DECYZJA WYKONAWCZA KOMISJI

z dnia 14 października 2013 r.

zmieniająca decyzję 2009/767/WE w odniesieniu do tworzenia, prowadzenia i publikowania zaufanych list podmiotów świadczących usługi certyfikacyjne nadzorowanych/akredytowanych przez państwa członkowskie

(notyfikowana jako dokument nr C(2013) 6543)

(Tekst mający znaczenie dla EOG)

(2013/662/UE)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając dyrektywę 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotyczącą usług na rynku wewnętrznym [1], w szczególności jej art. 8 ust. 3,

a także mając na uwadze, co następuje:

(1) 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 [2] zobowiązuje państwa członkowskie do udostępnienia informacji niezbędnych do zweryfikowania zaawansowanych podpisów elektronicznych weryfikowanych certyfikatem kwalifikowanym. Informacje te mają być podane w jednolity sposób na tak zwanych „zaufanych listach" zawierających informacje dotyczące nadzorowanych/akredytowanych przez państwa członkowskie podmiotów świadczących powszechne usługi certyfikacyjne, wystawiających certyfikaty kwalifikowane zgodnie z dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych [3].

(2) Praktyczne doświadczenia z wdrażaniem decyzji 2009/767/WE przez państwa członkowskie wykazały, że niezbędne są pewne udoskonalenia, by uzyskać maksymalne korzyści wynikające z zaufanych list. Ponadto Europejski Instytut Norm Telekomunikacyjnych (ETSI) opublikował nowe specyfikacje techniczne dla zaufanych list (TS 119 612), oparte na specyfikacjach zawartych obecnie w załączniku do decyzji, wprowadzając jednak równocześnie szereg udoskonaleń w obowiązujących specyfikacjach.

(3) Dlatego też należy zmienić decyzję 2009/767/WE, wprowadzając odniesienie do specyfikacji technicznych ETSI 119 612 oraz zmiany uznawane za potrzebne do usprawnienia i ułatwienia wprowadzania w życie zaufanych list i korzystania z nich.

(4) W celu umożliwienia państwom członkowskim przeprowadzenia wymaganych zmian technicznych w aktualnych zaufanych listach niniejszą decyzję należy stosować od dnia 1 lutego 2014 r.

(5) Środki przewidziane w niniejszej decyzji są zgodne z opinią Komitetu ds. Dyrektywy o Usługach,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

Artykuł 1

Zmiany w decyzji 2009/767/WE

W decyzji 2009/767/WE wprowadza się następujące zmiany:

1) w art. 2 wprowadza się następujące zmiany:

a) ust. 1, 2 i 2a otrzymują brzmienie:

„1. Każde państwo członkowskie tworzy, prowadzi i publikuje, zgodnie ze specyfikacjami technicznymi określonymi w załączniku, »zaufaną listę« zawierającą co najmniej informacje dotyczące nadzorowanych/akredytowanych przez to państwo członkowskie podmiotów świadczących powszechne usługi certyfikacyjne, wystawiających certyfikaty kwalifikowane.";

„2. Państwa członkowskie tworzą i publikują zaufaną listę w postaci przetwarzalnej maszynowo, zgodnie ze specyfikacjami określonymi w załączniku. Jeżeli państwa członkowskie podejmują decyzję o opublikowaniu zaufanej listy w wersji czytelnej dla człowieka, format takiej listy jest zgodny ze specyfikacjami określonymi w załączniku.";

„2a. Państwa członkowskie podpisują elektronicznie zaufaną listę w postaci przetwarzalnej maszynowo w celu zagwarantowania jej autentyczności i integralności. Jeżeli państwo członkowskie publikuje zaufaną listę w wersji czytelnej dla człowieka, zapewnia, by ta postać listy zawierała te same dane, co postać przetwarzalna maszynowo oraz podpisuje ją elektronicznie tym samym certyfikatem, którego używa w przypadku postaci przetwarzalnej maszynowo.";

[1] Dz.U. L 376 z 27.12.2006, s. 36.
[2] Dz.U. L 274 z 20.10.2009, s. 36.
[3] Dz.U. L 13 z 19.1.2000, s. 12.

b) dodaje się ust. 2b w brzmieniu:

„2b. Państwa członkowskie zapewniają, by ich zaufana lista w postaci przetwarzalnej maszynowo była dostępna w każdym czasie w miejscu ich publikacji, w sposób nieprzerwany, z wyjątkiem przerw potrzebnych w celu przeprowadzenia prac konserwacyjnych.";

c) ust. 3 otrzymuje brzmienie:

„3. Państwa członkowskie przekazują Komisji informacje o:

a) organie lub organach odpowiedzialnych za tworzenie, prowadzenie i publikowanie zaufanej listy w postaci przetwarzalnej maszynowo;

b) miejscu, w którym zaufana lista w postaci przetwarzalnej maszynowo została opublikowana;

c) dwóch lub więcej certyfikatach klucza publicznego operatora systemu, których okresy ważności różnią się o co najmniej trzy miesiące, które odpowiadają kluczom prywatnym, które mogą zostać wykorzystane do podpisania przetwarzalnej maszynowo postaci zaufanych list;

d) wszelkich zmianach w informacjach zawartych w lit. a), b) i c).";

d) dodaje się ust. 3a w brzmieniu:

„3a. Jeżeli państwo członkowskie publikują zaufaną listę w postaci czytelnej dla człowieka, przekazuje ono również informacje, o których mowa w ust. 3 w odniesieniu do tej postaci listy.";

2) załącznik zastępuje się załącznikiem do niniejszej decyzji.

Artykuł 2

Stosowanie

Niniejszą decyzję stosuje się od dnia 1 lutego 2014 r.

Artykuł 3

Adresaci

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 14 października 2013 r.

W imieniu Komisji

Michel BARNIER

Członek Komisji

ZAŁĄCZNIK

SPECYFIKACJA TECHNICZNA DOTYCZĄCA WSPÓLNEGO WZORU „ZAUFANEJ LISTY NADZOROWANYCH/AKREDYTOWANYCH PODMIOTÓW ŚWIADCZĄCYCH USŁUGI CERTYFIKACYJNE"

WYMOGI OGÓLNE

1. **Wprowadzenie**

Wspólny wzór dla państw członkowskich – „Zaufana lista nadzorowanych/akredytowanych podmiotów świadczących usługi certyfikacyjne" służyć ma ustanowieniu jednolitego sposobu przekazywania przez każde państwo członkowskie informacje na temat statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne (ang. Certification Service Providers – CSPs ([1])), które są nadzorowane/akredytowane przez te państwa w zakresie spełniania wymogów zawartych w odpowiednich przepisach dyrektywy 1999/93/WE. Obejmuje to także dostarczanie informacji historycznych o statusie nadzorowania/akredytacji nadzorowanych/akredytowanych usług certyfikacyjnych.

Informacje te mają służyć przede wszystkim wspieraniu weryfikacji kwalifikowanych podpisów elektronicznych (ang. Qualified Electronic Signatures - QES) i zaawansowanych podpisów elektronicznych (ang. Advanced Electronic Signatures, AdES ([2])) weryfikowanych certyfikatem kwalifikowanym ([3]) ([4]).

Informacje podawane obowiązkowo w zaufanej liście muszą obejmować co najmniej informacje o nadzorowanych CSP wydających certyfikaty kwalifikowane (ang. Qualified Certificates – QCs) ([5]), zgodnie z przepisami ustanowionymi w dyrektywie 1999/93/WE (art. 3 ust. 2 i art. 3 ust. 3 oraz art. 7 ust. 1 lit. a), w tym, jeśli nie stanowi to elementu certyfikatu kwalifikowanego, informacje o certyfikatach kwalifikowanych służących weryfikacji podpisu elektronicznego oraz o tym, czy podpis został stworzony poprzez bezpieczne urządzenie służące do składania podpisu elektronicznego (ang. Secure Signature Creation Device - SSCD) ([6]).

Dodatkowe informacje dotyczące innych nadzorowanych/akredytowanych CSP niewystawiających certyfikatu kwalifikowanego, ale świadczących usługi związane z podpisami elektronicznymi (np. CSP świadczące usługi znakowania czasem i wydające tokeny znaczników czasu, CSP wydające certyfikaty niekwalifikowane itp.) można dobrowolnie umieścić na zaufanej liście na szczeblu krajowym, o ile są one akredytowane lub nadzorowane w podobny sposób, co CSP wydające certyfikaty kwalifikowane lub zatwierdzone w ramach odmiennego krajowego systemu zatwierdzania. Krajowe systemy zatwierdzania mogą w niektórych państwach członkowskich różnić się od systemów nadzoru lub dobrowolnej akredytacji stosowanych wobec CSP wydających certyfikaty kwalifikowane, pod względem obowiązujących wymogów lub odpowiedzialnej organizacji. Terminy „akredytowany" lub „nadzorowany" w niniejszej specyfikacji obejmują również krajowe systemy zatwierdzania, jednak dodatkowe informacje na temat właściwości wszelkich krajowych systemów zostaną podane przez państwa członkowskie w ich zaufanej liście. Obejmuje to także wyjaśnienia dotyczące ewentualnych różnic w stosunku do systemów akredytacji/nadzoru stosowanych wobec CSP wydających certyfikaty kwalifikowane.

Wspólny wzór opiera się na specyfikacji technicznej ETSI TS 119 612 v1.1.1 ([7]) (zwanej dalej „ETSI TS 119 612") dotyczącej tworzenia, publikacji, lokalizacji, uwierzytelnienia i integralności takich list oraz dostępu do nich.

2. **Struktura wspólnego wzoru zaufanej listy**

Struktura proponowanego wspólnego wzoru zaufanej listy państwa członkowskiego jest podzielona – zgodnie z ETSI TS 119 612 – na następujące kategorie informacji:

1. Znacznik zaufanej listy ułatwiający identyfikację zaufanej listy podczas wyszukiwania elektronicznego.

2. Informacje dotyczące zaufanej listy i systemu jej wydawania.

3. Sekwencja pól zawierających jednoznaczne informacje identyfikacyjne dotyczące każdego nadzorowanego/akredytowanego CSP zgodnie z systemem (sekwencja jest fakultatywna, tzn. jeżeli nie jest stosowana, lista zostanie uznana za pustą, co oznacza, że w odniesieniu do zakresu listy w przedmiotowym państwie członkowskim nie ma CSP podlegających nadzorowi lub objętych akredytacją na potrzeby zaufanej listy).

4. W przypadku każdego CSP na liście, szczegółowe informacje na temat konkretnych świadczonych przez niego usług zaufania, których obecny status zapisano w zaufanej liście, podawane są jako sekwencja pól jednoznacznie identyfikujących nadzorowane/akredytowane usługi certyfikacyjne świadczone przez CSP oraz ich obecny status (sekwencja musi składać się z co najmniej jednej pozycji).

([1]) Zgodnie z definicją zawartą w art. 2 pkt 11 dyrektywy 1999/93/WE.
([2]) Zgodnie z definicją zawartą w art. 2 pkt 2 dyrektywy 1999/93/WE.
([3]) W całym niniejszym dokumencie akronim „$AdES_{QC}$" jest stosowany w odniesieniu do zaawansowanego podpisu elektronicznego weryfikowanego certyfikatem kwalifikowanym.
([4]) Należy zwrócić uwagę, że istnieje szereg usług elektronicznych opartych na zwykłym zaawansowanym podpisie elektronicznym, którego stosowanie transgraniczne także zostanie ułatwione, pod warunkiem że wspierające usługi certyfikacyjne (np. wystawianie certyfikatów niekwalifikowanych) stanowią część nadzorowanych/akredytowanych usług uwzględnionych przez państwo członkowskie w części zaufanej listy zawierającej informacje udzielane dobrowolnie.
([5]) Zgodnie z definicją zawartą w art. 2 pkt 10 dyrektywy 1999/93/WE.
([6]) Zgodnie z definicją zawartą w art. 2 pkt 6 dyrektywy 1999/93/WE.
([7]) ETSI TS 119 612 v1.1.1 (2013-06) – Electronic Signatures and Infrastructures (ESI); Trusted Lists.

5. W odpowiednich przypadkach, w odniesieniu do każdej nadzorowanej/akredytowanej usługi certyfikacyjnej na liście – historia jej statusu.

6. Podpis zastosowany na zaufanej liście.

W kontekście CSP wystawiającego certyfikaty kwalifikowane, struktura zaufanej listy, a w szczególności element dotyczący informacji o usłudze (zob. pkt 4 powyżej) umożliwia uzyskanie informacji uzupełniających w rozszerzeniach informacji o usłudze, które można wykorzystać w sytuacjach, w których certyfikat kwalifikowany nie zawiera wystarczających (przetwarzalnych maszynowo) informacji dotyczących „kwalifikowanego" statusu certyfikatu, fakt ewentualnej obsługi certyfikatu przez SSCD oraz w szczególności, by uwzględnić dodatkową okoliczność, a mianowicie to, że większość (komercyjnych) CSP wykorzystuje jeden wystawiający urząd certyfikacji (ang. Certification Authority – CA) do wystawiania kilku rodzajów zarówno kwalifikowanych, jak i niekwalifikowanych certyfikatów wierzchołka ścieżki.

W kontekście usług generowania certyfikatów, liczba pozycji dotyczących usług na liście dla CSP może zostać zmniejszona, jeśli jedna lub więcej CA wyższego poziomu istnieje w ramach infrastruktury klucza publicznego (ang. Public Key Infrastructure – PKI) danego CSP (np. w kontekście hierarchii CA od Root CA aż do szeregu wystawiających CA) poprzez wyszczególnienie takich CA wyższego poziomu, a nie usług CA, w ramach których wydawane są certyfikaty końca ścieżki (np. wyszczególnienie jedynie CSP głównego CA). Jednakże w tych przypadkach informacja o statusie dotyczy całej hierarchii usług CA poniżej wyszczególnionej usługi, musi być także zachowana i zagwarantowana zasada zobowiązująca do jednoznacznego powiązania między usługą certyfikacyjną CSP_{QC} a zestawem certyfikatów, które mają zostać oznaczone jako certyfikaty kwalifikowane.

2.1. *Opis informacji w każdej kategorii*

1. Znacznik zaufanej listy

2. Informacje dotyczące zaufanej listy i systemu jej wydawania

Do kategorii tej należą następujące informacje:

— **identyfikator wersji formatu** zaufanej listy,

— **sygnatura (lub numer wydania)** zaufanej listy,

— **informacje dotyczące rodzaju** zaufanej listy (np. służące do ustalenia, czy przedmiotowa zaufana lista zawiera informacje dotyczące statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez CSP nadzorowane/akredytowane przez przedmiotowe państwo członkowskie pod względem zgodności z przepisami dyrektywy 1999/93/WE),

— **informacje dotyczące operatora (właściciela)** zaufanej listy (np. nazwa, adres, informacje kontaktowe itp. organu państwa członkowskiego odpowiedzialnego za sporządzanie, bezpieczne publikowanie i prowadzenie zaufanej listy),

— **informacje dotyczące podstawowych systemów nadzoru/akredytacji**, z którymi powiązana jest zaufana lista, obejmujące m.in.:

  — kraj, w którym lista ma zastosowanie,

  — informacje lub odniesienie do informacji o systemach (model systemu, zasady, kryteria, obowiązująca wspólnota, rodzaj itp.),

  — okres przechowywania informacji (historycznych),

— **polityka lub informacje prawne, zobowiązania, odpowiedzialność** w odniesieniu do zaufanej listy,

— **data i godzina wydania** zaufanej listy,

— **data następnej zaplanowanej aktualizacji** zaufanej listy.

3. Jednoznaczne informacje identyfikacyjne dotyczące każdego CSP nadzorowanego/akredytowanego w systemie

Ten zbiór obejmie co najmniej następujące informacje:

— nazwę organizacji CSP wykorzystaną podczas formalnej rejestracji prawnej (może obejmować identyfikator użytkownika (UID) organizacji CSP zgodnie z praktykami państwa członkowskiego),

— adres i informacje kontaktowe CSP,

— dodatkowe informacje dotyczące CSP bezpośrednio lub w formie odniesienia do miejsca, z którego można pobrać takie informacje.

4. W odniesieniu do każdego wymienionego na liście CSP sekwencja pól zawierających jednoznaczną identyfikację usługi certyfikacyjnej świadczonej przez CSP i nadzorowanej/akredytowanej w kontekście dyrektywy 1999/93/WE

Ten zbiór informacji obejmie co najmniej następujące dane w odniesieniu do każdej usługi certyfikacyjnej świadczonej przez CSP wymieniony na liście:

— identyfikator rodzaju usługi: identyfikator rodzaju usługi certyfikacyjnej (np. identyfikator wskazujący, że nadzorowana/akredytowana usługa certyfikacyjna świadczona przez CSP jest urzędem certyfikacji wystawiającym certyfikaty kwalifikowane),

— nazwa (handlowa) usługi: nazwa (handlowa) przedmiotowej usługi certyfikacyjnej,

— cyfrowy identyfikator usługi: jednoznaczny niepowtarzalny identyfikator usługi certyfikacyjnej,

— obecny status usługi: identyfikator obecnego statusu usługi,

— początkową datę i godzinę bieżącego statusu,

— w stosownych przypadkach, rozszerzone informacje o usługach: dodatkowe informacje dotyczące usługi (np. zamieszczone bezpośrednio lub w formie odniesienia do miejsca, z którego można pobrać informacje): informacje definiujące usługę dostarczone przez operatora systemu, informacje o dostępie do usługi, informacje definiujące usługę dostarczone przez CSP oraz rozszerzone informacje o usłudze. w odniesieniu do usług CA/QC fakultatywna sekwencja krotek informacji, z których każda zawiera:

  — kryteria wykorzystywane do dalszej identyfikacji (filtrowania) w ramach zidentyfikowanej usługi zaufania precyzyjnie określonego zestawu produktów (np. zestaw (kwalifikowanych) certyfikatów), w odniesieniu do którego wymagane/zawarte są dodatkowe informacje dotyczące jego statusu, zaznaczenie obsługi przez SSCD lub wystawienia na rzecz osoby prawnej, oraz

  — powiązane „kwalifikatory" zawierające informacje dotyczące tego, czy zestaw produktów dostarczanych w ramach usługi określa certyfikaty, które mają być uznawane za kwalifikowane lub czy zidentyfikowane certyfikaty kwalifikowane z tej usługi są obsługiwane przez SSCD, lub informacje dotyczące tego, czy takie certyfikaty kwalifikowane wystawia się osobom prawnym (domyślnie uznaje się je za wystawiane wyłącznie osobom fizycznym).

5. W przypadku każdej usługi certyfikacyjnej znajdującej się na liście, historia jej statusu

6. Podpis wygenerowany na potrzeby uwierzytelnienia dla wszystkich pól zaufanej listy, z wyjątkiem wartości samego podpisu

3. **Wytyczne dotyczące edycji wpisów na zaufanej liście**

3.1. *Informacje o statusie nadzorowanych/akredytowanych usług certyfikacyjnych i podmiotach świadczących te usługi na pojedynczej liście*

Zaufana lista państwa członkowskiego oznacza „wykaz statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne nadzorowane/akredytowane przez dane państwo członkowskie w zakresie zgodności z odnośnymi przepisami dyrektywy 1999/93/WE".

Taka zaufana lista jest pojedynczym instrumentem wykorzystywanym przez dane państwo członkowskie do dostarczania informacji na temat statusu nadzoru/akredytacji usług certyfikacyjnych i podmiotów świadczących takie usługi.

— **wszystkie podmioty świadczące usługi certyfikacyjne** zdefiniowane w art. 2 pkt 11 dyrektywy 1999/93/WE, tj. „podmioty lub osoby prawne bądź fizyczne, które wystawiają certyfikaty lub świadczą inne usługi związane z podpisami elektronicznymi",

— **które są nadzorowane/akredytowane** w zakresie zgodności z odnośnymi przepisami określonymi w dyrektywie 1999/93/WE.

Uwzględniając definicje i przepisy ustanowione w dyrektywie 1999/93/WE, w szczególności dotyczące odpowiednich CSP i ich systemów nadzoru/dobrowolnej akredytacji, można wyróżnić dwie grupy CSP: CSP powszechnie wystawiające certyfikaty kwalifikowane i CSP niewystawiające powszechnie certyfikaty kwalifikowane, ale świadczące „inne (dodatkowe) usługi związane z podpisami elektronicznymi":

— **CSP wystawiające certyfikaty kwalifikowane**:

  — Muszą być nadzorowane przez państwo członkowskie, w którym mają siedzibę (jeżeli mają siedzibę w państwie członkowskim) i mogą być także akredytowane w zakresie zgodności z przepisami dyrektywy 1999/93/WE, w tym z wymogami z załącznika I (wymogi dotyczące certyfikatów kwalifikowanych) i z załącznika II (wymogi dotyczące CSP wystawiających certyfikaty kwalifikowane). CSP wystawiające certyfikaty kwalifikowane, które są akredytowane w państwie członkowskim, muszą także podlegać właściwemu systemowi nadzoru tego państwa członkowskiego, chyba że nie mają siedziby w tym państwie członkowskim.

— Stosowany system „nadzoru" (odpowiednio system „dobrowolnej akredytacji") jest określony i musi spełnić odpowiednie wymogi dyrektywy 1999/93/WE, w szczególności te ustanowione w art. 3 ust. 3, art. 8 ust. 1, art. 11, w motywie 13 (odpowiednio w art. 2 pkt 13, art. 3 ust. 2, art. 7 ust. 1 lit. a), art. 8 ust. 1, art. 11, w motywach 4, 11, 12 i 13).

— **CSP niewystawiające certyfikatów kwalifikowanych:**

— Podmioty te mogą zostać objęte systemem „dobrowolnej akredytacji" (zdefiniowanym w dyrektywie 1999/93/WE i zgodnie z tą dyrektywą) lub określonym w prawie krajowym „uznanym systemem zatwierdzania" wdrożonym na szczeblu krajowym w celu nadzorowania zgodności z przepisami dyrektywy oraz, o ile to możliwe, z przepisami krajowymi dotyczącymi świadczenia usług certyfikacyjnych (w rozumieniu art. 2 pkt 11 dyrektywy 1999/93/WE).

— Niektórym obiektom fizycznym lub binarnym (logicznym) wygenerowanym lub wydanym w wyniku świadczenia usług certyfikacyjnych może przysługiwać szczególna „kwalifikacja" na podstawie zgodności tych obiektów z przepisami i wymogami ustanowionymi na szczeblu krajowym, ale znaczenie takiej „kwalifikacji" będzie prawdopodobnie ograniczone tylko do szczebla krajowego.

Dla każdego państwa członkowskiego należy utworzyć i prowadzić jedną zaufaną listę, by przedstawiać status nadzoru lub akredytacji tych usług certyfikacyjnych świadczonych przez te CSP, które są nadzorowane/akredytowane przez to państwo członkowskie. Zaufana lista obejmuje co najmniej te CSP, które wydają certyfikaty kwalifikowane. Zaufana lista może również przedstawiać status innych usług certyfikacyjnych nadzorowanych lub akredytowanych w ramach systemu zatwierdzania określonego na szczeblu krajowym.

3.2. *Pojedynczy zbiór wartości statusu nadzoru/akredytacji*

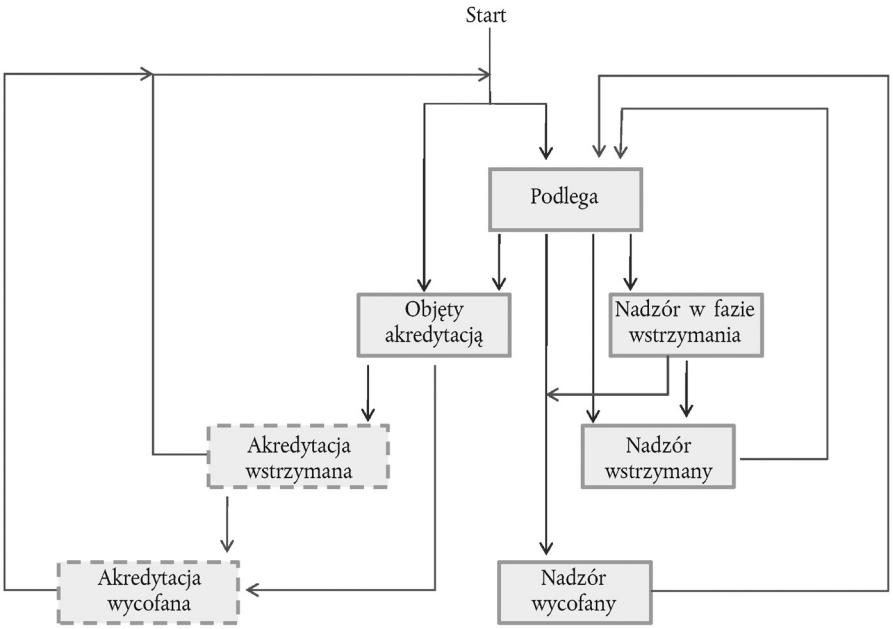
Na zaufanej liście fakt, że usługa jest obecnie „nadzorowana" lub „akredytowana" oznaczany jest jako wartość jej obecnego statusu. Ponadto status nadzoru lub akredytacji może być pozytywny („podlega nadzorowi", „objęty akredytacją", „nadzór w fazie wstrzymania"), wstrzymany („nadzór wstrzymany", „akredytacja wstrzymana") lub nawet cofnięty („nadzór wycofany", „akredytacja wycofana") z przypisaniem mu odpowiedniej wartości. Przez cały okres świadczenia usługi certyfikacyjnej jej status może się zmieniać z nadzoru na akredytację i odwrotnie [1].

Poniższy schemat 1 przedstawia przewidywaną zmianę możliwych statusów nadzoru/akredytacji w odniesieniu do pojedynczej usługi certyfikacyjnej:

[1] Np. podmiot świadczący usługi certyfikacyjne mający siedzibę w państwie członkowskim, świadczący usługę certyfikacyjną, którą początkowo nadzoruje państwo członkowskie (organ ds. nadzoru), po pewnym czasie może zadecydować o przejściu dobrowolnej akredytacji w odniesieniu do aktualnie nadzorowanej usługi certyfikacyjnej. Z drugiej strony podmiot świadczący usługi certyfikacyjne w innym państwie członkowskim może zadecydować o nieprzerywaniu świadczenia akredytowanej usługi certyfikacyjnej, ale o zmianie jej statusu z akredytowanej na nadzorowaną, np. ze względów biznesowych lub gospodarczych.

Schemat 1

Oczekiwane zmiany statusu nadzoru/akredytacji w odniesieniu do pojedynczej usługi CSP



Legenda:

Status przejściowy, gdy istnieje powiązany model nadzoru (np. musi tak być w przypadku podmiotu świadczącego usługi certyfikacyjne wystawiającego certyfikat kwalifikowany mającego siedzibę w państwie członkowskim). Możliwy bieżący status, gdy nie istnieje powiązany model nadzoru (np. w przypadku podmiotu świadczącego usługi certyfikacyjne niewystawiającego certyfikatu kwalifikowanego)

Możliwy bieżący status

Podmiot certyfikacyjny wystawiający certyfikaty kwalifikowane mający siedzibę w jednym z państw członkowskich musi podlegać nadzorowi (przez państwo członkowskie siedziby) i może być objęty dobrowolna akredytacją. Gdy podmiot jest wymieniony na zaufanej liście jego statusu musi przyjmować jedną ze wskazanych powyżej wartości statusu określaną jako „bieżąca wartość statusu", zgodnie z jego obecnym statusem. Musi ona ulec zmianie, w odpowiednich przypadkach, jeśli status ulegnie zmianie, zgodnie z powyższym schematem. Należy jednak zauważyć, że „akredytacja wstrzymana" i „akredytacja wycofana" muszą stanowić wartości „statusu przejściowego" tylko w odniesieniu do odpowiednich usług CSP_{QC}, które są wyszczególnione na zaufanej liście państwa członkowskiego, w którym ma on siedzibę, ponieważ takie usługi podlegają domyślnemu nadzorowi (nawet, jeżeli nie mają akredytacji lub jeżeli akredytacja wygasła). Gdy odpowiednia usługa jest wyszczególniona (akredytowana) w innym państwie członkowskim niż państwo siedziby, wartości te mogą być traktowane jako ostateczne.

Wymaga się, aby państwa członkowskie, które tworzą lub już utworzyły określony w prawie krajowym „przyjęty (przyjęte) system (systemy) zatwierdzania" wdrożony (wdrożone) na szczeblu krajowym w celu nadzorowania zgodności usług świadczonych przez CSP **niewystawiające** certyfikatów kwalifikowanych zgodnie z przepisami dyrektywy 1999/93/WE oraz z ewentualnymi przepisami krajowymi dotyczącymi świadczenia usług certyfikacyjnych (w rozumieniu art. 2 pkt 11 dyrektywy 1999/93/WE), zaklasyfikowały taki system (takie systemy) zatwierdzania do jednej z dwóch wskazanych poniżej kategorii:

— „akredytacja dobrowolna" zdefiniowana i regulowana dyrektywą 1999/93/WE (art. 2 pkt 13, art. 3 ust. 2, art. 7 ust. 1 lit. a), art. 8 ust. 1, art. 11, motywy 4, 11, 12 i 13);

— „nadzór" zgodny z wymogami dyrektywy 1999/93/WE i wdrożony na podstawie przepisów krajowych i wymogów prawa krajowego.

Zatem podmiot certyfikacyjny niewystawiający certyfikatów kwalifikowanych może podlegać nadzorowi lub być objęty dobrowolną akredytacją. Gdy podmiot jest wyszczególniony na zaufanej liście wartość jego statusu musi przyjmować jedną ze wskazanych powyżej wartości statusu jako „bieżąca wartość statusu" tego podmiotu (zob. schemat 1), zgodnie z jego obecnym statusem. Musi ona ulec zmianie, w odpowiednich przypadkach, jeśli status ulegnie zmianie, zgodnie z powyższym schematem.

Zaufana lista musi zawierać informacje dotyczące podstawowego systemu (systemów) nadzoru/akredytacji, w szczególności:

— informacje dotyczące systemu nadzoru mającego zastosowanie do każdego CSP_{QC},

— w stosownych przypadkach, informacje dotyczące krajowego systemu „dobrowolnej akredytacji" mającego zastosowanie do każdego CSP_{QC},

— w stosownych przypadkach, informacje dotyczące systemu nadzoru mającego zastosowanie do każdego CSP niewystawiającego certyfikatów kwalifikowanych,

— w stosownych przypadkach, informacje dotyczące krajowego systemu „dobrowolnej akredytacji" mającego zastosowanie do każdego CSP niewystawiającego certyfikatów kwalifikowanych.

Dwa ostatnie zbiory informacji mają zasadnicze znaczenie dla stron, które się na nich opierają przy dokonywaniu oceny poziomu jakości i bezpieczeństwa takich systemów nadzoru/akredytacji mających zastosowanie na szczeblu krajowym w odniesieniu do CSP niewystawiających certyfikatów kwalifikowanych. Jeżeli zaufana lista zawiera informacje dotyczące statusu nadzoru/akredytacji w odniesieniu do usług świadczonych przez CSP niewystawiające certyfikatów kwalifikowanych, wymienione wcześniej zbiory informacji są udostępniane na zaufanej liście z użyciem „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 i fakultatywnych szczególnych informacji udostępnianych przez państwa członkowskie) i „TSL policy/legal notice" (klauzula 5.3.11 – tekst wspólny dla wszystkich państw członkowskich odnoszący się do dyrektywy 1999/93/WE oraz możliwość dodania przez każde państwo członkowskie swojego własnego tekstu/odniesień).

Dodatkowe informacje dotyczące „kwalifikacji" określone na szczeblu krajowych systemów nadzoru/akredytacji w odniesieniu do CSP niewystawiających certyfikatów kwalifikowanych mogą być w stosownych przypadkach i w razie potrzeby udostępniane na poziomie usług (np. aby umożliwić rozróżnienie kilku poziomów jakości/bezpieczeństwa) z użyciem rozszerzenia „additionalServiceInformation" (klauzula 5.5.9.4) jako części „Service information extension" (klauzula 5.5.9). Dalsze informacje dotyczące stosownych specyfikacji technicznych znajdują się wśród specyfikacji szczegółowych w rozdziale I.

Mimo że nadzorem i akredytacją usług certyfikacyjnych w państwie członkowskim mogą kierować oddzielne organy państwa członkowskiego, oczekuje się, że jednej usłudze certyfikacyjnej będzie odpowiadał tylko jeden wpis i że status nadzoru/akredytacji tej usługi będzie odpowiednio aktualizowany.

3.3. *Wpisy na zaufanej liście mające na celu ułatwienie weryfikacji QES i* $AdES_{QC}$

Najważniejszym etapem tworzenia zaufanej listy jest przygotowanie części obowiązkowej tej listy, a mianowicie „Listy usług" w podziale na CSP wystawiające certyfikaty kwalifikowane, co ma na celu poprawne odzwierciedlenie rzeczywistej sytuacji każdego podmiotu wystawiającego te certyfikaty, związanej z wystawianiem certyfikatów i dopilnowanie, aby informacje udostępnione w każdym wpisie były wystarczające do ułatwienia weryfikacji QES i $AdES_{QC}$ (w przypadku połączenia z treścią certyfikatu wierzchołka ścieżki wydanego przez CSP w ramach usługi certyfikacyjnej wymienionej w danym wpisie).

Wymagane informacje mogą obejmować informacje inne niż „cyfrowy identyfikator usługi" pojedynczego (głównego) CA, w szczególności informacje określające status certyfikacji kwalifikowanej certyfikatów wydanych przez taką usługę CA oraz to, czy SSCD tworzy obsługiwane podpisy. Dlatego też organ wyznaczony w państwie członkowskim do utworzenia, redagowania i prowadzenia zaufanej listy musi uwzględnić aktualny profil i treść każdego wystawionego certyfikatu kwalifikowanego w odniesieniu do każdej usługi CSP_{QC} wymienionej na zaufanej liście.

Najlepiej byłoby, gdyby każdy wystawiony certyfikat kwalifikowany zawierał określone przez ETSI poświadczenie zgodności certyfikatu kwalifikowanego (ang. QcCompliance statement) ([1]), jeżeli twierdzi się, że jest to certyfikat kwalifikowany, oraz określone przez ETSI poświadczenie o obsłudze certyfikatu kwalifikowanego za pomocą bezpiecznego urządzenia służącego do składania podpisu (ang. QcSSCD statement), jeżeli twierdzi się, że składanie podpisów elektronicznych odbywa się za pomocą SSCD lub jeżeli twierdzi się, że każdy wystawiony certyfikat kwalifikowany zawiera jeden z identyfikatorów obiektów (OID) polityk certyfikatów QCP/QCP + określonych w ETSI EN 319 411-2 ([2]). Stosowanie przez CSP wystawiające certyfikaty kwalifikowane różnych norm jako odniesień, szeroka interpretacja tych norm oraz brak wiedzy na temat istnienia i nadrzędności pewnych normatywnych specyfikacji technicznych lub norm doprowadziło do różnic w rzeczywistej treści aktualnie wystawianych certyfikatów kwalifikowanych (np. stosowanie lub niestosowanie poświadczeń certyfikatu kwalifikowanego określonych przez ETSI) i w rezultacie nie pozwala stronom otrzymującym po prostu polegać na certyfikacie podpisującego (i na towarzyszącym łańcuchu/towarzyszącej ścieżce) przy ocenie, przynajmniej w drodze odczytu maszynowego, czy certyfikat, który weryfikuje podpis elektroniczny, jest certyfikatem kwalifikowanym, czy nie, oraz czy jest powiązany z SSCD, przy pomocy którego złożono podpis.

([1]) Zob. ETSI EN 319 412-5 (Electronic Signatures and Infrastructures (ESI); Profiles for Trust Service Providers issuing certificates; Część 5: Extension for Qualified Certificate profile) zawierające definicję takiego poświadczenia.

([2]) ETSI EN 319 411-2 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Część 2: Policy requirements for certification authorities issuing qualified certificates.

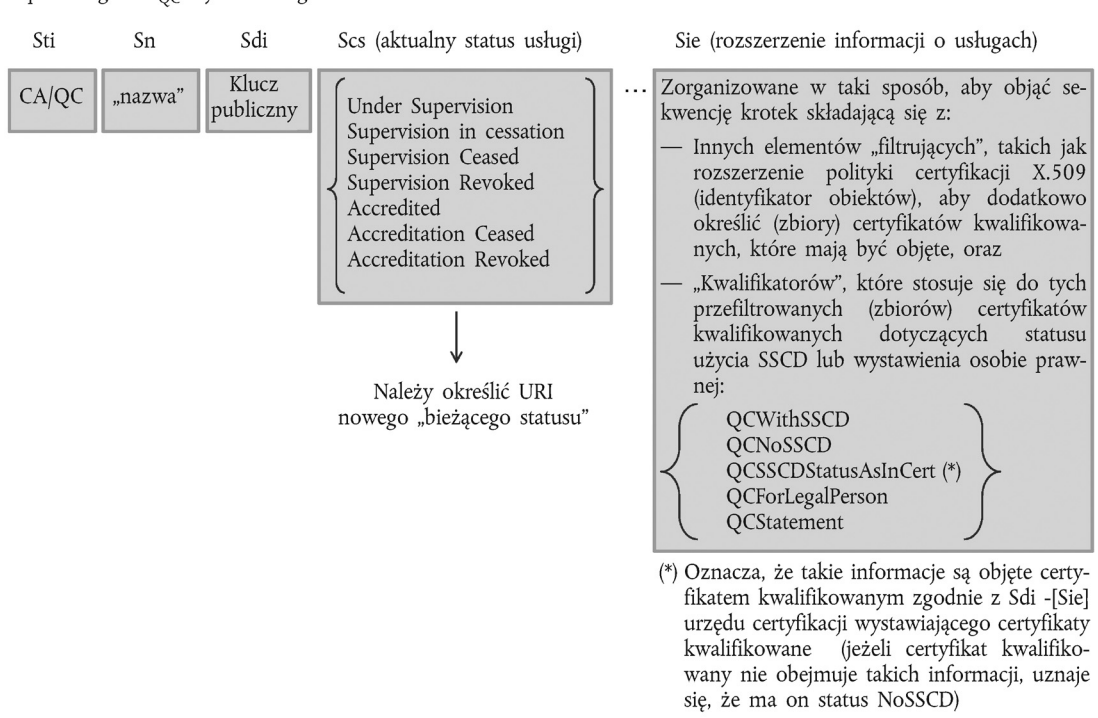
Uzupełnienie pól zaufanej listy: „Service type identifier" („Sti"), „Service name" („Sn") i „Service digital identity" („Sdi") informacjami podanymi w polu „Service information extensions" („Sie") umożliwia pełne określenie konkretnego rodzaju certyfikatu kwalifikowanego wystawionego przez CSP wymieniony na liście i wystawiający certyfikaty kwalifikowane oraz poinformowanie, czy dany certyfikat kwalifikowany jest obsługiwany przez SSCD (jeżeli wystawiony certyfikat kwalifikowany nie zawiera takiej informacji). Z wpisem tym powiązana jest odpowiednia informacja dotycząca „Service current status" („Scs"). Przedstawia to zamieszczony poniżej schemat 2.

Umieszczenie na liście usługi z podaniem tylko „Sdi" (głównego) CA oznaczałoby, że dopilnowano (z udziałem CSP wystawiającego certyfikaty kwalifikowane oraz organu ds. nadzoru/akredytacji odpowiedzialnego za nadzór/akredytację danego CSP), aby każdy certyfikat wierzchołka ścieżki wystawiony w ramach takiej hierarchii przez (główny) CA zawierał wystarczającą ilość informacji określonych przez ETSI i nadających się do przetworzenia maszynowego, aby można było ocenić, czy jest to certyfikat kwalifikowany, oraz czy jest on obsługiwany przez SSCD. Przykładowo w przypadku, gdy drugie z tych twierdzeń jest fałszywe (np. w certyfikacie kwalifikowanym nie ma znormalizowanego przez ETSI oznaczenia nadającego się do przetwarzania maszynowego świadczącego o tym, że ten certyfikat jest obsługiwany przez SSCD), wówczas poprzez podanie w liście tylko „Sdi" (głównego) CA można tylko przyjąć, że certyfikaty kwalifikowane wystawione zgodnie z hierarchią tego (głównego) CA nie są obsługiwane przez żaden SSCD. W celu wskazania, że certyfikaty te należy traktować jako obsługiwane przez SSCD należy zastosować pole „Sie" („Sie" wskazuje także, że fakt wystawienia za pomocą danego urządzenia jest gwarantowany przez CSP wystawiający certyfikaty kwalifikowane oraz nadzorowany/akredytowany odpowiednio przez organ ds. nadzoru lub akredytacji).

Schemat 2

Wpis usługi CSP wystawiającego certyfikaty kwalifikowane na liście

Zasady ogólne – Zasady edycji – wpisy CSP_{QC} (usługi wymienione na liście)



(*) Oznacza, że takie informacje są objęte certyfikatem kwalifikowanym zgodnie z Sdi -[Sie] urzędu certyfikacji wystawiającego certyfikaty kwalifikowane (jeżeli certyfikat kwalifikowany nie obejmuje takich informacji, uznaje się, że ma on status NoSSCD)

Niniejsza specyfikacja techniczna wspólnego wzoru zaufanej listy umożliwia stosowanie we wpisie usługi kombinacji pięciu głównych części informacji:

— „Service type identifier" („Sti"), np. identyfikujący CA wystawiający certyfikaty kwalifikowane („CA/QC"),

— „Service name" („Sn"),

— informacji o „Service digital identity" („Sdi") identyfikującej wyszczególnioną usługę np. klucz publiczny (jako minimum) CA wystawiającego certyfikaty kwalifikowane,

— w przypadku usług CA/QC fakultatywne informacje o „Service information extensions" („Sie"), które dopuszczają włączenie szeregu informacji na temat danej usługi, dotyczących statusu wycofania wygasłych certyfikatów, dodatkowych właściwości certyfikatów kwalifikowanych, przejęcia CSP przez inny CSP, jak również dodatkowych informacji o usłudze. przykładowo dodatkowe właściwości certyfikatów kwalifikowanych opisane są w sekwencji jednej lub większej liczby krotek, z których każda zawiera:

— kryteria wykorzystywane do dalszej identyfikacji (filtrowania), zgodnie ze zidentyfikowaną usługą certyfikacyjną „Sdi", tej właśnie usługi (tj. zbioru kwalifikowanych certyfikatów), w odniesieniu do której wymagane/zawarte są dodatkowe informacje dotyczące wskazania statusu „kwalifikowanego", obsługi przez SSCD lub wystawienia na rzecz osoby prawnej, oraz

— powiązane informacje („kwalifikatory") dotyczące tego, czy ten zestaw certyfikatów kwalifikowanych ma być uznawany za „kwalifikowany", czy jest obsługiwany przez SSCD, lub tego, czy przedmiotowe powiązane informacje stanowią element certyfikatu kwalifikowanego zgodnie ze znormalizowaną formą nadającą się do przetwarzania maszynowego, lub informacje dotyczące tego, że takie certyfikaty kwalifikowane wystawia się osobom prawnym (domyślnie uznaje się je za wystawione tylko osobom fizycznym),

— informacje o „bieżącym statusie" dla danego wpisu usługi, zawierające informacje:

— czy jest to usługa podlegająca nadzorowi lub objęta akredytacją, oraz

— o statusie samego nadzoru/akredytacji.

3.4. *Wytyczne dotyczące edycji i użycia wpisów usług CSP_{QC}*

Ogólne wytyczne dotyczące edycji:

1. Jeżeli w odniesieniu do wymienionej na liście usługi zidentyfikowanej przez „Sdi" zagwarantowano, że (gwarancja udzielona przez CSP_{QC} i nadzorowana/akredytowana przez organ ds. nadzoru/organ ds. akredytacji (ang. Supervisory Body - SB, Accreditation Body - AB)) każdy certyfikat kwalifikowany obsługiwany przez SSCD zawiera poświadczenie zgodności certyfikatu kwalifikowanego określone przez ETSI (poświadczenie zgodności - QcCompliance) i zawiera poświadczenie o wystawieniu certyfikatu kwalifikowanego za pomocą bezpiecznego urządzenia służącego do składania podpisu (poświadczenie QcSSCD) lub identyfikator obiektu (OID) QCP+, wówczas wystarczające jest zastosowanie odpowiedniej „Sdi", a pole „Sie" można stosować fakultatywnie i nie musi ono zawierać informacji na temat obsługi przez SSCD.

2. Jeżeli w odniesieniu do wymienionej na liście usługi zidentyfikowanej przez „Sdi" zagwarantowano, że (gwarancja udzielona przez CSP_{QC} i nadzorowana/akredytowana przez SB/AB) każdy certyfikat kwalifikowany nieobsługiwany przez SSCD zawiera poświadczenie QcCompliance lub QCP OID i nie zawiera poświadczenia QcSSCD lub QCP + OID, wówczas wystarczy użyć odpowiedniej „Sdi", a pole „Sie" można stosować fakultatywnie i nie musi ono zawierać informacji na temat obsługi przez SSCD (co oznacza, że nie jest on obsługiwany przez SSCD).

3. Jeżeli w odniesieniu do wymienionej na liście usługi zidentyfikowanej przez „Sdi" zagwarantowano, że (gwarancja udzielona przez CSP_{QC} i nadzorowana/akredytowana przez SB/SA) każdy certyfikat kwalifikowany zawiera poświadczenie QcCompliance, a niektóre z tych certyfikatów kwalifikowanych są przeznaczone do obsługiwania przez SSCD, zaś inne nie są (rozróżnienia można dokonać np. na podstawie różnych szczególnych OID polityki certyfikacyjnej CSP lub na podstawie innych szczególnych informacji na temat CSP zawartych w certyfikacie kwalifikowanym, bezpośrednio lub pośrednio, w sposób nadający się do przetworzenia maszynowego lub nie), ale certyfikat obsługiwany przez SSCD NIE zawiera poświadczenia QcSSCD ANI TEŻ QCP(+) OID określonego przez ETSI, wówczas zastosowanie odpowiedniej „Sdi" może nie być wystarczające ORAZ pole „Sie" musi być zastosowane w celu wskazania wyraźnych informacji na temat obsługi przez SSCD wraz z potencjalnym rozszerzeniem zakresu informacji mających na celu zidentyfikowanie przedmiotowego zbioru certyfikatów. Przy wypełnianiu pola „Sie" może pojawić się potrzeba włączenia do tej samej „Sdi" różnych „wartości informacji na temat obsługi przez SSCD".

4. Jeżeli w odniesieniu do wymienionej na liście usługi zidentyfikowanej przez „Sdi" zagwarantowano, że (gwarancja udzielona przez CSP_{QC} i nadzorowana/akredytowana przez SA/SB) żaden certyfikat kwalifikowany nie zawiera poświadczenia QcCompliance, QCP OID, poświadczenia QcSSCD ani QCP + OID, ale zagwarantowano, że niektóre z tych certyfikatów wierzchołka ścieżki wystawionych zgodnie z „Sdi" mają być certyfikatami kwalifikowanymi lub mają być obsługiwane przez SSCD, a inne nie (rozróżnienia można dokonać np. na podstawie różnych szczególnych OID polityki certyfikacyjnej CSPQC lub na podstawie innych szczególnych informacji na temat CSP_{QC} zawartych w certyfikacie kwalifikowanym, bezpośrednio lub pośrednio, w sposób nadający się do przetworzenia maszynowego lub nie), wówczas zastosowanie odpowiedniej „Sdi" nie będzie wystarczające ORAZ w polu „Sie" należy umieścić wyraźne informacje dotyczące statusu kwalifikowanego. Przy wypełnianiu pola „Sie" może pojawić się potrzeba włączenia do tej samej „Sdi" różnych „wartości informacji na temat obsługi przez SSCD".

Zgodnie z ogólną domyślną zasadą w odniesieniu do CSP wymienionego na zaufanej liście musi istnieć jeden wpis usługi dla pojedynczego klucza publicznego dotyczącego usługi certyfikacyjnej typu CA/QC tzn. urzędu certyfikacji (bezpośrednio) wystawiającego certyfikaty kwalifikowane. W pewnych wyjątkowych okolicznościach i w starannie kontrolowanych warunkach, organ ds. nadzoru/akredytacji państwa członkowskiego może podjąć decyzję o zastosowaniu, jako „Sdi" pojedynczego wpisu w wykazie usług tego CSP ujętego w wykazie, klucza publicznego CA głównego lub wyższego

szczebla w ramach infrastruktury klucza publicznego danego CSP (np. w kontekście hierarchii CA tego CSP, od głównego CA do szeregu wystawiających CA), zamiast umieszczać w wykazie wszystkie podległe usługi urzędu certyfikacji wystawiające certyfikaty (tzn. wyszczególnienie urzędu certyfikacji niewystawiającego bezpośrednio certyfikatów kwalifikowanych wierzchołka ścieżki, lecz certyfikującego hierarchię CA aż do CA wystawiających certyfikaty kwalifikowane wierzchołka ścieżki). Konsekwencje (wady i zalety) stosowania klucza publicznego takiego głównego CA lub CA wyższego szczebla jako wartości „Sdi" wpisów dotyczących usług na zaufanej liście muszą być dokładnie rozważone przez podejmujące się tego państwa członkowskie. Ponadto jeżeli państwo członkowskie stosuje dopuszczalne wyjątki od tej domyślnej zasady, musi ono przedstawić niezbędne dokumenty ułatwiające tworzenie i weryfikację ścieżki certyfikatu. Przykładowo, w kontekście CSP_{QC} z wykorzystaniem jednego głównego CA, w powiązaniu z którym szereg CA wystawia certyfikaty kwalifikowane i niekwalifikowane, ale w odniesieniu do których certyfikaty kwalifikowane zawierają tylko poświadczenie QcCompliance i nie zawierają wskazania, czy są one obsługiwane przez SSCD, wymienienie w wykazie tylko „Sdi" głównego urzędu certyfikacji zgodnie z zasadami wyjaśnionymi powyżej oznaczałoby, że żaden certyfikat kwalifikowany wystawiony w ramach hierarchii głównego CA nie jest obsługiwany przez SSCD. Jeśli istnieją certyfikaty kwalifikowane, które są faktycznie obsługiwane przez SSCD, ale w certyfikatach nie ma poświadczenia dotyczącego przetwarzania maszynowego, które wskazywałoby na taką obsługę, usilnie zaleca się zamieszczenie poświadczenia QcSSCD w certyfikatach kwalifikowanych wystawianych w przyszłości. W międzyczasie (do czasu wygaśnięcia ostatniego certyfikatu kwalifikowanego nie zawierającego takich informacji) na zaufanej liście powinno wykorzystywać się pole „Sie" i powiązane „rozszerzenie kwalifikacji" np. zapewniając filtrowanie certyfikatów z użyciem szczególnego (szczególnych) OID określonych przez CSP_{QC}, stosowanego (stosowanych) potencjalnie przez CSP_{QC} do rozróżnienia różnych rodzajów certyfikatów kwalifikowanych (jedne obsługiwane przez SSCD, a inne nie) i zawierającego (zawierających) wyraźne „informacje na temat obsługi przez SSCD" w odniesieniu do przedmiotowych certyfikatów filtrowanych z użyciem zestawu (zestawów) „kwalifikatorów".

Ogólne wytyczne dotyczące stosowania aplikacji, usług lub produktów wykorzystujących podpis elektroniczny opierających się na zaufanej liście zgodnej z niniejszymi specyfikacjami technicznymi są następujące:

Wpis „Sti" dotyczący CA/QC (podobnie jak wpis dotyczący CA/QC zakwalifikowanego dodatkowo jako „główny CA/QC" (ang. Root CA/QC) poprzez zastosowanie rozszerzenia „Sie" additionalServiceInformation Extension)

— wskazuje, że wszystkie certyfikaty wierzchołka ścieżki wystawione przez CA zidentyfikowany jako „Sdi" (podobnie jak w ramach hierarchii CA rozpoczynającej się od głównego CA zidentyfikowanego jako „Sdi") są certyfikatami kwalifikowanymi, **pod warunkiem że** są za takie uznane w certyfikacie poprzez zastosowanie odpowiednich przetwarzalnych maszynowo poświadczeń certyfikatu kwalifikowanego (tzn. poświadczeń QcCompliance) lub określonych przez ETSI QCP(+) OID (i jest to gwarantowane przez organ ds. nadzoru/akredytacji, zob. wyżej „ogólne wytyczne dotyczące edycji"),

Uwaga: Jeżeli nie ma żadnej informacji „Sie" dotyczącej „rozszerzenia kwalifikacji" lub jeżeli certyfikat wierzchołka ścieżki podawany za certyfikat kwalifikowany nie jest dodatkowo identyfikowany poprzez powiązany wpis „Sie" dotyczący „rozszerzenia kwalifikacji", wówczas poprawność nadających się do przetworzenia maszynowego informacji zawartych w certyfikacie kwalifikowanym podlega nadzorowi/akredytacji. Oznacza to, że zapewnione zostaje, że stosowanie (lub niestosowanie) odpowiednich poświadczeń certyfikatu kwalifikowanego (tzn. poświadczenia QcC i QcSSCD) lub określonych przez ETSI QCP(+) OID jest zgodne z deklaracjami CSP_{QC}.

— **i JEŻELI** przedstawiono „Sie" dotyczące „rozszerzenia kwalifikacji", wówczas obok przedstawionej powyżej domyślnej zasady interpretacji stosowania, certyfikaty, które są identyfikowane na podstawie tego wpisu „Sie" dotyczącego „rozszerzenia kwalifikacji" opartego na zasadzie sekwencji filtrów dodatkowo identyfikujących zbiór certyfikatów, należy traktować zgodnie ze zbiorem „kwalifikatorów" przedstawiających pewne dodatkowe informacje dotyczące, statusu kwalifikowanego, „obsługi przez SSCD" lub „osoby prawnej jako podmiotu" (np. certyfikaty zawierające szczególny OID w rozszerzeniu polityki certyfikatu, posiadające szczególny wzór „stosowania klucza" lub filtrowane z użyciem szczególnej wartości pojawiającej się w jednym szczególnym polu lub rozszerzeniu certyfikatu itp.). Kwalifikatory te stanowią element następujące zestawu „kwalifikatorów" mających zrekompensować brak informacji w treści odpowiedniego certyfikatu kwalifikowanego, wykorzystywanych odpowiednio do:

  — oznaczenia statusu kwalifikowanego: „poświadczenia certyfikatu kwalifikowanego" oznaczające, że dany certyfikat kwalifikowany (certyfikaty kwalifikowane) jest (są) kwalifikowany (kwalifikowane),

    LUB

  — wskazania statusu obsługi przez SSCD

    — wartość kwalifikatora „QCWithSSCD" oznacza „certyfikat kwalifikowany obsługiwany przez SSCD", lub

    — wartość kwalifikatora „QCNoSSCD" oznacza „certyfikat kwalifikowany nieobsługiwany przez SSCD", lub

    — wartość kwalifikatora „QCSSCDStatusAsInCert" oznacza, że gwarantuje się zamieszczenie informacji o obsłudze przez SSCD w każdym certyfikacie kwalifikowanym w informacjach o „Sdi"-„Sie" zawartych w danym wpisie CA/QC,

    LUB

— wskazania, że certyfikat wystawia się osobie prawnej:

— wartość kwalifikatora „QCForLegalPerson" oznacza „certyfikat wystawiony osobie prawnej".

3.5. *Usługi obsługujące usługi CA/QC, ale niestanowiące części „Sdi" CA/QC*

Usługi określające status ważności certyfikatu związane z certyfikatami kwalifikowanymi (np. odpowiedzi CRLS i OCSP), w przypadku których informacje o statusie ważności certyfikatu podpisywane są przez podmiot, którego klucz prywatny nie jest certyfikowany w ramach ścieżki certyfikacji prowadzącej do urzędu certyfikacji ujętego na liście wystawiającego certyfikaty kwalifikowane („CA/QC") są wymieniane na zaufanej liście poprzez wyszczególnienie tych usług określających status ważności certyfikatu jako takich na tej liście (tzn. odpowiednio jako usługa typu „OCSP/QC" lub „CRL/QC"), ponieważ usługi te można uznawać za element nadzorowanych/akredytowanych „kwalifikowanych" usług związanych ze świadczeniem usług certyfikacji certyfikatów kwalifikowanych. Oczywiście certyfikaty podmiotów obsługujących zapytania OCSP i certyfikaty wydawców CRL, które zostały podpisane przez urzędy certyfikacji w ramach hierarchii usług CA/QC wymienionego na liście, uznaje się za „ważne" i zgodne z wartością statusu wymienionych na liście usług CA/QC.

Podobną zasadę można zastosować do usług certyfikacyjnych wystawiających certyfikaty niekwalifikowane (typ usługi „CA/PKC").

Na zaufanej liście wyszczególniane są usługi określające status ważności certyfikatów, jeśli powiązane informacje o lokalizacji takich usług nie zostały podane w certyfikatach wierzchołka ścieżki, wobec których stosuje się usługi określające status ważności certyfikatów.

4. **Definicje i skróty**

Do celów niniejszego dokumentu stosuje się następujące definicje i akronimy:

Termin	Akronim	Definicja
Podmiot świadczący usługi certyfikacyjne	CSP	Zgodnie z definicją zawartą w art. 2 pkt 11 dyrektywy 1999/93/WE.
Urząd certyfikacji	CA	1) podmiot świadczący usługi certyfikacyjne tworzący i przydzielający certyfikaty klucza publicznego; lub 2) techniczna usługa generowania certyfikatów stosowana przez podmiot świadczący usługi certyfikacyjne tworzący i przydzielający certyfikaty klucza publicznego. *UWAGA*: Dalsze objaśnienia koncepcji urzędu certyfikacji zawarte są w klauzuli 4 w EN 319 411-2 [1].
Urząd certyfikacji wystawiający certyfikaty kwalifikowane	CA/QC	Urząd certyfikacji spełniający wymogi określone w załączniku II do dyrektywy 1999/93/WE i wystawiający certyfikaty kwalifikowane spełniające wymogi ustanowione w załączniku I do dyrektywy 1999/93/WE.
Certyfikat	Certyfikat	Zgodnie z definicją zawartą w art. 2 pkt 9 dyrektywy 1999/93/WE.
Certyfikat kwalifikowany	QC	Zgodnie z definicją zawartą w art. 2 pkt 10 dyrektywy 1999/93/WE.
Podpisujący	Podpisujący	Zgodnie z definicją zawartą w art. 2 pkt 3 dyrektywy 1999/93/WE.
Nadzór	Nadzór	Dotyczy nadzoru określonego w art. 3 ust. 3 dyrektywy 1999/93/WE. Zgodnie z dyrektywą 1999/93 od państw członkowskich wymaga się utworzenia odpowiedniego systemu umożliwiającego nadzór nad CSP mającymi siedzibę na terytorium zainteresowanych państw członkowskich i powszechnie wystawiającymi certyfikaty kwalifikowane, który to system zapewniłby nadzór nad przestrzeganiem przepisów tej dyrektywy.
Dobrowolna akredytacja	Akredytacja	Zgodnie z definicją zawartą w art. 2 pkt 13 dyrektywy 1999/93/WE.
Zaufana zaufania	TL	Oznacza wykaz wskazujący status nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne nadzorowane/akredytowane przez przedmiotowe państwo członkowskie pod względem zgodności z przepisami dyrektywy 1999/93/WE.

Termin	Akronim	Definicja
Lista statusu usług zaufania	TSL	Ma formę podpisanej listy stosowanej jako podstawa prezentacji informacji dotyczących statusu usług zaufania zgodnie ze specyfikacją ustanowioną w ETSI TS 119 612.
Usługa zaufania		Usługa, która zwiększa zaufanie do transakcji zawieranych droga elektroniczną (zazwyczaj, ale niekoniecznie z zastosowaniem technik kryptograficznych lub z użyciem materiałów poufnych) (ETSI TS 119 612). *UWAGA*: Jest to termin szerzej stosowany w porównaniu z usługą certyfikacyjną wystawiającą certyfikaty lub świadczącą inne usługi związane z podpisami elektronicznymi.
Dostawca usługi zaufania	TSP	Podmiot świadczący jedną lub większą liczbę (elektronicznych) usług zaufania (termin ten ma szersze zastosowanie niż pojęcie CSP).
Token usługi zaufania	TrST	Obiekt fizyczny lub binarny (logiczny) wygenerowany lub wydany w wyniku świadczenia usługi zaufania. Przykłady binarnych TrSTs to certyfikaty, listy unieważnionych certyfikatów (CRL), tokeny znacznika czasu (TST) oraz odpowiedzi udzielane za pośrednictwem protokołu statusu certyfikatu online (OCSP)
Kwalifikowany podpis elektroniczny	QES	AdES weryfikowany certyfikatem kwalifikowanym i wygenerowany przez bezpieczne urządzenie służące do składania podpisów zgodnie z definicją zawartą w art. 2 dyrektywy 1999/93/WE.
Zaawansowany podpis elektroniczny	AdES	Zgodnie z definicją zawartą w art. 2 pkt 2 dyrektywy 1999/93/WE.
Zaawansowany podpis elektroniczny weryfikowany certyfikatem kwalifikowanym	$AdES_{QC}$	Oznacza podpis elektroniczny spełniający wymogi AdES i weryfikowany przez QC zgodnie z definicją zawartą w art. 2 dyrektywy 1999/93/WE.
Bezpieczne urządzenie służące do składania podpisu	SSCD	Zgodnie z definicją zawartą w art. 2 pkt 6 dyrektywy 1999/93/WE.

([1]) EN 319 411-2 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Część 2: Policy requirements for certification authorities issuing qualified certificates.

W poniższej części dokumentu słowa kluczowe MUSI (MUST, SHALL), NIE MOŻNA (MUST NOT, SHALL NOT), WYMAGANY (REQUIRED), POWINIEN (SHOULD), NIE POWINIEN (SHOULD NOT), ZALECANY (RECOMMENDED), MOŻE (MAY) i FAKULTATYWNY (OPTIONAL) należy interpretować zgodnie z RFC 2119 ([1]).

ROZDZIAŁ I

SZCZEGÓŁOWA SPECYFIKACJA DOTYCZĄCA WSPÓLNEGO WZORU „ZAUFANEJ LISTY NADZOROWANYCH/AKREDYTOWANYCH PODMIOTÓW ŚWIADCZĄCYCH USŁUGI CERTYFIKACYJNE”

Niniejsza specyfikacja opiera się na specyfikacji i wymogach określonych w ETSI TS 119 612 v1.1.1 (zwanej dalej ETSI TS 119 612).

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

Scheme operator name (klauzula 5.3.4)

Pole to MUSI występować i MUSI być zgodne ze specyfikacją zawartą w klauzuli 5.3.4 TS 119 612.

([1]) IETF RFC 2119 – „Key words for use in RFCs to indicate Requirements Levels”.

Kraj MOŻE mieć odrębne organy ds. nadzoru i akredytacji, a nawet dodatkowe organy zajmujące się wszelkimi powiązanymi działaniami operacyjnymi. Wyznaczenie operatora systemu zaufanej listy w państwie członkowskim należy do danego państwa. Oczekuje się, że na organie ds. nadzoru, organie ds. akredytacji i operatorze systemu (jeżeli są odrębnymi organami) będą spoczywały określone dla każdego z nich obowiązki i odpowiedzialność.

Każda sytuacja, w której szereg organów jest odpowiedzialnych za nadzór, akredytację lub aspekty operacyjne, MUSI być konsekwentnie odzwierciedlona i identyfikowana jako taka w informacjach dotyczących systemu stanowiących część zaufanej listy, w tym także w określonych informacjach dotyczących systemu wskazanych w „Scheme information URI" (klauzula 5.3.7).

Scheme name (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" = „lista statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne nadzorowanych/akredytowanych przez przedmiotowego operatora systemu państwa członkowskiego w zakresie zgodności z odpowiednimi przepisami dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych".

Scheme information 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" MUSZĄ obejmować jako minimum:

— Informacje wprowadzające wspólne dla wszystkich państw członkowskich odnoszące się do zakresu i kontekstu zaufanej listy i podstawowego systemu (podstawowych systemów) nadzoru/akredytacji. Należy zastosować wspólny tekst zamieszczony poniżej, w którym wyrażenie „[*nazwa danego państwa członkowskiego*]" MUSI zostać zastąpione nazwą danego państwa członkowskiego:

„Niniejsza lista to „zaufana lista nadzorowanych/akredytowanych podmiotów świadczących usługi certyfikacyjne" dostarczająca informacji na temat statusu nadzoru/akredytacji usług certyfikacyjnych realizowanych przez podmioty świadczące usługi certyfikacyjne (CSP) nadzorowane/akredytowane przez [*nazwa danego państwa członkowskiego*] w zakresie zgodności z właściwymi przepisami dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.

Zaufana lista służy:

— wyszczególnieniu i dostarczaniu rzetelnych informacji na temat statusu nadzoru/akredytacji usług certyfikacyjnych realizowanych przez podmioty świadczące usług certyfikacyjne nadzorowane/akredytowane przez [*nazwa danego państwa członkowskiego*] w zakresie zgodności z właściwymi przepisami dyrektywy 1999/93/WE,

— umożliwieniu wiarygodnej weryfikacji podpisów elektronicznych obsługiwanych przez te wyszczególnione nadzorowane/akredytowane usługi certyfikacyjne realizowane przez CSP umieszczone na liście.

Zaufana lista państwa członkowskiego dostarcza co najmniej informacji na temat nadzorowanych/akredytowanych CSP wystawiających certyfikaty kwalifikowane zgodnie z przepisami dyrektywy 1999/93/WE (art. 3 ust. 2 i 3 oraz art. 7 ust. 1 lit. a)), w tym, jeśli nie stanowią one elementu certyfikatów kwalifikowanych, informacje o certyfikacie kwalifikowanym weryfikującym podpis elektroniczny oraz o tym, czy podpis został wygenerowany za pomocą bezpiecznego urządzenia służącego do składania podpisu.

CSP wystawiające certyfikaty kwalifikowane umieszczone na liście są nadzorowane przez [*nazwa danego państwa członkowskiego*], mogą być także akredytowane w zakresie zgodności z przepisami ustanowionymi w dyrektywie 1999/93/WE, w tym zgodności z wymogami załącznika I (wymogi dotyczące certyfikatów kwalifikowanych) oraz załącznika II (wymogi dla CSP wystawiających certyfikaty kwalifikowane). Stosowany system „nadzoru" (odpowiednio system „dobrowolnej akredytacji") jest określony w dyrektywie 1999/93/WE i musi spełniać odpowiednie ustanowione w niej wymogi, w szczególności te ustanowione w art. 3 ust. 3, art. 8 ust. 1, art. 11 (odpowiednio w art. 2 pkt 13, art. 3 ust. 2, art. 7 ust. 1 lit. a), art. 8 ust. 1, art. 11).

Dodatkowe informacje dotyczące innych nadzorowanych/akredytowanych CSP niewystawiających certyfikatów kwalifikowanych, ale świadczących usługi związane z podpisami elektronicznymi (np. CSP świadczące usługi związane ze znakowaniem czasem i wydawaniem tokenów znacznika czasu, CSP wystawiające certyfikaty niekwalifikowane itp.) można dobrowolnie umieścić na zaufanej liście na szczeblu krajowym".

— Określone informacje dotyczące podstawowego systemu (podstawowych systemów) nadzoru/akredytacji, w szczególności ([1]):

  — informacje dotyczące systemu nadzoru mającego zastosowanie do każdego CSP_{QC},

  — w stosownych przypadkach informacje dotyczące krajowego systemu dobrowolnych akredytacji mającego zastosowanie do każdego CSP_{QC},

  — w stosownych przypadkach informacje dotyczące systemu nadzoru mającego zastosowanie do każdego CSP niewystawiającego certyfikatów kwalifikowanych,

  — w stosownych przypadkach informacje dotyczące krajowego systemu dobrowolnej akredytacji mającego zastosowanie do każdego CSP niewystawiającego certyfikatów kwalifikowanych.

  W odniesieniu do każdego podstawowego systemu wymienionego powyżej te szczególne informacje MUSZĄ obejmować co najmniej:

  — ogólny opis,

  — informacje dotyczące postępowania organu ds. nadzoru/akredytacji w zakresie nadzorowania/akredytowania CSP i postępowania CSP w zakresie podlegania nadzorowi/akredytacji,

  — informacje dotyczące kryteriów nadzorowania/akredytowania CSP,

— W stosownych przypadkach określone informacje dotyczące szczególnych „kwalifikacji" niektórych obiektów fizycznych lub binarnych (logicznych) wygenerowanych lub wydanych w wyniku świadczenia usług certyfikacyjnych, którym może przysługiwać ta szczególna „kwalifikacja" na podstawie zgodności tych obiektów z przepisami i wymogami określonymi na szczeblu krajowym, w tym znaczenie takiej „kwalifikacji" i powiązanych przepisów i wymogów krajowych.

Dodatkowe właściwe dla danego państwa członkowskiego informacje dotyczące systemu MOŻNA podawać dobrowolnie. Mogą to być przykładowo:

— informacje dotyczące kryteriów i zasad wyboru inspektorów/audytorów i określające sposób przeprowadzania przez nich nadzoru (kontroli)/akredytacji (audytu) CSP,

— inne informacje kontaktowe i ogólne dotyczące funkcjonowania systemu.

Scheme type/community/rules (klauzula 5.3.9)

Pole to MUSI występować i MUSI być zgodne ze specyfikacją zawartą w klauzuli 5.3.9 TS 119 612 oraz MUSI zawierać co najmniej dwa URI:

— URI wspólny dla zaufanych list wszystkich państw członkowskich wskazujący tekst opisowy, który MUSI mieć zastosowanie do wszystkich zaufanych list, zamieszczony poniżej:

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

  Tekst opisowy:

  „Udział w systemie

  Każde państwo członkowskie musi stworzyć „zaufaną listę nadzorowanych/akredytowanych podmiotów świadczących usługi certyfikacyjne" dostarczającą informacji na temat statusu nadzoru/akredytacji usług certyfikacyjnych realizowanych przez podmioty świadczące usługi certyfikacyjne nadzorowane/akredytowane przez dane państwo członkowskie w zakresie zgodności z właściwymi przepisami dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.

  Na liście należy odnieść się także do aktualnego wdrażania takich zaufanych list w ramach wykazu linków do zaufanej listy każdego państwa członkowskiego stworzonego przez Komisję Europejską.

  Polityka/zasady oceny usług zamieszczonych na liście

  Zaufana lista państwa członkowskiego musi dostarczać co najmniej informacji o nadzorowanych/akredytowanych CSP wydających certyfikaty kwalifikowane zgodnie z przepisami ustanowionymi w dyrektywie 1999/93/WE (art. 3 ust. 2 i 3 oraz art. 7 ust. 1 lit. a)), w tym informacji o certyfikacie kwalifikowanym weryfikującym podpis elektroniczny oraz o tym, czy został on wygenerowany za pomocą bezpiecznego urządzenia służącego do składania podpisu.

([1]) Dwa ostatnie zbiory informacji mają zasadnicze znaczenie dla stron, które się na nich opierają przy dokonywaniu oceny poziomu jakości i bezpieczeństwa takich systemów nadzoru/akredytacji mających zastosowanie do CSP niewystawiających QS. 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 odnoszący się do dyrektywy 1999/93/WE wraz z możliwością dodania przez każde państwo członkowskie swojego własnego tekstu/odniesień). Dodatkowe informacje dotyczące krajowych systemów nadzoru/akredytacji w odniesieniu do CSP niewystawiających certyfikatów kwalifikowanych 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).

CSP wydające certyfikaty kwalifikowane musza być nadzorowane przez państwo członkowskie, w którym mają siedzibę (jeśli mają siedzibę w państwie członkowskim), mogą być one także akredytowane w zakresie zgodności z przepisami ustanowionymi w dyrektywie 1999/93/WE, w tym zgodności z wymogami załącznika I (wymogi dotyczące certyfikatów kwalifikowanych) oraz załącznika II (wymogi dotyczące CSP wystawiających certyfikaty kwalifikowane). CSP wystawiające certyfikaty kwalifikowane, które są akredytowane w państwie członkowskim, muszą także podlegać właściwemu systemowi nadzoru tego państwa członkowskiego, chyba że nie mają siedziby w tym państwie członkowskim. Stosowany system „nadzoru" (odpowiednio system „dobrowolnej akredytacji") jest określony w dyrektywie 1999/93/WE i musi spełnić odpowiednie ustanowione w niej wymogi, w szczególności te ustanowione w art. 3 ust. 3, art. 8 ust. 1, art. 11 (odpowiednio w art. 2 pkt 13, art. 3 ust. 2, art. 7 ust. 1 lit. a), art. 8 ust. 1, art. 11).

Dodatkowe informacje dotyczące innych nadzorowanych/akredytowanych CSP niewystawiających certyfikatów kwalifikowanych, ale świadczących usługi związane z podpisami elektronicznymi (np. CSP świadczące usługi związane ze znakowaniem czasem i wydawaniem tokenów znacznika czasu, CSP wystawiające certyfikaty niekwalifikowane itp.) można dobrowolnie umieścić na zaufanej liście na szczeblu krajowym.

CSP nie wystawiające certyfikatów kwalifikowanych, ale świadczące usługi pomocnicze mogą zostać objęte systemem „dobrowolnej akredytacji" (określonym w dyrektywie 1999/93/WE i zgodnym z tym aktem) lub określonym na szczeblu krajowym „uznanym systemem zatwierdzania" wdrożonym na szczeblu krajowym w celu nadzorowania zgodności z przepisami ustanowionymi w dyrektywie 1999/93/WE oraz, o ile to możliwe, z przepisami krajowymi dotyczącymi świadczenia usług certyfikacyjnych (w rozumieniu art. 2 pkt 11 dyrektywy 1999/93/WE). Niektórym obiektom fizycznym lub binarnym (logicznym) wygenerowanym lub wydanym w wyniku świadczenia usług certyfikacyjnych może przysługiwać szczególna „kwalifikacja" na podstawie zgodności tych obiektów z przepisami i wymogami ustanowionymi na szczeblu krajowym, ale znaczenie takiej „kwalifikacji" będzie prawdopodobnie ograniczone tylko do szczebla krajowego.

Interpretacja zaufanej listy

Ogólne wytyczne dotyczące stosowania aplikacji, usług lub produktów wykorzystujących podpis elektroniczny opierających się na wdrożeniu zaufanej listy zgodnie z załącznikiem do decyzji Komisji [odniesienie do niniejszej decyzji] są następujące:

wpis CA/QC „Service type identifier" („Sti") (podobnie, wpis CA/QC kwalifikowany dalej jako „RootCA/QC" poprzez zastosowanie „Service information extension" („Sie") additionalServiceInformation Extension)

— wskazuje, że CA zidentyfikowany przez „Service digital identifier" („Sdi") (podobnie jak w hierarchii CA rozpoczynającej się od RootCA zidentyfikowanego przez „Sdi") od odpowiedniego CSP (zob. powiązane pola informacyjne TSP), wszystkie wystawione certyfikaty wierzchołka ścieżki są certyfikatami kwalifikowanymi, **o ile** są one podawane jako takie poprzez zastosowanie odpowiednich poświadczeń certyfikatów kwalifikowanych określonych w EN 319 412-5 (tzn. QcCompliance, QcSSCD itp..) lub QCP(+) OIDs określonych w EN 319 411-2 (i jest to gwarantowane przez wystawiający CSP oraz zapewniane przez organ nadzoru/akredytacji państwa członkowskiego),

Uwaga: Jeżeli nie ma żadnej informacji „Sie" dotyczącej „rozszerzenia kwalifikacji" lub jeżeli certyfikat wierzchołka ścieżki podawany za certyfikat kwalifikowany nie jest dodatkowo identyfikowany poprzez powiązany wpis „Sie" dotyczący „rozszerzenia kwalifikacji", wówczas poprawność nadających się do przetworzenia maszynowego informacji zawartych w certyfikacie kwalifikowanym podlega nadzorowi/akredytacji. Oznacza to, że zapewnione zostaje, że stosowanie (lub niestosowanie) odpowiednich poświadczeń certyfikatu kwalifikowanego (tzn. poświadczenia QcC i QcSSCD) lub określonych przez ETSI QCP(+) OID jest zgodne z informacjami przedstawianymi przez CSP wystawiający certyfikaty kwalifikowane.

— **i JEŻELI** przedstawiono „Sie" dotyczące „rozszerzenia kwalifikacji", wówczas obok przedstawionej powyżej domyślnej zasady interpretacji stosowania, certyfikaty, które są identyfikowane na podstawie tego wpisu „Sie" dotyczącego „rozszerzenia kwalifikacji" opartego na zasadzie sekwencji filtrów identyfikujących dodatkowo zbiór certyfikatów, należy traktować zgodnie ze zbiorem „kwalifikatorów" przedstawiających pewne dodatkowe informacje dotyczące „obsługi przez SSCD" lub „osoby prawnej jako podmiotu" (np. certyfikaty zawierające szczególny OID w rozszerzeniu polityki certyfikatu, posiadające szczególny wzór „stosowania klucza" lub filtrowane z użyciem szczególnej wartości pojawiającej się w jednym szczególnym polu lub rozszerzeniu certyfikatu itp.). Kwalifikatory te stanowią element następującego zestawu „kwalifikatorów" mających zrekompensować brak informacji w treści odpowiedniego certyfikatu kwalifikowanego, wykorzystywanych odpowiednio do:

— oznaczenia statusu kwalifikowanego: „poświadczenia certyfikatu kwalifikowanego"(QCStatement) oznaczającego, że dany certyfikat kwalifikowany (certyfikaty kwalifikowane) jest (są) kwalifikowany (kwalifikowane),

LUB

— wskazania statusu obsługi przez SSCD:

— wartość kwalifikatora „QCWithSSCD" oznacza „certyfikat kwalifikowany obsługiwany przez SSCD", lub

— wartość kwalifikatora „QCNoSSCD" oznacza „certyfikat kwalifikowany nieobsługiwany przez SSCD", lub

— wartość kwalifikatora „QCSSCDStatusAsInCert" oznacza, że gwarantuje się zamieszczenie informacji o obsłudze przez SSCD w każdym certyfikacie kwalifikowanym w informacjach o „Sdi"-„Sie" zawartych w danym wpisie CA/QC,

LUB

— wskazania, że certyfikat wystawia się osobie prawnej:

— wartość kwalifikatora „QCForLegalPerson" oznacza „certyfikat wystawiony osobie prawnej".

Ogólna reguła interpretacyjna wszelkich innych wpisów rodzaju „Sti" jest taka, że wyszczególnione usługi nazwane stosowanie do wartości w polu „Sn" i identyfikowane w jednoznaczny sposób przez wartość w polu „Sdi" mają aktualny status nadzoru/akredytacji zgodny z wartością w polu „Scs" od daty podanej w polu „Początkowa data i godzina bieżącego statusu". Szczególne reguły interpretacji wszelkich dodatkowych informacji dotyczących wyszczególnionej usługi (np. pole „Service information extensions") można w odpowiednich przypadkach znaleźć w URI właściwego dla danego państwa członkowskiego, jako element obecnego pola „Scheme type/community/rules".

Bliższe informacje na temat pól, opisów i znaczenia dla zaufanych list państw członkowskich można znaleźć w specyfikacji technicznej wspólnego wzoru „Zaufanej listy nadzorowanych/akredytowanych podmiotów świadczących usługi certyfikacyjne" w załączniku do decyzji Komisji 2009/767/WE."

— 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] alpha-2 umieszczany w polu „Scheme territory" (klauzula 5.3.10)

— Gdzie użytkownicy mogą uzyskać dostęp do określonej polityki/zasad przedmiotowego państwa członkowskiego, na podstawie których usługi zawarte na liście MUSZĄ być oceniane zgodnie z odpowiednim systemem nadzoru państwa członkowskiego i systemami dobrowolnej akredytacji.

— Gdzie użytkownicy mogą uzyskać dostęp do określonego opisu przedmiotowego państwa członkowskiego dotyczącego sposobu korzystania z treści zaufanej listy i interpretowania jej w odniesieniu do usług certyfikacyjnych niezwiązanych z wystawianiem certyfikatów kwalifikowanych. Można to wykorzystać do wskazania potencjalnej szczegółowości krajowych systemów nadzoru/akredytacji 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 na podstawie wskazanego powyżej URI właściwego dla państwa członkowskiego (tzn. URI zdefiniowanego na podstawie danego hierarchicznego określonego URI).

TSL policy/legal notice (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 i warunków, na których zaufana lista jest prowadzona i publikowana, MUSI być wielojęzycznym ciągiem znaków (zwykły tekst) składającym się z dwóch części:

1. Pierwszej obowiązkowej części wspólnej dla wszystkich zaufanych list państw członkowskich (w języku angielskim (UK) jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych) wskazującej, że obowiązujące ramy prawne stanowią dyrektywa 1999/93/WE i stosowne akty wdrażające tę dyrektywę w prawodawstwie państwa członkowskiego wskazanego w polu „Scheme Territory".

   Angielska wersja wspólnego tekstu brzmi następująco:

   The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.

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

Oficjalne tłumaczenie powyższego tekstu na język polski brzmi następująco: W odniesieniu do aktualnego wdrożenia TSL zaufanej listy nadzorowanych/akredytowanych podmiotów świadczących usługi certyfikacyjne dla [nazwa odpowiedniego państwa członkowskiego] obowiązujące ramy prawne stanowią dyrektywa 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych oraz wdrażające tę dyrektywę akty prawne [nazwa odpowiedniego państwa członkowskiego].

2. Drugiej fakultatywnej części określonej dla każdej zaufanej listy (w języku angielskim (UK) jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych) wskazującej odniesienia do szczególnych obowiązujących krajowych ram prawnych (np. w szczególności odnoszących się do narodowych systemów nadzoru/akredytacji dotyczących CSP niewystawiających certyfikatów kwalifikowanych).

ROZDZIAŁ II

KONTYNUACJA ZAUFANYCH LIST

Certyfikaty, o których należy zawiadamiać Komisję na mocy art. 3 lit. c) niniejszej decyzji, MUSZĄ być wystawiane w taki sposób, by:

— ich daty ważności dzieliły co najmniej trzy miesiące,

— były tworzone z zastosowaniem nowych par kluczy, ponieważ nie należy ponownie certyfikować uprzednio używanych par kluczy.

W przypadku ujawnienia lub wycofania JEDNEGO z kluczy prywatnych odpowiadających kluczowi publicznego, który może być stosowany do weryfikacji podpisu zaufanej listy, który został zgłoszony Komisji i opublikowany na centralnej liście wskaźników KOMISJI, państwa członkowskie MUSZĄ:

— niezwłocznie wydać nową zaufaną listę podpisaną nieujawnionym kluczem prywatnym, w przypadku gdy wcześniej opublikowana zaufana lista została podpisana ujawnionym lub wycofanym kluczem prywatnym,

— szybko zgłosić Komisji nową listę certyfikatów klucza publicznego odpowiadających kluczom prywatnym, które mogą zostać wykorzystane do podpisania zaufanej listy.

W przypadku ujawnienia lub wycofania WSZYSTKICH prywatnych kluczy odpowiadających kluczom publicznym, który mogą być stosowane do weryfikacji podpisu zaufanej listy, które zostały zgłoszone Komisji i opublikowane na centralnej liście wskaźników KOMISJI, państwa członkowskie MUSZĄ:

— wygenerować nowe pary kluczy, które mogą zostać wykorzystane do podpisania zaufanej listy, i odpowiadające im certyfikaty klucza publicznego,

— niezwłocznie wydać nową zaufaną listę podpisaną jednym z tych nowych kluczy prywatnych, których odpowiedni certyfikat klucza publicznego należy zgłosić,

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

ROZDZIAŁ III

SPECYFIKACJE FORMY ZAUFANEJ LISTY CZYTELNEJ DLA CZŁOWIEKA

Jeżeli ustanowiono i opublikowano zaufaną listę w formie czytelnej dla człowieka, POWINNA ona być udostępniona w postaci dokumentu w formacie PDF zgodnie z ISO 32000 [1], a dokument ten MUSI być sformatowany zgodnie z profilem PDF/A (ISO 19005 [2]).

Zawartość opartej na pliku PDF/A czytelnej dla człowieka formy zaufanej listy POWINNA spełniać następujące wymogi:

— struktura czytelnej dla człowieka formy POWINNA odzwierciedlać model logiczny opisany w TS 119 612,

— każde pole POWINNO być widoczne i POWINNO zawierać:

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

  — wartość pola (np. „CA/QC"),

  — w odpowiednich przypadkach znaczenie (opis) wartości tego pola („np. urząd certyfikacji wystawiający certyfikaty kluczy publicznych"),

  — w stosownych przypadkach wiele wersji języków naturalnych zgodnie z zawartością zaufanej listy,

[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).

— co najmniej następujące pola i odpowiadające im wartości certyfikatów cyfrowych występujące w polu „Service digital identity" POWINNY być przedstawione w formie czytelnej dla człowieka:

  — wersja

  — serial number (numer seryjny)

  — algorytm podpisu

  — wystawca

  — ważny od

  — ważny do

  — Podmiot

  — klucz publiczny

  — polityka certyfikacji

  — identyfikator klucza podmiotu

  — punkty dystrybucji CRL

  — identyfikator klucza urzędu

  — użycie klucza

  — podstawowe warunki ograniczające

  — algorytm odcisku palca

  — odcisk palca

— forma czytelna dla człowieka POWINNA być łatwa do wydrukowania,

— forma czytelna dla człowieka musi zostać podpisana przez operatora systemy zgodnie z podstawowym profilem PAdES Signatures ([1]).

([1]) ETSI TS 103 172 (March 2012) – Electronic Signatures and Infrastructures (ESI); PAdES Baseline Profile.