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".