Dziennik Urzędowy L 235

Unii Europejskiej

Tom 58

Wydanie polskie **Legislacja** 9 września 2015

Spis treści

[1] Tekst mający znaczenie dla EOG

PL

Akty, których tytuły wydrukowano zwykłą czcionką, odnoszą się do bieżącego zarządzania sprawami rolnictwa i generalnie zachowują ważność przez określony czas.

Tytuły wszystkich innych aktów poprzedza gwiazdka, a drukuje się je czcionką pogrubioną.

[1] Tekst mający znaczenie dla EOG

II

(Akty o charakterze nieustawodawczym)

ROZPORZĄDZENIA

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1501

z dnia 8 września 2015 r.

w sprawie ram interoperacyjności na podstawie art. 12 ust. 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE ([1]), w szczególności jego art. 12 ust. 8,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 12 ust. 2 rozporządzenia (UE) nr 910/2014 należy ustanowić ramy interoperacyjności do celów współdziałania krajowych systemów identyfikacji elektronicznej notyfikowanych na podstawie art. 9 ust. 1 tegoż rozporządzenia.

(2) Węzły odgrywają kluczową rolę w łączeniu systemów identyfikacji elektronicznej państw członkowskich. Ich rola, w tym funkcje i komponenty „węzła eIDAS", została wyjaśniona w dokumentacji dotyczącej instrumentu „Łącząc Europę" ustanowionego rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1316/2013 ([2]).

(3) Jeżeli państwo członkowskie lub Komisja dostarcza oprogramowanie umożliwiające uwierzytelnianie do węzła eksploatowanego w innym państwie członkowskim, strona, która dostarcza i uaktualnia oprogramowanie wykorzystywane do mechanizmu uwierzytelniającego, może uzgodnić ze stroną hostingującą oprogramowanie sposób zarządzania eksploatacją mechanizmu uwierzytelniającego. Takie porozumienie nie powinno obciążać strony hostingującej niewspółmiernymi wymaganiami technicznymi i kosztami (w tym w zakresie asysty technicznej, odpowiedzialności, hostingu i innych kosztów).

(4) W zakresie uzasadnionym wdrażaniem ram interoperacyjności Komisja – we współpracy z państwami członkowskimi i ze szczególnym uwzględnieniem opinii sieci współpracy, o których mowa w art. 14 lit. d) decyzji wykonawczej Komisji (UE) 2015/296 ([3]) – może opracować dalsze specyfikacje techniczne zawierające szczegółowe informacje o wymaganiach technicznych określonych w niniejszym rozporządzeniu. Takie specyfikacje powinny zostać opracowane w ramach infrastruktury usług cyfrowych, której dotyczy rozporządzenie (UE) nr 1316/2013, w którym określono środki umożliwiające praktycznego wdrożenia podstawowych elementów systemu identyfikacji elektronicznej.

([1]) Dz.U. L 257 z 28.8.2014, s. 73.

([2]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1316/2013 z dnia 11 grudnia 2013 r. ustanawiające instrument „Łącząc Europę", zmieniające rozporządzenie (UE) nr 913/2010 oraz uchylające rozporządzenia (WE) nr 680/2007 i (WE) nr 67/2010 (Dz.U. L 348 z 20.12.2013, s. 129).

([3]) Decyzja wykonawcza Komisji (UE) 2015/296 z dnia 24 lutego 2015 r. ustanawiająca proceduralne warunki współpracy między państwami członkowskimi w zakresie identyfikacji elektronicznej na podstawie art. 12 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz.U. L 53 z 25.2.2015, s. 14).

(5) Wymagania techniczne określone w niniejszym rozporządzeniu powinny mieć zastosowanie niezależnie od wszelkich zmian w specyfikacjach technicznych, które mogłyby zostać opracowane zgodnie z art. 12 niniejszego rozporządzenia.

(6) Przy ustalaniu warunków ram interoperacyjności, określonych w niniejszym rozporządzeniu, w możliwie jak największym stopniu uwzględniono pilotażowy projekt na dużą skalę STORK, w tym opracowane w jego ramach specyfikacje oraz zasady i koncepcje europejskich ram interoperacyjności dla europejskich usług użyteczności publicznej.

(7) Wyniki współpracy pomiędzy państwami członkowskimi zostały w jak największym stopniu wzięte pod uwagę.

(8) Środki przewidziane w niniejszym rozporządzeniu są zgodne z opinią komitetu ustanowionego na podstawie art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Przedmiot

Niniejszym rozporządzeniem ustanawia się wymagania techniczne i operacyjne ram interoperacyjności w celu zapewnienia interoperacyjności systemów identyfikacji elektronicznej, które państwa członkowskie zgłaszają Komisji.

Wymagania te obejmują w szczególności:

a) minimalne wymagania techniczne związane z poziomami zaufania i przyporządkowanie krajowych poziomów zaufania notyfikowanych środków identyfikacji elektronicznej wydanych w ramach notyfikowanych systemów identyfikacji elektronicznej zgodnie z art. 8 rozporządzenia (UE) nr 910/2014, określone w artykułach 3 i 4;

b) minimalne wymagania techniczne dotyczące interoperacyjności, określone w artykułach 5 i 8;

c) wymagania dotyczące minimalnego zbioru danych identyfikujących osobę reprezentujących niepowtarzalnie osobę fizyczną lub prawną, określone w art. 11 i załączniku;

d) wspólne operacyjne normy bezpieczeństwa określone w artykułach 6, 7, 9 i 10;

e) ustalenia dotyczące rozstrzygania sporów określone w art. 13.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „węzeł" oznacza punkt przyłączenia będący częścią architektury systemu interoperacyjności identyfikacji elektronicznej, który jest wykorzystywany w procesie transgranicznego uwierzytelniania osób i który ma zdolność do rozpoznawania i przetwarzania lub przesyłania danych do innych węzłów poprzez umożliwienie sprzężenia krajowej infrastruktury identyfikacji elektronicznej jednego państwa członkowskiego z krajowymi infrastrukturami służącymi do identyfikacji elektronicznej innych państw członkowskich;

2) „operator węzła" oznacza podmiot odpowiedzialny za zapewnienie prawidłowego i niezawodnego funkcjonowania węzła jako punktu przyłączenia.

Artykuł 3

Minimalne wymagania techniczne związane z poziomami zaufania

Minimalne wymagania techniczne odnoszące się do poziomów zaufania zostały określone w rozporządzeniu wykonawczym Komisji (UE) 2015/1502 ([1]).

Artykuł 4

Przyporządkowanie krajowych poziomów zaufania

Przyporządkowanie krajowych poziomów zaufania notyfikowanych systemów identyfikacji elektronicznej musi być zgodne z wymaganiami określonymi w rozporządzeniu wykonawczym Komisji (UE) 2015/1502. Wyniki tego przyporządkowania są przekazywane Komisji przy użyciu formularza powiadomienia określonego w decyzji wykonawczej Komisji (UE) 2015/1505 ([2]).

Artykuł 5

Węzły

1. Węzeł w jednym państwie członkowskim ma możliwość połączenia się z węzłami w innych państwach członkowskich.

2. Węzły są w stanie za pomocą środków technicznych dokonać rozróżnienia między organami sektora publicznego i innymi stronami ufającymi.

3. Wdrożenie przez państwo członkowskie wymagań technicznych określonych w niniejszym rozporządzeniu nie może obciążać innych państw członkowskich niewspółmiernymi wymaganiami technicznymi i kosztami koniecznymi do osiągnięcia interoperacyjności z systemem wdrożonym przez to państwo członkowskie.

Artykuł 6

Bezpieczeństwo i poufność danych

1. Ochronę prywatności i poufności wymienianych danych oraz utrzymanie integralności danych pomiędzy węzłami należy zapewnić poprzez stosowanie najlepszych dostępnych rozwiązań technicznych i praktyk ochrony.

2. Węzły nie przechowują żadnych danych osobowych, z wyjątkiem przechowywania do celów określonych w art. 9 ust. 3.

Artykuł 7

Integralność i autentyczność danych na potrzeby przekazywania

W łączności między węzłami należy zapewnić integralność i autentyczność danych, tak aby wszystkie zapytania i odpowiedzi były autentyczne i nie ulegały manipulacjom. W tym celu w węzłach stosuje się rozwiązania, które są z powodzeniem wykorzystywane w transgranicznym ruchu operacyjnym.

([1]) Rozporządzenie wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (zob. s. 7 niniejszego Dziennika Urzędowego).

([2]) Decyzja wykonawcza Komisji (UE) 2015/1505 z dnia 8 września 2015 r. ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (zob. s. 26 niniejszego Dziennika Urzędowego).

Artykuł 8

Format przekazywania wiadomości

Węzły wykorzystują składnię powszechnych formatów komunikatów opartych na normach, które zastosowano już więcej niż jeden raz między państwami członkowskimi i które sprawdziły się w środowisku operacyjnym. Składnia ta umożliwia:

a) prawidłowe przetwarzanie minimalnego zbioru danych identyfikujących osobę reprezentujących niepowtarzalnie osobę fizyczną lub prawną;

b) właściwe przetwarzanie poziomu bezpieczeństwa środków identyfikacji elektronicznej;

c) rozróżnienie między organami sektora publicznego i innymi stronami ufającymi;

d) elastyczność służącą spełnieniu potrzeb w zakresie dodatkowych atrybutów odnoszących się do identyfikacji.

Artykuł 9

Zarządzanie bezpieczeństwem informacji i metadane

1. Operator węzła przekazuje metadane związane z zarządzaniem węzłem w znormalizowanej postaci przetwarzalnej maszynowo oraz w sposób bezpieczny i godny zaufania.

2. Przynajmniej parametry dotyczące bezpieczeństwa są pobierane automatycznie.

3. Operator węzła przechowuje dane, które w razie incydentu umożliwią odbudowę sekwencji wymiany komunikatów w celu określenie miejsca i charakteru incydentu. Dane przechowywane są przez czas określony zgodnie z wymaganiami krajowymi i obejmują one co najmniej następujące elementy:

a) dane identyfikujące węzeł;

b) dane identyfikujące wiadomość;

c) datę i godzinę wiadomości.

Artykuł 10

Bezpieczeństwo informacji i normy bezpieczeństwa

1. Operatorzy węzłów zapewniających uwierzytelnienie muszą udowodnić – poprzez certyfikację lub równoważne metody oceny, bądź dzięki zgodności z przepisami krajowymi – że w odniesieniu do węzłów uczestniczących w ramach interoperacyjności dany węzeł spełnia wymogi normy ISO/IEC 27001.

2. Operatorzy węzłów niezwłocznie dokonują aktualizacji o krytycznym znaczeniu dla bezpieczeństwa.

Artykuł 11

Dane identyfikujące osobę

1. Minimalny zbiór danych identyfikujących osobę reprezentujących niepowtarzalnie osobę fizyczną lub prawną musi spełniać wymagania określone w załączniku, jeśli dane te są stosowane w ruchu transgranicznym.

2. Minimalny zestaw danych dotyczących osoby fizycznej reprezentującej osobę prawną musi zawierać połączenie atrybutów wymienionych w załączniku dotyczących osób fizycznych i osób prawnych, jeśli dane te są stosowane w ruchu transgranicznym.

3. Dane są przekazywane w oparciu o oryginalne znaki, a w stosownych przypadkach także w transliteracji na alfabet łaciński.

Artykuł 12

Specyfikacja techniczna

1. W przypadkach uzasadnionych procesem wdrażania ram interoperacyjności sieć współpracy ustanowiona decyzją wykonawczą Komisji (UE) 2015/296 może zgodnie z art. 14 lit. d) tejże decyzji wydawać opinie na temat potrzeby opracowania specyfikacji technicznych. Specyfikacje techniczne zawierają bardziej szczegółowe informacje o wymaganiach technicznych określonych w niniejszym rozporządzeniu.

2. Na podstawie opinii, o której mowa w ust. 1, Komisja we współpracy z państwami członkowskimi opracowuje specyfikacje techniczne w ramach infrastruktury usług cyfrowych określonej rozporządzeniem (UE) nr 1316/2013.

3. Sieć współpracy przyjmuje opinię zgodnie z art. 14 lit. d) decyzji wykonawczej Komisji (UE) 2015/296, zawierającej ocenę, czy i w jakim stopniu specyfikacje techniczne opracowane zgodnie z ust. 2 odpowiadają na potrzebę wskazaną w opinii, o której mowa w ust. 1, lub są zgodne z wymaganiami określonymi w niniejszym rozporządzeniu. Sieć współpracy może zalecić państwom członkowskim uwzględnienie specyfikacji technicznych przy wdrażaniu ram interoperacyjności.

4. Komisja dostarcza przykładu interpretacji specyfikacji technicznych w postaci modelowego wdrożenia. Państwa członkowskie mogą zastosować to wdrożenie modelowe lub wykorzystać je jako wzorzec, testując inne wdrożenia specyfikacji technicznych.

Artykuł 13

Rozstrzyganie sporów

1. W miarę możliwości wszelkie spory dotyczące ram interoperacyjności są rozwiązywane przez zainteresowane państwa członkowskie w drodze negocjacji.

2. Jeżeli nie uda się znaleźć rozwiązania zgodnie z ust. 1, sieć współpracy ustanowiona zgodnie z art. 12 decyzji wykonawczej (UE) 2015/296 dysponuje kompetencjami w odniesieniu do sporu zgodnie ze swoim regulaminem wewnętrznym.

Artykuł 14

Wejście w życie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 8 września 2015 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

ZAŁĄCZNIK

Wymagania dotyczące minimalnego zbioru danych identyfikujących osobę, reprezentujących niepowtarzalnie osobę fizyczną lub prawną, o których mowa w art. 11

1. **Minimalny zestaw danych dotyczących osoby fizycznej**

Minimalny zestaw danych dotyczących osoby fizycznej zawiera wszystkie poniższe elementy obowiązkowe:

a) obecnie używane nazwisko lub nazwiska;

b) obecnie używane imię lub imiona;

c) data urodzenia;

d) niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy.

Minimalny zestaw danych dotyczących osoby fizycznej może zawierać co najmniej jeden z następujących elementów dodatkowych:

a) imię lub imiona oraz nazwisko lub nazwiska rodowe;

b) miejsce urodzenia;

c) aktualny adres;

d) płeć.

2. **Minimalny zestaw danych dotyczących osoby prawnej**

Minimalny zestaw danych dotyczących osoby prawnej zawiera wszystkie poniższe atrybuty obowiązkowe:

a) obecnie używana nazwa prawna;

b) niepowtarzalny identyfikator zbudowany przez wysyłające państwo członkowskie zgodnie ze specyfikacjami technicznymi do celów transgranicznej identyfikacji, który jest możliwie jak najtrwalszy.

Minimalny zestaw danych dotyczących osoby prawnej może zawierać co najmniej jeden z następujących elementów dodatkowych:

a) aktualny adres;

b) identyfikator płatnika podatku VAT;

c) numer identyfikacji podatkowej;

d) identyfikator odnoszący się do art. 3 ust. 1 dyrektywy 2009/101/WE Parlamentu Europejskiego i Rady ([1]);

e) identyfikator podmiotu prawnego (LEI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) nr 1247/2012 ([2]);

f) identyfikator Wspólnotowego Systemu Rejestracji i Identyfikacji Podmiotów Gospodarczych (EORI), o którym mowa w rozporządzeniu wykonawczym Komisji (UE) nr 1352/2013 ([3]);

g) numer akcyzowy określony w art. 2 ust. 12 rozporządzenia Rady nr 389/2012 ([4]).

([1]) Dyrektywa 2009/101/WE Parlamentu Europejskiego i Rady z dnia 16 września 2009 r. w sprawie koordynacji gwarancji, jakie są wymagane w państwach członkowskich od spółek w rozumieniu art. 48 akapit drugi Traktatu, w celu uzyskania ich równoważności, dla zapewnienia ochrony interesów zarówno wspólników, jak i osób trzecich (Dz.U. L 258 z 1.10.2009, s. 11).

([2]) Rozporządzenie wykonawcze Komisji (UE) nr 1247/2012 z dnia 19 grudnia 2012 r. ustanawiające wykonawcze standardy techniczne w odniesieniu do formatu i częstotliwości dokonywania zgłoszeń dotyczących transakcji do repozytoriów transakcji zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 648/2012 w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz.U. L 352 z 21.12.2012, s. 20).

([3]) Rozporządzenie wykonawcze Komisji (UE) nr 1352/2013 z dnia 4 grudnia 2013 r. ustanawiające formularze przewidziane w rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 608/2013 w sprawie egzekwowania praw własności intelektualnej przez organy celne (Dz.U. L 341 z 18.12.2013, s. 10).

([4]) Rozporządzenie Rady (UE) nr 389/2012 z dnia 2 maja 2012 r. w sprawie współpracy administracyjnej w dziedzinie podatków akcyzowych oraz uchylenia rozporządzenia (WE) nr 2073/2004 (Dz.U. L 121 z 8.5.2012, s. 1).

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1502

z dnia 8 września 2015 r.

w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE ([1]), w szczególności jego art. 8 ust. 3,

a także mając na uwadze, co następuje:

(1) art. 8 rozporządzenia (UE) nr 910/2014 stanowi, że system identyfikacji elektronicznej notyfikowany zgodnie z art. 9 ust. 1 musi określać niski, średni i wysoki poziom zaufania w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach tego systemu.

(2) Ustanowienie minimalnych specyfikacji technicznych, standardów i procedur jest niezbędne w celu zapewnienia jednolitego rozumienia szczegółów dotyczących poziomów zaufania oraz zapewnienia interoperacyjności podczas przyporządkowywania krajowych poziomów zaufania notyfikowanych systemów identyfikacji elektronicznej względem poziomów zaufania zgodnie z art. 8, jak określono w art. 12 ust. 4 lit. b) rozporządzenia (UE) nr 910/2014.

(3) Na potrzeby specyfikacji i procedur ustanowionych w niniejszym akcie wykonawczym uwzględniono normę międzynarodową ISO/IEC 29115 jako podstawową normę międzynarodową w zakresie poziomów zaufania środków identyfikacji elektronicznej. Treść rozporządzenia (UE) nr 910/2014 różni się jednak od tej normy międzynarodowej, w szczególności w odniesieniu do wymogów wykazywania i weryfikacji tożsamości, jak również sposobu, w jaki brane są pod uwagę różnice między ustaleniami poszczególnych państw członkowskich w zakresie tożsamości oraz istniejące w UE narzędzia służące do tego samego celu. W związku z tym załącznik, mimo że został oparty na tej normie międzynarodowej, nie powinien zawierać odniesień do żadnych określonych treści normy ISO/IEC 29115.

(4) Podstawą opracowania niniejszego rozporządzenia było podejście opierające się na wynikach, uznane za najodpowiedniejsze, czego odzwierciedleniem są również definicje stosowane w celu określenia terminów i pojęć. Uwzględnia się w nich cel rozporządzenia (UE) nr 910/2014 w odniesieniu do poziomów zaufania środków identyfikacji elektronicznej. W związku z tym podczas określania specyfikacji i procedur ustanowionych w tym akcie wykonawczym należy szczególnie wziąć pod uwagę pilotażowy projekt na dużą skalę STORK, w tym opracowane w jego ramach specyfikacje, oraz definicje i pojęcia zawarte w normie ISO/IEC 29115.

(5) W zależności od kontekstu, w jakim musi być weryfikowany aspekt dowodu tożsamości, wiarygodne źródła mogą przybierać różne formy, takie jak m.in. rejestry, dokumenty czy organy. Wiarygodne źródła mogą się różnić w poszczególnych państwach członkowskich, nawet w podobnej sytuacji.

(6) Wymagania dotyczące testów i weryfikacji tożsamości powinny uwzględniać różne systemy i praktyki, przy zapewnieniu wystarczająco wysokiego poziomu zaufania w celu zapewnienia niezbędnego zaufania. Dlatego też przyjęcie procedur stosowanych wcześniej do celów innych niż wydawanie środków identyfikacji elektronicznej powinno być uzależnione od potwierdzenia, że procedury te spełniają wymagania przewidziane dla odpowiedniego poziomu zaufania.

([1]) Dz.U. L 257 z 28.8.2014, s. 73.

(7) Zwykle stosuje się pewne czynniki uwierzytelniania, takie jak dzielenie sekretu (ang. *shared secrets*), urządzenia techniczne i atrybuty fizyczne. Należy jednak zachęcać do korzystania z większej liczby czynników uwierzytelniania, zwłaszcza należących do różnych kategorii, w celu zwiększenia bezpieczeństwa procesu uwierzytelniania.

(8) Niniejsze rozporządzenie nie powinno naruszać praw reprezentacji osób prawnych. W załączniku należy jednak określić wymagania dotyczące powiązania między środkami identyfikacji elektronicznej osób fizycznych i prawnych.

(9) Należy uznać znaczenie bezpieczeństwa informacji oraz systemów zarządzania usługą, podobnie jak wagę stosowania uznanych metod i stosowania zasad zawartych w normach takich jak normy ISO/IEC serii 27000 i serii 20000.

(10) Należy również uwzględnić dobre praktyki w odniesieniu do poziomów zaufania w państwach członkowskich.

(11) Certyfikacja bezpieczeństwa informatycznego oparta na normach międzynarodowych jest ważnym narzędziem weryfikacji zgodności produktów w zakresie bezpieczeństwa z wymaganiami określonymi w niniejszym akcie wykonawczym.

(12) Komitet, o którym mowa w art. 48 rozporządzenia (UE) nr 910/2014, nie wydał opinii w terminie ustalonym przez swego przewodniczącego,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

1. Niski, średni i wysoki poziom zaufania w odniesieniu do środka identyfikacji elektronicznej wydanego zgodnie z notyfikowanym systemem identyfikacji elektronicznej ustala się z uwzględnieniem wymagań i procedur określonych w załączniku.

2. Specyfikacje i procedury określone w załączniku są wykorzystywane do określenia poziomu zaufania środka identyfikacji elektronicznej wydanego zgodnie z notyfikowanym systemem identyfikacji elektronicznej za pomocą określenia wiarygodności i jakości następujących elementów:

a) wprowadzenie do systemu, jak określono w sekcji 2.1 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. a) rozporządzenia (UE) nr 910/2014;

b) zarządzanie środkiem identyfikacji elektronicznej, jak określono w sekcji 2.2 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. b) rozporządzenia (UE) nr 910/2014;

c) uwierzytelnianie, jak określono w sekcji 2.3 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. c) rozporządzenia (UE) nr 910/2014;

d) zarządzanie i organizacja, jak określono w sekcji 2.4 załącznika do niniejszego rozporządzenia zgodnie z art. 8 ust. 3 lit. d) oraz e) rozporządzenia (UE) nr 910/2014.

3. Jeśli środek identyfikacji elektronicznej wydany w ramach notyfikowanego systemu identyfikacji elektronicznej spełnia wymaganie wymienione w odniesieniu do wyższego poziomu zaufania, wówczas zakłada się, że spełnia on równoważne wymaganie dotyczące niższego poziomu zaufania.

4. Wszystkie elementy wymienione w załączniku w odniesieniu do danego poziomu zaufania środka identyfikacji elektronicznej wydanego zgodnie z notyfikowanym systemem identyfikacji elektronicznej powinny zostać spełnione, aby zapewnić zgodność z deklarowanym poziomem zaufania, chyba że w odpowiedniej części załącznika określono inaczej.

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 8 września 2015 r.

W imieniu Komisji

Jean-Claude JUNCKER

Przewodniczący

ZAŁĄCZNIK

Specyfikacje techniczne i procedury dotyczące niskiego, średniego i wysokiego poziomu zaufania w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach notyfikowanego systemu identyfikacji elektronicznej

1. Stosowane definicje

Na potrzeby niniejszego załącznika stosuje się następujące definicje:

1) „wiarygodne źródło" oznacza każde źródło, niezależnie od jego formy, co do którego można mieć pewność, że dostarcza ono dokładnych danych, informacji lub dowodów, które mogą służyć do potwierdzenia tożsamości;

2) „czynnik uwierzytelniania" oznacza czynnik, którego związek z osobą jest potwierdzony i który należy do jednej z poniższych kategorii:

   a) „czynnik uwierzytelniania na podstawie posiadania" oznacza czynnik uwierzytelniania, w przypadku którego od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego posiadania;

   b) „czynnik uwierzytelniania na podstawie wiedzy" oznacza czynnik uwierzytelniania, w przypadku którego od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania jego znajomości;

   c) „czynnik uwierzytelniania na podstawie cech przyrodzonych" oznacza czynnik uwierzytelnienia, który opiera się na rzeczywistym atrybucie osoby fizycznej, w którego przypadku od podmiotu podlegającego uwierzytelnieniu wymaga się wykazania, że tę cechę fizyczną posiada;

3) „uwierzytelnianie dynamiczne" oznacza proces elektroniczny z zastosowaniem kryptografii lub innych technik służący dostarczeniu na żądanie elektronicznego dowodu, iż podmiot podlegający uwierzytelnieniu jest w posiadaniu danych identyfikacyjnych lub dane te znajdują się pod jego kontrolą, oraz który ulega zmianie z każdym uwierzytelnieniem zachodzącym między podmiotem podlegającym uwierzytelnieniu a systemem weryfikacji tożsamości danego podmiotu;

4) „system zarządzania bezpieczeństwem informacji" oznacza zbiór procesów i procedur służących do zarządzania dopuszczalnymi poziomami zagrożeń związanych z bezpieczeństwem informacji.

2. Specyfikacje techniczne i procedury

Elementy specyfikacji technicznych i procedury przedstawione w niniejszym załączniku stosuje się do określenia, w jaki sposób wymagania i kryteria określone w art. 8 rozporządzenia (UE) nr 910/2014 należy stosować w odniesieniu do środka identyfikacji elektronicznej wydanego w ramach systemu identyfikacji elektronicznej.

2.1. *Wprowadzenie do systemu*

2.1.1. Wniosek o rejestrację i rejestracja

Poziom zaufania	Wymagane elementy
Niski	1. Zapewnienie znajomości przez wnioskodawcę warunków odnoszących się do stosowania środków identyfikacji elektronicznej. 2. Zapewnienie znajomości przez wnioskodawcę zalecanych środków zaufania odnoszących się do środków identyfikacji elektronicznej. 3. Zebranie odpowiednich danych identyfikacyjnych wymaganych do sprawdzenia i weryfikacji tożsamości.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.1.2. Sprawdzenie i weryfikacja tożsamości (osoba fizyczna)

Poziom zaufania	Wymagane elementy
Niski	1. Można zakładać, że dana osoba posiada dowody uznane przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, oraz reprezentuje deklarowaną tożsamość. 2. Dowody te można uznać za autentyczne lub istniejące zgodnie z informacjami z wiarygodnego źródła i dowody wydają się zachowywać ważność. 3. Wiadomo z wiarygodnego źródła, że deklarowana tożsamość istnieje, oraz można przypuszczać, że deklaruje ją jedna i ta sama osoba.
Średni	Jak przy poziomie niskim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w pkt 1–4: 1. potwierdzono, że dana osoba posiada dowody uznane przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, oraz reprezentuje deklarowaną tożsamość, oraz dowody zostały sprawdzone w celu ustalenia ich autentyczności lub z wiarygodnego źródła wiadomo, że dowody istnieją i dotyczą rzeczywistej osoby, oraz podjęto działania w celu zminimalizowania ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dowodu; lub 2. dokument tożsamości zostaje przedstawiony w trakcie procesu rejestracji w państwie członkowskim, w którym go wydano, i okazuje się, że odnosi się on do osoby okazującej, oraz podjęto działania w celu zminimalizowania ryzyka, że tożsamość danej osoby nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dokumentów; lub 3. w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają poziom zaufania równoważny do zapewnionego przez środki określone w sekcji 2.1.2 dla średniego poziomu zaufania, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny poziom zaufania jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 ([1]), lub przez równoważny organ; lub 4. jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się średnim lub wysokim poziomem zaufania i biorąc pod uwagę ryzyko zmiany danych identyfikujących osobę, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, średni lub wysoki poziom zaufania musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ.

Poziom zaufania	Wymagane elementy
Wysoki	Muszą zostać spełnione wymagania pkt 1 albo pkt 2: 1. jak przy poziomie średnim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w lit. a)–c): a) potwierdzono, że dana osoba posiada dowody identyfikacji fotograficznej lub biometrycznej uznane przez państwo członkowskie, w którym złożono wniosek o wydanie środka identyfikacji elektronicznej, oraz że dowody te stanowią potwierdzenie deklarowanej tożsamości, dowody są sprawdzane w celu ustalenia, czy zachowują ważność zgodnie z informacjami z wiarygodnego źródła, oraz wnioskodawca jest identyfikowany jako osoba o deklarowanej tożsamości poprzez porównanie jego jednej cechy fizycznej lub większej liczby takich jego cech z informacjami z wiarygodnego źródła; lub b) w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają poziom zaufania równoważny do zapewnionego przez środki określone w sekcji 2.1.2 dla wysokiego poziomu zaufania, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny poziom zaufania jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że wyniki poprzednich procedur zachowują ważność; lub c) jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się wysokim poziomem zaufania i biorąc pod uwagę ryzyko zmiany danych identyfikujących osobę, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, wysoki poziom zaufania musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że rezultaty tej poprzedniej procedury wydawania notyfikowanych środków identyfikacji elektronicznej zachowują ważność; LUB 2. jeżeli wnioskodawca nie przedstawił uznanych dowodów identyfikacji fotograficznej lub biometrycznej, zastosowanie mają te same procedury uzyskiwania takich uznanych dowodów identyfikacji fotograficznej lub biometrycznej co stosowane na poziomie krajowym w państwie członkowskim podmiotu odpowiedzialnego za rejestrację.

([1]) Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz.U. L 218 z 13.8.2008, s. 30).

2.1.3. Sprawdzenie i weryfikacja tożsamości (osoba prawna)

Poziom zaufania	Wymagane elementy
Niski	1. Deklarowaną tożsamość osoby prawnej wykazuje się na podstawie dowodów uznanych przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej.

Poziom zaufania	Wymagane elementy
	2. Dowody wydają się zachowywać ważność i można uznać, że są autentyczne lub istniejące zgodnie z informacjami z wiarygodnego źródła, jeżeli wprowadzenie osoby prawnej do wiarygodnego źródła jest dobrowolne i jest regulowane za pomocą ustalenia między osobą prawną oraz wiarygodnym źródłem. 3. Wiarygodne źródło nie dysponuje wiedzą o statusie osoby prawnej, który uniemożliwiałby jej działanie jako osoby prawnej.
Średni	Jak przy poziomie niskim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w pkt 1–3: 1. deklarowaną tożsamość osoby prawnej wykazuje się na podstawie dowodów uznanych przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, obejmujących nazwę osoby prawnej, jej formę prawną oraz, w stosownych przypadkach, jej numer rejestracyjny, oraz dowody są sprawdzane w celu ustalenia, czy są autentyczne bądź czy wiadomo, że istnieją zgodnie z informacjami z wiarygodnego źródła, jeżeli wprowadzenie osoby prawnej do wiarygodnego źródła jest wymagane do prowadzenia przez nią działalności w odnośnym sektorze, oraz podjęto działania w celu zminimalizowania ryzyka, że tożsamość danej osoby prawnej nie jest tożsamością deklarowaną, biorąc pod uwagę np. ryzyko utraty, kradzieży, zawieszenia, unieważnienia bądź upływu terminu ważności dokumentów; lub 2. w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają poziom zaufania równoważny do zapewnionego przez środki określone w sekcji 2.1.3 dla średniego poziomu zaufania, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny poziom zaufania jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ; lub 3. jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się średnim lub wysokim poziomem zaufania, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, średni lub wysoki poziom zaufania musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ.
Wysoki	Jak przy poziomie średnim oraz konieczność spełnienia jednego z alternatywnych warunków wymienionych w pkt 1–3: 1. deklarowaną tożsamość osoby prawnej wykazuje się na podstawie dowodów uznanych przez państwo członkowskie, w którym złożono wniosek o środek identyfikacji elektronicznej, obejmujących nazwę osoby prawnej, jej formę prawną oraz co najmniej jeden niepowtarzalny identyfikator osoby prawnej stosowany w warunkach krajowych, oraz dowody zostały sprawdzone w celu ustalenia ich ważności zgodnie z wiarygodnym źródłem; lub

Poziom zaufania	Wymagane elementy
	2. w przypadku gdy procedury stosowane uprzednio przez podmiot publiczny lub prywatny w tym samym państwie członkowskim w celu innym niż wydawanie środków identyfikacji elektronicznej zapewniają poziom zaufania równoważny do zapewnionego przez środki określone w sekcji 2.1.3 dla wysokiego poziomu zaufania, podmiot odpowiedzialny za rejestrację nie musi powtarzać tych wcześniejszych procedur, pod warunkiem że taki równoważny poziom zaufania jest potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że wyniki poprzednich procedur zachowują ważność; lub 3. jeżeli środki identyfikacji elektronicznej są wydawane na podstawie ważnych zgłoszonych środków identyfikacji elektronicznej charakteryzujących się wysokim poziomem zaufania, nie jest konieczne powtarzanie sprawdzania tożsamości oraz procedur weryfikacji. Jeżeli środek identyfikacji elektronicznej służący jako podstawa nie został notyfikowany, wysoki poziom zaufania musi być potwierdzony przez jednostkę oceniającą zgodność, o której mowa w art. 2 ust. 13 rozporządzenia (WE) nr 765/2008, lub przez równoważny organ, oraz podejmowane są działania mające na celu wykazanie, że rezultaty tej poprzedniej procedury wydawania notyfikowanych środków identyfikacji elektronicznej zachowują ważność.

2.1.4. Powiązanie między środkami identyfikacji elektronicznej osób fizycznych i prawnych

W stosownych przypadkach w odniesieniu do powiązania między środkami identyfikacji elektronicznej osoby fizycznej i środkami identyfikacji elektronicznej osoby prawnej („powiązania") mają zastosowanie następujące warunki:

1) Musi istnieć możliwość zawieszania lub cofnięcia powiązania. Cykl życia powiązania (np. aktywacja, zawieszenie, odnowienie, cofnięcie) odbywa się zgodnie z krajowymi uznanymi procedurami.

2) Osoba fizyczna, której środek identyfikacji elektronicznej jest powiązany ze środkiem identyfikacji elektronicznej osoby prawnej, może powierzyć użytkowanie powiązania innej osobie fizycznej w oparciu o krajowe uznane procedury. Jednakże delegująca osoba fizyczna nadal ponosi odpowiedzialność.

3) Powiązanie realizowane jest w następujący sposób:

Poziom zaufania	Wymagane elementy
Niski	1. Sprawdzenie tożsamości osoby fizycznej działającej w imieniu osoby prawnej jest weryfikowane jako przeprowadzone na co najmniej niskim poziomie. 2. Powiązanie zostało ustanowione w oparciu o krajowe uznane procedury. 3. Wiarygodne źródło nie dysponuje wiedzą o statusie osoby fizycznej, który uniemożliwiałby jej działanie w imieniu osoby prawnej.
Średni	Pkt 3 z poziomu niskiego oraz: 1. Sprawdzenie tożsamości osoby fizycznej działającej w imieniu osoby prawnej jest weryfikowane jako przeprowadzone na poziomie średnim lub wysokim.

Poziom zaufania	Wymagane elementy
	2. Powiązanie zostało ustanowione w oparciu o krajowe uznane procedury, które doprowadziły do jego zarejestrowania w wiarygodnym źródle. 3. Powiązanie zostało zweryfikowane na podstawie informacji z wiarygodnego źródła.
Wysoki	Pkt 3 z poziomu niskiego i pkt 2 z poziomu średniego oraz: 1. Sprawdzenie tożsamości osoby fizycznej działającej w imieniu osoby prawnej jest weryfikowane jako przeprowadzone na poziomie wysokim. 2. Powiązanie zostało zweryfikowane w oparciu o niepowtarzalny identyfikator osoby prawnej stosowany w warunkach krajowych oraz na podstawie informacji z wiarygodnego źródła w sposób jednoznaczny identyfikujących osobę fizyczną.

2.2. *Zarządzanie środkami identyfikacji elektronicznej*

2.2.1. Cechy charakterystyczne i konstrukcja środków identyfikacji elektronicznej

Poziom zaufania	Wymagane elementy
Niski	1. Środek identyfikacji elektronicznej wykorzystuje co najmniej jeden czynnik uwierzytelniania. 2. Środek identyfikacji elektronicznej jest zaprojektowany w taki sposób, aby wystawiający podejmował rozsądne kroki w celu sprawdzenia, czy jest on stosowany jedynie przez osobę, do której należy, lub pod jej kontrolą.
Średni	1. Środek identyfikacji elektronicznej wykorzystuje co najmniej dwa czynniki uwierzytelniania należące do różnych kategorii. 2. Środek identyfikacji elektronicznej jest zaprojektowany w taki sposób, że można zakładać, iż jest on stosowany jedynie przez osobę, do której należy, lub pod jej kontrolą.
Wysoki	Jak przy poziomie średnim oraz: 1. Środek identyfikacji elektronicznej stanowi ochronę przed powielaniem i manipulacją oraz przed atakującymi dysponującymi wysokim potencjałem ataku. 2. Środek identyfikacji elektronicznej jest zaprojektowany w taki sposób, że może być niezawodnie chroniony przez osobę, do której należy, przed wykorzystaniem przez innych.

2.2.2. Wydawanie, dostarczanie i aktywacja

Poziom zaufania	Wymagane elementy
Niski	Po wydaniu środek identyfikacji elektronicznej jest dostarczany za pośrednictwem mechanizmu, co do którego można zakładać, iż przez jego zastosowanie środek dotrze wyłącznie do przeznaczonej osoby.
Średni	Po wydaniu środek identyfikacji elektronicznej jest dostarczany za pośrednictwem mechanizmu, co do którego można zakładać, iż przez jego zastosowanie środek zostanie oddany w posiadanie wyłącznie osobie, do której należy.
Wysoki	W procesie aktywacji sprawdza się, czy środek identyfikacji elektronicznej został oddany w posiadanie wyłącznie osobie, do której należy.

2.2.3. Zawieszenie, cofnięcie i przywrócenie

Poziom zaufania	Wymagane elementy
Niski	1. Można zawiesić lub wycofać środek identyfikacji elektronicznej w sposób terminowy i skuteczny. 2. Istnieją środki umożliwiające zapobieżenie nieuprawnionemu zawieszeniu, cofnięciu lub przywróceniu środka. 3. Przywrócenie środka odbywa się jedynie, jeśli w dalszym ciągu spełnione są wymagania w zakresie zaufania ustanowione przed zawieszeniem lub cofnięciem.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.2.4. Wznowienie i wymiana

Poziom zaufania	Wymagane elementy
Niski	Biorąc pod uwagę ryzyko wystąpienia zmiany w danych identyfikujących osobę, przy wznowieniu bądź wymianie muszą zostać spełnione te same wymagania w zakresie zaufania jak przy wstępnym sprawdzeniu i weryfikacji tożsamości lub wznowienia bądź wymiany dokonuje się na podstawie ważnego środka identyfikacji elektronicznej o tym samym lub wyższym poziomie zaufania.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Jak przy poziomie niskim oraz: w przypadku gdy wznowienie bądź wymiana odbywają się się na podstawie ważnego środka identyfikacji elektronicznej, dane dotyczące tożsamości są weryfikowane z wykorzystaniem wiarygodnego źródła.

2.3. *Uwierzytelnienie*

W tej części opisano zagrożenia związane ze stosowaniem mechanizmu uwierzytelniania i wymieniono wymagania odnoszące się do każdego poziomu zaufania. W niniejszej części kontrolę uznaje się za proporcjonalną do ryzyka na danym poziomie.

2.3.1. Mechanizm uwierzytelniania

W poniższej tabeli zestawiono wymagania na poszczególnych poziomach zaufania w odniesieniu do mechanizmu uwierzytelniania, za którego pośrednictwem osoba fizyczna lub prawna używa środka identyfikacji elektronicznej do potwierdzenia swojej tożsamości wobec strony ufającej.

Poziom zaufania	Wymagane elementy
Niski	1. Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności. 2. Jeżeli dane identyfikujące osobę są przechowywane w ramach mechanizmu uwierzytelniania, informacje ta są zabezpieczone w celu ochrony przed utratą i narażeniem na szwank, w tym analizą *off-line*. 3. Mechanizm uwierzytelniania jest sposobem realizacji kontroli zaufania na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o wyższym podstawowym potencjale ataku mogło zachwiać mechanizmami uwierzytelniania.

Poziom zaufania	Wymagane elementy
Średni	Jak przy poziomie niskim oraz: 1. Uwolnienie danych identyfikujących osobę jest poprzedzone wiarygodną weryfikacją środka identyfikacji elektronicznej oraz jego ważności za pomocą uwierzytelniania dynamicznego. 2. Mechanizm uwierzytelniania jest sposobem realizacji kontroli zaufania na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o umiarkowanym potencjale ataku mogło zachwiać mechanizmami uwierzytelniania.
Wysoki	Jak przy poziomie średnim oraz: mechanizm uwierzytelniania jest sposobem realizacji kontroli zaufania na potrzeby weryfikacji środków identyfikacji elektronicznej, dzięki któremu jest mało prawdopodobne, aby takie działania jak zgadywanie, podsłuchiwanie, odtwarzanie lub manipulowanie komunikacji przez atakującego o wysokim potencjale ataku mogło zachwiać mechanizmami uwierzytelniania.

2.4. *Zarządzanie i organizacja*

Wszystkie podmioty świadczące usługi związane z identyfikacją elektroniczną w obrocie transgranicznym („dostawcy") ustanawiają udokumentowane praktyki zarządzania bezpieczeństwem informacji, strategie, sposoby podejścia do zarządzania ryzykiem oraz inne uznane mechanizmy kontrolne, aby właściwe organy zarządzające odpowiedzialne za systemy identyfikacji elektronicznej w poszczególnych państwach członkowskich mogły mieć pewność, że skuteczne praktyki zostały wprowadzone. W części 2.4 wszystkie wymagania/elementy należy rozumieć jako współmierne z poziomem ryzyka dla danego poziomu.

2.4.1. Przepisy ogólne

Poziom zaufania	Wymagane elementy
Niski	1. Dostawcami świadczącymi usługi operacyjne objęte niniejszym rozporządzeniem są organy publiczne lub podmioty prawne uznane za takie przez prawo krajowe państwa członkowskiego, posiadające ugruntowaną organizację i pełną zdolność operacyjną we wszystkich elementach istotnych dla świadczenia usług. 2. Dostawcy przestrzegają wszelkich wymogów prawnych nałożonych na nich w związku z funkcjonowaniem i świadczeniem usług, w tym dotyczących rodzajów informacji, o jakie można się zwracać, sposobów dokonywania potwierdzania tożsamości, a także tego, jakie informacje mogą być przechowywane i przez jak długi czas. 3. Dostawcy są w stanie wykazać zdolność do ponoszenia ryzyka odpowiedzialności za szkody, jak również posiadanie wystarczających środków finansowych na kontynuowanie działalności i świadczenie usług. 4. Dostawcy odpowiadają za realizację wszystkich zobowiązań przekazanych innemu podmiotowi oraz zapewnienie zgodności z założeniami systemu, tak jakby sami wykonywali te zadania. 5. W odniesieniu do systemów identyfikacji elektronicznej nieustanowionych prawem krajowym musi istnieć opracowany skuteczny plan zakończenia działalności. Plan taki obejmuje uporządkowane zaprzestawanie świadczenia usług lub kontynuację przez innego dostawcę, sposób informowania właściwych organów i użytkowników końcowych, jak również szczegółowe informacje na temat sposobu ochrony, przechowywania i niszczenia rejestrów zgodnie z założeniami systemu.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.4.2. Opublikowane informacje i informacje dla użytkowników

Poziom zaufania	Wymagane elementy
Niski	1. Istnienie opublikowanej definicji usługi obejmującej wszystkie mające zastosowanie zasady, warunki i opłaty, w tym ewentualne ograniczenia dotyczące korzystania z niej. Definicja usługi obejmuje politykę ochrony prywatności. 2. Należy ustanowić odpowiednie działania i procedury w celu zapewnienia, że użytkownicy usługi zostaną poinformowani w odpowiednim czasie i w niezawodny sposób o wszelkich zmianach w definicji usług i wszelkich mających zastosowanie zasadach i warunkach oraz polityce prywatności w odniesieniu do określonej usługi. 3. Należy zastosować odpowiednie działania i procedury w celu zapewnienia udzielania pełnych i prawidłowych odpowiedzi na wnioski o informacje.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.4.3. Zarządzanie bezpieczeństwem informacji

Poziom zaufania	Wymagane elementy
Niski	Istnieje skuteczny system zarządzania bezpieczeństwem informacji w zakresie zarządzania i kontroli zagrożeń dla zaufania informacji.
Średni	Jak przy poziomie niskim oraz: system zarządzania bezpieczeństwem informacji odpowiada sprawdzonym normom lub zasadom zarządzania i kontroli zagrożeń dla zaufania informacji.
Wysoki	Takie same jak przy poziomie średnim.

2.4.4. Prowadzenie rejestrów

Poziom zaufania	Wymagane elementy
Niski	1. Zapisywanie i zachowywanie właściwych informacji przy użyciu skutecznego systemu zarządzania rejestrami z uwzględnieniem obowiązujących przepisów i dobrych praktyk w odniesieniu do ochrony danych i ich zatrzymywania. 2. Zatrzymywanie, o ile jest to dozwolone przez prawo krajowe lub inne krajowe porozumienia administracyjne, i ochrona rejestrów tak długo, jak długo jest to wymagane do celów kontroli i dochodzenia w sprawach naruszeń zaufania, oraz przechowywanie, po czym rejestry te są niszczone w bezpieczny sposób.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.4.5. Obiekty i personel

W poniższej tabeli przedstawiono wymagania dotyczące obiektów i personelu oraz – w stosownych przypadkach – podwykonawców, wykonujących obowiązki objęte niniejszym rozporządzeniem. Zgodność ze wszystkimi wymaganiami powinna być proporcjonalna do poziomu ryzyka związanego z ustalonym poziomem zaufania.

Poziom zaufania	Wymagane elementy
Niski	1. Istnienie procedur zapewniających, że pracownicy i podwykonawcy są odpowiednio przeszkoleni i wykwalifikowani oraz dysponują doświadczeniem w zakresie umiejętności potrzebnych do wykonywania swoich funkcji. 2. Wystarczająca liczba pracowników i podwykonawców do odpowiedniego funkcjonowania i zapewnienia obsługi usługi, zgodnie z jej zasadami i procedurami. 3. Obiekty służące do świadczenia usługi są stale monitorowane i chronione przed szkodami spowodowanymi przez wydarzenia związane ze środowiskiem naturalnym, nieuprawniony dostęp i inne czynniki, które mogą mieć wpływ na bezpieczeństwo usługi. 4. Obiekty służące do świadczenia usługi gwarantują, że dostęp do stref przechowywania lub przetwarzania danych osobowych, kryptograficznych lub innych informacji podlegających szczególnej ochronie jest ograniczony do upoważnionych pracowników lub podwykonawców.
Średni	Takie same jak przy poziomie niskim.
Wysoki	Takie same jak przy poziomie niskim.

2.4.6. Kontrole techniczne

Poziom zaufania	Wymagane elementy
Niski	1. Istnienie proporcjonalnych kontroli technicznych w celu zarządzania ryzykiem, na jakie narażone jest bezpieczeństwo świadczonych usług, zapewnienie ochrony poufności, integralności i dostępności przetwarzanych informacji. 2. Elektroniczne kanały komunikacji wykorzystywane do wymiany informacji podlegających szczególnej ochronie lub informacji osobowych są zabezpieczone przed podsłuchem, manipulacją i odtwarzaniem. 3. Dostęp do szczególnie chronionych materiałów kryptograficznych, jeżeli są wykorzystywane do wydawania środków identyfikacji elektronicznej i elektronicznego uwierzytelniania, jest ograniczony do funkcji i zakresu zastosowania bezwzględnie wymagających dostępu. Należy zapewnić, aby materiały te nigdy nie były trwale przechowywane w postaci zwykłego tekstu. 4. Istnieją procedury zapewniające, że bezpieczeństwo jest trwale utrzymywane oraz że istnieje zdolność reagowania na zmiany poziomu ryzyka, incydenty i przypadki naruszenia zaufania. 5. Wszystkie nośniki zawierające informacje osobowe, kryptograficzne lub inne podlegające szczególnej ochronie są przechowywane, transportowane i usuwane w bezpieczny sposób.
Średni	Takie same jak przy poziomie niskim oraz: materiały kryptograficzne podlegające szczególnej ochronie, jeżeli są wykorzystywane do wydawania środków identyfikacji elektronicznej i uwierzytelniania elektronicznego, są chronione przed nieuprawnionymi manipulacjami.
Wysoki	Takie same jak przy poziomie średnim.

2.4.7. Zgodność i audyt

Poziom zaufania	Wymagane elementy
Niski	Istnienie okresowych audytów wewnętrznych ukierunkowanych na wszystkie elementy istotne dla dostawy świadczonych usług w celu zapewnienia zgodności ze stosowną polityką.

Poziom zaufania	Wymagane elementy
Średni	Istnienie okresowych niezależnych audytów wewnętrznych lub zewnętrznych ukierunkowanych na wszystkie elementy istotne dla dostawy świadczonych usług w celu zapewnienia zgodności ze stosowną polityką.
Wysoki	1. Istnienie okresowych niezależnych audytów zewnętrznych ukierunkowanych na wszystkie elementy istotne dla dostawy świadczonych usług w celu zapewnienia zgodności ze stosowną polityką. 2. Jeśli system zarządzany jest bezpośrednio przez organ publiczny, audyty przeprowadza się zgodnie z prawem krajowym.

ROZPORZĄDZENIE WYKONAWCZE KOMISJI (UE) 2015/1503

z dnia 8 września 2015 r.

ustanawiające standardowe wartości w przywozie dla ustalania ceny wejścia niektórych owoców i warzyw

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1308/2013 z dnia 17 grudnia 2013 r. ustanawiające wspólną organizację rynków produktów rolnych oraz uchylające rozporządzenia Rady (EWG) nr 922/72, (EWG) nr 234/79, (WE) nr 1037/2001 i (WE) nr 1234/2007 ([1]),

uwzględniając rozporządzenie wykonawcze Komisji (UE) nr 543/2011 z dnia 7 czerwca 2011 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1234/2007 w odniesieniu do sektorów owoców i warzyw oraz przetworzonych owoców i warzyw ([2]), w szczególności jego art. 136 ust. 1,

a także mając na uwadze, co następuje:

(1) Rozporządzenie wykonawcze (UE) nr 543/2011 przewiduje – zgodnie z wynikami wielostronnych negocjacji handlowych Rundy Urugwajskiej – kryteria, na których podstawie Komisja ustala standardowe wartości dla przywozu z państw trzecich, w odniesieniu do produktów i okresów określonych w części A załącznika XVI do wspomnianego rozporządzenia.

(2) Standardowa wartość w przywozie jest obliczana każdego dnia roboczego, zgodnie z art. 136 ust. 1 rozporządzenia wykonawczego (UE) nr 543/2011, przy uwzględnieniu podlegających zmianom danych dziennych. Niniejsze rozporządzenie powinno zatem wejść w życie z dniem jego opublikowania w *Dzienniku Urzędowym Unii Europejskiej*,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

Standardowe wartości celne w przywozie, o których mowa w art. 136 rozporządzenia wykonawczego (UE) nr 543/2011, są ustalone w załączniku do niniejszego rozporządzenia.

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie z dniem jego opublikowania w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 8 września 2015 r.

W imieniu Komisji,

za Przewodniczącego,

Jerzy PLEWA

Dyrektor Generalny ds. Rolnictwa i Rozwoju Obszarów Wiejskich

([1]) Dz.U. L 347 z 20.12.2013, s. 671.
([2]) Dz.U. L 157 z 15.6.2011, s. 1.

ZAŁĄCZNIK

Standardowe wartości w przywozie dla ustalania ceny wejścia niektórych owoców i warzyw

(EUR/100 kg)

Kod CN	Kod państw trzecich (1)	Standardowa wartość w przywozie
0702 00 00	MA	173,3
	MK	48,7
	XS	41,5
	ZZ	87,8
0707 00 05	MK	76,3
	TR	116,3
	XS	42,0
	ZZ	78,2
0709 93 10	TR	133,1
	ZZ	133,1
0805 50 10	AR	135,9
	BO	135,7
	CL	125,5
	UY	142,2
	ZA	136,9
	ZZ	135,2
0806 10 10	EG	239,8
	MK	63,9
	TR	129,5
	ZZ	144,4
0808 10 80	AR	188,7
	BR	93,9
	CL	134,4
	NZ	143,4
	US	112,5
	UY	110,5
	ZA	117,6
	ZZ	128,7
0808 30 90	AR	131,9
	CL	100,0
	TR	122,9
	ZA	113,5
	ZZ	117,1
0809 30 10, 0809 30 90	MK	80,1
	TR	141,7
	ZZ	110,9

(EUR/100 kg)

Kod CN	Kod państw trzecich (1)	Standardowa wartość w przywozie
0809 40 05	BA	54,8
	IL	336,8
	MK	44,1
	XS	70,3
	ZZ	126,5

(1) Nomenklatura krajów ustalona w rozporządzeniu Komisji (UE) nr 1106/2012 z dnia 27 listopada 2012 r. w sprawie wykonania rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 471/2009 w sprawie statystyk Wspólnoty dotyczących handlu zagranicznego z państwami trzecimi, w odniesieniu do aktualizacji nazewnictwa państw i terytoriów (Dz.U. L 328 z 28.11.2012, s. 7). Kod „ZZ" odpowiada „innym pochodzeniom".

DECYZJE

DECYZJA WYKONAWCZA KOMISJI (UE) 2015/1504

z dnia 7 września 2015 r.

w sprawie przyznania niektórym państwom członkowskim odstępstw dotyczących dostarczania danych statystycznych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 1099/2008 w sprawie statystyki energii

(notyfikowana jako dokument nr C(2015) 6105)

(Jedynie teksty w języku estońskim, greckim, francuskim, niderlandzkim i słowackim są autentyczne)

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1099/2008 z dnia 22 października 2008 r. w sprawie statystyki energii ([1]), w szczególności jego art. 5 ust. 4 i art. 10 ust. 2,

a także mając na uwadze, co następuje:

(1) Zgodnie z art. 5 ust. 4 rozporządzenia (WE) nr 1099/2008 na należycie uzasadniony wniosek państwa członkowskiego można przyznać odstępstwa w odniesieniu do tych części statystyki krajowej, których gromadzenie mogłoby stanowić zbytnie obciążenie dla respondentów.

(2) Wnioski o przyznanie odstępstw w odniesieniu do dostarczania za niektóre lata referencyjne szczegółowych danych statystycznych dotyczących zużycia energii w gospodarstwach domowych z podziałem na rodzaj końcowego przeznaczenia złożyły Belgia, Estonia, Cypr i Słowacja.

(3) Informacje przedstawione przez te państwa członkowskie stanowią uzasadnienie przyznania odstępstw.

(4) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu ds. Europejskiego Systemu Statystycznego,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Przyznaje się następujące odstępstwa od przepisów rozporządzenia (WE) nr 1099/2008:

1) Belgii przyznaje się odstępstwo od przedstawienia danych za rok referencyjny 2015 w zakresie pkt 1.2.3 pozycje 4.2.1–4.2.5, pkt 2.2.3 pozycje 4.2.1–4.2.5, pkt 3.2.3 pozycje 3.1–3.6, pkt 4.2.3 pozycje 7.2.1–7.2.5 oraz pkt 5.2.4 pozycje 4.2.1–4.2.5 załącznika B dotyczących statystyki szczegółowej w zakresie zużycia energii w gospodarstwach domowych z podziałem na rodzaj końcowego przeznaczenia (jak określono w pkt 2.3 pozycja 26 „Inne sektory – Gospodarstwa domowe" załącznika A);

([1]) Dz.U. L 304 z 14.11.2008, s. 1.

2) Estonii przyznaje się odstępstwo od przedstawienia danych za lata referencyjne 2015, 2016 i 2017 w zakresie pkt 1.2.3 pozycje 4.2.1–4.2.5, pkt 2.2.3 pozycje 4.2.1–4.2.5, pkt 3.2.3 pozycje 3.1–3.6, pkt 4.2.3 pozycje 7.2.1–7.2.5 oraz pkt 5.2.4 pozycje 4.2.1–4.2.5 załącznika B dotyczących statystyki szczegółowej w zakresie zużycia energii w gospodarstwach domowych z podziałem na rodzaj końcowego przeznaczenia (jak określono w pkt 2.3 pozycja 26 „Inne sektory – Gospodarstwa domowe" załącznika A);

3) Cyprowi przyznaje się odstępstwo od przedstawienia danych za lata referencyjne 2015, 2016 i 2017 w zakresie pkt 1.2.3 pozycje 4.2.1–4.2.5, pkt 2.2.3 pozycje 4.2.1–4.2.5, pkt 3.2.3 pozycje 3.1–3.6 oraz pkt 5.2.4 pozycje 4.2.1–4.2.5 załącznika B dotyczących statystyki szczegółowej w zakresie zużycia energii w gospodarstwach domowych z podziałem na rodzaj końcowego przeznaczenia (jak określono w pkt 2.3 pozycja 26 „Inne sektory – Gospodarstwa domowe" załącznika A);

4) Słowacji przyznaje się odstępstwo od przedstawienia danych za lata referencyjne 2015 i 2016 w zakresie pkt 1.2.3 pozycje 4.2.1–4.2.5, pkt 2.2.3 pozycje 4.2.1–4.2.5, pkt 3.2.3 pozycje 3.1–3.6, pkt 4.2.3 pozycje 7.2.1–7.2.5 oraz pkt 5.2.4 pozycje 4.2.1–4.2.5 załącznika B dotyczących statystyki szczegółowej w zakresie zużycia energii w gospodarstwach domowych z podziałem na rodzaj końcowego przeznaczenia (jak określono w pkt 2.3 pozycja 26 „Inne sektory – Gospodarstwa domowe" załącznika A).

Artykuł 2

Niniejsza decyzja jest skierowana do Królestwa Belgii, Republiki Estońskiej, Republiki Cypryjskiej i Republiki Słowackiej.

Sporządzono w Brukseli dnia 7 września 2015 r.

W imieniu Komisji
Marianne THYSSEN
Członek Komisji

DECYZJA WYKONAWCZA KOMISJI (UE) 2015/1505

z dnia 8 września 2015 r.

ustanawiająca specyfikacje techniczne i formaty dotyczące zaufanych list zgodnie z art. 22 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE ([1]), w szczególności jego art. 22 ust. 5,

a także mając na uwadze, co następuje:

(1) Zaufane listy są nieodzowne do budowania zaufania wśród podmiotów rynkowych, ponieważ wskazują status dostawcy usługi podczas nadzoru.

(2) Decyzja Komisji 2009/767/WE ([2]), w której nałożono na państwa członkowskie obowiązek tworzenia, prowadzenia i publikowania zaufanych list zawierających informacje dotyczące podmiotów, które świadczą usługi certyfikacyjne i powszechnie wystawiają kwalifikowane certyfikaty zgodnie z dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE ([3]) i które podlegają nadzorowi i są akredytowane przez państwa członkowskie, ułatwiła transgraniczne stosowanie podpisu elektronicznego.

(3) W art. 22 rozporządzenia (UE) nr 910/2014 zobowiązano państwa członkowskie do sporządzania, prowadzenia i publikowania – w zabezpieczony sposób – elektronicznie podpisanych lub opatrzonych pieczęcią zaufanych list w postaci umożliwiającej automatyczne przetwarzanie oraz do powiadomienia Komisji o podmiotach odpowiedzialnych za sporządzanie krajowych zaufanych list.

(4) Dostawcę usług zaufania należy uznać za kwalifikowanego dostawcę, a świadczone przez niego usługi zaufania – za kwalifikowane, jeśli kwalifikowany status został przypisany dostawcy na zaufanej liście. W celu zapewnienia, by inne obowiązki wynikające z rozporządzenia (UE) nr 910/2014, w szczególności te określone w artykułach 27 i 37, mogły z łatwością być wypełniane przez dostawców świadczących usługi na odległość oraz drogą elektroniczną, a także aby spełnić uzasadnione oczekiwania innych podmiotów świadczących usługi certyfikacyjne, które nie wystawiają certyfikatów kwalifikowanych, lecz świadczą usługi związane z podpisami elektronicznymi zgodnie z dyrektywą 1999/93/WE i zostały umieszczone na listach do dnia 30 czerwca 2016 r., należy umożliwić państwom członkowskim dodawanie do list usług zaufania innych niż kwalifikowane usługi zaufania, na zasadzie dobrowolności, na szczeblu krajowym, o ile zostanie wyraźnie wskazane, że usługi te nie są kwalifikowane zgodnie z rozporządzeniem (UE) nr 910/2014.

(5) Zgodnie z motywem 25 rozporządzenia (UE) nr 910/2014 państwa członkowskie mogą dodać inne rodzaje ustalonych na poziomie krajowym usług zaufania niż określone w art. 3 ust. 16 rozporządzenia (UE) nr 910/2014, o ile zostanie wyraźnie wskazane, że usługi te nie są kwalifikowane zgodnie z rozporządzeniem (UE) nr 910/2014.

(6) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na podstawie art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Każde państwo członkowskie tworzy, publikuje i prowadzi zaufane listy zawierające informacje dotyczące nadzorowanych przez nie dostawców kwalifikowanych usług zaufania, a także informacje na temat świadczonych przez nich kwalifikowanych usług zaufania. Listy te są zgodne ze specyfikacjami technicznymi określonymi w załączniku I.

([1]) Dz.U. L 257 z 28.8.2014, s. 73.

([2]) Decyzja Komisji 2009/767/WE z dnia 16 października 2009 r. ustanawiająca środki ułatwiające korzystanie z procedur realizowanych drogą elektroniczną poprzez „pojedyncze punkty kontaktowe" zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (Dz.U. L 274 z 20.10.2009, s. 36).

([3]) Dyrektywa 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych (Dz.U. L 13 z 19.1.2000, s. 12).

Artykuł 2

Państwa członkowskie mogą ująć w zaufanych listach informacje na temat dostawców niekwalifikowanych usług zaufania wraz z informacjami dotyczącymi świadczonych przez nich niekwalifikowanych usług zaufania. W liście wskazuje się wyraźnie, którzy dostawcy usług zaufania nie są dostawcami kwalifikowanymi oraz które świadczone przez nich usługi zaufania nie są kwalifikowane.

Artykuł 3

1. Zgodnie z art. 22 ust. 2 rozporządzenia (UE) nr 910/2014 państwa członkowskie są zobowiązane do podpisania elektronicznie lub opatrzenia pieczęcią elektroniczną swojej zaufanej listy w postaci dostosowanej do automatycznego przetwarzania, zgodnie ze specyfikacjami technicznymi określonymi w załączniku I.

2. Jeżeli państwo członkowskie publikuje zaufaną listę w wersji czytelnej dla człowieka, zapewnia ono, by ta postać listy zawierała te same dane co postać dostosowana do automatycznego przetwarzania, oraz podpisuje ją elektronicznie lub opatruje pieczęcią elektroniczną zgodnie ze specyfikacjami technicznymi określonymi w załączniku I.

Artykuł 4

1. Państwa członkowskie przekazują Komisji informacje, o których mowa w art. 22 ust. 3 rozporządzenia (UE) nr 910/2014 przy użyciu wzoru powiadomienia w załączniku II.

2. W skład informacji, o których mowa w ust. 1, wchodzą co najmniej dwa certyfikaty publicznego klucza operatora systemu o okresach ważności różniących się o co najmniej trzy miesiące, odpowiadające kluczom prywatnym, które mogą zostać wykorzystane do elektronicznego podpisania lub opatrzenia pieczęcią elektroniczną zaufanej listy w postaci dostosowanej do automatycznego przetwarzania oraz w postaci czytelnej dla człowieka, gdy jest publikowana.

3. Zgodnie z art. 22 ust. 4 rozporządzenia (UE) nr 910/2014 Komisja podaje do wiadomości publicznej za pośrednictwem bezpiecznego kanału do uwierzytelnionego serwera internetowego informacje, o których mowa w ust. 1 i 2, zgłoszone przez państwa członkowskie, podpisane elektronicznie lub opatrzone pieczęcią elektroniczną, w postaci dostosowanej do automatycznego przetwarzania.

4. Komisja może podać do wiadomości publicznej za pośrednictwem bezpiecznego kanału do uwierzytelnionego serwera internetowego informacje, o których mowa w ust. 1 i 2, zgłoszone przez państwa członkowskie, podpisane lub opatrzone pieczęcią, w postaci czytelnej dla człowieka.

Artykuł 5

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsza decyzja wiąże w całości i jest bezpośrednio stosowana we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 8 września 2015 r.

W imieniu Komisji

Jean-Claude JUNCKER

Przewodniczący

ZAŁĄCZNIK I

SPECYFIKACJA TECHNICZNA DOTYCZĄCA WSPÓLNEGO WZORU ZAUFANYCH LIST

ROZDZIAŁ I

WYMOGI OGÓLNE

Zaufane listy zawierają zarówno aktualne, jak i wszystkie historyczne informacje, począwszy od daty umieszczenia dostawcy usług zaufania na zaufanych listach, dotyczące statusu usług zaufania wymienionych na listach.

Terminy „zatwierdzony", „akredytowany" lub „nadzorowany" w niniejszej specyfikacji obejmują również krajowe systemy zatwierdzania, jednak dodatkowe informacje na temat właściwości wszelkich takich krajowych systemów zostaną podane przez państwa członkowskie w ich zaufanej liście. Obejmuje to także wyjaśnienia dotyczące ewentualnych różnic w stosunku do systemów nadzoru stosowanych wobec kwalifikowanych dostawców usług zaufania oraz świadczonych przez nich kwalifikowanych usług zaufania.

Informacje zawarte w zaufanej liście mają służyć przede wszystkim wspieraniu walidacji tokenów kwalifikowanych usług zaufania, tj. obiektów fizycznych lub binarnych (logicznych) wygenerowanych lub wydanych w wyniku korzystania z kwalifikowanej usługi zaufania, np. kwalifikowanych podpisów elektronicznych/kwalifikowanych pieczęci elektronicznych, zaawansowanych podpisów elektronicznych/zaawansowanych pieczęci elektronicznych weryfikowanych certyfikatem kwalifikowanym, kwalifikowanymi znacznikami czasu, kwalifikowanymi dowodami doręczenia elektronicznego itp.

ROZDZIAŁ II

SZCZEGÓŁOWA SPECYFIKACJA DOTYCZĄCA WSPÓLNEGO WZORU ZAUFANYCH LIST

Niniejsza specyfikacja opiera się na specyfikacji i wymogach określonych w ETSI TS 119 612 v2.1.1 (zwanej dalej ETSI TS 119 612).

W przypadku braku określenia szczególnego wymogu w niniejszej specyfikacji w całości zastosowanie mają wymogi określone w klauzulach 5 i 6 ETSI TS 119 612. Jeśli w niniejszej specyfikacji określono wymogi szczególne, mają one pierwszeństwo przed odpowiednimi wymogami ETSI TS 119 612. W przypadku rozbieżności między niniejszą specyfikacją a specyfikacją określoną w ETSI TS 119 612 pierwszeństwo ma niniejsza specyfikacja.

Scheme name (nazwa systemu) (klauzula 5.3.6)

Pole to musi występować i musi być zgodne ze specyfikacją zawartą w klauzuli 5.3.6 TS 119 612, przy czym system musi być określany następującą nazwą:

„EN_name_value" = „Zaufana lista zawierająca informacje dotyczące kwalifikowanych dostawców usług zaufania, którzy są objęci nadzorem przez wydające państwo członkowskie, wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania, zgodnie z odpowiednimi przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE".

Scheme information (informacje o systemie) URI (klauzula 5.3.7)

Pole to musi występować i musi być zgodne ze specyfikacją zawartą w klauzuli 5.3.7 TS 119 612, przy czym „odpowiednie informacje o systemie" obejmują co najmniej:

a) informacje wprowadzające wspólne dla wszystkich państw członkowskich odnoszące się do zakresu i kontekstu zaufanej listy, podstawowego systemu nadzoru oraz w stosownych przypadkach mającego zastosowanie krajowego systemu (krajowych systemów) zatwierdzania (np. akredytacji). Należy zastosować wspólny tekst zamieszczony poniżej, w którym łańcuch znaków „[*nazwa danego państwa członkowskiego*]" zastępuje się nazwą danego państwa członkowskiego:

> „Niniejsza lista jest zaufaną listą zawierającą informacje dotyczące kwalifikowanych dostawców usług zaufania, którzy są objęci nadzorem przez [*nazwa danego państwa członkowskiego*], wraz z informacjami dotyczącymi świadczonych przez nich kwalifikowanych usług zaufania, zgodnie z odpowiednimi przepisami rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE.

Transgraniczne stosowanie podpisów elektronicznych zostało ułatwione poprzez decyzję Komisji 2009/767/WE z dnia 16 października 2009 r., w której nałożono na państwa członkowskie obowiązek tworzenia, prowadzenia i publikowania zaufanych list zawierających informacje dotyczące nadzorowanych/akredytowanych przez państwa członkowskie podmiotów świadczących usługi certyfikacyjne i powszechnie wystawiających kwalifikowane certyfikaty zgodnie z dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych. Niniejsza zaufana lista jest kontynuacją zaufanej listy ustanowionej decyzją 2009/767/WE".

Zaufane listy są podstawowym elementem procesu budowania zaufania wśród operatorów rynku elektronicznego, ponieważ umożliwiają użytkownikom ustalenie statusu kwalifikowanego i historii statusu dostawców usług zaufania oraz ich usług.

Zaufane listy państw członkowskich zawierają co najmniej informacje określone w art. 1 i 2 decyzji wykonawczej Komisji (UE) 2015/1505.

Państwa członkowskie mogą zamieszczać na zaufanych listach informacje dotyczące niekwalifikowanych dostawców usług zaufania wraz z informacjami dotyczącymi świadczonych przez nich niekwalifikowanych usług zaufania. Wyraźnie wskazuje się, że dostawcy ci nie są kwalifikowani zgodnie z rozporządzeniem (UE) nr 910/2014.

Państwa członkowskie mogą zamieszczać na zaufanych listach informacje dotyczące określonych na szczeblu krajowym usług zaufania innego rodzaju niż te określone w art. 3 ust. 16 rozporządzenia (UE) nr 910/2014. Wyraźnie wskazuje się, że usługi te nie są kwalifikowane zgodnie z rozporządzeniem (UE) nr 910/2014;

b) określone informacje dotyczące podstawowego systemu nadzoru oraz w stosownych przypadkach mającego zastosowanie krajowego systemu lub systemów zatwierdzania (np. akredytacji), w szczególności ([1]):

   1) informacje na temat krajowego systemu nadzoru mającego zastosowanie do kwalifikowanych i niekwalifikowanych dostawców usług zaufania oraz do świadczonych przez nich kwalifikowanych i niekwalifikowanych usług zaufania zgodnie z rozporządzeniem (UE) nr 910/2014;

   2) w stosownych przypadkach informacje dotyczące krajowego systemu dobrowolnych akredytacji mającego zastosowanie do podmiotów świadczących usługi certyfikacyjne, które to podmioty wydawały kwalifikowane certyfikaty na podstawie dyrektywy 1999/93/WE.

   W odniesieniu do każdego podstawowego systemu wymienionego powyżej te określone informacje muszą obejmować co najmniej:

   1) ogólny opis;

   2) informacje dotyczące procesu stosowanego na potrzeby krajowego systemu nadzoru oraz – w stosownych przypadkach – na potrzeby zatwierdzenia w ramach krajowego systemu zatwierdzania;

   3) informacje dotyczące kryteriów nadzorowania lub – w stosownych przypadkach – zatwierdzania dostawców usług zaufania;

   4) informacje dotyczące kryteriów i zasad wyboru inspektorów/audytorów i określające sposób oceniania przez nich dostawców usług zaufania oraz świadczonych przez nich usług zaufania;

   5) w stosownych przypadkach inne informacje kontaktowe i ogólne dotyczące funkcjonowania systemu.

Scheme type/community/rules (rodzaj systemu/wspólnota/zasady) (klauzula 5.3.9)

Pole to musi występować i musi być zgodne ze specyfikacją zawartą w klauzuli 5.3.9 TS 119 612.

Zawiera ono URI wyłącznie w języku angielskim (ZK).

([1]) Te zbiory informacji mają zasadnicze znaczenie dla stron ufających przy dokonywaniu oceny poziomu jakości i bezpieczeństwa takich systemów. Takie zbiory informacji są udostępniane na poziomie zaufanej listy za pośrednictwem „Scheme information URI" (klauzula 5.3.7 – informacje udostępniane przez państwa członkowskie), „Scheme type/community/rules" (klauzula 5.3.9 – z użyciem tekstu wspólnego dla wszystkich państw członkowskich), „TSL policy/legal notice" (klauzula 5.3.11 – tekst wspólny dla wszystkich państw członkowskich, wraz z możliwością dodania przez każde państwo członkowskie swojego własnego tekstu/odniesień). Dodatkowe informacje dotyczące takich systemów w odniesieniu do niekwalifikowanych usług zaufania i określonych na szczeblu krajowym (kwalifikowanych) usług zaufania mogą być w stosownych przypadkach i w razie potrzeby udostępniane na poziomie usług (np. aby umożliwić rozróżnienie kilku poziomów jakości/bezpieczeństwa) za pośrednictwem „Scheme service definition URI" (klauzula 5.5.6).

Zawiera ono co najmniej dwa URI:

1) URI wspólny dla zaufanych list wszystkich państw członkowskich wskazujący tekst opisowy, który musi mieć zastosowanie do wszystkich zaufanych list, w brzmieniu:

URI: http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon

Tekst opisowy:

„Participation in a scheme

Each Member State must create a trusted list including information related to the qualified trust service providers that are under supervision, together with information related to the qualified trust services provided by them, in accordance with the relevant provisions laid down in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

The present implementation of such trusted lists is also to be referred to in the list of links (pointers) towards each Member State's trusted list, compiled by the European Commission.

Policy/rules for the assessment of the listed services

Member States must supervise qualified trust service providers established in the territory of the designating Member State as laid down in Chapter III of Regulation (EU) No 910/2014 to ensure that those qualified trust service providers and the qualified trust services that they provide meet the requirements laid down in the Regulation.

The trusted lists of Member States include, as a minimum, information specified in Articles 1 and 2 of Commission Implementing Decision (EU) 2015/1505.

The trusted lists include both current and historical information about the status of listed trust services.

Each Member State's trusted list must provide information on the national supervisory scheme and where applicable, national approval (e.g. accreditation) scheme(s) under which the trust service providers and the trust services that they provide are listed.

Interpretation of the Trusted List

The general user guidelines for applications, services or products relying on a trusted list published in accordance with Regulation (EU) No 910/2014 are as follows:

The »qualified« status of a trust service is indicated by the combination of the »Service type identifier« (»Sti«) value in a service entry and the status according to the »Service current status« field value as from the date indicated in the »Current status starting date and time«. Historical information about such a qualified status is similarly provided when applicable.

Regarding qualified trust service providers issuing qualified certificates for electronic signatures, for electronic seals and/or for website authentication:

A »CA/QC« »Service type identifier« (»Sti«) entry (possibly further qualified as being a »RootCA-QC« through the use of the appropriate »Service information extension« (»Sie«) additionalServiceInformation Extension)

— indicates that any end-entity certificate issued by or under the CA represented by the »Service digital identifier« (»Sdi«) CA's public key and CA's name (both CA data to be considered as trust anchor input), is a qualified certificate (QC) provided that it includes at least one of the following:

  — the id-etsi-qcs-QcCompliance ETSI defined statement (id-etsi-qcs 1),

  — the 0.4.0.1456.1.1 (QCP+) ETSI defined certificate policy OID,

— the 0.4.0.1456.1.2 (QCP) ETSI defined certificate policy OID,

and provided this is ensured by the Member State Supervisory Body through a valid service status (i.e. »undersupervision«, »supervisionincessation«, »accredited« or »granted«) for that entry.

— **and IF** »Sie« »Qualifications Extension« information is present, then in addition to the above default rule, those certificates that are identified through the use of »Sie« »Qualifications Extension« information, constructed as a sequence of filters further identifying a set of certificates, must be considered according to the associated qualifiers providing additional information regarding their qualified status, the »SSCD support« and/or »Legal person as subject« (e.g. certificates containing a specific OID in the Certificate Policy extension, and/or having a specific »Key usage« pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). These qualifiers are part of the following set of »Qualifiers« used to compensate for the lack of information in the corresponding certificate content, and that are used respectively:

— to indicate the qualified certificate nature:

— »QCStatement« meaning the identified certificate(s) is(are) qualified under Directive 1999/93/EC,

— »QCForESig« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic signature under Regulation (EU) No 910/2014,

— »QCForESeal« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for electronic seal under Regulation (EU) No 910/2014,

— »QCForWSA« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), is (are) qualified certificate(s) for web site authentication under Regulation (EU) No 910/2014,

— to indicate that the certificate is not to be considered as qualified:

— »NotQualified« meaning the identified certificate(s) is(are) not to be considered as qualified; and/or

— to indicate the nature of the SSCD support:

— »QCWithSSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in an SSCD, or

— »QCNoSSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in an SSCD, or

— »QCSSCDStatusAsInCert« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key residing in an SSCD,

— to indicate the nature of the QSCD support:

— »QCWithQSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have their private key residing in a QSCD, or

— »QCNoQSCD« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), have not their private key residing in a QSCD, or

— »QCQSCDStatusAsInCert« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), does(do) contain proper machine processable information about whether or not their private key is residing in a QSCD,

— »QCQSCDManagedOnBehalf« indicating that all certificates identified by the applicable list of criteria, when they are claimed or stated as qualified, have their private key is residing in a QSCD for which the generation and management of that private key is done by a qualified TSP on behalf of the entity whose identity is certified in the certificate; and/or

— to indicate issuance to Legal Person:

— »QCForLegalPerson« meaning the identified certificate(s), when claimed or stated as qualified certificate(s), are issued to a Legal Person under Directive 1999/93/EC.

Note: The information provided in the trusted list is to be considered as accurate meaning that:

— if none of the id-etsi-qcs 1 statement, QCP OID or QCP+ OID information is included in an end-entity certificate, and

— if no »Sie« »Qualifications Extension« information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a »QCStatement« qualifier, or

— an »Sie« »Qualifications Extension« information is present for the trust anchor CA/QC corresponding service entry to qualify the certificate with a »NotQualified« qualifier,

then the certificate is not to be considered as qualified.

»Service digital identifiers« are to be used as Trust Anchors in the context of validating electronic signatures or seals for which signer's or seal creator's certificate is to be validated against TL information, hence only the public key and the associated subject name are needed as Trust Anchor information. When more than one certificate are representing the public key identifying the service, they are to be considered as Trust Anchor certificates conveying identical information with regard to the information strictly required as Trust Anchor information.

The general rule for interpretation of any other »Sti« type entry is that, for that »Sti« identified service type, the listed service named according to the »Service name« field value and uniquely identified by the »Service digital identity« field value has the current qualified or approval status according to the »Service current status« field value as from the date indicated in the »Current status starting date and time«.

Specific interpretation rules for any additional information with regard to a listed service (e.g. »Service information extensions« field) may be found, when applicable, in the Member State specific URI as part of the present »Scheme type/community/rules« field.

Please refer to the applicable secondary legislation pursuant to Regulation (EU) No 910/2014 for further details on the fields, description and meaning for the Member States' trusted lists.".

2) URI określony dla zaufanej listy każdego państwa członkowskiego wskazujący na tekst opisowy, który musi mieć zastosowanie do zaufanej listy tego państwa członkowskiego:

http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC, w którym CC = kod kraju zgodny z ISO 3166-1 ([1]) alfa-2 umieszczany w polu dotyczącym terytorium objętego systemem – „Scheme territory" (klauzula 5.3.10),

— gdzie użytkownicy mogą uzyskać dostęp do określonej polityki/zasad danego państwa członkowskiego, na których podstawie usługi zaufania zawarte na liście są oceniane zgodnie z systemem nadzoru państwa członkowskiego oraz w stosownych przypadkach zgodnie z systemem zatwierdzania,

— gdzie użytkownicy mogą uzyskać dostęp do określonego opisu danego państwa członkowskiego, dotyczącego sposobu korzystania z treści zaufanej listy i interpretowania jej w odniesieniu do wyszczególnionych na niej niekwalifikowanych usług zaufania lub usług zaufania określonych na szczeblu krajowym. Można to wykorzystać do wskazania potencjalnego poziomu szczegółowości krajowych systemów zatwierdzania związanych z CSP niewystawiającymi certyfikatów kwalifikowanych oraz do wskazania sposobu wykorzystania do tego celu pól „Scheme service definition URI" (klauzula 5.5.6) i „Service information extension" (klauzula 5.5.9).

Państwa członkowskie MOGĄ definiować i stosować dodatkowe URI rozszerzające wskazany powyżej URI właściwy dla państwa członkowskiego (tzn. URI zdefiniowany na podstawie danego hierarchicznego określonego URI).

TSL policy/legal notice (zastrzeżenie dot. polityki/prawne) (klauzula 5.3.11)

Pole to musi występować i musi być zgodne ze specyfikacją zawartą w klauzuli 5.3.11 TS 119 612, przy czym zastrzeżenie dotyczące polityki/zastrzeżenie prawne odnoszące się do statusu prawnego systemu lub wymogów prawnych spełnianych przez system, w którego jurysdykcji lista została ustanowiona, lub wszelkich ograniczeń

([1]) ISO 3166-1:2006: Kody nazw krajów i ich jednostek administracyjnych – Część 1: Kody krajów.

i warunków, z których uwzględnieniem zaufana lista jest prowadzona i publikowana, musi być sekwencją wielojęzycznych łańcuchów znaków (zob. klauzula 5.1.4) stanowiącą w języku angielskim (ZK) jako w języku obowiązkowym i ewentualnie w jednym języku krajowym lub w większej liczbie języków krajowych faktyczny tekst każdej takiej polityki lub zastrzeżenia sformułowany w następujący sposób:

1) pierwsza, obowiązkowa część, wspólna dla zaufanych list wszystkich państw członkowskich, wskazująca mające zastosowanie ramy prawne i mająca w języku angielskim następujące brzmienie:

   The applicable legal framework for the present trusted list is Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

   Tekst w języku urzędowym państwa członkowskiego:

   Ramy prawne mające zastosowanie do celów niniejszej zaufanej listy stanowi rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

2) druga, fakultatywna część, specyficzna dla każdej zaufanej listy, wskazująca odniesienia do szczególnych mających zastosowanie krajowych ram prawnych.

Service current status (obecny status usługi) (klauzula 5.5.4)

Pole to musi występować i musi być zgodne ze specyfikacją zawartą w klauzuli 5.5.4 TS 119 612.

Przeniesienie wartości pola „Service current status" dla usług wymienionych w zaufanej liście EUMS od dnia poprzedzającego datę wejścia w życie rozporządzenia (UE) nr 910/2014 (tj. od dnia 30 czerwca 2016 r.) wykonuje się w dniu rozpoczęcia stosowania rozporządzenia (tj. w dniu 1 lipca 2016 r.), jak określono w załączniku J do ETSI TS 119 612.

ROZDZIAŁ III

KONTYNUACJA ZAUFANYCH LIST

Certyfikaty, o których należy zawiadamiać Komisję zgodnie z art. 4 ust. 2 niniejszej decyzji, muszą spełniać wymogi klauzuli 5.7.1. TS 119 612 i muszą być wystawiane w taki sposób, aby:

— ich końcowe daty ważności dzieliły co najmniej trzy miesiące („Not After" – nie później niż),

— były tworzone z zastosowaniem nowych par kluczy. Nie wolno ponownie certyfikować uprzednio używanych par kluczy.

W przypadku upłynięcia okresu ważności jednego z certyfikatów klucza publicznego, który może być stosowany do weryfikacji podpisu lub pieczęci zaufanej listy i który został zgłoszony Komisji i opublikowany na centralnej liście wskaźników Komisji, państwa członkowskie:

— w przypadku gdy aktualnie opublikowana zaufana lista została podpisana lub opatrzona pieczęcią przy użyciu klucza prywatnego, którego certyfikat klucza publicznego stracił ważność, niezwłocznie wydają nową zaufaną listę podpisaną lub opatrzoną pieczęcią przy użyciu klucza prywatnego, którego certyfikat klucza publicznego nie stracił ważności,

— w razie potrzeby generują nowe pary kluczy, które mogą zostać wykorzystane do podpisania lub opatrzenia pieczęcią zaufanej listy, i odpowiadające im certyfikaty klucza publicznego,

— niezwłocznie zgłaszają Komisji nową listę certyfikatów klucza publicznego odpowiadających kluczom prywatnym, które mogą zostać wykorzystane do podpisania lub opatrzenia pieczęcią zaufanej listy.

W przypadku ujawnienia lub wycofania jednego z kluczy prywatnych odpowiadających jednemu z certyfikatów klucza publicznego, który może być stosowany do weryfikacji podpisu lub pieczęci zaufanej listy i który został zgłoszony Komisji i opublikowany na centralnej liście wskaźników Komisji, państwa członkowskie:

— niezwłocznie wydają nową zaufaną listę podpisaną lub opatrzoną pieczęcią przy użyciu nieujawnionego klucza prywatnego, w przypadku gdy wcześniej opublikowana zaufana lista została podpisana lub opatrzona pieczęcią przy użyciu ujawnionego lub wycofanego klucza prywatnego,

— w razie potrzeby generują nowe pary kluczy, które mogą zostać wykorzystane do podpisania lub opatrzenia pieczęcią zaufanej listy, i odpowiadające im certyfikaty klucza publicznego,

— niezwłocznie zgłaszają Komisji nową listę certyfikatów klucza publicznego odpowiadających kluczom prywatnym, które mogą zostać wykorzystane do podpisania lub opatrzenia pieczęcią zaufanej listy.

W przypadku ujawnienia lub wycofania wszystkich prywatnych kluczy odpowiadających certyfikatom klucza publicznego, które mogą być stosowane do weryfikacji podpisu zaufanej listy, które zostały zgłoszone Komisji i opublikowane na centralnej liście wskaźników Komisji, państwa członkowskie:

— generują nowe pary kluczy, które mogą zostać wykorzystane do podpisania lub opatrzenia pieczęcią zaufanej listy, i odpowiadające im certyfikaty klucza publicznego,

— niezwłocznie wydają nową zaufaną listę podpisaną lub opatrzoną pieczęcią przy użyciu jednego z tych nowych kluczy prywatnych, których odpowiedni certyfikat klucza publicznego należy zgłosić,

— niezwłocznie zgłaszają Komisji nową listę certyfikatów klucza publicznego odpowiadających kluczom prywatnym, które mogą zostać wykorzystane do podpisania lub opatrzenia pieczęcią zaufanej listy.

ROZDZIAŁ IV

SPECYFIKACJA CZYTELNEJ DLA CZŁOWIEKA POSTACI ZAUFANEJ LISTY

Jeżeli ustanowiono i opublikowano zaufaną listę w postaci czytelnej dla człowieka, udostępnia się ją jako dokument w formacie PDF zgodnie z ISO 32000 ([1]), a dokument ten formatuje się zgodnie z profilem PDF/A (ISO 19005 ([2])).

Zawartość opartej na pliku PDF/A zaufanej listy w postaci czytelnej dla człowieka spełnia następujące wymogi:

— struktura postaci czytelnej dla człowieka odzwierciedla model logiczny opisany w TS 119 612,

— każde pole jest widoczne i zawiera:

  — tytuł pola (np. „Service type identifier”),

  — wartość pola (np. „http://uri.etsi.org/TrstSvc/Svctype/CA/QC”),

  — w odpowiednich przypadkach znaczenie (opis) wartości tego pola (np. „Usługa generowania certyfikatów służąca tworzeniu i podpisywaniu kwalifikowanych certyfikatów w oparciu o tożsamość i inne cechy weryfikowane przez właściwe podmioty świadczące usługi rejestracji.”),

  — w stosownych przypadkach wersje w wielu językach naturalnych zgodnie z zawartością zaufanej listy,

— co najmniej następujące pola i odpowiadające im wartości certyfikatów cyfrowych ([3]), jeżeli występują w polu „Service digital identity”, przedstawia się w postaci czytelnej dla człowieka:

  — wersja,

  — numer seryjny certyfikatu,

  — algorytm podpisu,

  — wystawca – wszystkie właściwe wyróżnione pola odnoszące się do nazwy,

  — okres ważności,

  — podmiot – wszystkie właściwe wyróżnione pola odnoszące się do nazwy,

([1]) ISO 32000-1:2008: Document management – Portable document format – Część 1: PDF 1.7.
([2]) ISO 19005-2:2011: Document management – Electronic document file format for long-term preservation – Część 2: Use of ISO 32000-1 (PDF/A-2).
([3]) Zalecenie ITU-T X.509 | ISO/IEC 9594-8: Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks (zob. http://www.itu.int/ITU-T/recommendations/rec.aspx?rec=X.509).

— klucz publiczny,

— identyfikator klucza organu,

— identyfikator klucza podmiotu,

— stosowanie klucza,

— rozszerzone stosowanie klucza,

— polityka certyfikacji – wszystkie identyfikatory i kwalifikatory polityki,

— przyporządkowanie polityki,

— alternatywna nazwa podmiotu,

— atrybuty katalogu podmiotu,

— podstawowe warunki ograniczające,

— ograniczenia wynikające z polityki,

— punkty dystrybucji CRL ([1]),

— dostęp do informacji organu,

— dostęp do informacji podmiotu,

— poświadczenia certyfikatu kwalifikowanego ([2]),

— algorytm haszowania,

— wartość skrótu certyfikatu,

— lista w postaci czytelnej dla człowieka musi być łatwa do wydrukowania,

— lista w postaci czytelnej dla człowieka musi być podpisana lub opatrzona pieczęcią przez operatora systemu zgodnie z zaawansowanym podpisem PDF określonym w art. 1 i 3 decyzji wykonawczej Komisji (UE) 2015/1505.

([1]) RFC 5280: Internet X.509 PKI – certyfikat i profil CRL.
([2]) RFC 3739: Internet X.509 PKI – profil certyfikatów kwalifikowanych.

ZAŁĄCZNIK II

WZÓR POWIADOMIENIA PRZEZ PAŃSTWO CZŁONKOWSKIE

Informacje, które państwa członkowskie są zobowiązane przekazać zgodnie z art. 4 ust. 1 niniejszej decyzji, zawierają następujące dane oraz wszelkie kolejne ich zmiany:

1) Państwo członkowskie, z zastosowaniem kodów ISO 3166-1 ([1]) alfa-2 z następującymi wyjątkami:

   a) kodem państwa w przypadku Zjednoczonego Królestwa jest „UK";

   b) kodem państwa w przypadku Grecji jest „EL";

2) Podmiot lub podmioty odpowiedzialne za tworzenie, prowadzenie i publikowanie zaufanych list w postaci dostosowanej do automatycznego przetwarzania oraz w postaci czytelnej dla człowieka:

   a) nazwa operatora systemu: podane informacje muszą być identyczne – z uwzględnieniem wielkich i małych liter – z wartością w polu „Scheme operator name" podaną w zaufanej liście, w tylu językach, iloma się w niej posłużono;

   b) nieobowiązkowe informacje przeznaczone wyłącznie do użytku wewnętrznego Komisji w przypadku konieczności skontaktowania się z danym podmiotem (informacje te nie zostaną opublikowane w opracowanym przez Komisję zbiorczym wykazie zaufanych list):

      — adres operatora systemu,

      — dane teleadresowe osoby odpowiedzialnej lub osób odpowiedzialnych (imię i nazwisko, nr telefonu, adres e-mail);

3) miejsce opublikowania zaufanej listy w postaci dostosowanej do automatycznego przetwarzania (*miejsce, w którym opublikowana jest bieżąca zaufana lista*);

4) W stosownych przypadkach miejsce opublikowania zaufanej listy w postaci czytelnej dla człowieka (*miejsce, w którym opublikowana jest bieżąca zaufana lista*). Jeżeli zaufana lista w postaci czytelnej dla człowieka nie jest już publikowana, informacja o tym fakcie;

5) certyfikaty kluczy publicznych odpowiadające kluczom prywatnym, które mogą zostać wykorzystane do podpisania elektronicznie lub opatrzenia pieczęcią elektroniczną zaufanej listy w postaci dostosowanej do automatycznego przetwarzania oraz w postaci czytelnej dla człowieka: certyfikaty te przekazuje się zakodowane w formacie DER jako wiadomości PEM (Privacy Enhanced Mail) Base64. Przy powiadamianiu o zmianie: informacje dodatkowe w przypadku gdy nowy certyfikat zastępuje określony certyfikat w wykazie Komisji i w przypadku gdy zgłaszany certyfikat należy dodać do już istniejącego lub istniejących bez dokonywania zamiany;

6) data przekazania danych zgłoszonych w pkt 1–5.

Dane zgłoszone zgodnie z pkt 1, pkt 2 lit. a), pkt 3, 4 i 5 zostają ujęte w opracowanym przez Komisję zbiorczym wykazie zaufanych list w celu zastąpienia wcześniej przekazanych informacji zawartych w tym wykazie.

([1]) ISO 3166-1: „Kody nazw państw i ich jednostek administracyjnych – Część 1: Kody państw".

DECYZJA WYKONAWCZA KOMISJI (UE) 2015/1506

z dnia 8 września 2015 r.

ustanawiająca specyfikacje dotyczące formatów zaawansowanych podpisów elektronicznych oraz zaawansowanych pieczęci elektronicznych, które mają być uznane przez podmioty sektora publicznego, zgodnie z art. 27 ust. 5 i art. 37 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym

(Tekst mający znaczenie dla EOG)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE [1], w szczególności jego art. 27 ust. 5 i art. 37 ust. 5,

a także mając na uwadze, co następuje:

(1) Państwa członkowskie muszą wdrożyć niezbędne środki techniczne umożliwiające im przetwarzanie elektronicznie podpisanych dokumentów wymaganych przy korzystaniu z usług *on-line* oferowanych przez podmiot sektora publicznego lub w jego imieniu.

(2) Rozporządzenie (UE) nr 910/2014 zobowiązuje państwa członkowskie wymagające zaawansowanego podpisu elektronicznego lub pieczęci elektronicznej do korzystania z usługi online oferowanej przez podmiot sektora publicznego lub w jego imieniu do uznania zaawansowanych podpisów i pieczęci elektronicznych opartych na kwalifikowanym certyfikacie oraz kwalifikowanych podpisów i pieczęci elektronicznych w określonych formatach lub formatach alternatywnych zatwierdzonych zgodnie ze szczególnymi metodami referencyjnymi.

(3) Przy definiowaniu poszczególnych formatów i metod referencyjnych należy brać pod uwagę istniejące praktyki, normy i unijne akty prawne.

(4) W decyzji wykonawczej Komisji 2014/148/UE [2] określono szereg najbardziej rozpowszechnionych formatów zaawansowanego podpisu elektronicznego, które mają być obsługiwane technicznie przez państwa członkowskie w przypadkach gdy w internetowych procedurach administracyjnych wymagane są zaawansowane podpisy elektroniczne. Celem ustanowienia formatów referencyjnych jest ułatwienie transgranicznej walidacji podpisów elektronicznych oraz udoskonalenie transgranicznej interoperacyjności procedur elektronicznych.

(5) Normy wymienione w załączniku do niniejszej decyzji są zgodne z istniejącymi normami formatów zaawansowanych podpisów elektronicznych. Z uwagi na trwający proces przeglądu przez organy normalizacyjne formatów do celów długoterminowej archiwizacji, normy określające długoterminową archiwizację wyłącza się z zakresu niniejszej decyzji. Gdy dostępne będą nowe wersje odnośnych norm, odniesienia do norm i klauzule dotyczące długoterminowego archiwizowania zostaną poddane przeglądowi.

(6) Zaawansowane podpisy elektroniczne i zaawansowane pieczęcie elektroniczne są podobne pod względem technicznym. W związku z tym normy dotyczące formatów zaawansowanych podpisów elektronicznych powinny mieć zastosowanie *mutatis mutandis* do formatów zaawansowanych pieczęci elektronicznych.

(7) W przypadku gdy do podpisania lub opatrzenia pieczęcią stosowane są formaty podpisu elektronicznego lub pieczęci elektronicznej inne niż formaty powszechnie technicznie obsługiwane, należy zapewnić środki walidacji umożliwiające weryfikację podpisu elektronicznego lub pieczęci w ruchu transgranicznym. Aby zapewnić państwom członkowskim będących odbiorcami możliwość polegania na tych narzędziach walidacji innego państwa członkowskiego, należy dostarczyć łatwo dostępne informacje dotyczące takich narzędzi walidacji poprzez włączenie tych informacji do dokumentów elektronicznych, podpisów elektronicznych lub kontenerów dokumentów elektronicznych.

---

[1] Dz.U. L 257 z 28.8.2014, s. 73.

[2] Decyzja wykonawcza Komisji 2014/148/UE z dnia 17 marca 2014 r. zmieniająca decyzję 2011/130/UE w sprawie ustalenia minimalnych wymagań dotyczących transgranicznego przetwarzania dokumentów podpisanych elektronicznie przez właściwe organy zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym (Dz.U. L 80 z 19.3.2014, s. 7).

(8) Jeżeli metody walidacji podpisu elektronicznego lub pieczęci elektronicznej umożliwiające automatyczne przetwarzanie są dostępne w usługach publicznych państw członkowskich, takie metody walidacji powinny zostać udostępnione i przekazane odbierającemu państwu członkowskiemu. Niniejsza decyzja nie powinna jednak utrudniać stosowania art. 27 ust. 1 i 2 oraz art. 37 ust. 1 i 2 rozporządzenia (UE) nr 910/2014, jeżeli automatyczne przetwarzanie metod walidacji w odniesieniu do metod alternatywnych nie jest możliwe.

(9) Aby zapewnić porównywalne wymagania dotyczące walidacji oraz zwiększyć zaufanie do metod walidacji ustanowionych przez państwa członkowskie w odniesieniu do formatów podpisu elektronicznego lub pieczęci elektronicznej innych niż powszechnie obsługiwane, wymagania określone w niniejszej decyzji odnośnie do narzędzi walidacji są oparte na wymaganiach w zakresie walidacji kwalifikowanych podpisów elektronicznych i pieczęci elektronicznych, o których mowa w art. 32 i 40 rozporządzenia (UE) nr 910/2014.

(10) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ustanowionego na podstawie art. 48 rozporządzenia (UE) nr 910/2014,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Państwo członkowskie wymagające zaawansowanego podpisu elektronicznego lub zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie, jak określono w art. 27 ust. 1 i 2 rozporządzenia (UE) nr 910/2014, uznaje zaawansowane podpisy elektroniczne w formatach XML, CMS lub PDF na poziomie zgodności B, T lub LT bądź zastosowanie formatu ASiC, jeżeli podpisy te są zgodne ze specyfikacjami technicznymi wymienionymi w załączniku.

Artykuł 2

1. Państwo członkowskie wymagające zaawansowanego podpisu elektronicznego lub zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie, jak określono w art. 27 ust. 1 i 2 rozporządzenia (UE) nr 910/2014, uznaje formaty podpisu elektronicznego inne niż określone w art. 1 niniejszej decyzji, pod warunkiem że państwo członkowskie, w którym ma siedzibę dostawca usług zaufania, z których korzysta podpisujący, oferuje metody walidacji podpisów innego państwa członkowskiego, nadające się w miarę możliwości do automatycznego przetwarzania.

2. Metody walidacji podpisu:

a) umożliwiają pozostałym państwom członkowskim walidację otrzymanego podpisu elektronicznego w trybie online, nieodpłatnie i w sposób zrozumiały dla osób, dla których dany język nie jest językiem ojczystym;

b) są wskazane w podpisanym dokumencie, w podpisie elektronicznym lub w nośniku dokumentu elektronicznego; oraz

c) potwierdzają ważność zaawansowanego podpisu elektronicznego, pod warunkiem że:

   1) certyfikat potwierdzający zaawansowany podpis elektroniczny był ważny w momencie składania podpisu, a w przypadku gdy zaawansowany podpis elektroniczny jest potwierdzany certyfikatem kwalifikowanym, kwalifikowany certyfikat potwierdzający podpis elektroniczny był w momencie podpisywania kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z załącznikiem I do rozporządzenia (UE) nr 910/2014, oraz że został on wydany przez kwalifikowanego dostawcę usług zaufania; a ponadto:

   2) dane służące do walidacji podpisu odpowiadają danym dostarczonym stronie ufającej;

   3) niepowtarzalny zestaw danych reprezentujących podpisującego został prawidłowo dostarczony stronie ufającej;

   4) jeżeli w momencie składania podpisu użyto pseudonimu, zostaje to wyraźnie wskazane stronie ufającej;

5) jeżeli zaawansowany podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego, użycie takiego urządzenia zostaje wyraźnie wskazane stronie ufającej;

6) integralność podpisanych danych nie została naruszona;

7) wymagania określone w art. 26 rozporządzenia (UE) nr 910/2014 zostały spełnione w momencie składania podpisu;

8) system wykorzystany do walidacji zaawansowanego podpisu elektronicznego zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia wykrycie przez nią wszelkich kwestii istotnych dla bezpieczeństwa.

Artykuł 3

Państwo członkowskie wymagające zaawansowanej pieczęci elektronicznej lub zaawansowanej pieczęci elektronicznej opartej na kwalifikowanym certyfikacie, jak określono w art. 37 ust. 1 i 2 rozporządzenia (UE) nr 910/2014, uznaje zaawansowane pieczęcie elektroniczne w formatach XML, CMS lub PDF na poziomie zgodności B, T lub LT bądź zastosowanie formatu ASiC, jeżeli są one zgodne ze specyfikacjami technicznymi wymienionymi w załączniku.

Artykuł 4

1. Państwo członkowskie wymagające zaawansowanej pieczęci elektronicznej lub zaawansowanej pieczęci elektronicznej opartej na kwalifikowanym certyfikacie, jak określono w art. 37 ust. 1 i 2 rozporządzenia (UE) nr 910/2014, uznaje formaty pieczęci elektronicznej inne niż określone w art. 3 niniejszej decyzji, pod warunkiem że państwo członkowskie, w którym ma siedzibę dostawca usług zaufania, z których korzysta podmiot składający pieczęć, oferuje metody walidacji pieczęci innego państwa członkowskiego, nadające się w miarę możliwości do automatycznego przetwarzania.

2. Metody walidacji pieczęci:

a) umożliwiają pozostałym państwom członkowskim walidację otrzymanej pieczęci elektronicznej w trybie online, nieodpłatnie i w sposób zrozumiały dla osób, dla których dany język nie jest językiem ojczystym;

b) są wskazane w dokumencie opatrzonym pieczęcią, w pieczęci elektronicznej lub w nośniku dokumentu elektronicznego;

c) potwierdzają ważność zaawansowanej pieczęci elektronicznej, pod warunkiem że:

1) certyfikat potwierdzający zaawansowaną pieczęć elektroniczną był ważny w momencie składania pieczęci, a w przypadku gdy zaawansowana pieczęć elektroniczna jest potwierdzana certyfikatem kwalifikowanym, kwalifikowany certyfikat potwierdzający pieczęć elektroniczną był w momencie składania pieczęci kwalifikowanym certyfikatem pieczęci elektronicznej zgodnym z załącznikiem III do rozporządzenia (UE) nr 910/2014, oraz że został on wydany przez kwalifikowanego dostawcę usług zaufania; a ponadto:

2) dane służące do walidacji pieczęci elektronicznej odpowiadają danym dostarczonym stronie ufającej;

3) niepowtarzalny zestaw danych reprezentujących podmiot składający pieczęć został prawidłowo dostarczony stronie ufającej;

4) jeżeli w momencie składania pieczęci użyto pseudonimu, zostaje to wyraźnie wskazane stronie ufającej;

5) jeżeli zaawansowana pieczęć elektroniczna została złożona za pomocą kwalifikowanego urządzenia do składania pieczęci elektronicznej, użycie takiego urządzenia zostaje wyraźnie wskazane stronie ufającej;

6) integralność danych potwierdzonych pieczęcią elektroniczną nie została naruszona;

7) wymagania określone w art. 36 rozporządzenia (UE) nr 910/2014 zostały spełnione w momencie składania pieczęci elektronicznej;

8) system wykorzystany do walidacji zaawansowanej pieczęci elektronicznej zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia wykrycie przez nią wszelkich kwestii istotnych dla bezpieczeństwa.

Artykuł 5

Niniejsza decyzja wchodzi w życie dwudziestego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsza decyzja wiąże w całości i jest bezpośrednio stosowana we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia 8 września 2015 r.

W imieniu Komisji
Jean-Claude JUNCKER
Przewodniczący

ZAŁĄCZNIK

Wykaz specyfikacji technicznych w odniesieniu do zaawansowanych podpisów elektronicznych w formatach XML, CMS lub PDF oraz ASiC (Associated Signature Container)

Zaawansowane podpisy elektroniczne, o których mowa w art. 1 niniejszej decyzji, muszą być zgodne z jedną z następujących specyfikacji technicznych ETSI, z wyłączeniem ich klauzuli 9:

Podstawowy profil XAdES	ETSI TS 103171 v.2.1.1 ([1])
Podstawowy profil CAdES	ETSI TS 103173 v.2.2.1 ([2])
Podstawowy profil PAdES	ETSI TS 103172 v.2.2.2 ([3])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
([2]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
([3]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.02.02_60/ts_103172v020202p.pdf

Format ASiC podpisu, o którym mowa w art. 1 niniejszej decyzji, musi być zgodny z następującą specyfikacją techniczną ETSI:

Podstawowy profil ASiC	ETSI TS 103174 v.2.2.1 ([1])

([1]) http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.02.01_60/ts_103174v020201p.pdf

Wykaz specyfikacji technicznych w odniesieniu do zaawansowanych pieczęci elektronicznych w formatach XML, CMS lub PDF oraz ASiC (Associated Signature Container)

Zaawansowane pieczęci elektroniczne, o których mowa w art. 3 niniejszej decyzji, muszą być zgodne z jedną z następujących specyfikacji technicznych ETSI, z wyłączeniem ich klauzuli 9:

Podstawowy profil XAdES	ETSI TS 103171 v.2.1.1
Podstawowy profil CAdES	ETSI TS 103173 v.2.2.1
Podstawowy profil PAdES	ETSI TS 103172 v.2.2.2

Format ASiC pieczęci, o którym mowa w art. 3 niniejszej decyzji, musi być zgodny z następującą specyfikacją techniczną ETSI:

Podstawowy profil ASiC	ETSI TS 103174 v.2.2.1

ISSN 1977-0766 (wydanie elektroniczne)
ISSN 1725-5139 (wydanie papierowe)

Urząd Publikacji Unii Europejskiej
2985 Luksemburg
LUKSEMBURG

PL