku osób prawnych) lub certyfikaty podpisu elektronicznego (w przypadku osób fizycznych);

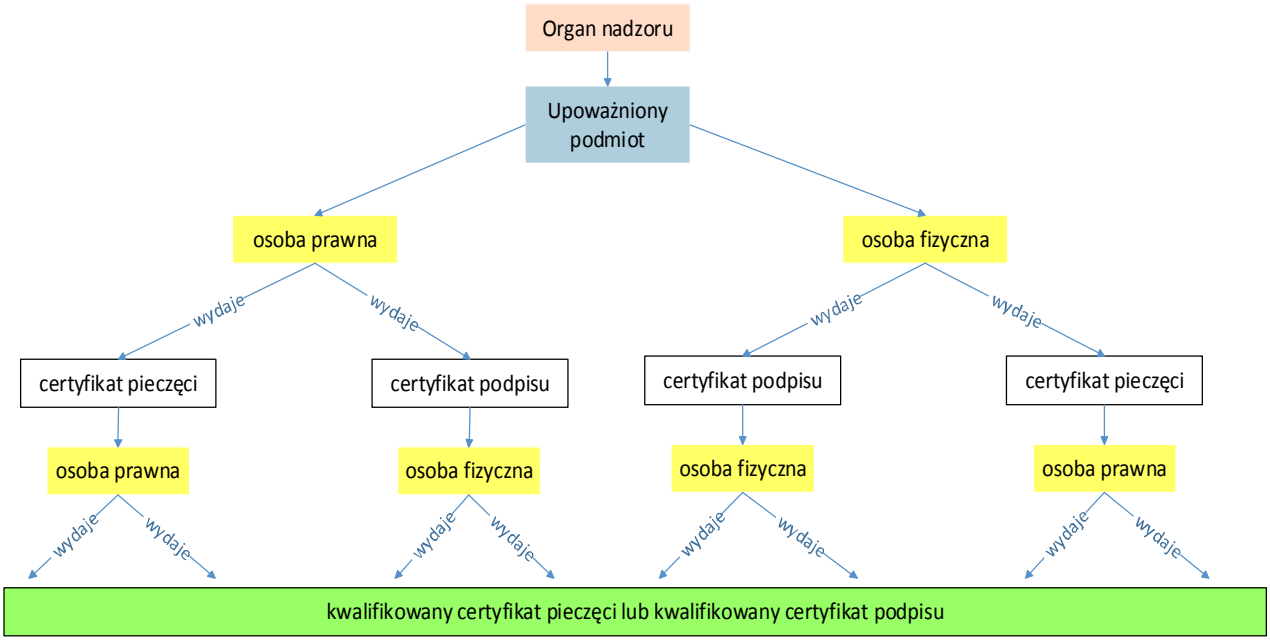
- rolę auto-zaświadczeń wydawanych sobie przez główne urzędy certyfikacji będą pełnić auto-certyfikaty pieczęci elektronicznych (w przypadku osób prawnych) lub auto-certyfikaty podpisu elektronicznego (w przypadku osób fizycznych);
- certyfikaty i auto-certyfikaty pieczęci elektronicznej oraz certyfikaty podpisu elektronicznego wystawiane przez osoby prawne będą poświadczane za pomocą zaawansowanej pieczęci elektronicznej;
- z kolei certyfikaty pieczęci elektronicznej oraz certyfikaty i auto-certyfikaty podpisu elektronicznego wystawiane przez osoby fizyczne będą poświadczane za pomocą zaawansowanego podpisu elektronicznego.

W efekcie powielenie obecnej krajowej hierarchicznej infrastruktury z głównym urzędem certyfikacji będzie wymagało rozważenia czterech możliwych przypadków (patrz rys. 5.2):

(1) podmiotem upoważnionym przez organ nadzoru jest **osoba prawna**, kwalifikowanym dostawcą usług zaufania jest także **osoba prawna**;
(2) podmiotem upoważnionym przez organ nadzoru jest **osoba prawna**, kwalifikowanym dostawcą usług zaufania jest z kolei **osoba fizyczna**;
(3) podmiotem upoważnionym przez organ nadzoru jest **osoba fizyczna**, kwalifikowanym dostawcą usług zaufania jest z kolei **osoba prawna**;
(4) podmiotem upoważnionym przez organ nadzoru jest **osoba fizyczna**, kwalifikowanym dostawcą usług zaufania jest także **osoba fizyczna**;

Jeśli przyjąć, że po wejściu w życie rozporządzenia eIDAS nadal będzie obowiązywała dwupoziomowa infrastruktura zaufania, to główny urząd certyfikacji NCCert może nadal działać z upoważnienia krajowego organu nadzoru, tj. ministra właściwego do spraw gospodarki i wystawiać kwalifikowanym dostawcom usług zaufania certyfikaty pieczęci (w przypadku, gdy dostawca jest osobą prawną) lub certyfikaty podpisu (w przypadku, gdy dostawca jest osobą prawną).

Uwaga 1. Kwalifikowany dostawca usług zaufania powinien wystawiać kwalifikowane certyfikaty podpisu elektronicznego lub kwalifikowane certyfikaty pieczęci elektronicznej weryfikowane za pomocą różnych certyfikatów wystawionych temu dostawcy przez upoważniony podmiot. Oba typy kwalifikowanych certyfikatów muszą być wystawiane w ramach różnych polityk certyfikacji.



Rys. 5.2 Możliwe warianty krajowej dwupoziomowej hierarchicznej kwalifikowanej infrastruktury zaufania po wejściu w życie rozporządzenia eIDAS

Uwaga 2. Organ nadzoru może pełnić swoją rolę w ramach scentralizowanej struktury nadzoru przedstawionej w rozdz. 4.3.1. Koordynator nadzoru (MG) może pełnić nadzór z MAiC lub z innymi organami administracji publicznej (np. Ministerstwem Spraw Wewnętrznych) nad określonymi kwalifikowanymi dostawcami usług zaufania, którym certyfikaty wystawia główny urząd certyfikacji NCCert. Takie rozwiązanie zapewni zbudowanie jednej krajowej kwalifikowanej infrastruktury zaufania.

Rodzi się jednak pytanie, czy główny urząd certyfikacji NCCert powinien wystawiać certyfikaty podpisu kwalifikowanym dostawcom usług zaufania, którzy są osobami fizycznymi? Co więcej, czy krajowa infrastruktura zaufania powinna wspierać wszystkie cztery przypadki pokazane na rys. 5.2? Problem ten można rozstrzygnąć na podstawie art. 17 ust. 5 rozporządzenia eIDAS:

> Państwa członkowskie mogą wymagać, by organ nadzoru utworzył, utrzymywał i aktualizował infrastrukturę zaufania zgodnie z warunkami określonymi w prawie krajowym.

W oparciu o ten zapis infrastrukturę zaufania proponujemy zdefiniować w ustawie o usługach zaufania lub w towarzyszącym jej rozporządzeniu. Dodatkowo, ponieważ w rozporządzeniu eIDAS nie określono, kto wystawia certyfikat podmiotowi świadczącemu usługę kwalifikowaną, to można rozważyć dwie infrastruktury zaufania: hierarchiczną dwupoziomową infrastrukturę zaufania oraz niezależne jednopoziomowe domeny zaufania.

- Hierarchiczna dwupoziomowa infrastrukturę zaufania (model hierarchiczny) może odpowiadać obecnej infrastrukturze zaufania, tj. głównym będzie urząd certyfikacji NCCert, który będzie wystawiać certyfikaty pieczęci kwalifikowanym dostawcom usług zaufania, będącymi osobami prawnymi.
- Niezależne jednopoziomowe domeny zaufania (model wyspowy) będą składały się tylko z kwalifikowanych dostawców usług zaufania podlegających bezpośrednio krajowemu organowi nadzoru, tj. ministrowi właściwemu do spraw gospodarki. W tym przypadku kwalifikowanymi dostawcami usług zaufania mogłyby być zarówno podmioty prawne, jak również fizyczne.

Pierwsza propozycja infrastruktury zaufania ma tą zaletę, że funkcjonuje już od 2002 roku i jest dobrze znana zarówno dostawcom usług, jak również konsumentom tych usług. Jej dostosowanie do wymagań rozporządzenia eIDAs nie powinno być zbyt uciążliwe i ograniczy się raczej do zmian na poziomie terminologii oraz polityk i kodeksów postępowania certyfikacyjnego. Scentralizowana infrastruktura z głównym urzędem certyfikacji NCCert, funkcjonującym w ramach Narodowego Banku Polskiego pozwala na centralne zarządzanie certyfikatami wydawanymi kwalifikowanym dostawcom usług zaufania oraz ich weryfikowanie względem jednego wspólnego punktu zaufania.

Zaletą drugiego typu infrastruktury jest przede wszystkim możliwość świadczenia kwalifikowanych usług zaufania zarówno przez osoby prawne, jak również osoby fizyczne oraz brak konieczności budowania ścieżek certyfikacji. W tego typu zdecentralizowanym modelu zaufania (nazywanym także wyspowym modelem zaufania) wszyscy kwalifikowani dostawcy usług zaufania wystawialiby sobie auto-certyfikaty (pieczęci lub podpisu), które umieszczane byłyby następnie na liście usług zaufania (TSL). Z kolei wadą tego rozwiązania może być konieczność szybkiego aktualizowania list TSL, zwłaszcza w przypadku unieważnienia któregoś z auto-certyfikatów, oraz rozstrzygnięcie problemu, kto będzie poświadczał autentyczność list TSL. Dodatkowo jednopoziomowa infrastruktura zaufania, ale z wieloma punktami zaufania może wymagać zmian w istniejących aplikacjach generowania i weryfikowania podpisu elektronicznego.

W ekspertyzie z roku 2012 przedstawionej w [MG2014] przytoczono stanowisko Narodowego Banku Polski (NBP), który zwracał uwagę, że rozporządzenie eIDAS nie reguluje funkcjonowania hierarchicznej struktury urzędów certyfikacji (brak urzędu głównego), a jedynie listy TSL. *Przy założeniu, że wybór formy prawnej unijnego rozporządzenia nie pozwala zasadniczo na uszczegółowienie/suplementowanie krajowymi przepisami, cała krajowa infrastruktura może zawisnąć w regulacyjnej pustce. Co więcej, w niektórych krajach (np. we Włoszech), stosowane są tylko listy TSL i nie ma głównego urzędu certyfikacji. Zasadne jest więc pytanie, czy pod rządami rozporządzenia tak właśnie ma wyglądać infrastruktura nadzorcza w państwie członkowskim? Co to oznacza dla polskiej kwalifikowanej*

infrastruktury PKI, gdyby zaszła konieczność likwidacji urzędu głównego, jako komponentu nieprzewidzianego przepisami prawa?

Obawy NBP nie znalazły odzwierciedlenia w finalnej wersji rozporządzenia eIDAS – rozwiewa je wspomniany powyżej art.3 pkt. 20, zgodnie z którym infrastrukturę zaufania kraje członkowskie mogą uregulować zgodnie z warunkami określonymi w prawie krajowym. Nadal jednak pozostaje pytanie, czy *należy utrzymać urząd główny skoro są dostępne listy TSL?* W odpowiedzi na to pytanie - postawione podczas pisania tej ekspertyzy - Narodowy Bank Polski stwierdził, co następuje:

Zdaniem NBP, rozwiązanie z root'em jest lepsze – jest to rozwiązanie „klasyczne", pozwalające na centralne zarządzanie, w którym występuje tylko jeden punkt zaufania. W przypadku TSL mamy listę równoległych „root'ów", w której każdy podmiot świadczący usługi certyfikacyjne posiada swój autocertyfikat, a nie certyfikat podpisany przez root'a – aktualnie przez NBP. Powyższa *sytuacja powoduje, że wzrasta ilość zaświadczeń, których nie da się unieważnić w klasyczny sposób, tzn. umieścić na liście CRL. Jedyna informacja o unieważnieniu to zmiana statusu na liście TSL.*

Zdaniem NBP, na chwilę obecną lista TSL nie jest wystarczająco zaufanym narzędziem by oprzeć na nim całą infrastrukturę klucza publicznego, gdyż np. nie ma przepisów określających „czas reakcji", czyli maksymalny czas, po którym zmiana statusu musi być odzwierciedlona na liście TSL.

Stanowisko NBP jest bardzo praktyczne i odzwierciedla obecną infrastrukturę zaufania. Co więcej każdy kraj członkowski ma prawa wybrać taki model zaufania, który mu odpowiada. Takie oczekiwanie wynika z art. 17 ust. 5 rozporządzenia eIDAS, a także z następującego zapisu:

> Preambuła (28). W celu zapewnienia porównywalnego poziomu bezpieczeństwa kwalifikowanych usług zaufania wszystkie państwa członkowskie powinny stosować wspólne podstawowe wymogi dotyczące nadzoru. Aby ułatwić spełnianie tych wymogów w jednolity sposób w całej Unii, państwa członkowskie powinny przyjąć porównywalne procedury i powinny wymieniać się informacjami na temat swoich działań nadzorczych oraz najlepszymi praktykami stosowanymi w tej dziedzinie.

Z drugiej strony rozporządzenia eIDAS bardzo mocno wzmacnia znaczenie list zaufania:

> Preambuła (45). Aby umożliwić efektywne zainicjowanie procedury, która powinna doprowadzić do umieszczenia kwalifikowanych dostawców usług zaufania i świadczonych przez nich kwalifikowanych usług zaufania **na zaufanych listach**, należy dążyć do nawiązania wstępnych interakcji między potencjalnymi kwalifikowanymi dostawcami usług zaufania a właściwym organem nadzoru w celu ułatwienia należytej staranności niezbędnej do świadczenia kwalifikowanych usług zaufania.
>
> Preambuła (46) **Zaufane listy** są podstawowym elementem procesu budowania zaufania wśród operatorów rynku, ponieważ wskazują kwalifikowany status dostawcy usługi podczas nadzoru.

Z preambuły (46) wynika, że podstawowym mechanizmem identyfikowania kwalifikowanego statusu dostawcy usługi jest lista zaufania. Element ten musi w takim razie wystąpić obligatoryjnie w krajowej infrastrukturze zaufania. Teoretycznie można więc zrezygnować z głównego urzędu certyfikacji, ale wystawca takiej listy musi zagwarantować, że certyfikaty związane z usługa zaufania są ważne w momencie pobierania ich z listy TSL. To ostatnie wymaganie można osłabić w przypadku, gdy listy zaufania zostaną wzmocnione przez krajową infrastrukturę zaufania opartą na modelu hierarchicznym.

5.2.3 Zmiany infrastruktury dostawców usług zaufania, w tym infrastruktury, którą powinny dysponować podmioty, aby realizować usługi wymienione w katalogu eIDAS

W ramach przedstawionej w rozdz. 5.1.2 podstawowej dwupoziomowej hierarchicznej infrastruktury zaufania świadczone powinny być dwie usługi:

(1) kwalifikowana usługa tworzenia, weryfikacji i walidacji kwalifikowanych certyfikatów podpisu elektronicznego;
(2) kwalifikowana usługa tworzenia, weryfikacji i walidacji kwalifikowanych certyfikatów pieczęci elektronicznej.

W ramach tej samej infrastruktury mogą być świadczone pozostałe usługi zaufania należące do katalogu usług zaufania przewidzianych przez rozporządzenie eIDAS (patrz także rozdz. 5.1.1). Są to:

(1) kwalifikowana usługa tworzenia, weryfikacji i walidacji kwalifikowanych certyfikatów uwierzytelniania witryn internetowych;
(2) kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych;
(3) kwalifikowana usługa konserwacji kwalifikowanych podpisów elektronicznych;
(4) kwalifikowana usługa walidacji kwalifikowanych pieczęci elektronicznych;
(5) kwalifikowana usługa konserwacji kwalifikowanych pieczęci elektronicznych;
(6) kwalifikowana usługa tworzenia kwalifikowanych elektronicznych znaczników czasu;
(7) kwalifikowana usługa rejestrowanego doręczenia elektronicznego.

W obecnie obowiązującej polskiej ustawie o podpisie elektronicznym nazwano wprost praktycznie dwie usługi kwalifikowane (patrz np. [MG2012]): wydawanie kwalifikowanych certyfikatów i kwalifikowanych znaczników czasu. Niemniej niektórzy usługodawcy widzieli celowość wprowadzenia nowych usług związanych z bezpieczeństwem transakcji elektronicznych, takich jak walidacja danych, poświadczenie odbioru i przedłożenia, archiwa elektroniczne, czy też wydawania certyfikatów atrybutów. Usługi te, mimo, że niewskazane wprost w ustawie, zostały uznane przez krajowy organ nadzorczy na gruncie ustawy jako usługi inne związane z podpisem elektronicznym. Usługi te są świadczone praktycznie na bardzo małą skalę, co częściowo wynika z braku odpowiedniego prawnego umocowania tych usług w przepisach prawnych. Pewien wyjątek stanowią tu usługi walidacji, na które w sposób naturalny następuje wzrost zapotrzebowania wraz ze wzrostem zastosowania podpisu elektronicznego. Rozporządzenie eIDAS poprzez jawne nazwanie usług kwalifikowanych pozwala usunąć nie tylko pewne wątpliwości prawne, ale również mentalne, wyrażane w stosunku do usług innych niż wydawanie certyfikatów.

Z rys. 5.2 wynika, że kwalifikowani dostawcy usług zaufania dotyczących tworzenia, weryfikacji i walidacji kwalifikowanych certyfikatów podpisu elektronicznego, kwalifikowanych certyfikatów pieczęci elektronicznej oraz kwalifikowanych certyfikatów uwierzytelniania witryn internetowych (usługi (1) – (3) z przedstawionej powyżej listy usług) znajdują się na drugim poziomie infrastruktury zaufania i będą świadczyć usługi w oparciu o certyfikaty pieczęci wystawione przez upoważniony podmiot (tj. przez główny urząd certyfikacji NCCert). Urząd NCCert jest przystosowany do wykonywania tego typu czynności, stąd nie ma potrzeby wprowadzania zamian do istniejącej infrastruktury zaufania.

Podobnie jest z pozostałymi usługami (4) – (10), które kwalifikowani dostawcy usług zaufania będą mogli świadczyć po otrzymaniu certyfikatu pieczęci od urzędu NCCert. Do świadczenia niektórych spośród tych usług przystosowane są także kwalifikowane lub niekwalifikowane podmioty działające obecnie na rynku polskim. Dotyczy to w szczególności usługi walidacji certyfikatów i podpisu elektronicznego, usługi wydawania certyfikatów uwierzytelniania witryn internetowych, usługi generowania znaczników czasu, usługi archiwizowania i konserwacji podpisu elektronicznego.

Należy zauważyć, że rozporządzenie eIDAS wprowadza zamknięty katalog kwalifikowanych usług zaufania na poziomie unijnym, ale dopuszcza otwarty katalog innych usług zaufania, które na poziomie państw członkowskich mogą być uznane za usługi kwalifikowane (patrz Preambuła (25)).

> Preambuła (25). Państwa członkowskie powinny zachować swobodę określania innych rodzajów usług zaufania oprócz tych, które figurują w zamkniętym wykazie usług zaufania przewidzianym w niniejszym rozporządzeniu, do celów uznania ich na szczeblu krajowym jako kwalifikowanych usług zaufania.

Możliwość ta jest o tyle istotna, że w Polsce na rynku w praktyce dostępne są inne usługi kwalifikowane zaufania[32] niż te, które znajdują się w zamkniętym wykazie usług zdefiniowanym w rozporządzeniu eIDAS. Są to tzw. usługi nienazwane, które co prawda nie zostały uregulowane w przepisach ustawy o podpisie elektronicznym, ale jednocześnie nie zostały one przez prawo zniesione, uchylone czy zabronione. Z chwilą uchylenia przepisów ustawy o podpisie elektronicznym należy zachować otwarty charakter krajowego wykazu kwalifikowanych usług zaufania, umieszczając w ustawie o usługach zaufania zapis podobny do zapisu z ustawy o podpisie elektronicznym:

> Usługi zaufania – usługi zdefiniowane w rozporządzeniu eIDAS oraz inne usługi związane z podpisem elektronicznym, pieczęcią elektroniczną lub uwierzytelnianiem witryn internetowych.

Tego typu definicja wpisuje się w oczekiwania preambuły (26) rozporządzenia eIDAS oraz powinna pozwolić na zakwalifikowanie nowych lub istniejących usług nienazwanych do usług kwalifikowanych.

> Preambuła (26). Ze względu na tempo zmian technologicznych w niniejszym rozporządzeniu należy przyjąć podejście otwarte na innowacje.

5.2.4 Jedna, dwie, a może więcej krajowych hierarchicznych infrastruktur zaufania?

Rozporządzenie eIDAS określa wymagania nakładane przede wszystkim na kwalifikowanych dostawców usług zaufania. Dostawcy ci funkcjonują w obrębie krajowej kwalifikowanej infrastruktury zaufania i podlegają nadzorowi organu lub organów nadzoru wskazanych przez państwo członkowskie (patrz preambuła (30)). Poza kwalifikowaną infrastrukturą nadzoru mogą funkcjonować niekwalifikowani dostawcy usług zaufania, którzy *powinni podlegać łagodnym i reaktywnym działaniom nadzorczym ex post* (patrz Preambuła (36)).

> Preambuła (30). Państwa członkowskie powinny wyznaczyć organ nadzoru lub organy nadzoru do celów prowadzenia działań nadzorczych na mocy niniejszego rozporządzenia. Państwa członkowskie powinny także mieć możliwość podjęcia decyzji, za obopólnym porozumieniem z innym państwem członkowskim, w sprawie wyznaczenia organu nadzoru na terytorium tego innego państwa członkowskiego.
>
> Preambuła (36). Ustanowienie systemu nadzoru dla wszystkich dostawców usług zaufania powinno zapewnić jednakowe zasady dotyczące bezpieczeństwa i rozliczalności ich operacji i usług, przyczyniając się w ten sposób do ochrony użytkowników i do funkcjonowania rynku wewnętrznego. Niekwalifikowani dostawcy usług zaufania powinni podlegać łagodnym i reaktywnym działaniom nadzorczym ex post, uzasadnionym przez charakter ich usług i operacji. Organ nadzoru nie powinien zatem mieć ogólnego obowiązku nadzorowania niekwalifikowanych dostawców usług. Organ nadzoru powinien podejmować działania wyłącznie wtedy, gdy został poinformowany (na przykład przez samego niekwalifikowanego dostawcę usług zaufania, przez inny organ nadzoru, w drodze zgłoszenia od użytkownika lub partnera handlowego lub na podstawie własnego dochodzenia), że niekwalifikowany dostawca usług zaufania nie spełnia wymogów niniejszego rozporządzenia.

Teoretycznie krajowa kwalifikowana infrastruktura zaufania może być nadzorowana przez więcej niż jeden organ nadzoru. W praktyce nie musi to oznaczać, że z każdym organem nadzoru może być związana jedna lub więcej kwalifikowanych infrastruktur zaufania. Łatwo jednak zauważyć, że kwalifikowane infrastruktury zaufania nadzorowane przez różne organy nadzoru będą od siebie niezależne i może istnieć pokusa do tworzenia wyspowych lub hierarchiczne modele zaufania.

[32] Przykładami takich usług są usługi poświadczania odbioru i przedłożenia oraz poświadczenie rejestrowe i repozytoryjne.

W rozdz. 4.3.1 zaproponowano scentralizowany schemat nadzoru nad dostawcami (w tym przede wszystkim nad kwalifikowanymi dostawcami) usług zaufania. Kwalifikowani dostawcy usług zaufania powinni - biorąc pod uwagę propozycję z rozdz. 5.1.2 – funkcjonować w ramach dwupoziomowej hierarchicznej infrastruktury zaufania z jednym głównym urzędem certyfikacji NCCert, nad którą nadzór będzie koordynowany przez Ministerstwo Gospodarki. Pozostali dostawcy usług zaufania powinni działać poza tą infrastrukturą.

Jeśli proponowany scentralizowany schemat nadzoru nie zostanie zaakceptowany w ustawie o usługach zaufania, to mogą powstać zdecentralizowane niezależne schematy nadzoru. Na przykład, Ministerstwo Gospodarki może nadzorować usługi zaufania, których dostawcami są firmy komercyjne, zaś Ministerstwo Administracji i Cyfryzacji będzie sprawowało nadzór nad usługami zaufania, których dostawcami jest administracja rządowa. **Takie rozwiązanie jest do zaakceptowania tylko w przypadku, gdy administracja rządowa będzie świadczyła usługi zaufania wyłącznie na własne potrzeby (tzw. usługi zamknięte, patrz rozdz. 5.4.1)**. Usługi tego typu są wyłączone spod działania rozporządzenia eIDAS, co oznacza, że w szczególności nie mogą być kwalifikowanymi usługami zaufania.

Na uzasadnienie powyższej propozycji można przedstawić m. in. następujące argumenty:

- dostawcy otwartych usług zaufania (zarówno kwalifikowanych, jak również niekwalifikowanych) podlegają wymaganiom określonym w rozporządzeniu eIDAS (patrz preambuła (35)); stąd niewywiązywanie się przez rządowych dostawców usług zaufania z wymagań wynikających z rozporządzenia eIDAs, z ustawy o usługach zaufania oraz innych krajowych rozporządzeń może skutkować dużymi karami nakładanymi na dostawców rządowych, których skutki będą ponosić polscy podatnicy (patrz preambuła (37));
- jeśli administracja rządowa będzie kwalifikowanym lub niekwalifikowanym dostawcą otwartych usług zaufania, to systemy rządowe, które będą korzystały z kwalifikowanych lub niekwalifikowanych usług zaufania i tak będą musiały akceptować użytkowników usług kwalifikowanych i niekwalifikowanych świadczonych przez firmy komercyjne; inaczej przeczyłoby to idei równego traktowania dostawców usług i obywateli oraz idei konkurencyjności na rynku usług zaufania;
- administracja jest stroną w wielu sporach z obywatelami, firmami, instytucjami, itp.; stąd sytuacja, w której administracja rządowa byłaby jednocześnie dostawcą otwartych usług zaufania byłaby dwuznaczna i może prowadzić do konfliktu interesów organu będącego dostawą otwartych usług zaufania.

Uwaga 1. Te same argumenty można odnieść także do sytuacji, gdy rządowi dostawcy usług zaufania będą działali w ramach scentralizowanego schematu nadzoru z hierarchiczną kwalifikowaną infrastrukturą zaufania.

Wniosek. Administracja rządowa może świadczyć kwalifikowane i niekwalifikowane usługi zaufania tylko za pośrednictwem firm, które będą działały na zasadach rynkowych i będą dostępne dla wszystkich użytkowników (tj. będą usługami otwartymi). W pozostałych przypadkach usługi zaufania mogą być tylko usługami zamkniętymi.

> Preambuła (35). Wszyscy dostawcy usług zaufania powinni podlegać wymogom niniejszego rozporządzenia, w szczególności wymogom dotyczącym bezpieczeństwa i odpowiedzialności, aby zapewnić należytą staranność, przejrzystość i rozliczalność ich operacji i usług. Biorąc jednak pod uwagę rodzaj usług świadczonych przez dostawców usług zaufania, należy, w odniesieniu do tych wymogów, dokonać rozróżnienia między kwalifikowanymi i niekwalifikowanymi dostawcami usług zaufania.
>
> Preambuła (37). Niniejsze rozporządzenie powinno przewidywać odpowiedzialność wszystkich dostawców usług zaufania. W szczególności ustanawia system odpowiedzialności, w ramach którego wszyscy dostawcy usług zaufania powinni być odpowiedzialni za szkody wyrządzone osobie fizycznej lub osobie prawnej w związku z niewypełnieniem obowiązków na mocy niniejszego rozporządzenia. (…)

Uwaga 2. W § 3, ust. 1 Zarządzenia Ministra Zdrowia z dnia 25 marca 2014 r. *w sprawie powołania Zespołu do spraw wdrożenia karty ubezpieczenia zdrowotnego i karty specjalisty medycznego* zapisano, że do zadań Zespołu należy m.in.: *1) przygotowanie rozwiązań w zakresie funkcjonalności elektronicznej karty ubezpieczenia zdrowotnego (eKUZ) i karty specjalisty medycznego (KSM) oraz infrastruktury Narodowego Funduszu Zdrowia (Infrastruktura Klucza Publicznego) i świadczeniodawców - bezpieczne czytniki umożliwiające złożenie podpisu elektronicznego za pomocą*

eKUZ i KSM. Z opublikowanych ostatnio propozycji zmian w ustawie o systemie informacji w ochronie zdrowia oraz innych ustaw (stan na dzień 28 luty 2015 r.) wynika, że w ramach infrastruktury PKI NFZ wydawane będą certyfikaty kwalifikowane i niekwalifikowane. Certyfikaty te będą instalowane na kartach eKUZ, KSM i KSA (karta specjalisty administracyjnego). Czy można zatem przyjąć, że kwalifikowane usługi zaufania świadczone przez PKI NFZ są zamkniętymi usługami świadczonymi? Z dyskusji przedstawionej w rozdz. 5.5.1 wynika, że tego typu usługi są usługami otwartymi i tym samym podlegają wymaganiom określonym w rozporządzeniu eIDAS. Dodatkowo, biorąc pod uwagę przedstawiony powyżej wniosek, należy założyć, że usługi te powinny być świadczone za pośrednictwem firm, które będą działały na zasadach rynkowych (zasada ta powinna dotyczyć także usług niekwalifikowanych w przypadku, gdy PKI NFZ nie świadczy ich jedynie na potrzeby własne).

5.2.5 Propozycje

Na podstawie analizy przestawionej w rozdz. 5.1.2 proponujemy, aby w ustawie o usługach zaufania lub powiązanych z nią rozporządzeniach:

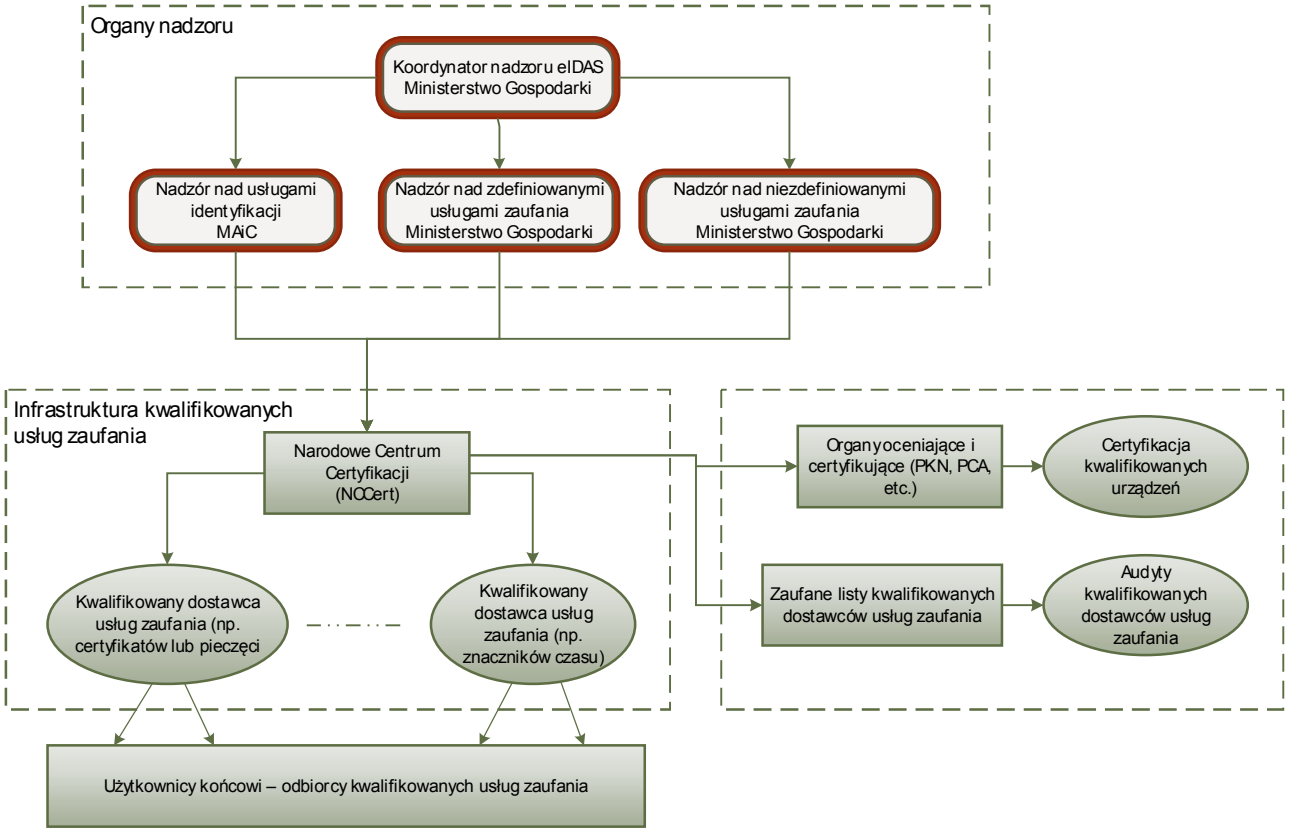
1) pozostawić obecną dwupoziomową hierarchiczną kwalifikowaną infrastrukturę zaufania, w której głównym urzędem certyfikacji byłby nadal NCCert zarządzany z upoważnienia ministra właściwego do spraw gospodarki przez Narodowy Bank Polski; NBP oraz NCCert bardzo dobrze sprawdził się w tej roli i nie ma powodów, aby zastępować go innym podmiotem; przyjęcie takiego rozwiązania nie będzie wymagało wprowadzenia istotnych zmian na każdym z dwóch poziomów infrastruktury zaufania, w tym przede wszystkim na poziomie kwalifikowanych podmiotów świadczących obecnie usługi certyfikacyjne;
2) opcjonalnie należy dopuścić tworzenie dodatkowych jedno- lub dwupoziomowych kwalifikowanych infrastruktur zaufania nadzorowane przez wskazany lub wskazane organy nadzoru; nadzór sprawowany przez te organy powinien być koordynowany przez Ministerstwo Gospodarki (patrz rozdz. 4.3.1);
3) role kwalifikowanych dostawców usług zaufania w krajowej infrastrukturze zaufania, zwłaszcza w zakresie wydawania i unieważniania certyfikatów podpisu elektronicznego, powierzyć tylko osobom prawnym; daje to gwarancję większej stabilności krajowej infrastruktury zaufania oraz ułatwia egzekwowanie odpowiedzialności podmiotu za swoje działania;
4) urząd główny (NCCert) oraz kwalifikowanych dostawców usług zaufania wyposażyć w certyfikaty pieczęci; stąd NCCert będzie poświadczał certyfikaty pieczęci wydawane kwalifikowanym dostawcom usług zaufania za pomocą zaawansowanej pieczęci, zaś kwalifikowane certyfikaty podpisu lub pieczęci wydawane użytkownikom końcowym przez kwalifikowanych dostawców usług będą poświadczane za pomocą zaawansowanej pieczęci elektronicznej;
5) wskazać profile certyfikatów pieczęci, profile podpisu, profile kwalifikowanych certyfikatów pieczęci, profile kwalifikowanych certyfikatów podpisu oraz profile kwalifikowanych certyfikatów uwierzytelniania witryn internetowych; co więcej, wystawcy certyfikatów (zwłaszcza certyfikatów kwalifikowanych) powinni obligatoryjnie umieszczać w polu polityki każdego certyfikatu właściwego identyfikatora polityki certyfikacji; identyfikatory te lub sposoby ich tworzenia są wskazane w następujących specyfikacjach technicznych:

   (a) EN 319 411-1 *Policy and security requirements for Trust Service Providers issuing certificates; Part 1: Policy requirements for Certification Authorities issuing web site certificates*;
   (b) EN 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates*;
   (c) EN 319 411-3 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates*;

6) jawnie wskazać NCCert jako podmiot odpowiedzialny za zarządzanie krajową listą usług zaufania (TSL); jednocześnie rozważyć przyjęcie możliwości umieszczania na liście TSL jedynie auto-certyfikatu urzędu NCCert

oraz auto-certyfikatów głównych urzędów certyfikacji dodatkowych kwalifikowanych infrastruktur zaufania (patrz propozycja 2)); rozwiązanie takie uprości listę TSL; w przeciwnym przypadku istnieje ryzyko, że przy dużej lub nawet bardzo dużej liczbie kwalifikowanych dostawców usług zaufania lista TSL będzie bardzo obszerna i trudna w zarządzaniu; należy zauważyć, że umieszczanie na liście TSL certyfikatów wszystkich kwalifikowanych dostawców usług zaufania ma sens tylko wtedy, gdy krajowa infrastruktura zaufania oparta byłaby na wyspowym modelu zaufania (lista TSL pełni wówczas także rolę listy certyfikatów unieważnionych CRL); w przypadku proponowanego podtrzymania hierarchicznej infrastruktury zaufania listę CRL kwalifikowanych dostawców usług zaufania publikuje zawsze NCCert i obecność listy TSL w tej roli można ograniczyć jedynie do certyfikatu głównego urzędu NCCert.

Powyższe propozycje zobrazowano na rys. 5.3. Rysunek ten ilustruje infrastrukturę zaufania w ramach, której świadczone powinny być kwalifikowane usługi zaufania. Kwalifikowane usługi zaufania nadzorowane są przez Ministerstwo Gospodarki, pełniące rolę koordynatora nadzoru (patrz propozycja z rozdz. 4.3.1). Nadzorcy akredytują kwalifikowanych dostawców usług zaufania za pośrednictwem Narodowego Centrum Certyfikacji (NCCert).



Rys. 5.3 Propozycja hierarchicznego kwalifikowanej infrastruktury zaufania na tle schematu nadzoru w Polsce

Dodatkowo, ponieważ od 17 września 2014 roku powinny być stosowane art. 28 ust. 6, art. 38 ust. 6 oraz art. 45 ust. 2, proponujemy, aby numery referencyjne norm dotyczących kwalifikowanych certyfikatów podpisów elektronicznych, kwalifikowanych certyfikatów pieczęci elektronicznych oraz kwalifikowanych certyfikatów uwierzytelniania witryn internetowych wskazać w rozporządzeniu wydanym na podstawie delegacji wynikającej z ustawy o usługach zaufania, chyba, że do tego czasu Komisja wyda odpowiednie akty wykonawcze. Podobne rozwiązanie proponujemy zastosować w przypadku pozostałych kwalifikowanych usług zaufania należących do katalogu usług zaufania wskazanych w rozporządzeniu eIDAs.

5.3 Określenie zmian, które będą niezbędne w dokumentacji centrów certyfikacji w związku z wejściem rozporządzenia eIDAS

Podstawowymi dokumentami regulującymi funkcjonowanie upoważnionego podmiotu NCCert oraz kwalifikowanych dostawców usług zaufania są i nadal będą polityka certyfikacji (ang. *Certificate Policy*, CP) oraz kodeks postępowania

certyfikacyjnego (ang. *Certificate Policy Statement*, CPs). Dokumenty te opisują usługi oraz zasady ich świadczenia, obowiązki i odpowiedzialność stron świadczących oraz korzystających z usług, profile certyfikatów, list CRL oraz wystawianych poświadczeń.

Zmiany, które należy wprowadzić w dokumentacji typu CP i CPS można podzielić na trzy kategorie:

1) nowe usługi kwalifikowane;
2) zmiany profili certyfikatów;
3) zmiany wymagań nakładanych na podmioty kwalifikowane;
4) zmiany terminologiczne.

Dla każdej nowej usługi kwalifikowanej w CP i CPS należy określić wymagania nakładane na kwalifikowanego dostawcę usługi zaufania. Wymagania te zależą od typu usługi i są określone w rozporządzeniu eIDAs oraz dodatkowo zostaną zdefiniowane w związanych z nim aktach delegowanych oraz aktach wykonawczych. W przypadku świadczenia przez podmiot kwalifikowany podstawowych usług zaufania, tj. wydawania kwalifikowanych certyfikatów pieczęci, kwalifikowanych certyfikatów podpisu, kwalifikowanych certyfikatów uwierzytelniania witryn internetowych oraz kwalifikowanych znaczników czasu, pod uwagę należy wziąć następujące normy techniczne:

(a) EN 319 401 *General Policy Requirements for Trust Service Providers supporting Electronic Signatures*
(b) EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services*
(c) EN 319 411-1 *Policy and security requirements for Trust Service Providers issuing certificates; Part 1: Policy requirements for Certification Authorities issuing web site certificates*
(d) EN 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates*
(e) EN 319 411-3 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates*
(f) EN 319 412-1 *Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 1: Overview and common data structures*
(g) EN 319 412-2 *Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons*
(h) EN 319 412-3 *Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 3: Certificate Profile for certificates issued to legal persons*
(i) EN 319 412-4 *Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 4: Certificate Profile for TLS/SSL certificates issued to organisations*
(j) EN 319 412-5 *Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Qualified Certificate Statements for Qualified Certificate*

Zmiany profili kwalifikowanych certyfikatów podpisu elektronicznego mogą wynikać z konieczności zachowania zgodności z profilami zdefiniowanymi w normach EN 319 412-1, EN 319 412-2 i EN 319 412-5. Podobne zmiany mogą dotyczyć profili kwalifikowanych certyfikatów uwierzytelniania witryn internetowych oraz kwalifikowanych znaczników czasu (odpowiednio normy EN 319 411-1 i EN 319 421).

Kolejna kategoria wprowadzanych zmian może mieć na celu zachowanie przez dostawcę usługi wymagań nakładanych na podmioty kwalifikowane. Ponieważ w polskiej ustawie o podpisie elektronicznym oraz w związanych z nią rozporządzeniach wymagania nakładane na kwalifikowanych dostawców usług zaufania są raczej restrykcyjne, stąd zmiany w istniejących CP i CPS nie powinny być znaczące.

Ostatnia grupa zmian wynika z wprowadzenia nowych pojęć w rozporządzeniu eIDAs. Dotyczy to w szczególności braku w rozporządzeniu pojęcia zaświadczenia i poświadczenia certyfikacyjnego oraz bezpiecznego urządzenia do weryfikacji podpisu, wprowadzenia pojęcia zaawansowanego podpisu elektronicznego, pieczęci elektronicznej (w tym

pieczęci zaawansowanej i kwalifikowanej), certyfikatu podpisu elektronicznego oraz certyfikatu pieczęci. Lista tych pojęć powinna być uważnie przejrzana i uwzględniona w dokumentach CP i CPS.

Uwaga 1. Należy zauważyć, że wymienione powyżej kategorie zmian muszą być uwzględnione także w CP i CPS określających funkcjonowanie urzędu NCCert.

Uwaga 2. Zgodnie z art. 21, ust.1 rozporządzenia eIDAS (patrz ramka poniżej) kwalifikowany dostawca usługi jest zobowiązany do przeprowadzenia identyfikacji podmiotu, na rzecz którego świadczy usługę. Mechanizmy weryfikacji podmiotu powinny być określone w krajowej ustawie o usługach zaufania.

Artykuł 24 Wymogi dla kwalifikowanych dostawców usług zaufania

1. Wydając kwalifikowany certyfikat dla usługi zaufania, kwalifikowany dostawca usług zaufania weryfikuje, za pomocą odpowiednich środków i zgodnie z prawem krajowym, tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej lub prawnej, której wydaje kwalifikowany certyfikat.

Informacje, o których mowa w akapicie pierwszym, są weryfikowane przez kwalifikowanego dostawcę usług zaufania albo bezpośrednio, albo polegając na stronie trzeciej zgodnie z prawem krajowym (…).

5.4 Wpływ eIDAS na aplikacje do składania podpisu, sposób składania podpisu i znakowania czasem

5.4.1 Dostępność dla osób niepełnosprawnych

Rozporządzenie eIDAS wskazuje, iż usługi zaufania i produkty tych usług powinny być dostępne dla osób niepełnosprawnych.

Preambuła (29). Zgodnie z obowiązkami wynikającymi z Konwencji Narodów Zjednoczonych o prawach osób niepełnosprawnych, zatwierdzonej decyzją Rady 2010/48/WE (1), w szczególności art. 9 tej konwencji, osoby niepełnosprawne powinny mieć możliwość korzystania z usług zaufania i produktów przeznaczonych dla użytkownika końcowego stosowanych do świadczenia tych usług na równych zasadach z innymi konsumentami. Dlatego, gdy jest to wykonalne, świadczone usługi zaufania i produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług powinny być dostępne dla osób niepełnosprawnych. Ocena wykonalności powinna obejmować między innymi względy techniczne i gospodarcze.

Artykuł 15 **Dostępność dla osób niepełnosprawnych**
Gdy jest to wykonalne, świadczone usługi zaufania i produkty przeznaczone dla użytkownika końcowego stosowane do świadczenia tych usług są dostępne dla osób niepełnosprawnych.

Na dzień dzisiejszy ustawodawstwo krajowe (*Rozporządzenie Rady Ministrów, z dnia 12 kwietnia 2012r., w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych,* par. 19) zobowiązuje podmioty realizujące zadania publiczne, do dostosowania w systemach teleinformatycznych prezentacji zasobów informacji do wytycznych dotyczących ułatwień w dostępie do treści publikowanych w Internecie (Web Content Accessibility Guidelines WCAG 2.0), do dnia 15 maja 2015 r. Także ustawodawstwo krajowe gwarantuje częściowo realizację wymagań z artykułu 15 eIDAS. Nie jest to pełna realizacja postulatu z artykułu 15, gdyż wymagania nałożone przez Krajowe Ramy Interoperacyjności dotyczą wyłącznie prezentacji zasobów informatycznych na stronach WWW w systemach teleinformatycznych podmiotów realizujących zadania publiczne. Nie obejmują więc m.in. aplikacji przeznaczonych dla użytkownika końcowego, wytworzonych przez Zaufanego Usługodawcę, nie będącego przedstawicielem administracji publicznej. Dostawcy usług zaufania zarówno z sektora publicznego jak i prywatnego powinni więc w procesie projektowania uwzględnić wymagania grupy osób niepełnosprawnych. W rozporządzeniu eIDAS nie ma zapisów o prowadzonych przez Komisję pracach nad aktami wykonawczymi, które mogłyby określić stosowne specyfikacje techniczne.

5.4.2 Znak zaufania UE dla kwalifikowanych usług zaufania

Preambuła (47) Zaufanie do usług *online* i ich wygoda mają podstawowe znaczenie dla użytkowników, by mogli w pełni korzystać z zalet usług elektronicznych i świadomie na tych usługach polegali. W tym celu należy stworzyć unijny znak zaufania, aby oznaczać kwalifikowane usługi zaufania świadczone przez kwalifikowanych dostawców usług zaufania. Unijny znak zaufania dotyczący kwalifikowanych usług zaufania pozwoliłby na wyraźne odróżnienie kwalifikowanych usług zaufania od innych usług zaufania, przyczyniając się tym samym do przejrzystości na rynku. Używanie unijnego znaku zaufania przez kwalifikowanych dostawców usług zaufania powinno być dobrowolne i nie powinno prowadzić do jakiegokolwiek wymogu innego niż wymogi przewidziane w niniejszym rozporządzeniu.

Artykuł 23 **Znak zaufania UE dla kwalifikowanych usług zaufania**

1. Po tym jak w zaufanej liście, o której mowa w art. 22 ust. 1, wskazany zostanie status kwalifikowany, o którym mowa w art. 21 ust. 2 akapit drugi, kwalifikowani dostawcy usług zaufania mogą używać znaku zaufania UE, aby w prosty, rozpoznawalny i jasny sposób wskazać świadczone przez siebie kwalifikowane usługi zaufania.
2. Gdy kwalifikowani dostawcy usług zaufania używają znaku zaufania UE w odniesieniu do kwalifikowanych usług zaufania, o których mowa w ust. 1, zapewniają, aby na ich witrynie internetowej dostępny był link do odpowiedniej zaufanej listy.
3. Do dnia 1 lipca 2015 r. Komisja w drodze aktów wykonawczych wprowadza specyfikacje dotyczące formy, a w szczególności prezentacji, kompozycji, rozmiaru i wzoru znaku zaufania UE dla kwalifikowanych usług zaufania. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Zgodnie z zapisem w pkt. 3 artykułu 23 eIDAS, najpóźniej do dnia 1 lipca 2015 r. Usługodawcy dowiedzą się jak będzie wyglądał znak zaufania UE dla kwalifikowanych usług zaufania. Na dzień dzisiejszy wiadomo, że będzie to jeden z pośród 3 znaków, wyłonionych w publicznym konkursie ogłoszonym przez KE latem 2014r.:

Rys. 5.4 Propozycje dla znaku zaufania UE

W planowanym akcie wykonawczym znajdą się informacje na temat prezentacji, kompozycji i rozmiaru znaku.

Znak zaufania UE dla kwalifikowanych usług zaufania jest jednym ze znaków, które w najbliższych latach zostaną wprowadzane w UE w obszarze usług cyfrowych. Na dzień dzisiejszy trwają pracę m.in. nad znakiem potwierdzającym zgodność z rozporządzeniem w zakresie ochrony danych osobowych ([3] artykuł 39), oraz nad europejskim znakiem zaufania w handlu elektronicznym [2].

Warto wspomnieć, że pod koniec 2012 roku, Ministerstwo Gospodarki wraz z Narodowym Centrum Certyfikacji i jednym z polskich QTSP – Unizeto Technologies SA, widząc potrzebę wyróżnienia dla użytkownika końcowego usług bazujących na europejskim systemie list TSL, podjęło próbę wprowadzenia znaku graficznego, widniejącego na witrynach internetowych tych usług (https://www.biznes.gov.pl/, http://nccert.pl/tsl.htm, https://www.webnotarius.eu/webnotariuseu/main.xml).

Rys. 5.5 Polska propozycja znaku identyfikującego usługi bazujące na europejskim systemie list TSL

Znak zaufania UE wydaje się być analogią do tych działań. Z punktu widzenia kwalifikowanego zaufanego usługodawcy posługiwanie się znakiem zaufania UE, nakłada na QTSP obowiązek umieszczenia i aktualizacji odwołań w serwisach informacyjnych do zaufanej listy TSL. Dodatkowo znak zaufania UE wywiera wpływ na stronę wizualną produktów, powinien być uwzględniany na etapie prac projektowych nad interfejsem graficznym produktu/ usługi.

Prawdziwym wyzwaniem będzie przedstawienie użytkownikowi usług w łatwy sposób. Problemem z punktu widzenia użytkownika usług jest niska czytelność/zrozumiałość list TSL. Listy są przystosowane do przetwarzania maszynowego. Zainteresowany użytkownik, który będzie chciał zweryfikować źródło pochodzenia znaku zaufania usługi, nie będzie wiedział, które informacje z listy TSL są dla niego istotne.

Żeby unijny znak zaufania spełnił swoją podstawową rolę, czyli wzmacniał zaufanie użytkowników do kwalifikowanych usług, wydaje się, że zarówno na szczeblu europejskim jak i krajowym należy uruchomić działania związane z kampanią informacyjną znaku, oraz zastanowić się nad działaniami/ systemem, który byłby odpowiedzialny za monitorowanie poprawności użycia znaku przez Usługodawców czy możliwość wniesienia zastrzeżeń związanych z niepoprawnym użyciem znaku zaufania przez użytkowników.

5.4.3 Implementacja obsługi zaufanych list w aplikacjach do składania i weryfikacji podpisów elektronicznych

Zgodnie z punktem 46 preambuły rozporządzenia eIDAS system zaufanych listy kwalifikowanych usługodawców i kwalifikowanych usług jest i będzie centralnym filarem zaufania wśród operatorów na rynku wewnątrz UE.

> Preambuła (46). Zaufane listy są podstawowym elementem procesu budowania zaufania wśród operatorów rynku, ponieważ wskazują kwalifikowany status dostawcy usługi podczas nadzoru.

Wymagania dotyczące systemu zaufanych list zostały sformułowane w artykule 22 rozporządzenia eIDAS.

> Artykuł 22 **Zaufane listy**
> 1. Każde państwo członkowskie sporządza, prowadzi i publikuje zaufane listy zawierające informacje dotyczące kwalifikowanych dostawców usług zaufania, za których jest ono odpowiedzialne, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania.
> 2. Państwa członkowskie sporządzają, prowadzą i publikują – w zabezpieczony sposób – elektronicznie podpisane lub opatrzone pieczęcią elektroniczną zaufane listy, o których mowa w ust. 1, w postaci dostosowanej do automatycznego przetwarzania.
> 3. Bez zbędnej zwłoki państwa członkowskie przekazują Komisji informacje o podmiocie odpowiedzialnym za sporządzenie, prowadzenie i publikowanie krajowych zaufanych list wraz ze szczegółowymi informacjami dotyczącymi miejsca publikacji tych list, certyfikatów użytych do podpisania lub opatrzenia pieczęcią zaufanych list i wszelkich zmian, jakie są do nich wprowadzane.
> 4. Komisja udostępnia publicznie informacje, o których mowa w ust. 3, w elektronicznie podpisanej lub opatrzonej pieczęcią elektroniczną postaci dostosowanej do automatycznego przetwarzania, używając w tym celu zabezpieczonego kanału komunikacji.

> 5. Do dnia 18 września 2015 r. Komisja w drodze aktów wykonawczych określi informacje, o których mowa w ust. 1, oraz techniczne specyfikacje i formaty dotyczące zaufanych list mające zastosowanie na użytek ust. 1–4. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 48 ust. 2.

Zgodnie z pkt.5 artykułu 22 rozporządzenia dostawcy aplikacji zależnych od list TSL zapoznają się z treścią aktu wykonawczego do dnia 18 września 2015 roku.

System zaufanych list w UE funkcjonuje od 2009 roku, na podstawie decyzji CD 2009/767/EC, zmienionej przez CD 2010/425/EU i CD 2013/662/EU. Decyzja powołuje się na specyfikację i wymagania zawarte w TS 119 612 v1.1.1.

W końcu czerwca 2015 roku zostanie opublikowana wersja 2.1.1 tej specyfikacji i najprawdopodobniej do niej znajdą się odwołania w akcie wykonawczym.

Kolejna wersja standardu będzie wymagała wprowadzenia zmian w implementacji obsługi list TSL przez dostawców rozwiązań korzystających z list TSL. Zakres tych zmian będzie możliwy do określenia dopiero w momencie publikacji aktu wykonawczego.

Bazując na doświadczeniach usługi WebNotarius, świadczonej przez jednego z krajowych kwalifikowanych zaufanych dostawców-Unizeto Technologies SA, która to obsługuje listy TSL od początku ich wprowadzenia, należy wyraźnie zaznaczyć, że europejski system list TSL, pomimo ciągle podejmowanych przez KE wysiłków na rzecz ulepszenia tego systemu, nie osiągnął jeszcze takiego poziomu dojrzałości, który pozwoliłby zapewnić pełną transgraniczność kwalifikowanemu podpisowi elektronicznemu w krajach członkowskich UE i krajach grupy EEA.

Do głównych przyczyn tego stanu zaliczyć należy:

- brak możliwości zbudowania pełnej ścieżki certyfikacji dla weryfikowanych certyfikatów,
- brak danych dotyczących zaufanych usługodawców,
- brak kompletności opisu kwalifikowanego usługodawcy (rzetelność wypełnienia przez operatora, brak specyficznych informacji w standardzie)

Rozwiązaniem powyższych problemów jest model usługowy, który pozwala na centralne gromadzenie danych konfiguracyjnych i poprzez to na ciągłe rozszerzanie zakresu obsługiwanych TS i będących w użyciu rodzajów podpisów elektronicznych. Ponadto w modelu usługowym możliwe jest delegowanie żądań do innych usługodawców, poprzez co dodatkowo minimalizowane jest ryzyko nieobsłużenia żądania przesłanego do usługi. Model usługowy zarówno dla weryfikacji certyfikatu jak i weryfikacji podpisu elektronicznego został zaproponowany i przetestowany w LSP PEPPOL.

Przydatnym narzędziem do monitorowania aktualnego stanu list wskazanych w liście list publikowanej przez Komisję Europejską (KE) jest portal dostępny pod adresem: http://eutsl.3xasecurity.com/tools/index.jsp

Należy jednak zauważyć, że nie jest to oficjalne narzędzie KE. Nikt nie daje gwarancji poprawności i ciągłości jego działania. Jest jednak jedynym narzędziem umożliwiającym stosunkowo proste przeszukanie interesujących informacji z list TSL krajów członkowskich. Informacje te zawsze powinny być możliwe do potwierdzenia na źródłowej liście.

5.5 Inne problemy techniczne

5.5.1 Otwarte i zamknięte usługi zaufania

W Preambule (21) usługi zaufania podzielono na usługi zamknięte i otwarte. Pojęcia te należy rozumieć następująco:

1) zamknięte usługi zaufania oznaczają zestaw usług zaufania świadczonych na rzecz określonej, dobrze zdefiniowanej grupy użytkowników i niemających skutków dla stron trzecich;

2) otwarte usługi zaufania oznaczają zestaw usług zaufania świadczonych na rzecz społeczeństwa (ang. to the public) i mające skutki dla stron trzecich.

Preambuła (21). W niniejszym rozporządzeniu należy również ustanowić ogólne ramy prawne dotyczące korzystania z usług zaufania. Nie należy jednak wprowadzać ogólnego obowiązku korzystania z nich ani instalowania punktu dostępu dla wszystkich istniejących usług zaufania. W szczególności niniejsze rozporządzenie nie powinno obejmować świadczenia usług wykorzystywanych wyłącznie w obrębie **systemów zamkniętych** przez określoną grupę uczestników i niemających skutków dla stron trzecich. Wymogom niniejszego rozporządzenia nie powinny na przykład podlegać systemy utworzone w przedsiębiorstwach lub administracjach publicznych w celu zarządzania procedurami wewnętrznymi przy użyciu usług zaufania. **Wymogi określone w rozporządzeniu powinny spełniać jedynie usługi zaufania świadczone na rzecz społeczeństwa, mające skutki dla stron trzecich**. Niniejsze rozporządzenie nie powinno również obejmować aspektów związanych z zawieraniem i ważnością umów lub innych obowiązków prawnych, w przypadku, gdy istnieją wymogi dotyczące formy wprowadzone na mocy prawa krajowego lub unijnego. Dodatkowo nie powinno ono mieć wpływu na krajowe wymogi w zakresie formy dotyczące rejestrów publicznych, w szczególności rejestrów handlowych i rejestrów gruntów.

Przedstawiony podział usług pozwala na określenie granicy pomiędzy usługami zaufanymi podlegającymi nadzorowi i wymaganiom rozporządzenia eIDAS (usługi otwarte), a usługi zaufania świadczonymi poza nadzorem i działaniem rozporządzenia eIDAS. Rozgraniczenie to jest wprost wskazane w art.2 ust.2.

Rozporządzenie eIDAS, art. 2, ust. 2. Niniejsze rozporządzenie nie ma zastosowania do świadczenia usług zaufania wykorzystywanych wyłącznie w obrębie zamkniętych systemów wynikających z prawa krajowego lub z porozumień zawartych przez określoną grupę uczestników.

Podleganie lub niepodleganie wymaganiom rozporządzenia eIDAS ma istotne znaczenie dla podmiotów, które są zainteresowane świadczeniem usług zaufania tylko na własne wewnętrzne potrzeby. Podstawowym czynnikiem odróżniającym otwarte usługi zaufania od usług zamkniętych jest wpływ ich skutków na strony trzecie. Brak takiego wpływu usługi zaufania na osoby trzecie stanowi więc podstawę do zaliczenia takiej usługi do zamkniętej usługi zaufania (patrz definicja poniżej).

Zamknięte usługi zaufania – są to usługi zaufania świadczone na podstawie zawartej umowy, porozumienia lub oświadczenia dla dobrze zdefiniowanej grupy użytkowników, których skutki dotyczą tylko członków tej grupy, a ewentualne spory rozstrzygane są w oparciu o regulamin pracy, politykę bezpieczeństwa firmy, zasady świadczenia usługi zaufania lub inne uregulowania przyjęte i akceptowane przez członków grupy.

Dobre zdefiniowanie grupy użytkowników, do których jest adresowana usługa zaufania można uzyskać albo poprzez wyliczenie wszystkich członków grupy albo podanie reguły przynależności do grupy. Przykładami takich reguł mogą być przynależność zawodowa (np. komornicy, radcy prawni), przynależność do tej samej korporacji lub wspólne zainteresowania. O takiej grupie możemy mówić, że jest grupą zamkniętą, jeśli istnieją formalne lub nieformalne bariery uniemożliwiające lub utrudniające przyłączenie się do tej grupy podmiotów z zewnątrz, zaś skutki usług zaufania nie wykraczają poza członków tej grupy.

W szczególności wymogom rozporządzenia eIDAS *nie powinny na przykład podlegać systemy utworzone w przedsiębiorstwach lub administracjach publicznych w celu zarządzania procedurami wewnętrznymi przy użyciu usług zaufania*. Za zamknięte usługi zaufania należy zatem uważać tylko takie usługi, które są świadczone w obrębie określonej instytucji na rzecz pracowników lub innych osób powiązanych z instytucją oraz na rzecz zabezpieczeń systemów tej instytucji.

Przykład 1. Narodowy Bank Polski (NPB) ma swój system PKI i wydaje certyfikaty dla swoich *klientów*, którymi są zarówno jednostki budżetowe, jak również banki komercyjne i inne podmioty (np. kantory). Wydawane certyfikaty są wykorzystywane w naszych systemach informatycznych NPB. Wymienione podmioty (tj. NBP, jednostki budżetowe,

banki komercyjne, kantory, itp.) stanowią zamkniętą grupę podmiotów tworzoną w oparciu o pewne formalne zasady utrudniające przyjęcie do grupy dowolnego podmiotu. Usługa zaufania NPB świadczona jest tylko na potrzeby tej grupy i wykorzystywana tylko w obrębie systemu informatycznego NBP. Co więcej skutki tej usługi nie wykraczają poza tą grupę. Stąd usługa zaufania PKI (własny system NPB) jest zamkniętą usługą zaufania.

Przykład 2. Załóżmy, że banki komercyjne wydają certyfikaty swoim klientom w ramach bankowości elektronicznej. W tym przypadku grupa klientów jest grupą otwartą (każdy ma prawo założyć konto w banku i korzystać z bankowości elektronicznej) i skutki przynależności wykraczają poza tą grupę (np. skutki oszustwa będące efektem wykorzystania usługi zaufania mogą dotyczyć zarówno klientów banku, jak również podmioty spoza tej grupy).

Przykład 3. Gmina świadczy usługi zaufania na rzecz mieszkańców gminy, wydając im certyfikaty. Za pomocą tych certyfikatów mieszkańcy zapewniają autentyczność pism wysyłanych do gminy. W oparciu o te pisma urzędnicy gminy podejmują decyzje, które mogą mieć wpływ na strony trzecie, np. spadkobierców mieszkających poza gminą. Łatwo zauważyć, że mieszkańców można uznać za zamknięta grupę, ale skutki świadczenia usług zaufania wykraczają poza członków tej grupy.

Przykład 4. Zgodnie z Rozporządzeniem Ministra Pracy i Polityki Społecznej z dnia 9 stycznia 2009 r. *w sprawie refundacji składek na ubezpieczenia społeczne osób niepełnosprawnych* (Dz.U. nr 8 poz. 42 z późn. zm.) wnioskodawca uwierzytelnia wnioski Wn-U-G lub Wn-U-A za pomocą podpisu elektronicznego weryfikowanego za pomocą kwalifikowanego certyfikatu lub certyfikatu dostarczonego przez Państwowy Fundusz Rehabilitacji Osób Niepełnosprawnych. Podobnie jak w przykładzie 3 grupa wnioskodawców, której PFRON wydaje certyfikaty (świadczy usługę zaufania) jest grupą zamkniętą, ale skutki tej usługi dotyczą stron trzecich. Załóżmy, że osobie uprawnionej ukradziono dane służące do uwierzytelnienia wniosku, dane te są słabej jakości i adwersarz je łatwo odtworzyć lub dane poświadczające certyfikat stosowane przez PFRON zostały przełamane. Wówczas adwersarz może uprzedzić uprawniony podmiot i w jego imieniu złożyć wniosek o refundację i otrzymać zgodnie § 10, pkt. 4 *kwot pkt. 4 refundację na wskazany przez siebie rachunek bankowy*. Skutki tej kradzieży dotyczą strony trzeciej, czyli Skarbu Państwa, który będzie musiał tą kwotę oddać uprawnionemu podmiotowi, a następnie wystąpić z roszczeniami do przestępcy (o ile uda się wykryć). W praktyce kwotę tą powinien oddać dostawca usługi zaufania w ramach gwarancji udzielonych swojemu klientowi, co jest to jeden z symptomów otwartej usługi zaufania.

Przykład 5. Systemy teleinformatyczne, o których jest mowa w art. 46 i art. 63 Kodeksu postępowania administracyjnego bazują na usługach zaufania. Usługi te nie mogą być świadczone w obrębie zamkniętych systemów teleinformatycznych, ponieważ grupa użytkowników usług zaufania nie jest grupą zamkniętą, zaś skutki tych usług mają wpływ na strony trzecie. W szczególności stwierdzenie to dotyczy usług zaufania świadczonych w ramach systemu ePUAP (patrz także dyskusja w rozdz. 5.1.4).

Przykład 6. Czy usługi zaufania (np. usługi rejestrowanego doręczenia elektronicznego, których elementem są stosowane obecnie elektroniczne skrzynki podawcze) wykorzystywane na potrzeby systemów używanych w sądownictwie (np. elektroniczne postępowanie upominawcze) są usługami zamkniętymi? Albo inaczej, czy usługi zaufania są wykorzystywane jedynie w obrębie systemu zamkniętego? Nie, ponieważ systemy udostępniane w sądownictwie i pozwalające na elektroniczne załatwianie spraw nie są systemami zamkniętymi. Należy przypomnieć, że w art. 2, ust. 2 rozporządzenia eIDAS jest mowa o systemie zamkniętym, którego integralną częścią są użytkownicy. Jest więc oczywiste, że użytkownicy korzystający, np. z systemu elektronicznego postępowania upominawczego, nie stanowią grupy zamkniętej.

Uwaga 1. W ustawie o usługach zaufania należy precyzyjnie określić pojęcie zamkniętych usług zaufania, w oparciu o którą możliwe będzie jednoznaczne wyłączenie dostawców usług zaufania (także w formie imiennej listy) spod działania rozporządzenia eIDAS, a tym samym jednoznaczne wskazanie dostawców, którzy będą podlegały wymaganiom rozporządzenia eIDAS. Co więcej tego typu definicja powoli ustrzec się wielu instytucjom (szczególnie instytucjom rządowym) przed pochopną chęcią budowania usług zaufania i świadczenia usług zaufania podmiotom w sytuacji, gdy takie usługi ewidentnie powinny być usługami otwartymi (np. usługi świadczone na rzecz petentów urzędów gminnych, pacjentów służby zdrowia, stron w postępowaniach sądowych, podmiotów dokonujących zgłoszeń celnych). Jednym z możliwych rozwiązań problemu otwartości lub zamkniętości usług zaufania może być umieszczenie

w ustawie o usługach zaufania zapisu podobnego do art. 9, ust.2 zawartego w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym. Zapis ten może mieć postać:

> Organy władzy publicznej, jednostki samorządu terytorialnego i Narodowy Bank Polski mogą świadczyć usługi certyfikacyjne wyłącznie na użytek własny.

Uwaga 2. Jeśli dostawca usługi zaufania nieprawidłowo zaliczył świadczoną usługę do zamkniętych usług zaufania, to stanowi to podstawę do zgłoszenia tego faktu organowi nadzoru. Organ ten, na podstawie otrzymanych faktów, zakresu i sposobu świadczenia usługi oraz stopnia szkodliwości oddziaływania na osoby trzecie powinien rozstrzygnąć zasadność traktowania świadczonej usługi jako usługi zamkniętej. Niepodporządkowanie się przez dostawcę usługi zaufania decyzji organu nadzoru powinno podlegać karze do zakazu świadczenia usługi włącznie.

Uwaga 3. Kwalifikowane usługi zaufania nie mogą być świadczone w obrębie systemów zamkniętych (nie są więc zamkniętymi usługami zaufania). Wynika to z definicji kwalifikowanej usługi zaufania oraz definicji kwalifikowanego dostawcy usług zaufania.

> Art. 3, pkt. 17): kwalifikowana usługa zaufania oznacza usługę zaufania, która **spełnia stosowne wymogi określone w niniejszym rozporządzeniu**;
>
> Art. 3, pkt. 20): kwalifikowany dostawca usług zaufania oznacza dostawcę usług zaufania, który **świadczy przynajmniej jedną kwalifikowaną usługę zaufania** i któremu **status kwalifikowany nadał organ nadzoru**.

5.5.2 Czy usługi zaufania świadczone przez administrację rządową pomogą w walce z cyberprzestępczością?

Często można spotkać się z opinią, że jeśli administracja ma jakieś problemy z bezpieczeństwem informacji, to najlepiej rozwiązać je za pomocą usług zaufania świadczonych przez administrację rządową.

W praktyce nieważne jest, kto jest dostawcą usług zaufania. Ważne jest, aby usługi zaufania były świadczone zgodnie z określonymi wymaganiami i pomagały rozwiązać zidentyfikowany problem bezpieczeństwa (dokładniej, eliminowały zidentyfikowaną podatność).

> **Podatność** (ang. vulnerability) – słabość w przedmiocie oceny (ang. Target of Evaluation, TOE), która w pewnym otoczeniu może być wykorzystana do naruszenia wymagań funkcjonalności zabezpieczeń (ang. Security Functional Requirements, SFR).
>
> **Podatność systemu teleinformatycznego** – właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie (wg Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz.U. z dnia 16 maja 2012 r., poz. 5261).

Na przykład, jeśli witryny rządowe są podatne na ataki naruszające ich autentyczność (tj. źródło ich pochodzenia oraz integralność udostępnianej informacji), to nie ma potrzeby budowania usługi świadczonej przez administrację rządową. Co więcej usługa ta powinna być usługą otwartą, ponieważ konsekwencje korzystania z witryny rządowej mogą mieć skutki dla stron trzecich (każdego użytkownika witryny). Stąd wystarczy wybrać rynkowego dostawcę, który wystawi odpowiedni certyfikat uwierzytelnienia witryny zgodny np. z wymaganiami Web Trust. Certyfikat taki będzie zaufany we wszystkich przeglądarkach, które wspierają specyfikację Web Trust.

Oczywiście, jeśli do wyeliminowania zidentyfikowanej podatności wystarczy lub wystarczą zamknięte usługi zaufania, to dostawcą usług zaufania może być administracja rządowa, o ile świadczenie tego typu usług będzie ekonomicznie uzasadnione. Wydaje się, że jest to jedyny przypadek, gdy sensowne jest budowanie w administracji sektorowych usług zaufania (patrz także dyskusja w rozdz. 5.1.4). W pozostałych przypadkach do wyeliminowania

zidentyfikowanych podatności można używać kwalifikowanych lub niekwalifikowanych usług zaufania powszechnie dostępnych na rynku. Podjęcie decyzji o zastosowaniu właściwej usługi zaufania (kwalifikowanej lub niekwalifikowanej) powinno być poprzedzone oceną ryzyka związanego z taką usługą i jej wpływu na poziom uzasadnienia zaufania do zaproponowanych zabezpieczeń.

5.5.3 Definiowanie zakresu stosowania certyfikatów

Należy przyjąć, że certyfikaty, których zastosowania zostały określone w rozporządzeniu eIDAS, będą wydawane zgodnie z formatem X.509, określonym w normie ISO/IEC 9594-8 [X.509]. Jeśli tak, to bardzo ważnym elementem technicznym, który powinien być uregulowany w ustawie o usługach zaufania jest odpowiednia interpretacja pola zastosowania klucza publicznego (ang. *key usage*).

Zgodnie z rozporządzeniem eIDAS dostawcy usług zaufania mogą wydawać następujące rodzaje certyfikatów:

1) kwalifikowane certyfikaty podpisu elektronicznego (kCertPodpisu);
2) niekwalifikowane certyfikaty podpisu elektronicznego (nkCertPodpisu);
3) kwalifikowane certyfikaty pieczęci elektronicznej (kCertPieczęci);
4) niekwalifikowane certyfikaty pieczęci elektronicznej (nkCertPieczęci);
5) kwalifikowane certyfikaty uwierzytelniania witryn internetowych (kCertWEB);
6) niekwalifikowane certyfikaty uwierzytelniania witryn internetowych (nkCertWEB).

Każdy z powyższych certyfikatów będzie stosowany do weryfikacji i potwierdzenia ważności podpisów elektronicznego lub pieczęci elektronicznych (zgodnie z rozporządzenie eIDAS do walidacji). Podpisy te powinny być niezaprzeczalne, potwierdzać pochodzenie i integralność danych, z którymi związany jest podpis oraz pozwalać na uwierzytelnienie osoby fizycznej. Z kolei pieczęcie elektroniczne powinny potwierdzać pochodzenie i integralność dokumentu (wynika to wprost z Preambuły (59)). Czy zatem można ją stosować do uwierzytelniania osoby prawnej? Tak, ponieważ proces uwierzytelniania bazuje na potwierdzaniu przez osobę prawną (ale także fizyczną) autentyczności[33] dokumentu (szerzej danych). Dokonywanie tego typu potwierdzeń nie jest sprzeczne z rozporządzeniem eIDAS.

> Preambuła (59). Pieczęcie elektroniczne powinny służyć jako dowód wydania danego dokumentu elektronicznego przez daną osobę prawną, dając pewność co do **pochodzenia i integralności dokumentu**.

To do czego stosowany jest podpis elektroniczny (zwykły, zaawansowany lub kwalifikowany) lub pieczęć elektroniczna (zwykła, zaawansowana lub kwalifikowana) z technicznego punktu widzenia sprowadza się do rozróżnienia poniższych przypadków:

1) niezaprzeczalności podpisu;
2) uwierzytelniania osoby fizycznej;
3) uwierzytelniania osoby prawnej;
4) autentyczności danych.

Uwaga. Proces uwierzytelniania witryny internetowej może wymagać złożenia przez system wspierający witrynę zwykłego/zaawansowanego podpisu elektronicznego (przypadek witryny pod opieką osoby fizycznej), lub zwykłej/zaawansowanej/kwalifikowanej pieczęci elektronicznej (przypadek witryny pod opieką osoby prawnej).

Najważniejszym problemem technicznym jest rozróżnienie za pomocą pola certyfikatu „keyUsage" użycia certyfikatu w procesie uwierzytelnienia (podmiotu lub danych), szyfrowania, składania podpisu lub pieczęci (w sensie ich niezaprzeczalności). Rekomendacja właściwego ustawienia bitów tego pola jest przedstawiona w najnowszej

[33] Pod pojęciem autentyczności rozumie się własność, która pozwala na określenie pochodzenia oraz integralności danych.

specyfikacji technicznej ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons" (patrz Tab. 5.1). Zgodnie z tą rekomendacją

1) certyfikaty powinny zwierać jedno i tylko jedno ustawienie pola keyUsage (profil) spośród ustawień przedstawionych w Tab. 5.1 (tj. A, B, C, D, E lub F);
2) certyfikaty stosowane do walidacji niezaprzeczalności zobowiązania wynikającego z treści podpisanej zawartości, takiego jak podpis elektroniczny złożony pod umową i/lub transakcją, powinny być zawężone do typu A, B lub F; z tych trzech typów ETSI rekomenduje stosowanie typu A
3) jeśli certyfikat jest certyfikatem kwalifikowanym, to ustawienie pola *keyUsage* musi być ograniczone do typów A, B, C, D lub F;
4) w niezaufanych środowiskach (tj. w środowiskach, w których proces składania podpisu nie jest pod całkowitą kontrolą podpisującego)) w certyfikatach podpisu nie można łączyć bitu non-*repudiation* z innymi bitami pola *keyUsage*.

Tab. 5.1 Rekomendowane ustawienia bitów pola *keyUsage* wg ETSI EN 319 412-2 (draft ze stycznia 2015 r.)

Typ	Non-Repudiation (Bit 1)	Digital Signature (Bit 0)	Key Encipherment or Key Agreement (Bit 2 or 4)
A	tak		
B	tak	tak	
C		tak	
D		tak	tak
E			tak
F	tak	tak	tak

Ponieważ pieczęć elektroniczna zapewnia możliwość walidacji **pochodzenia i integralności dokumentu** (szerzej danych), stąd w certyfikatach pieczęci nie można używać profili A, B i F, a jedynie profili C i D. Nie jest to jawnie zapisane ani w normie ETSI EN 319 412-2, ani też w ETSI EN 319 412-3 "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 3: Certificate profile for certificates issued to legal persons", ale wydaje się, że jest to logiczne i eliminuje potencjalne nieporozumienia, które mogłyby wynikać z ustawienia bitu *non-repudiation* zarówno w certyfikatach podpisu, jak również w certyfikatach pieczęci.

W Tab. 5.2 przedstawione rekomendowane przez autorów ekspertyzy profile ustawień pola *keyUsage* w certyfikatach podpisu, certyfikatach pieczęci oraz certyfikatach do uwierzytelniania witryn internetowych.

Tab. 5.2 Rekomendowane ustawienia bitów pola *keyUsage* dla różnych typów certyfikatów określonych w rozporządzeniu eIDAS

Przypadek	A	B	C	D	E	F
kwalifikowany certyfikat podpisu kwalifikowanego	tak					
kwalifikowany certyfikat podpisu zaawansowanego	tak	tak	tak	tak		
niekwalifikowany certyfikat podpisu zaawansowanego	tak	tak	tak	tak		tak
niekwalifikowany certyfikat podpisu zwykłego	tak	tak	tak	tak		tak
kwalifikowany certyfikat pieczęci			tak			

kwalifikowanej						
kwalifikowany certyfikat pieczęci zaawansowanej			tak	tak		
niekwalifikowany certyfikat pieczęci zaawansowanej			tak	tak		
niekwalifikowany certyfikat pieczęci zwykłej			tak	tak		
kwalifikowany certyfikat uwierzytelniania witryn internetowych			tak	tak		
niekwalifikowany certyfikat uwierzytelniania witryn internetowych			tak	tak		

Uwaga. Propozycje przedstawione w Tab. 5.1 i 5.2 powinny być także wzięte pod uwagę w przypadku wydawania certyfikatów na potrzeby różnych zastosowań profilu zaufanego w systemie ePUAP.

5.5.4 Jak odróżniać certyfikaty kwalifikowane?

W Tab. 5.1 (rozdz. 5.4.3) przestawiono pięć różnych typów certyfikatów kwalifikowanych. Są to:

1) kwalifikowany certyfikat podpisu kwalifikowanego;
2) kwalifikowany certyfikat podpisu zaawansowanego;
3) kwalifikowany certyfikat pieczęci kwalifikowanej;
4) kwalifikowany certyfikat pieczęci zaawansowanej;
5) kwalifikowany certyfikat uwierzytelniania witryn internetowych

Zgodnie z wymaganiami określonymi w rozporządzeniu eIDAS i zaimplementowanymi w normie ETSI EN 319 411-2: *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for Trust Service Providers issuing qualified certificates* prowadzi to do konieczności rozpatrzenia pięciu następujących przypadków:

1) kwalifikowany certyfikat podpisu kwalifikowanego musi być stosowany[34] z kwalifikowanym urządzeniem do składania podpisu elektronicznej (QSCD);
2) kwalifikowany certyfikat podpisu zaawansowanego musi być stosowany z bezpiecznym urządzeniem kryptograficznym (SCD) lub bez SCD;
3) kwalifikowany certyfikat pieczęci kwalifikowanej musi być stosowany z kwalifikowanym urządzeniem do składania pieczęci elektronicznej (QSCD);
4) kwalifikowany certyfikat pieczęci zaawansowanej z SCD lub bez SCD;
5) kwalifikowany certyfikat uwierzytelniania witryn internetowych z SCD lub bez SCD.

Bezpieczne urządzenie kryptograficzne (wg ETSI EN 319 411-1): urządzenie, które zawiera klucz prywatny użytkownika, chroni ten klucz przed ujawnieniem oraz w imieniu użytkownika wykonuje operacje podpisywania lub deszyfrowania.

Zastosowanie każdego z przedstawionych powyżej typów kwalifikowanych certyfikatów niesie za sobą różne skutki prawne. Istotna jest zatem możliwość rozróżnienia certyfikatów, a tym samym ocena ich skutków prawnych. Na rozróżnienie kwalifikowanych certyfikatów oraz kontekstu ich użycia (z QSCD, z SCD lub bez QSCD i SCD) pozwala

[34] Sformułowanie „musi być stosowany" należy rozumieć jako wymóg stosowania kwalifikowanego urządzenia podczas generowania kwalifikowanego podpisu elektronicznego. Sformułowanie to należy podobnie rozumieć w przypadku pozostałych typów certyfikatów kwalifikowanych.

zastosowanie zapisów przedstawionych w normach ETSI EN 319 411-2 i EN 319 412-5. Zgodnie z tymi zapisami w polu rozszerzenia *QCStatements*:

1) każdego kwalifikowanego certyfikatu należy umieść deklarację, że jest kwalifikowanym certyfikatem (patrz rozdz. 4.2.1 w normie EN 319 412-5);
2) kwalifikowanego certyfikatu podpisu kwalifikowanego stosownego do weryfikacji podpisu kwalifikowanego należy:
   - w polu rozszerzenia `PolicyInformation` umieścić identyfikator polityki certyfikacji o wartości `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)` (rozdz. 5.2 w ETSI EN 319 411-2);
   - w polu rozszerzenia *QCStatements* umieścić deklarację, że klucz prywatny związany z kluczem publicznym certyfikatu znajduje się w kwalifikowanym urządzeniu do składania podpisu elektronicznego, QSCD (rozdz. 4.2.2 w EN 319 412-5);
   - w polu rozszerzenia *QCStatements* umieścić deklarację, że certyfikat jest kwalifikowanym certyfikatem podpisu elektronicznego (rozdz. 4.2.3 w EN 319 412-5);
3) kwalifikowanego certyfikatu podpisu zaawansowanego stosownego do weryfikacji podpisu zaawansowanego należy:
   - w polu rozszerzenia `PolicyInformation` umieścić identyfikator polityki certyfikacji o wartości `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural (0)` (rozdz. 5.2 w ETSI EN 319 411-2);
   - w polu rozszerzenia *QCStatements* umieścić deklarację, że certyfikat jest kwalifikowanym certyfikatem UE podpisu elektronicznego (rozdz. 4.2.3 w EN 319 412-5);
4) kwalifikowanego certyfikatu pieczęci kwalifikowanej stosownego do weryfikacji kwalifikowanej pieczęci należy:
   - w polu rozszerzenia `PolicyInformation` umieścić identyfikator polityki certyfikacji o wartości `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)` (rozdz. 5.2 w ETSI EN 319 411-2);
   - w polu rozszerzenia *QCStatements* umieścić deklarację, że klucz prywatny związany z kluczem publicznym certyfikatu znajduje się w kwalifikowanym urządzeniu do składania pieczęci elektronicznej, QSCD (rozdz. 4.2.2 w EN 319 412-5);
   - w polu rozszerzenia *QCStatements* umieścić deklarację, że certyfikat jest kwalifikowanym certyfikatem pieczęci elektronicznej (rozdz. 4.2.3 w EN 319 412-5);
5) kwalifikowanego certyfikatu pieczęci zaawansowanej stosownego do weryfikacji zaawansowanej pieczęci należy:
   - w polu rozszerzenia `PolicyInformation` umieścić identyfikator polityki certyfikacji o wartości `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-legal (1)` (rozdz. 5.2 w ETSI EN 319 411-2);
   - w polu rozszerzenia *QCStatements* umieścić deklarację, że certyfikat jest kwalifikowanym certyfikatem UE pieczęci elektronicznej (rozdz. 4.2.3 w EN 319 412-5);
6) kwalifikowanego certyfikatu uwierzytelniania witryn internetowych stosownego w procesie uwierzytelniania witryny internetowej:
   - w polu rozszerzenia `PolicyInformation` umieścić identyfikator polityki certyfikacji o wartości `itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-web (2)` (rozdz. 5.2 w ETSI EN 319 411-2);
   - w polu rozszerzenia *QCStatements* umieścić deklarację, że certyfikat jest kwalifikowanym certyfikatem UE uwierzytelniania strony interentowej (rozdz. 4.2.3 w EN 319 412-5);

Kwalifikowane certyfikaty, które zawierają m.in. informacje wymienione powyżej w punktach 2) - 6) będziemy nazywać kwalifikowanymi certyfikatami Unii Europejskiej (w skrócie kwalifikowany certyfikat UE).

Uwaga 1. W normie EN 319 412-5 pojęcie **kwalifikowanego certyfikatu UE** (ang. EU Qualified Certificate) jest równoważne pojęciu kwalifikowanego certyfikatu określonemu w rozporządzeniu eIDAS. Cechą charakterystyczną **kwalifikowanego certyfikatu UE** (certyfikatu podpisu, pieczęci lub uwierzytelniania witryn internetowych) jest odpowiedni identyfikator polityki certyfikacji umieszczony polu rozszerzenia `PolicyInformation` (patrz powyżej punkty 2) - 6).

Uwaga 2. Zgodnie z normą **ETSI EN 319 411-2** dopuszczalne jest w kontekście uregulowań innych niż uregulowania Unii Europejskiej ustanawianie przez organy (domyślnie krajów UE) własnych wymagań z zakresie ogólnych wymagań dotyczących polityki certyfikacji i zabezpieczeń określonych w normie ETSI EN 319 411-1. Własne rozwiązania muszą jednak korzystać z najlepszych ogólnoświatowych praktyk oraz określić dodatkowe wymagania w sposób podobny w zdefiniowanych w normie ETSI EN 319 411-2.

Z uwagi 2 wynika, że możliwe jest wydawanie krajowych kwalifikowanych certyfikatów wydawanych w oparciu o krajowe polityki certyfikacji oraz krajowe identyfikatory polityk certyfikacji.

Propozycja. Polscy kwalifikowani dostawcy usług zaufania powinni wydawać kwalifikowane certyfikaty zgodnie z wymaganiami określonych w normach ETSI EN i zgodnie politykami certyfikacji zdefiniowanymi w tych normach. Pozwoli to łatwą rozpoznawalność oraz interoperacyjność w obrębie całej Unii Europejskiej. Zapis taki należy umieścić w krajowej ustawie o usługach zaufania.

5.5.5 Semantyka identyfikatorów osób fizycznych i osób prawnych

W normie ETSI EN 319 412-1 *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures* zdefiniowano semantykę identyfikatorów osób fizycznych i prawnych. Identyfikatory te są zapisywane w atrybucie *serialNumber* pola podmiot (ang. subject) umieszczanego w certyfikacie osoby fizycznej lub prawnej i pozwalającym na jej jednoznaczną identyfikację. Sama informacja o semantyce atrybutu *serialNumber* umieszczana jest w rozszerzeniu *QCStatement* z identyfikatorem *id-qcs-pkixQCSyntax-v2*. Dla tego identyfikatora w rozdz. 3.2.6.1 specyfikacji RFC 3739 predefiniowano składnię typu *SemanticsInformation*, pozwalającego na definiowanie semantyki różnego typu informacji:

```
SemanticsInformation  ::= SEQUENCE {
    semanticsIndentifier        OBJECT IDENTIFIER OPTIONAL,
    nameRegistrationAuthorities NameRegistrationAuthorities OPTIONAL
} -- At least one field shall be present

NameRegistrationAuthorities ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

Umieszczenie w polu *semanticsIndentifier* idntyfikatora `id-etsi-qcs-SemanticsId-Natural` oznacza, że odnosi się on do semantyki identyfikatora osoby fizycznej, którego wartość jest umieszczona w atrybucie *serialNumber* pola *subject*. Struktura takiego identyfikatora ma postać:

- 3 znakowe oznaczenie typu tożsamości osoby;
- 2 znakowy kod kraju wg ISO 3166;
- myślinik – minus "–" (0x2D (ASCII), U+002D (UTF-8)); oraz
- identyfikator (zgodny z oznaczeniem krajowym i typem tożsamości).

Trzy pierwsze znaki identyfikatora mają jedną z następujących zdefiniowanych wartości:

1) "PAS" do identyfikacji na podstawie numeru paszportu;
2) "IDC" do identyfikacji w oparciu o krajowy numer dowodu tożsamości;
3) "PNO" do identyfikacji na podstawie (krajowego) numeru osoby fizycznej (w Polsce jest to numer PESEL);
4) "TAX" do identyfikacji na podstawie osobistego numeru rejestracji podatkowej wydanej przez krajowy organ podatkowy; ta wartość ta jest przestarzała i w jej miejsce powinien być używany numer TIN;
5) "TIN", czyli NIP według Komisji Europejskiej - podatki i unia celna (http://ec.europa.eu/taxation_customs/tin/tinByCountry.html); lub
6) dwa znaki według lokalnej definicji w określonym kraju i organu rejestracji nazw, identyfikujące krajowy system, który jest uważany za odpowiedni na szczeblu krajowym i europejskim, a następnie znak ":" (dwukropek).

Przykłady identyfikatorów: "PASSK-P3000180", "IDCBE-590082394654" oraz "EI:SE-200007292386".

W przypadku osób prawnych w polu *semanticsIndentifier* umieszczany jest identyfikator `id-etsi-qcs-SemanticsId-Legal`, zaś struktura identyfikatora tego typu osób umieszczanego w atrybucie *serialNumber* pola *subject* ma taka samą postać jak w przypadku osób fizycznych.

Trzy pierwsze znaki identyfikatora mają jedną z następujących zdefiniowanych wartości:

1) "VAT" do identyfikacji na podstawie krajowego numeru identyfikacji podatkowej (w Polsce jest to numer NIP poprzedzony przez PL);
2) "NTR" do identyfikacji na podstawie identyfikatora krajowego rejestru handlowego(w Polsce jest to numer KRS). . Lub
3) dwa znaki według lokalnej definicji w określonym kraju i organu rejestracji nazw, identyfikujące krajowy system, który jest uważany za odpowiedni na szczeblu krajowym i europejskim, a następnie znak ":" (dwukropek).

6. PODSUMOWANIE

Wprowadzenie w życie rozporządzenia eIDAS wymaga szybkiego opracowania towarzyszących jej aktów delegowanych i wykonawczych. Ze względu na przewidywalną w początkowym okresie niestabilność, zwłaszcza aktów wykonawczych, proponujemy, aby krajowa ustawa o usługach zaufania zawierała tylko najważniejsze przepisy niezbędne do wdrożenia rozporządzenia eIDAS dotyczące:

- funkcjonowania organu nadzoru;
- krajowej infrastruktury zaufania;
- wskazania organu odpowiedzialnego za krajową zaufana listę;
- określenia warunków wyłączania usług zaufania spod działania rozporządzania eIDAS;
- rozszerzenia zamkniętej listy usług z rozporządzenia eIDAS na poziomie krajowym, np. o usługi walidacji certyfikatów;
- spójnego systemu odpowiedzialności (w tym finansowej) i kar dotyczących dostawców usług zaufania;
- doprecyzowania skutków prawnych podpisu elektronicznego i pieczęci, za wyjątkiem kwalifikowanego podpisu elektronicznego i kwalifikowanej pieczęci elektronicznej; w prawie krajowym należy określić skutki prawne usług zaufania, o ile nie zostały określone w rozporządzeniu eIDAS, np. skutek złożenia pieczęci kwalifikowanej na dokumencie urzędowym;
- możliwość zawarcia w kwalifikowanych certyfikatach szczególnych atrybutów, takich jak unikalne identyfikatory;
- okresu (innego niż w rozporządzeniu eIDAS) pomiędzy zgłoszeniem unieważnienia certyfikatu, a publikacją informacji o jego unieważnieniu;
- dozwolonych sposobów identyfikacji osób fizycznych i prawnych, którym są wydawane certyfikaty kwalifikowane;
- tymczasowego zawieszania kwalifikowanych certyfikatów, łącznie z brakiem takiej możliwości na poziomie krajowym.

Poniżej przedstawiono dodatkowo propozycje podziału pomiędzy organy rządowe zadań związanych z wdrożeniem eIDAS w Polsce oraz określono działania dostosowujące administrację centralną do zmian wynikających z tego rozporządzenia.

6.1 Propozycja podziału dalszych prac nad wdrożeniem eIDAS w Polsce

Poniższa tabela zawiera propozycję dalszego podziału prac nad wdrożeniem usług zaufania i identyfikacji elektronicznej w Polsce. Lista interesariuszy powinna być uzupełniana o podmioty wyrażające wolę współpracy w zakresie związanym z eIDAS, ustawą o usługach zaufania i powiązanymi rozporządzeniami.

Tab. 6.1 Podział prac nad wdrożeniem eIDAS w Polsce

Zakres prac	Usługi zaufania - ts	Identyfikacja elektroniczna - eid
Nadzór główny	Ministerstwo Gospodarki	Ministerstwo Administracji i Cyfryzacji (w tym wypłata odszkodowań), wsparcie MSW
Współpraca z organami nadzoru w PL	GIODO - ochrona danych osobowych CERT - bezpieczeństwo teleinformatyczne UOKIK - nadzór konsumencki	Tak jak w TS
Współpraca z organami nadzoru w EU	ENISA - bezpieczeństwo teleinformatyczne Komisja Europejska Nadzory PCz	Tak jak w TS
Podmioty objęte nadzorem pełnoskalowym	QTSP	Notyfikowani dostawcy usług identyfikacji elektronicznej i uwierzytelniania
Podmioty objęte nadzorem ad-hoc	non QTSP	Brak
Wsparcie nadzoru - krajowy organ oceny zgodności	Polskie Centrum Akredytacji	Nie dotyczy

Wsparcie nadzoru - ocena zgodności	Conformity Assesment Bodies - potencjalnie IMM, EY, PWC, TICONS, Galach Consulting, instytucje posiadające akredytację ISO 27001	Tak jak w TS
Wsparcie nadzoru - ocena zgodności sprzętu	NCK (wspólnie z WAT i SILTEC), SKW, ABW	Nie dotyczy
Wsparcie nadzoru - infrastruktura nadzoru	TS Status Notification Body - NBP-NCCERT - elektroniczny rejestr QTSP, zarządzanie certyfikatami CA, zarządzanie TSL	CPI, IMM - w zakresie huba PEPS
Legislacja - ustawa o usługach zaufania	Ministerstwo Gospodarki	Ministerstwo Administracji i Cyfryzacji
Legislacja - rozporządzenia do ustawy o usługach zaufania	Ministerstwo Gospodarki	Ministerstwo Administracji i Cyfryzacji
Legislacja - akty prawne zawierające odniesienia do usług zaufania i identyfikacji elektronicznej	Ministerstwa odpowiedzialne za dany akt prawny, RCL, Ministerstwo Gospodarki	Ministerstwa odpowiedzialne za dany akt prawny, RCL, Ministerstwo Administracji i Cyfryzacji, NFZ
Legislacja - współpraca	E-doręczenia - Ministerstwo Administracji i Cyfryzacji, Ministerstwo Sprawiedliwości, Ministerstwo Finansów, Rozporządzenia - IMM-współpraca z MG, Rada Ministrów Konserwacja podpisu/pieczęci - NDAP Znakowanie czasem - GUM Infrastruktura PKI - NCCERT Wszystkie usługi zaufania - Usługodawcy biznesowi i publiczni	NFZ - wsad do ustawy o usługach zaufania w zakresie eID np. w zakresie odpowiedzialności usługodawcy eID, procedur notyfikacji/denotyfikacji systemów eID z sektora prywatnego, pozostałe wymagania dla notyfikowanych systemów eID (eIDAS, art. 7).
Legislacja - prace unijne	Ministerstwo Gospodarki	NFZ, Ministerstwo Administracji i Cyfryzacji
Świadczenie usług - QTSP komercyjni	Z wieloletnim doświadczeniem - PWPW, KIR, Enigma SOI, Unizeto Technologies, Nowi gracze - Eurocert, Poczta Polska	Potencjalnie - QTSP, których certyfikaty wykorzystywane są w procesie identyfikacji lub uwierzytelniania (mechanizm tzw. "ticketingu").
Świadczenie usług - QTSP administracja publiczna	QTSP - Ministerstwo Administracji i Cyfryzacji - docelowo spółki z udziałem skarbu państwa, które będą utrzymywać usługi zaufania administracji publicznej, na zasadach identycznych z podmiotami komercyjnymi. KSM (w zakresie podpisu kwalifikowanego) - NFZ Dostosowanie samorządów - Ministerstwo Administracji i Cyfryzacji Dostosowanie ePUAP - CPI Obsługa administracji w zakresie akceptacji zagranicznych podpisów kwalifikowanych i zaawansowanych z zagranicy - Ministerstwo Administracji i Cyfryzacji (art. 27 eIDAS)	Zaufany profil ePUAP- Ministarstwo Administracji i Cyfryzacji, CPI EKUZ - NFZ KSM, KSA - NFZ pl.ID - MSW Mechanizm identyfikacji ZUS - ZUS
Prace standaryzacyjne (mandat M460)	Polski Komitet Normalizacyjny (CEN), IMM (ETSI), PWPW (ETSI)	Nie dotyczy

6.2 Działania dostosowujące administrację centralną do zmian wynikających z rozporządzenia eIDAS

Przed dniem 1 lipca 2016 przepisy polskiego prawa muszą być dostosowane do wymagań rozporządzenia eIDAS. Zmian będzie wymagała m.in. ustawa o informatyzacji oraz zmieniane przez nią akty prawne (w szczególności dotyczy to Kodeksu Postępowania Administracyjnego). Za przygotowanie i przeprowadzenie zamian w przepisach prawnych będzie odpowiedzialny Parlament RP oraz właściwi ministrowie. Zamiany te będą miały z kolei wpływ na obsługę interesantów przez administrację publiczną wszędzie tam, gdzie wykorzystywane są środki komunikacji elektronicznej.

Wejście w życie rozporządzenia eIDAS oraz uwzględnienie zmian, które muszą być prowadzone w krajowych aktach prawnych będzie wymagało także zmian w systemach administracji stosowanych do obsługi klientów oraz zarządzania elektronicznym obiegiem informacji. Zakres tych zmian oraz ich koszty trudno jest oszacować bez dokładnej analizy stosowanych obecnie systemów oraz procedur zarządzania. Ogólny zakres działań, które musza być wykonane przez administrację przedstawiono w Tab. 6.2.

Szczególną odpowiedzialność w dostosowaniu prawa i obsługi klientów do nowych przepisów ponosić będzie centralna administracja. Z uwagi na możliwość wzrostu liczby dokumentów obsługiwanych elektronicznie i mając na względzie konieczność zapewnienia sprawnej obsługi interesantów, konieczne jest zrealizowanie przez właściwe ministerstwa resortowe zaleceń zaproponowanych w Tab. 6.2.

Tab. 6.2 Działania dostosowawcze administrację centralną do zmian wynikających z rozporządzenia eIDAS

Lp.	Propozycję działań
1	Dokonanie przez administracje centralną przeglądu obowiązujących aktów i przepisów prawnych z punktu widzenia wymagań wynikających z rozporządzenia eIDAS i zaproponowanie w tym kontekście odpowiednich zmian organizacyjno-prawnych
2	Dokonanie przeglądu procesów i procedur związanych z elektronicznym obiegiem dokumentów elektronicznych wspieranych przez usługi zaufania, z uwzględnieniem sposobu organizacji przyjmowania, przetwarzania i wysyłania korespondencji elektronicznej
3	Zidentyfikowanie zmian i ich zakresu w stosowanych przez administrację systemach obsługi klientów oraz systemach zarządzania elektronicznym obiegiem dokumentów. Oszacowanie kosztów zmian.
4	Zmodyfikowanie systemów i procedur dostosowujących je do wymagań rozporządzenia eIDAS i zmienionych krajowych aktów prawnych
5	Przeprowadzenie dla pracowników mających do czynienia z dokumentem elektronicznym oraz uczestniczących w elektronicznym obiegu dokumentów instruktażu wskazującego istotne zmiany wprowadzane do właściwych przepisów ustaw i rozporządzeń krajowych
6	Przeprowadzenie dla pracowników mających do czynienia z dokumentem elektronicznym oraz uczestniczących w elektronicznym obiegu dokumentów szkolenia z zakresu wiedzy o obsłudze usług zaufania wbudowanych w nowe mechanizmy i narzędzia, powiązane zwłaszcza z wysyłaniem i przyjmowaniem korespondencji elektronicznej.

Szczególnej uwagi wymaga akceptacja notyfikowanych systemów identyfikacji elektronicznej przez polskie systemy administracji publicznej świadczące usługi *on-line*. Obecnie w Polsce nie ma mechanizmów umożliwiających akceptację tego typu systemów, a tym samym nie istnieje możliwość swobodnego uznawania tożsamości przez Polskę i inne kraje członkowskie UE. Nadzieją na tego typu swobodny przepływ tożsamości jest mechanizm federacji usług identyfikacyjnych zaproponowanych i zaimplementowanych w ramach projektu STORK i jego następcy STORK2. Integracja usług administracji z krajowymi systemami identyfikacji i systemami z obszaru UE wymaga zbudowania krajowego systemu HUB-PEPS. Wiodącą rolę w zakresie tego typu projektu powinno pełnić Ministerstwo Administracji i Cyfryzacji (MAiC). Planowane przez MAiC działania zostały zestawione w Tab. 6.3.

Tab. 6.3 Działania MAiC mające na celu stworzenia krajowego systemu HUB-PEPS [STRG2014]

Lp.	Propozycję działań
1	Wytworzenie studium wykonalności dla rozwiązania polskiego HUB-a
2	Utworzenie pilotażu metod identyfikacji i uwierzytelnienia w oparciu o platformę zgodną ze STORK
3	Utworzenie komponentów integracyjnych dla usługodawców
4	Integracja systemów i usług administracji publicznej z systemem HUB
5	Utworzenie polskiego węzła STORK i notyfikacja Dostawcy Tożsamości systemu PZ jako systemu na poziomie 3 eIDAS

6.3 Zasada wzajemnej uznawalności usług zaufania

Istotą integracji usług zaufania pomiędzy państwami członkowskimi Unii Europejskiej jest wyrażona w art. 6 ust. 1 rozporządzenia eIDAS zasada wzajemnej uznawalności usług zaufania. Pod określonymi w tym przepisie warunkami państwo członkowskie (jego organy) ma obowiązek uznawania środków identyfikacji elektronicznej wydanych w innych państwach członkowskich, jeśli zgodnie z prawem krajowym dostęp do usługi online świadczonej przed podmiot sektora publicznego wymaga identyfikacji elektronicznej przy użyciu środka identyfikacji elektronicznej oraz uwierzytelniania. Powyższa zasada oznacza, że w przypadkach, gdy organy administracji, czy szerzej rozumiane podmioty sektora publicznego, udostępniają określoną usługę online, a skorzystanie z niej wymaga identyfikacji elektronicznej oraz uwierzytelniania, na organach tych i podmiotach spoczywa obowiązek uznawania nie tylko wydanych w Polsce środków identyfikacji elektronicznej, ale także środków wydanych w innych państwach członkowskich, które spełniają wymogi określone w rozporządzeniu eIDAS, czyli m.in. środków notyfikowanych w KE o poziomie bezpieczeństwa równym lub wyższym od poziomu bezpieczeństwa wymaganego przez podmiot sektora publicznego udostępniający daną usługę.

W związku z powyższym podmioty sektora publicznego winny zwrócić szczególną uwagę na obowiązek wdrożenia powyższej zasady w terminach określonych rozporządzeniem eIDAS. Uznawalność środków identyfikacji wydanych w państwach członkowskich należy wdrożyć nie później niż w okresie 12 miesięcy po opublikowaniu przez Komisję Europejską wykazu notyfikowanych środków identyfikacji. Zgodnie z art. 9 ust. 2 rozporządzenia eIDAS wykaz notyfikowanych systemów identyfikacji elektronicznej Komisja Europejska opublikuje w ciągu roku od rozpoczęcia stosowania niektórych aktów wykonawczych tyczących się tych systemów. Niemniej jednak już obecnie należy podjąć działania, które w przyszłości zapewnią uznawalność przez podmioty sektora publicznego środków identyfikacji elektronicznej wydanych w państwach członkowskich UE.

7. LITERATURA

[eIDAS] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 dnia 23.07.2014r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

[EN319403] Draft standardu *Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers*

[UoPE] *Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym* (Dz.U. 2001 Nr 130 poz. 1450, z póż.zmn.)

[RFC4210] *Internet X.509 Public Key Infrastructure - Certificate Management Protocol (CMP)*, September 2005

[MG2012] *Wspólnotowe prace legislacyjne nad rozporządzeniem Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym*, Ekspertyza wykonana na zlecenie Ministerstwa Gospodarki, Unizeto Technologies S.A., 2012 r., http://www.mg.gov.pl/files/upload/17652/Ekspertyza%20eIDAS.pdf

[X509] ISO/IEC 9594-8:2014 *Information technology -- Open Systems Interconnection -- The Directory -- Part 8: Public-key and attribute certificate frameworks*

[STRG2014] T. Jeruzalski, M. Ujejski, D. Wachnik *Strategia dojścia do rozwiązań interoperacyjnych z UE w zakresie uwierzytelnienia identyfikacji i usług zaufania*, Strategia Ministerstwa Administracji i Cyfryzacji, Uniwersytet Warszawski, stron 34, 2014

[RF2014] Rationalised Framework for e-signatures standards (Dec. 2014, Mandate M/460)

[SR2013] SR 019 530 V 0.0.2 (2013-09) Rationalised framework of Standards for Electronic Delivery Applying Electronic Signatures

[ED2009] Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive D1.2: National profiles deliverable (WP1) National Country Profiles, February 2009, http://ec.europa.eu/idabc/servlets/Doca132.pdf?id=32143

[eD2009] STORK: D6.4.1 eDelivery - Functional Specification, October 2009, https://www.eid-stork.eu/index.php?option=com_processes&Itemid=&act=streamDocument&did=971

[PCA2014] PCA, AJ-ER-535-35/14 – Ramowy plan działań PCA związany z uruchomieniem akredytacji do celów Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014r. (eIDAS).

[ENISA2013] *Trusted e-ID Infrastructures and services in EU*, Recommendations for Trusted Provision of e-Government services, Report, ENISA, December 2013, www.enisa.europa.eu

[UPE2001] Dz. U. z 2001 r. Nr 130, poz. 1450 Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym

[EUD1999] EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a *Community framework for electronic signatures*

[AW2012] A. Wróbel *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz.* Tom III, pod red. D. Kornobis-Romanowskiej i J. Łacny, Warszawa 2012

[SPA2014] *System Prawa Administracyjnego. Tom 3. Europeizacja prawa administracyjnego*, pod red. R. Hausera, Z. Niewiadomskiego, A. Wróbla, Warszawa 2014

[AM2010] A. Malinowski *Teksty prawne Unii Europejskiej. Opracowanie treściowe i redakcyjne oraz zasady ich publikacji*, Warszawa 2010

[RMG1101] Rozporządzenie Ministra Gospodarki z dn. 9 sierpnia 2002 r. *w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym* (Dz.U. 2002 nr 128 poz. 1101)

[RMG1099] Rozporządzenie Ministra Gospodarki z dnia 6 sierpnia 2002 r. *w sprawie sposobu prowadzenia rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne związane z podpisem elektronicznym, wzoru tego rejestru oraz szczegółowego trybu postępowania w sprawach o wpis do rejestru* (Dz.U.2002.128.1099)

[RMG1098] Rozporządzenie Ministra Gospodarki z dn. 6 sierpnia 2002 r. *w sprawie wysokości opłaty za rozpatrzenie wniosku o wpis do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym* (Dz.U.2002.128.1098)

[RMG1097] Rozporządzenie Ministra Gospodarki z dnia 6 sierpnia 2002 r *w sprawie wzoru i szczegółowego zakresu wniosku o dokonanie wpisu do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne, związane z podpisem elektronicznym* (Dz.U.2002.128.1097)

[EN419103] CEN prEN 419 103 *Conformity assessment for signature creation and validation applications*

[EN419211-1] CEN EN 419 211-1: Protection profiles for secure signature creation device — Part1: Overview.

[EN419211-2] CEN EN 419 211-2: Protection profiles for secure signature creation device — Part 2: Device with key generation

[EN419211-3] CEN EN 419 211-3: Protection profiles for secure signature creation device — Part 3: Device with key import

[EN419211-4] CEN EN 419211-4: Protection profiles for secure signature creation device — Part 4: Extension for device with key generation and trusted communication with certificate generation application;

[CEN419200] prCEN/TR 419200: Business guidance for signature creation and other related devices

[EN319412-1] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 1: Overview and common data structures

[EN319412-2] ETSI EN 319 412-2: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons"

[EN319412-3] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 3: Certificate Profile for certificates issued to legal persons".

[EN319412-4] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 4: Certificate Profile for TLS/SSL certificates issued to organisations"

[EN319412-5] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Part 5: Qualified Certificate Statements for Qualified Certificate profiles"

[ETSI101862] ETSI TS 101 862: "Qualified Certificate profile"

[RP2004] R. Podpłoński, P. Popis *Podpis elektroniczny. Komentarz*, Warszawa 2004

[TUE2012] Traktat o funkcjonowaniu Unii Europejskiej. Komentarz. Tom I, pod red. D. Miąsika i N. Półtorak, Warszawa 2012

[ET102640-1] ETSI TS 102 640-1: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 1: Architecture.

[ET102640-2] ETSI TS 102 640-2: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 2: Data requirements, Formats and Signatures for REM.

[ET102640-3] ETSI TS 102 640-3: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 3: Information Security Policy Requirements for REM Management Domains.

[ET102640-4] ETSI TS 102 640-4:Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 4: REM-MD Conformance Profiles.

[ET102640-5] ETSI TS 102 640-5: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 5: REM-MD Interoperability Profiles.

[ET102640-6.1] ETSI TS 102 640-6.1: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.1: REM-MD UPU PReM interoperability Profile

[ET102640-6.2] ETSI TS 102 640-6.2.: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.2: REM-MD BUSDOX Interoperability Profile

[ET102640-6.3] ETSI TS 102 640-6.3: Electronic Signatures and Infrastructures (ESI); Registered Electronic Mail (REM); Part 6.3: REM-MD SOAP Binding Profile

[EN319511] EN 319 511 Policy and security requirements for registered electronic mail (REM) service providers

[EN319512] EN 319 512 Registered electronic mail (REM) services

[EN319513] EN 319 513 Conformity assessment for REM service providers

[TS119514] TS 119 514 Testing compliance and interoperability of REM service providers

[ET101533-1] ETSI TS 101 533-1 V1.3.1 (2012-04) Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management

[BSI03125] BSI TR-ESOR – 03125 TR-ESOR Preservation of Evidence of Cryptographically Signed Documents, Federal Office for Information Security, Germany, 2011

[ISO18492] ISO/TR 18492:2005 Long-term preservation of electronic document-based information, 2005

[LT2008] Arne-Kristian Groven, Jon Ølnes, Habtamu Abie, Truls Fretland: Preservation of Trust in Long-Term Records Management Systems. A State of Art Overview for the LongRec Project, 2008

[EN319521] EN 319 521 Policy and security requirements for data preservation service providers

[EN319522] EN 319 522 Data preservation services through signing

[EN319522] EN 319 523 Conformity assessment of data preservation service providers

[EN319411-1] EN 319 411-1 *Policy and security requirements for Trust Service Providers issuing certificates; Part 1: Policy requirements for Certification Authorities issuing web site certificates*

[EN319411-2] EN 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Policy requirements for certification authorities issuing qualified certificates*

[EN319411-3] EN 319 411-3 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates*

[EN319401] EN 319 401 *General Policy Requirements for Trust Service Providers supporting Electronic Signatures*

[EN319421] EN 319 421 *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers providing Time-Stamping Services*