**Dokument ten służy wyłącznie do celów dokumentacyjnych i instytucje nie ponoszą żadnej odpowiedzialności za jego zawartość**

►**B** ►**C1** **DECYZJA KOMISJI**

**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**

*(notyfikowana jako dokument nr C(2009) 7806)*

**(Tekst mający znaczenie dla EOG)**

(2009/767/WE) ◄

(Dz.U. L 274 z 20.10.2009, s. 36)

zmieniona przez:

| | | Dziennik Urzędowy | | |
|---|---|---|---|---|
| | | nr | strona | data |
| ►**M1** | Decyzja Komisji 2010/425/UE z dnia 28 lipca 2010 r. | L 199 | 30 | 31.7.2010 |
| ►**M2** | Rozporządzenie Komisji (UE) nr 519/2013 z dnia 21 lutego 2013 r. | L 158 | 74 | 10.6.2013 |

sprostowane przez:

►**C1** Sprostowanie, Dz.U. L 299 z 14.11.2009, s. 18 (2009/767/WE)
►**C2** Sprostowanie, Dz.U. L 4 z 7.1.2011, s. 6 (2009/767/WE)

▼B
▼C1

# DECYZJA KOMISJI

**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**

*(notyfikowana jako dokument nr C(2009) 7806)*

**(Tekst mający znaczenie dla EOG)**

(2009/767/WE)

KOMISJA WSPÓLNOT EUROPEJSKICH,

uwzględniając Traktat ustanawiający Wspólnotę Europejską,

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

a także mając na uwadze, co następuje:

(1) Obowiązki uproszczenia procedur administracyjnych nałożone na państwa członkowskie w rozdziale II dyrektywy 2006/123/WE, w szczególności w jej art. 5 i 8, obejmują obowiązek uproszczenia procedur i formalności mających zastosowanie do podejmowania i prowadzenia działalności usługowej oraz obowiązek dopilnowania, aby te procedury i formalności były łatwe do dopełnienia przez usługodawców na odległość oraz drogą elektroniczną poprzez „pojedyncze punkty kontaktowe”.

(2) Zgodnie z art. 8 dyrektywy 2006/123/WE dopełnianie procedur i formalności poprzez „pojedyncze punkty kontaktowe” musi być możliwe transgranicznie między państwami członkowskimi.

(3) W celu spełnienia obowiązku dotyczącego uproszczenia procedur i formalności oraz ułatwienia transgranicznego korzystania z „pojedynczych punktów kontaktowych” procedury realizowane drogą elektroniczną powinny opierać się na prostych rozwiązaniach, również w odniesieniu do podpisów elektronicznych. W przypadkach, w których po przeprowadzeniu odpowiedniej oceny ryzyka konkretnych procedur i formalności uznaje się, że niezbędny jest wysoki poziom bezpieczeństwa lub równoważność z podpisem odręcznym, w odniesieniu do niektórych procedur i formalności od usługodawców można wymagać zastosowania zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie i składanego za pomocą bezpiecznego urządzenia służącego do składania podpisów lub bez takiego urządzenia.

([1]) Dz.U. L 376 z 27.12.2006, s. 36.

▼C1

(4) Wspólnotowe ramy w zakresie podpisu elektronicznego zostały ustanowione w dyrektywie 1999/93/WE Parlamentu Europejskiego i Rady z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych ([1]). W celu ułatwienia skutecznego transgranicznego wykorzystywania zaawansowanych podpisów elektronicznych opartych na kwalifikowanym certyfikacie należy zwiększyć zaufanie do podpisów elektronicznych niezależnie od tego, w którym państwie członkowskim znajduje się siedziba podpisującego lub podmiotu świadczącego usługi certyfikacyjne, który wystawia certyfikat kwalifikowany. Można to osiągnąć, ułatwiając dostęp do przedstawionych w wiarygodnej formie informacji niezbędnych do weryfikacji podpisów elektronicznych, w szczególności do informacji dotyczących podmiotów świadczących usługi certyfikacyjne, nadzorowanych/akredytowanych przez państwo członkowskie oraz do informacji dotyczących usług przez te podmioty świadczonych.

(5) Należy zapewnić upublicznienie tych informacji przez państwa członkowskie przy użyciu wspólnego wzoru w celu ułatwienia korzystania z tych informacji oraz zapewnienia właściwego poziomu szczegółowości pozwalającego stronie odbierającej na zweryfikowanie podpisu elektronicznego,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

*Artykuł 1*

**Stosowanie i akceptacja podpisów elektronicznych**

1. Jeżeli jest to uzasadnione na podstawie odpowiedniej oceny ryzyka i zgodne z art. 5 ust. 1 i 3 dyrektywy 2006/123/WE, państwa członkowskie mogą wymagać od usługodawcy, w celu dopełnienia pewnych procedur i formalności poprzez pojedyncze punkty kontaktowe zgodnie z art. 8 dyrektywy 2006/123/WE, zastosowania zaawansowanego podpisu elektronicznego opartego na kwalifikowanym certyfikacie i składanego za pomocą bezpiecznego urządzenia służącego do składania podpisów lub bez takiego urządzenia, jak zostało to zdefiniowane i uregulowane w dyrektywie 1999/93/WE.

2. Państwa członkowskie akceptują każdy zaawansowany podpis elektroniczny oparty na kwalifikowanym certyfikacie i składany za pomocą bezpiecznego urządzenia służącego do składania podpisów lub bez takiego urządzenia stosowany przy dopełnianiu procedur i formalności, o których mowa w ust. 1, bez uszczerbku dla przysługującej państwom członkowskim możliwości ograniczenia tej akceptacji do zaawansowanych podpisów elektronicznych opartych na kwalifikowanym certyfikacie i składanych za pomocą bezpiecznego urządzenia służącego do składania podpisów, jeżeli jest to zgodne z oceną ryzyka, o której mowa w ust. 1.

3. Państwa członkowskie nie uzależniają akceptacji zaawansowanych podpisów elektronicznych opartych na kwalifikowanym certyfikacie i składanych za pomocą bezpiecznego urządzenia służącego do składania podpisów lub bez takiego urządzenie, od spełnienia wymogów, które stwarzają przeszkody w korzystaniu przez usługodawców z procedur realizowanych drogą elektroniczną poprzez pojedyncze punkty kontaktowe.

([1]) Dz.U. L 13 z 19.1.2000, s. 12.

▼C1

4. Ust. 2 nie uniemożliwia państwom członkowskim akceptowania podpisów elektronicznych niebędących zaawansowanymi podpisami elektronicznymi opartymi na kwalifikowanym certyfikacie składanymi za pomocą bezpiecznego urządzenia służącego do składania podpisów lub bez takiego urządzenia.

*Artykuł 2*

**Tworzenie, prowadzenie i publikowanie zaufanych list**

1. Każde państwo członkowskie tworzy, prowadzi i publikuje, zgodnie ze specyfikacją techniczną określoną w załączniku, „zaufaną listę" zawierającą minimum informacji dotyczących nadzorowanych/akredytowanych przez to państwo członkowskie podmiotów świadczących usługi certyfikacyjne i powszechnie wystawiających kwalifikowane certyfikaty.

▼M1

2. Państwa członkowskie tworzą i publikują zaufaną listę zarówno w postaci czytelnej dla człowieka, jak i w wersji przetwarzalnej maszynowo, zgodnie ze specyfikacją określoną w załączniku.

2a. Państwa członkowskie podpisują elektronicznie swoją zaufaną listę w wersji przetwarzalnej maszynowo i, jako minimum, publikują za pomocą bezpiecznego kanału zaufaną listę w postaci czytelnej dla człowieka w celu zapewnienia jej autentyczności oraz integralności.

3. Państwa członkowskie przekazują Komisji informacje o:

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

b) miejscach, w których zaufana lista w postaci czytelnej dla człowieka i w postaci przetwarzalnej maszynowo została opublikowana;

c) certyfikacie klucza publicznego zastosowanym do wdrożenia bezpiecznego kanału, przez który publikuje się zaufaną listę w postaci czytelnej dla człowieka, lub, jeżeli lista w postaci czytelnej dla człowieka jest podpisana elektronicznie, certyfikacie klucza publicznego zastosowanym do jej podpisania;

d) certyfikacie klucza publicznego zastosowanym do elektronicznego podpisania zaufanej listy w postaci przetwarzalnej maszynowo;

e) wszelkich zmianach w informacjach zawartych w lit. a)–d).

4. Komisja udostępnia wszystkim państwom członkowskim przez bezpieczny kanał do uwierzytelnionego serwera internetowego przekazane przez państwa członkowskie informacje, o których mowa w ust. 3, zarówno w postaci czytelnej dla człowieka, jak i w podpisanej postaci przetwarzalnej maszynowo.

▼C1

*Artykuł 3*

**Stosowanie**

Niniejszą decyzję stosuje się od dnia 28 grudnia 2009 r.

*Artykuł 4*

**Adresaci**

Niniejsza decyzja skierowana jest do państw członkowskich.

▼C1

*ZAŁĄCZNIK*

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

PRZEDMOWA

1. **Kontekst ogólny**

Wspólny dla państw członkowskich wzór „Zaufanej listy nadzorowanych/akredytowanych podmiotów świadczących usługi certyfikacyjne” ma na celu stworzenie wspólnego sposobu udostępniania przez każde państwo członkowskie informacji dotyczących statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne (ang. *Certification Sernice Providers*, CSP) ([1]), które są przez nie nadzorowane/akredytowane pod względem zgodności z odpowiednimi przepisami dyrektywy 1999/93/WE. Obejmuje to także przepisy dotyczące informacji historycznych o statusie nadzoru/akredytacji nadzorowanych/akredytowanych usług certyfikacyjnych.

Obowiązkowe informacje na zaufanej liście (ang. *Trusted List*, TL) muszą zawierać minimum informacji o nadzorowanych/akredytowanych podmiotach świadczących usługi certyfikacyjne wystawiających certyfikaty kwalifikowane (ang. *Qualified Certificates*, QC) ([2]) zgodnie z przepisami dyrektywy 1999/93/WE (art. 3 ust. 3, art. 3 ust. 2 i art. 7 ust. 1 lit. a)), w tym informacje dotyczące certyfikatu kwalifikowanego, na którym opiera się podpis elektroniczny i dotyczące tego, czy podpis jest składany za pomocą bezpiecznego urządzenia służącego do składania podpisu (ang. *Secure Signature Creation Device*, SSCD) czy bez niego ([3]).

Dodatkowe informacje dotyczące innych nadzorowanych/akredytowanych CSP niewystawiających QC, 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.

Przedmiotowe informacje służą głównie wspomaganiu weryfikacji kwalifikowanych podpisów elektronicznych (ang. *Qualified Electronic Signatures*, QES) i zaawansowanych podpisów elektronicznych (ang. *Advanced Electronic Signatures*, AdES) ([4]) opierających się na certyfikacie kwalifikowanym ([5]) ([6]).

Zaproponowany wspólny wzór jest zgodny z wdrażaniem opartym na specyfikacji określonej w ETSI TS 102 231 ([7]), którą wykorzystuje się w odniesieniu do tworzenia, publikowania, umiejscowienia, dostępu, ustalenia autentyczności i zaufania do tego rodzaju wykazów.

([1]) Zgodnie z definicją zawartą w art. 2 ust. 11 dyrektywy 1999/93/WE.
([2]) Zgodnie z definicją zawartą w art. 2 ust. 10 dyrektywy 1999/93/WE.
([3]) Zgodnie z definicją zawartą w art. 2 ust. 6 dyrektywy 1999/93/WE.
([4]) Zgodnie z definicją zawartą w art. 2 ust. 2 dyrektywy 1999/93/WE.
([5]) W niniejszym dokumencie akronim „$AdES_{QC}$” jest stosowany w odniesieniu do zaawansowanego podpisu elektronicznego opartego na certyfikacie kwalifikowanym.
([6]) 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 dotyczącej dobrowolnie udzielanych informacji.
([7]) ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

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

2.1. *Zaufana lista dotycząca nadzorowanych/akredytowanych usług certyfikacyjnych*

Odpowiednie usługi certyfikacyjne i podmioty świadczące usługi certyfikacyjne znajdujące się na jednej liście

Zaufaną listę państwa członkowskiego określa się jako „wykaz statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne nadzorowane/akredytowane przez przedmiotowe państwo członkowskie pod względem zgodności z odnośnymi przepisami dyrektywy 1999/93/WE".

Taka zaufana lista musi obejmować:

— wszystkie podmioty świadczące usługi certyfikacyjne zdefiniowane w art. 2 ust. 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 ze względu na zgodność z odnośnymi przepisami określonymi w dyrektywie 1999/93/WE.

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

— **CSP wystawiające QC:**

  — Muszą być nadzorowane przez państwo członkowskie, w którym mają siedzibę lub miejsce zamieszkania (jeżeli mają siedzibę lub miejsce zamieszkania w państwie członkowskim) i mogą być także akredytowane pod względem zgodności z przepisami dyrektywy 1999/93/WE, w tym z wymogami z załącznika I (wymogi dotyczące QC) i z załącznika II (wymogi dotyczące CSP wystawiających QC). CSP wystawiające QC, które są akredytowane w państwie członkowskim, muszą także podlegać właściwemu systemowi nadzoru tego państwa członkowskiego, chyba że nie mają siedziby lub miejsca zamieszkania 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 zawarte w art. 3 ust. 3, art. 8 ust. 1, art. 11, w motywie 13 (odpowiednio w art. 2 ust. 13, art. 3 ust. 2, art. 7 ust. 1 lit. a), art. 8 ust. 1, art. 11, w motywach 4, 11–13).

— **CSP niewystawiające QC:**

  — Podmioty te mogą zostać objęte systemem „dobrowolnej akredytacji" (zgodnie z przepisami dyrektywy 1999/93/WE) lub określonym w prawie krajowym „przyjętym 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 ust. 11 dyrektywy).

  — 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 określonymi na szczeblu krajowym, ale znaczenie takiej „kwalifikacji" będzie prawdopodobnie ograniczone tylko do szczebla krajowego.

▼C1

Zaufana lista państwa członkowskiego musi zawierać minimum informacji o nadzorowanych/akredytowanych CSP powszechnie wystawiających QC zgodnie z przepisami dyrektywy 1999/93/WE (art. 3 ust. 3, art. 3 ust. 2 i art. 7 ust. 1 lit. a), informacje dotyczące QC, na którym opiera się podpis elektroniczny i określające, czy podpis jest składany za pomocą bezpiecznego urządzenia służącego do składania podpisu czy bez niego.

Dodatkowe informacje dotyczące innych nadzorowanych/akredytowanych usług świadczonych przez CSP niewystawiające powszechnie QC (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.

Zaufana lista służy:

— wymienieniu i przedstawieniu wiarygodnych informacji dotyczących statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne nadzorowane/akredytowane przez przedmiotowe państwo członkowskie odpowiedzialne za stworzenie i prowadzenie listy mającej na celu zapewnienie zgodności z odpowiednimi przepisami dyrektywy 1999/93/WE,

— ułatwieniu weryfikacji podpisów elektronicznych opierających się na wymienionych nadzorowanych/akredytowanych usługach certyfikacyjnych świadczonych przez wymienione CSP.

Pojedynczy zbiór wartości statusu nadzoru/akredytacji

Dla każdego państwa członkowskiego należy utworzyć i prowadzić jedną TL wskazującą status nadzoru lub akredytacji usług certyfikacyjnych świadczonych przez te CSP, które są nadzorowane/akredytowane przez to państwo członkowskie.

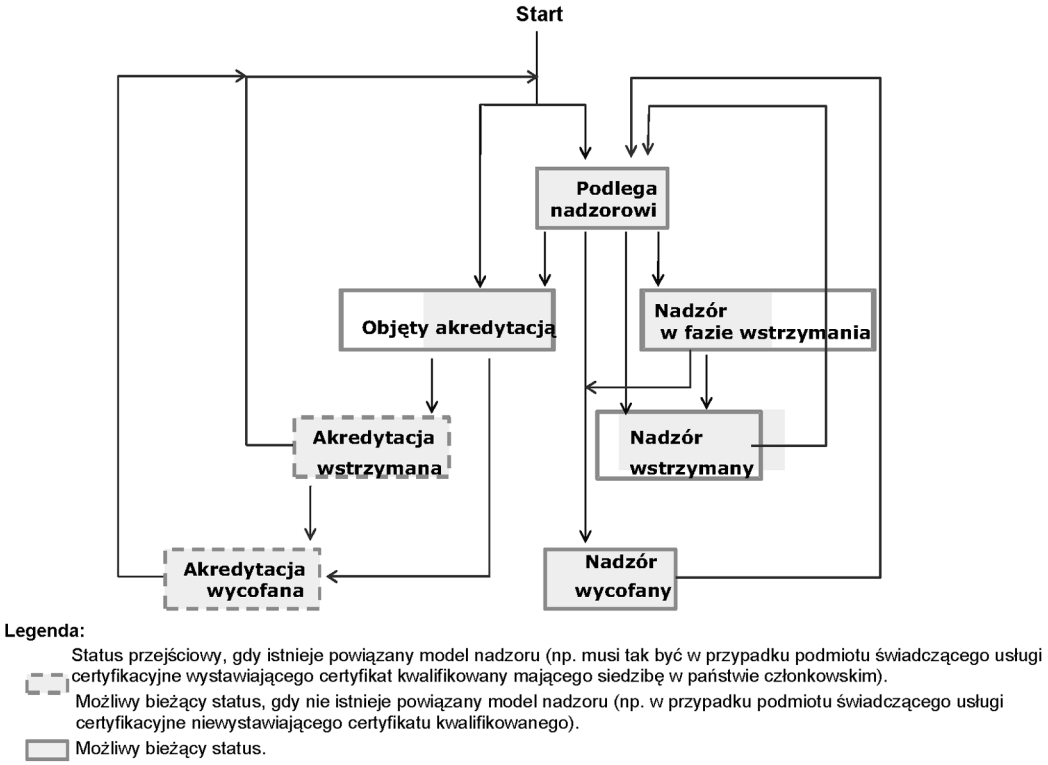
Fakt, że usługa podlega aktualnie nadzorowi lub akredytacji stanowi część jej bieżącego statusu. Ponadto status nadzoru lub akredytacji można oznaczyć jako „dostępny", „w fazie wstrzymania", „wstrzymany" lub nawet „wycofany". Przez cały okres świadczenia usługi certyfikacyjnej jej status może się zmieniać 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 przeniesieniu dobrowolnej akredytacji na aktualnie nadzorowaną usługę certyfikacyjną. Z drugiej strony podmiot świadczący usługi certyfikacyjne w innym państwie członkowskim może zadecydować nie o przerywaniu świadczenia akredytowanej usługi certyfikacyjnej, ale o zmianie jej statusu z akredytowanej na nadzorowaną, np. ze względów biznesowych lub gospodarczych.

▼C1

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




*Schemat 1*

Podmiot certyfikacyjny wystawiający QC musi podlegać nadzorowi (jeżeli ma siedzibę w państwie członkowskim) i może być objęty dobrowolna akredytacją. Gdy podmiot jest wymieniony na zaufanej liście wartość jego statusu może przyjmować dowolną wskazaną powyżej wartość statusu określaną jako „bieżącaa wartość statusu". Należy jednak zauważyć, że „akredytacja wstrzymana" i „akredytacja wycofana" muszą stanowić wartości „statusu przejściowego" tylko w odniesieniu do usług $CSP_{QC}$, które mają siedzibę lub miejsce zamieszkania w państwie członkowskim, ponieważ takie usługi podlegają nadzorowi w sposób domyślny (nawet, jeżeli nie mają akredytacji lub jeżeli akredytacja wygasła).

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 QC z przepisami dyrektywy 1999/93/WE oraz z ewentualnymi przepisami krajowymi dotyczącymi świadczenia usług certyfikacyjnych (w rozumieniu art. 2 ust. 11 dyrektywy), zaklasyfikowały taki system (takie systemy) zatwierdzania do jednej z dwóch wskazanych poniżej kategorii:

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

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

▼C1

Zatem podmiot certyfikacyjny niewydający QC może podlegać nadzorowi lub być objęty dobrowolną akredytacją. Gdy taki podmiot jest wymieniony na zaufanej liście, wartość jego statusu może przyjmować dowolną wskazaną powyżej wartość statusu określaną jako „aktualna wartość statusu" (zob. schemat 1).

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 „dobrowolnych akredytacji" mającego zastosowanie do każdego $CSP_{QC}$,

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

— w stosownych przypadkach informacje dotyczące krajowego systemu „dobrowolnych akredytacji" mającego zastosowanie do każdego CSP niewystawiającego QC.

Dwa ostatnie zbiory informacji mają istotne 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 QS. Jeżeli TL zawiera informacje dotyczące statusu nadzoru/akredytacji w odniesieniu do usług świadczonych przez CSP niewystawiające QC, wymienione wcześniej zbiory informacji są udostępniane na TL 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 QC 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 5.8.2) jako części „Service information extension" (klauzula 5.5.9). Dodatkowe 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 (identyfikowany na podstawie „Service digital identity", tak jak w ETSI TS 102 231 ([1]) i że status nadzoru/akredytacji tej usługi będzie odpowiednio aktualizowany. Znaczenie statusów wskazanych powyżej jest opisane w powiązanej klauzuli 5.5.4 szczegółowych specyfikacji technicznych w rozdz. I.

2.2. *Wpisy na TL mające na celu ułatwienie weryfikacji QES i AdESQC*

Najważniejszym etapem tworzenia TL jest przygotowanie części obowiązkowej TL, a mianowicie „Listy usług" w podziale na CSP wystawiające QC, co ma na celu poprawne odzwierciedlenie rzeczywistej sytuacji każdego podmiotu wystawiającego QC 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).

([1]) ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information.

▼C1

Dopóki nie istnieje w pełni interoperacyjny i transgraniczny profil QC, wymagane informacje mogą zawierać inne informacje niż „Service digital identity" pojedynczego (głównego) urzędu certyfikacji (ang. *Certification Authority*, CA), w szczególności informacje określające status QC wydanego certyfikatu oraz czy podpisy opierające się na certyfikatach są składane za pomocą SSCD. Dlatego też organ wyznaczony w państwie członkowskim do utworzenia, redagowania i prowadzenia TL (tzn. operator systemu określony w ETSI TS 102231) musi uwzględnić aktualny profil i treść każdego wystawionego QC w odniesieniu do $CSP_{QC}$ wymienionych na TL.

Najlepiej byłoby, gdyby każdy wystawiony QC zawierał określone przez ETSI poświadczenie zgodności certyfikatu kwalifikowanego (ang. *QcCompliance statement*) ([1]), jeżeli twierdzi się, że jest to QC, 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 QC zawiera jeden z identyfikatorów obiektów (OID) polityk certyfikatów QCP/QCP + określonych w ETSI TS 101 456 ([2]). Stosowanie przez CSP wystawiające QC 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 QC (np. stosowanie lub nie stosowanie 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, na którym opiera się podpis elektroniczny, jest QC, czy nie, oraz czy jest powiązany z SSCD, przy pomocy którego złożono podpis, czy nie.

Uzupełnienie pól „Service type identifier" („Sti"), „Service name" („Sn") i „Service digital identity" („Sdi") ([3]) informacjami podanymi w polu „Service information extensions" („Sie") umożliwia pełne określenie w zaproponowanym wspólnym wzorze TL szczególnego rodzaju certyfikatu kwalifikowanego wystawionego przez CSP wymieniony w liście i wystawiający QC oraz poinformowanie, czy dany certyfikat kwalifikowany został wystawiony za pomocą SSCD, czy nie (jeżeli wystawiony QC nie zawiera takiej informacji). Z wpisem tym oczywiście powiązana jest szczególna 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 QC oraz organu ds. nadzoru/akredytacji kierującego nadzorem/akredytacją 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 QC czy nie, oraz czy został wystawiony za pomocą SSCD, czy nie. Przykładowo w przypadku gdy drugie z tych twierdzeń jest fałszywe (np. na QC nie ma znormalizowanego przez ETSI oznaczenia nadającego się do przetwarzania maszynowego świadczącego o tym, że ten certyfikat został wystawiony za pomocą SSCD), wówczas poprzez podanie w liście tylko „Sdi" (głównego) CA można tylko przyjąć, że QC wystawione zgodnie z hierarchią tego (głównego) CA nie zostały wystawione za pomocą SSCD. W celu uznania tych QC za wystawione za pomocą SSCD stosuje się „Sie" („Sie" wskazuje także, że fakt wystawienia za pomocą danego urządzenia jest gwarantowany przez CSP wystawiający QC oraz nadzorowany/akredytowany odpowiednio przez organ ds. nadzoru lub akredytacji).

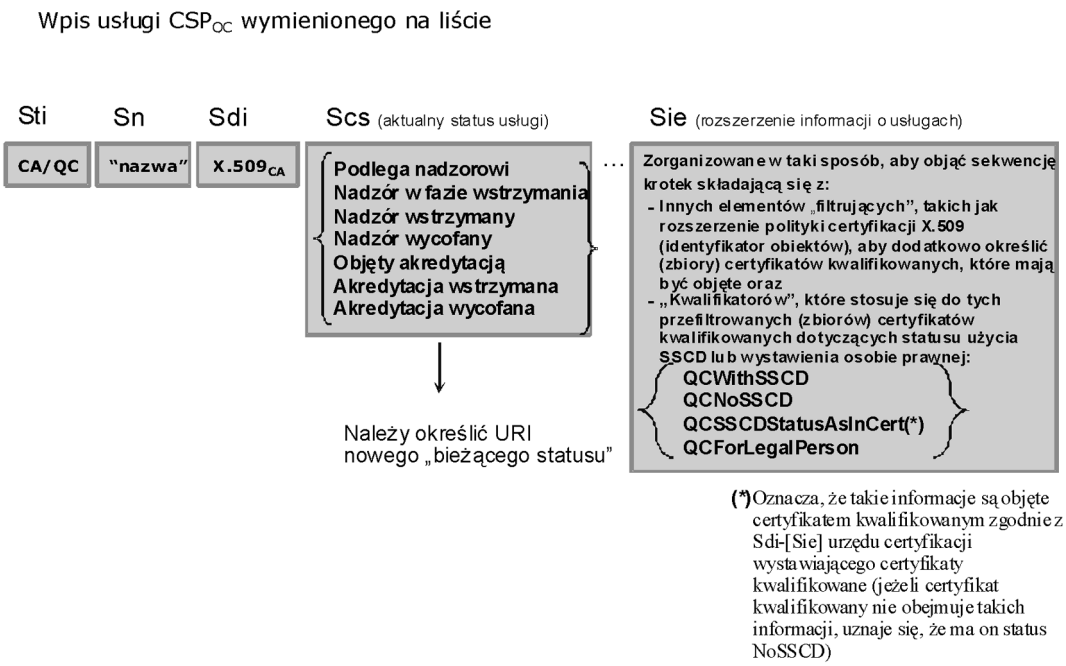
([1]) Zob. ETSI TS 101 862 – Electronic Signatures and Infrastructures (ESI): Qualified Certificate Profile.

([2]) ETSI TS 101 456 – Electronic Signature and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates.

([3]) Tzn. jako minimum certyfikat X.509 v3 urzędu certyfikacji wystawiającego certyfikaty kwalifikowane lub urzędu certyfikacji wyższego szczebla na ścieżce certyfikacji.

▼C1

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




*Schemat 2*

**Wpis usługi CSP wystawiającego QC wymienionego na liście wykonany w formacie listy statusu usług zaufania (ang. *Trust-service Status List*, TSL)**

Niniejsza specyfikacja techniczna wspólnego wzoru TL dopuszcza stosowanie we wpisie usługi kombinacji pięciu głównych części informacji:

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

— „Service name" („Sn"),

— informacji o „Service digital identity" („Sdi") identyfikującej wymienioną usługę np. certyfikat X.509v3 (jako minimum) należący do CA wystawiającego QC,

— w przypadku usług CA/QC fakultatywne informacje o „Service information extensions" („Sie"), które dopuszczają włączenie 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 identyfikacji użycia SSCD (lub wystawienia na rzecz osoby prawnej), oraz

  — informacje towarzyszące („kwalifikatory") dotyczące tego, czy ta dodatkowo zidentyfikowana usługa złożona z certyfikatów kwalifikowanych była świadczona za pomocą SSCD, czy nie, lub czy przedmiotowe informacje towarzyszące stanowią część QC zgodnie ze znormalizowaną formą nadającą się do przetwarzania maszynowego lub informacji dotyczących tego, że takie QC wystawia się osobom prawnym (domyślnie uznaje się je za wystawione tylko osobom fizycznym),

▼C1

— informacji o „bieżącym statusie” dla danego wpisu usługi, zawierających informacje:

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

— o statusie nadzoru/akredytacji.

2.3. *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 QC obsługiwany przez SSCD zawiera poświadczenie zgodności certyfikatu kwalifikowanego określone przez ETSI (poświadczenie 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 użycia 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 QC nieobsługiwany przez SSCD zawiera poświadczenie QcCompliance lub QCP OID i nie musi zawierać poświadczenia QcSSCD lub QCP + OID, wówczas wystarczy użyć odpowiedniej „Sdi”, a pole „Sie” można stosować fakultatywnie i nie musi ono zawierać informacji na temat użycia SSCD (co oznacza, że certyfikat nie jest składany za pomocą 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 QC zawiera poświadczenie QcCompliance, a niektóre z tych QC są przeznaczone do obsługiwania przez SSCD, zaś inne nie są (np. rozróżnienia można dokonać na podstawie różnych szczególnych OID polityki certyfikacyjnej CSP lub na podstawie innych szczególnych informacji na temat CSP zawartych na QC, bezpośrednio lub pośrednio, w sposób nadający się do przetworzenia maszynowego lub nie), ale NIE zawiera poświadczenia QcSSCD ANI QCP(+) OID określonego przez ETSI, wówczas zastosowanie odpowiedniej „Sdi” może nie być wystarczające, a pole „Sie” musi być zastosowane w celu wskazania wyraźnych informacji pomocniczych dotyczących SSCD wraz z potencjalnym rozszerzeniem informacji mających na celu zidentyfikowanie przedmiotowego zbioru certyfikatów. Przy wypełnianiu pola „Sie” może pojawić się potrzeba włączenia do tej samej „Sdi” różnych „wartości informacji pomocniczych dotyczących 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 QC nie zawiera poświadczenia QcCompliance, QCP OID, poświadczenia QcSSCD ani QCP + OID, ale zagwarantowano, że niektóre z tych certyfikatów wierzchołka ścieżki wystawionych zgodnie z „Sdi” są QC lub są obsługiwane za pomocą SSCD, a inne nie (np. rozróżnienia można dokonać na podstawie różnych szczególnych OID polityki certyfikacyjnej $CSP_{QC}$ lub na podstawie innych szczególnych informacji na temat $CSP_{QC}$ zawartych w QC, bezpośrednio lub pośrednio, w sposób nadający się do przetworzenia maszynowego lub nie), wówczas zastosowanie odpowiedniej „Sdi” nie będzie wystarczające, a w polu „Sie” należy umieścić wyraźne informacje dotyczące użycia SSCD. Przy wypełnianiu pola „Sie” może pojawić się potrzeba włączenia do tej samej „Sdi” różnych „wartości informacji pomocniczych dotyczących SSCD”.

▼C1

Zgodnie z ogólną zasadą domyślności w odniesieniu do CSP wymienionego na zaufanej liście musi istnieć jeden wpis usługi dla pojedynczego certyfikatu X.509v3 dotyczącego usługi certyfikacyjnej typu CA/QC tzn. urzędu certyfikacji (bezpośrednio) wystawiającego certyfikaty kwalifikowane. W niektórych starannie przewidzianych okolicznościach i starannie zarządzanych warunkach organ ds. nadzoru/organ ds. akredytacji państwa członkowskiego może zadecydować o wykorzystaniu certyfikatu X.509v3 głównego urzędu certyfikacji lub urzędu certyfikacji wyższego szczebla (tzn. urzędu certyfikacji niewystawiającego bezpośrednio certyfikatów kwalifikowanych wierzchołka ścieżki, ale certyfikujących hierarchię urzędów certyfikacji, łącznie z urzędami certyfikacji wystawiającymi certyfikaty kwalifikowane wierzchołka ścieżki) jako „Sdi" pojedynczego wpisu na wykazie usług świadczonych przez CSP wymienione na liście. Konsekwencje (wady i zalety) stosowania certyfikatu X.509v3 głównego urzędu certyfikacji lub urzędu certyfikacji wyższego szczebla jako wartości „Sdi" wpisów usług w TL muszą być dokładnie rozważone i zatwierdzone przez państwa członkowskie. Ponadto jeżeli państwo członkowskie stosuje dopuszczalne wyjątki od zasady domyślnej, musi ono przedstawić niezbędne dokumenty ułatwiające tworzenie i weryfikację ścieżki certyfikatu.

W celu zobrazowania ogólnych wytycznych dotyczących edycji można posłużyć się następującym przykładem: W odniesieniu do $CSP_{QC}$ z wykorzystaniem jednego głównego urzędu certyfikacji, w powiązaniu z którym kilka urzędów certyfikacji wystawia QC i non-OC (certyfikaty niekwalifikowane), ale w odniesieniu do których QC zawierają tylko poświadczenie QcCompliance i nie zawierają oznaczenia, czy zostały one wystawione za pomocą SSCD, wymienienie na wykazie tylko „Sdi" urzędu certyfikacji zgodnie z zasadami wyjaśnionymi powyżej oznaczałoby, że żaden QC wystawiony w ramach hierarchii głównego urzędu certyfikacji NIE jest obsługiwany za pomocą SSCD. Jeżeli te QC są obsługiwane za pomocą SSCD, zdecydowanie zaleca się stosowanie poświadczenia QcSSCD w odniesieniu do QC wystawianych w przyszłości. W międzyczasie (do czasu wygaśnięcia ostatniego QC nie zawierającego takich informacji) TSL powinna wykorzystywać pole „Sie" i towarzyszące rozszerzenie „kwalifikacje" np. filtrując certyfikaty z użyciem szczególnego (szczególnych) OID określonych przez $CSP_{QC}$, stosowanego (stosowanych) potencjalnie przez $CSP_{QC}$ do rozróżnienia różnych rodzajów QC (jedne obsługiwane za pomocą SSCD, a inne nie) i zawierającego (zawierających) wyraźne „informacje pomocnicze na temat SSCD" w odniesieniu do przedmiotowych certyfikatów filtrowanych z użyciem „kwalifikatorów".

**Ogólne wytyczne dotyczące stosowania** aplikacji podpisu elektronicznego, usług lub produktów opierających się na wdrożeniu TSL zaufanej listy zgodnie z aktualnymi specyfikacjami technicznymi są następujące:

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

— 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 poświadczeń certyfikatu kwalifikowanego (tzn. poświadczeń QcC i QcSSCD) lub określonych przez ETSI QCP(+) OID (jest to gwarantowane przez organ ds. nadzoru/akredytacji, zob. wyżej „ogólne wytyczne dotyczące edycji").

*Uwaga:* jeżeli nie ma żadnej informacji „Sie" dotyczącej „kwalifikacji" lub jeżeli certyfikat wierzchołka ścieżki uznawany za QC nie jest „dodatkowo identyfikowany" poprzez wpis „Sie", wówczas poprawność „nadających się do przetworzenia maszynowego" informacji zawartych w QC podlega nadzorowi/akredytacji. Oznacza to, że zagwarantowane jest stosowanie (lub niestosowanie) odpowiednich poświadczeń certyfikatu kwalifikowanego (tzn. poświadczenia QcC i QcSSCD) lub określonych przez ETSI QCP(+) OID jest zgodne z informacjami przedstawianymi przez $CSP_{QC}$,

▼C1

— **i JEŻELI** przedstawiono „Sie” dotyczące „kwalifikacji”, wówczas jako dodatek do przedstawionej powyżej zasady interpretacji domyślnego stosowania certyfikaty, które są identyfikowane na podstawie tego wpisu „Sie” dotyczącego „kwalifikacji” zbudowanego na zasadzie sekwencji „filtrów” identyfikujących dodatkowo zbiór certyfikatów i 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.), należy rozważyć zgodnie z następującym zbiorem „kwalifikatorów”, które kompensują brak informacji w odpowiednim QC, tzn.:

— w celu wskazania obsługi przez SSCD:

  — wartość kwalifikatora „QCWithSSCD” oznaczająca „QC wystawiony za pomocą SSCD”, lub

  — wartość kwalifikatora „QCNoSSCD” oznaczająca „QC nieobsługiwany przez SSCD”, lub

  — wartość kwalifikatora „QCSSCDStatusAsInCert” oznaczająca, że gwarantuje się, że informacje dotyczące użycia SSCD zostaną zawarte w każdym QC zgodnie z „Sdi”–„Sie” przedstawionymi w tym wpisie CA/QC,

  LUB

— w celu wskazania, że certyfikat wystawia się osobie prawnej:

  — wartość kwalifikatora „QCForLegalPerson” oznaczająca „Certyfikat wystawiono osobie prawnej”.

2.4. *Usługi obsługujące usługi CA/QC, ale niestanowiące części „Sdi” CA/QC*

Należy także uwzględnić przypadki, w których CRL i OCSP zostały podpisane z użyciem kluczy nienależących do CA wystawiającego QC. Można je uwzględnić wymieniając te usługi jako takie w TSL wdrażającej TL (tzn. z „Service type identifier” dodatkowo zakwalifikowanym przez rozszerzenie „additionalServiceInformation” odzwierciedlające OCSP lub usługę CRL jako część wystawiania QC, np. z rodzajem usługi odpowiednio „OCSP/QC” lub „CRL/QC”), ponieważ te usługi można uznać za część „kwalifikowanych” usług nadzoru/akredytacji związanych ze świadczeniem usług certyfikacyjnych polegających na wystawianiu certyfikatów kwalifikowanych. Niewątpliwie certyfikaty podmiotów udzielających odpowiedzi na 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.

Podobne przepisy można zastosować wobec usług certyfikacyjnych wystawiających certyfikaty niekwalifikowane (o rodzaju usługi „CA/PKC”) stosujących domyślne rodzaje usług OCSP i CRL określone w ETSI TS 102 231.

Należy zwrócić uwagę, że TSL implementująca TL MUSI obejmować usługi wycofania, jeżeli w polu dostępu do informacji urzędu (AIA) ostatecznych certyfikatów nie umieszczono odpowiednich informacji, lub jeżeli nie uzyskano podpisu urzędu certyfikacji wpisanego na listę urzędów certyfikacji.

2.5. *W kierunku interoperacyjnego profilu QC*

Co do zasady, należy dążyć do uproszczenia (ograniczenia) w miarę możliwości liczby wpisów usług (różnych „Sdi”). Należy to jednak zrównoważyć poprawną identyfikacją usług związanych z wystawianiem QC i udostępnianiem wiarygodnych informacji dotyczących tego, czy przedmiotowe QC są obsługiwane za pomocą SSCD, jeżeli informacji tych brakuje w wystawionym QC.

▼C1

Idealnym rozwiązaniem byłoby (ścisłe) ograniczenie stosowania pola „Sie” i rozszerzenia „kwalifikacji” do szczególnych przypadków rozstrzyganych w ten sposób, ponieważ QC powinny zawierać wystarczające informacje związane ze zgłoszonym statusem kwalifikowanym i zgłaszaną obsługą lub brakiem obsługi przez SSCD.

W miarę możliwości państwa członkowskie powinny wspierać przyjęcie i stosowanie interoperacyjnych profili QC.

3. **Struktura wspólnego wzoru zaufanej listy**

Struktura proponowanego wspólnego wzoru zaufanej listy państwa członkowskiego będzie podzielona na następujące kategorie informacji:

1. Informacje dotyczące zaufanej listy i systemu jej wydawania.

2. 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).

3. W odniesieniu do każdego wymienionego w liście CSP sekwencja pól zawierających jednoznaczną identyfikację nadzorowanej/akredytowanej usługi certyfikacyjnej świadczonej przez CSP (sekwencja ta musi składać się co najmniej z jednego wpisu).

4. W odniesieniu do każdej nadzorowanej/akredytowanej usługi certyfikacyjnej, identyfikacja bieżącego statusu usługi i historię tego statusu.

W odniesieniu do CSP wystawiającego QC, jednoznaczna identyfikacja nadzorowanej/akredytowanej usługi certyfikacyjnej, która ma zostać zamieszczona na liście, musi uwzględniać sytuacje, w których certyfikat kwalifikowany nie zawiera wystarczających informacji dotyczących „kwalifikowanego” statusu certyfikatu, fakt ewentualnej obsługi certyfikatu za pomocą SSCD oraz w szczególności fakt, że większość (komercyjnych) CSP wykorzystuje jeden wystawiający kwalifikowany urząd certyfikacji do wystawiania kilku rodzajów zarówno kwalifikowanych, jak i niekwalifikowanych certyfikatów wierzchołka ścieżki.

Liczbę wpisów dokonywanych na liście przez każdy uznany CSP można ograniczyć, jeżeli istnieje jedna lub większa liczba usług CA wyższego szczebla, np. w odniesieniu do komercyjnej hierarchii CA od głównego CA do CA wystawiających certyfikat. Nawet w tych przypadkach należy jednak utrzymać i zapewnić realizację zasady gwarantującej jednoznaczne połączenie między usługą certyfikacyjną $CSP_{QC}$ a zbiorem certyfikatów, które mają być zidentyfikowane jako QC.

1. *Informacje dotyczące zaufanej listy i systemu jej wydawania*

Częścią tej kategorii będą następujące informacje:

— **znacznik** zaufanej listy ułatwiający identyfikację zaufanej listy podczas elektronicznego wyszukiwania oraz potwierdzający jej cele, gdy ma formę czytelną dla człowieka,

— **format** zaufanej listy i **identyfikator wersji formatu**,

— **numer sekwencji (lub dopuszczenia)** zaufanej listy,

— informacje dotyczące **rodzaju** zaufanej listy (np. służące do identyfikacji, 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),

▼C1

— informacje dotyczące **właściciela** listy zaufania (np. nazwa, adres, informacje kontaktowe itp. organu państwa członkowskiego kierującego sporządzaniem, bezpiecznym publikowaniem i prowadzeniem zaufanej zaufania),

— **informacje dotyczące podstawowych systemów nadzoru/akredytacji**, z którymi powiązana jest zaufana lista, zawierające 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 oraz **następna przewidywana aktualizacja**.

2. *Jednoznaczne informacje identyfikacyjne dotyczące każdego CSP uznanego przez system*

*Ten zbiór obejmie co najmniej następujące informacje:*

— nazwę organizacji CSP wykorzystaną podczas oficjalnej rejestracji (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 informacje.

3. *W odniesieniu do każdego wymienionego na liście CSP sekwencja pól zawierających jednoznaczną identyfikację usługi certyfikacyjnej świadczonej przez CSP i nadzorowanej/akredytowanej w zakresie 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 certyfikacyjnej (np. identyfikator wskazujący, że nadzorowana/akredytowana usługa certyfikacyjna świadczona przez CSP jest CA wystawiającym QC),

— znak (towarowy) przedmiotowej usługi certyfikacyjnej,

— jednoznaczny niepowtarzalny identyfikator usługi certyfikacyjnej,

— dodatkowe informacje dotyczące usługi certyfikacyjnej (np. zamieszczone bezpośrednio lub w formie odniesienia do miejsca, z którego można pobrać informacje, dostęp do informacji dotyczących usługi),

— w odniesieniu do usług CA/QC fakultatywna sekwencja krotek informacji, z których każda zawiera:

  (i) kryteria wykorzystywane do dalszej identyfikacji (filtrowania), w ramach zidentyfikowanej usługi certyfikacyjnej „Sdi”, konkretnej usługi (tj. zbioru kwalifikowanych certyfikatów), w odniesieniu do której wymagane/zawarte są dodatkowe informacje dotyczące obsługi przez SSCD (lub wystawienia na rzecz osoby prawnej); oraz

  (ii) towarzyszące „kwalifikatory” zawierające informacje dotyczące tego, czy zbiór certyfikatów kwalifikowanych z tej dodatkowo zidentyfikowanej usługi jest obsługiwany za pomocą SSCD, lub informacje dotyczące tego, czy takie QC wystawia się osobom prawnym (domyślnie uznaje się je za wystawiane wyłącznie osobom fizycznym).

▼C1

4. *W odniesieniu do każdej usługi certyfikacyjnej wymienionej na liście identyfikacja bieżącego statusu usługi i historia tego statusu*

Ten zbiór obejmie co najmniej następujące informacje:

— identyfikator bieżącego statusu,

— początkową datę i godzinę bieżącego statusu,

— informacje historyczne dotyczące przedmiotowego statusu.

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 ust. 11 dyrektywy 1999/93/WE |
| Urząd certyfikacji | CA | CA jest CSP i przy wystawianiu certyfikatów wierzchołka ścieżki może korzystać z szeregu technicznych prywatnych kluczy urzędów certyfikacji, z których każdy ma certyfikat towarzyszący. Jeden lub większa liczba użytkowników powierza CA sporządzenie i przydzielenie certyfikatów. Fakultatywnie urząd certyfikacji może tworzyć klucze użytkowników [ETSI TS 102 042]. Uznaje się, że CA jest identyfikowany z pomocą informacji identyfikacyjnych znajdujących się w polu „wydawca" certyfikatu CA związanego z (certyfikującym) publicznym kluczem powiązanym z należącym do urzędu certyfikacji prywatnym kluczem i skutecznie wykorzystywanym przez urząd do wystawiania podmiotom certyfikatów. CA może mieć kilka kluczy. Każdy klucz CA jest niepowtarzalnie identyfikowany z pomocą niepowtarzalnego identyfikatora jako część pola „identyfikator klucza urzędu" na certyfikacie CA. |
| Urząd certyfikacji wystawiający certyfikaty kwalifikowane | CA/QC | CA spełniający wymogi określone w załączniku II do dyrektywy 1999/93/WE i wystawiający certyfikaty kwalifikowane spełniające wymogi określone w załączniku I do dyrektywy 1999/93/WE. |
| Certyfikat | Certyfikat | Zgodnie z definicją zawartą w art. 2 ust. 9 dyrektywy 1999/93/WE. |
| Certyfikat kwalifikowany | QC | Zgodnie z definicją zawartą w art. 2 ust. 10 dyrektywy 1999/93/WE. |
| Podpisujący | Podpisujący | Zgodnie z definicją zawartą w art. 2 ust. 3 dyrektywy 1999/93/WE. |
| Nadzór | Nadzór | Pojęcie „nadzór" jest stosowane w rozumieniu dyrektywy 1999/93/WE (art. 3 ust. 3). Zgodnie z dyrektywą 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 zgodności z przepisami dyrektywy. |
| Dobrowolna akredytacja | Akredytacja | Zgodnie z definicją zawartą w art. 2 ust. 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. |

▼C1

| Termin | Akronim | Definicja |
|---|---|---|
| Lista statusu usług zaufania | TSL | Ma formę podpisanej listy stosowanej jako podstawa przedstawienia informacji dotyczących statusu wiarygodnych usług zgodnie ze specyfikacją określoną w ETSI TS 102 231. |
| 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 102231). |
| Dostawca usługi zaufania | TSP | Organ obsługujący 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. Przykładami binarnych tokenów usługi zaufania są certyfikaty, CRL, tokeny znacznika czasu i odpowiedzi OSCP. |
| Kwalifikowany podpis elektroniczny | QES | AdES obsługiwany przez QC i wygenerowany za pomocą SSCD zgodnie z definicją zawartą w art. 2 dyrektywy 1999/93/WE. |
| Zaawansowany podpis elektroniczny | AdES | Zgodnie z definicją zawartą w art. 2 ust. 2 dyrektywy 1999/93/WE. |
| Zaawansowany podpis elektroniczny obsługiwany przez certyfikat kwalifikowany | $AdES_{QC}$ | Oznacza podpis elektroniczny spełniający wymogi AdES i opierający się na 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 ust. 6 dyrektywy 1999/93/WE. |

ROZDZIAŁ I

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

W niniejszej 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]).

►M1 Niniejsza specyfikacja opiera się na specyfikacji i wymogach określonych w ETSI TS 102 231 v.3.1.2. W przypadku braku szczególnego wymogu w niniejszej specyfikacji zastosowanie MUSZĄ mieć w całości wymogi określone w ETSI TS 102 231 v.3.1.2. ◄ Jeżeli niniejsza specyfikacja zawiera szczególne wymogi, wówczas MUSZĄ być one nadrzędne w stosunku do odpowiednich wymogów określonych w ETSI TS 102231, a jednocześnie uzupełniane specyfikacją formatu określoną w ETSI TS 102231. W przypadku rozbieżności między niniejszą specyfikacją i specyfikacją określoną w ETSI TS 102231 normatywna MUSI być niniejsza specyfikacja.

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

▼C1

Obsługa języków MUSI być wdrożona i zapewniona co najmniej dla języka angielskiego (EN) i ewentualnie dodatkowo dla jednego lub w większej liczby języków krajowych.

Oznaczenie data-czas MUSI być zgodne z klauzulą 5.1.4 ETSI TS 102231.

Stosowanie URI MUSI być zgodne z klauzulą 5.1.5 ETSI TS 102231.

**Informacje dotyczące systemu wydawania zaufanej listy**

*Tag*

T S L t a g (klauzula 5.2.1)

Pole to jest WYMAGANE i MUSI być zgodne z klauzulą 5.2.1 ETSI TS 102231.

▼M1

_____

▼C1

*Scheme Information*

T S L v e r s i o n i d e n t i f i e r (klauzula 5.3.1)

To pole jest WYMAGANE i MUSI być ustalone na poziomie „3” (liczba całkowita).

T S L s e q u e n c e n u m b e r (klauzula 5.3.2)

▼M1

To pole jest WYMAGANE. MUSI ono określać numer sekwencji TSL. Zaczynająca się od cyfry „1” przy pierwszym dopuszczeniu TSL wartość tej liczby całkowitej MUSI być powiększana przy każdej kolejnej wersji TSL. NIE MOŻNA jej ponownie zmniejszać do „1” w przypadku podwyższenia wartości powyższego „TSL version identifier.”

▼C1

T S L t y p e (klauzula 5.3.3)

▼M1

To pole jest WYMAGANE, aby określić rodzaj TSL. Musi być ustawione jako http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

*Uwaga:* Aby spełnić wymagania klauzuli 5.3.3 ETSI TS 102231 i, aby wskazać szczególny rodzaj TSL w nawiązaniu do istnienia niniejszych specyfikacji regulujących wdrożenie TSL państw członkowskich ([1]) oraz umożliwienia analizatorowi składniowemu na określenie, jakiej formy następujących pól ([2]) należy się spodziewać, jeśli zgodnie z reprezentowanym TSL (w tym przypadku oficjalną TSL państwa członkowskiego) pola te mają konkretne (lub alternatywne) znaczenia, wskazany powyżej konkretny URI MUSI być rejestrowany i określany w sposób następujący:

([1]) Tzn. „Lista statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne nadzorowane/akredytowane przez przedmiotowe państwo członkowskie pod względem zgodności z odpowiednimi przepisami dyrektywy 1999/93/WE” (w skrócie „zaufana lista”).

([2]) Oznacza pola określone w ETSI TS 102 231 – Electronic Signatures and Infrastructures (ESI): Provision of harmonized Trust-service status information, doprecyzowane w niniejszej specyfikacji i mające na celu określenie tworzenia zaufanej listy państwa członkowskiego.

▼M1

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic

▼C1

Opis: Wdrożenie TSL listy statusu nadzoru/akredytacji usług certyfikacyjnych świadczonych przez podmioty świadczące usługi certyfikacyjne nadzorowane/akredytowane przez właściwe państwo członkowskie wdrażające TSL pod względem 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, w drodze bezpośredniego nadzoru (dobrowolnego lub regulacyjnego).

Scheme operator name (klauzula 5.3.4)

Pole to jest WYMAGANE. MUSI ono określać nazwę organu państwa członkowskiego kierującego tworzeniem, publikowaniem i prowadzeniem krajowej zaufanej listy. MUSI określać oficjalną nazwę, pod którą działa stowarzyszona osoba prawna lub upoważniony podmiot (np. w przypadku rządowych organów administracyjnych) stowarzyszony z tym organem. MUSI to być nazwa wykorzystana przy oficjalnej rejestracji lub autoryzacji i pod którą powinny być kierowane wszystkie oficjalne powiadomienia. MUSI się ona składać z sekwencji wielojęzycznych ciągów znaków i MUSI być wdrażana w języku angielskim (EN), jako w języku obowiązkowym, i ewentualnie w jednym lub w większej liczbie języków krajowych.

*Uwaga:* Kraj MOŻE mieć odrębne organy ds. nadzoru i akredytacji, a nawet dodatkowe organy zajmujące się wszelkimi powiązanymi działaniami operacyjnymi. ►M1 Wyznaczenie Scheme operator wdrożenia TSL zaufanej listy w państwie członkowskim jest sprawą tego 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 cywilna.

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

▼M1

Określony Scheme Operator (klauzula 5.3.4) jest podmiotem, który podpisze TSL.

▼C1

Scheme operator address (klauzula 5.3.5)

Pole to jest WYMAGANE. MUSI w nim być określony adres osoby prawnej lub upoważnionej organizacji określonej w polu „Scheme operator name" (klauzula 5.3.4) używany do przesyłania korespondencji pocztą i do łączności elektronicznej. MUSI ono zawierać zarówno „PostalAddress" (tj. ulica, miejscowość, [stan lub prowincja], [kod pocztowy] i kod kraju zgodny z ISO 3166-1 alpha-2) zgodny z klauzulą 5.3.5.1 oraz „ElectronicAddress" (tj. e-mail: lub URI strony internetowej) zgodnie z klauzulą 5.3.5.2.

Scheme name (klauzula 5.3.6)

To pole jest WYMAGANE, aby określić nazwę, pod jaką system funkcjonuje. Nazwa ta MUSI składać się z sekwencji wielojęzycznych ciągów znaków (w języku angielskim (EN), jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych) definiowanych w następujący sposób:

▼C1

— wersja w języku angielskim MUSI być ciągiem znaków pogrupowanych w następujący sposób:

CC:EN_name_value

w którym to łańcuchu:

— „CC” = kod kraju według ISO 3166-1 alpha-2 użyty w polu „Scheme territory” (klauzula 5.3.10),

— „:” = jest stosowany jako znak rozdzielający,

▼M1

— „EN_name_value” = Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State’s laws,

▼C1

— każda wersja w języku urzędowym państwa członkowskiego MUSI być ciągiem znaków pogrupowanych w następujący sposób:

CC:name_value

w którym to łańcuchu:

— „CC” = kod kraju według ISO 3166-1 alpha-2 użyty w polu „Scheme territory” (klauzula 5.3.10),

— „:” = jest stosowany jako znak rozdzielający,

— „name_value” = oficjalne tłumaczenie wskazanego powyżej „EN_name_value” w języku krajowym.

Nazwa systemu jest wymagana w celu niepowtarzalnego identyfikowania na jej podstawie systemu określonego przez „Scheme information URI” oraz w celu zapewnienia nadania odróżniającej się nazwy każdemu systemowi, jeżeli operatorowi systemu podlega więcej systemów niż jeden.

Państwa członkowskie i operatorzy systemu MUSZĄ upewnić się, czy każdemu systemowi nadana jest odróżniająca się nazwa, jeżeli państwu członkowskiemu lub operatorowi systemu podlega więcej systemów niż jeden.

Scheme information URI (klauzula 5.3.7)

Pole to jest WYMAGANE i MUSI określać URI, gdzie użytkownicy (strony opierające się na danych informacjach) mogą uzyskać informacje dotyczące systemu (w języku angielskim (EN) jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych). MUSI to być sekwencja wielojęzycznych wskaźników (w języku angielskim (EN) jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych). Przedmiotowy (przedmiotowe) URI MUSI zapewnić ścieżkę dostępu do informacji zawierających „odpowiednie informacje dotyczące systemu”.

„Appropriate information about the scheme” MUSZĄ obejmować co najmniej:

— ogólne informacje wstępne wspólne dla wszystkich państw członkowskich odnoszące się do zakresu i kontekstu zaufanej listy i podstawowego systemu (podstawowych systemów) nadzoru/akredytacji. Wspólny tekst, który należy zastosować, brzmi:

▼C1

„The present list is the TSL implementation of [*name of the relevant Member State*] »Trusted List of supervised/accredited Certification Service Providers« providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable »supervision« system (respectively »voluntary accreditation« system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art. 7.1(a), Art. 8.1, Art. 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.”,

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

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

([1]) Dwa ostatnie zbiory informacji mają istotne znaczenie dla stron, które się na nich opierają przy dokonywaniu oceny poziomu jakości i bezpieczeństwa takich systemów nadzoru/akredytacji. Takie zbiory informacji są udostępniane na poziomie TL 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 QC 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).

▼C1

— 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 QC,

— w stosownych przypadkach informacje dotyczące krajowego systemu dobrowolnych akredytacji mającego zastosowanie do każdego CSP niewystawiającego QC,

— w odniesieniu do każdego podstawowego systemu wymienionego powyżej określone 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 określone informacje państwa członkowskiego dotyczące systemu MOŻNA podawać dobrowolnie. MUSZĄ one obejmować:

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

— inne informacje kontaktowe i ogólne mające zastosowanie do funkcjonowania systemu.

Status determination approach (klauzula 5.3.8)

Pole to jest WYMAGANE i MUSI określać identyfikator podejścia dotyczącego określania statusu. MUSI być stosowany następujący określony URI zarejestrowany i opisany w następujący sposób:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/appropriate

Opis: Wymienione usługi mają status określony przez operatora systemu lub w jego imieniu zgodnie z odpowiednim systemem przedmiotowego państwa członkowskiego umożliwiającym „nadzór" (w stosownych przypadkach „dobrowolną akredytację") podmiotów świadczących usługi certyfikacyjne mających siedzibę lub miejsce zamieszkania na terytorium przedmiotowego państwa członkowskiego (lub w przypadku „dobrowolnej akredytacji" mających siedzibę lub miejsce zamieszkania w kraju trzecim) i powszechnie wystawiających certyfikaty kwalifikowane zgodnie z art. 3 ust. 3 (odpowiednio art. 3 ust. 2 lub art. 7 ust. 1 lit. a)) dyrektywy 1999/93/WE i w stosownych przypadkach umożliwiającym „nadzór"/„dobrowolną akredytację" podmiotów świadczących usługi certyfikacyjne niewystawiających certyfikatów kwalifikowanych zgodnie ze zdefiniowanym i ustanowionym „przyjętym (przyjętymi) systemem (systemami) zatwierdzania" wdrożonym (wdrożonymi) na szczeblu krajowym w celu nadzorowania zgodności usług świadczonych przez CSP niewystawiające QC z przepisami dyrektywy 1999/93/WE oraz ewentualnie z przepisami krajowymi dotyczącymi świadczenia tych usług certyfikacyjnych.

▼C1

Scheme type/community/rules (klauzula 5.3.9)

Pole to jest WYMAGANE i MUSI zawierać co najmniej następujące zarejestrowane URI:

— URI wspólny dla TL wszystkich państw członkowskich wskazujący tekst opisowy, który MUSI mieć zastosowanie do wszystkich TL:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— oznaczający udział systemu państwa członkowskiego (identyfikowany na podstawie „TSL type" (klauzula 5.3.3) i „Scheme name" (klauzula 5.3.6)) w systemie systemów (tzn. TSL zawierającej listę odsyłaczy do wszystkich państw członkowskich publikujących i prowadzących TL w postaci TSL),

— w przypadku którego użytkownicy mogą mieć dostęp do polityki/zasad, na podstawie których usługi zawarte na liście są oceniane i na podstawie których można określić rodzaj TSL (zob. klauzulę 5.3.3),

— w przypadku którego użytkownicy mogą mieć dostęp do opisu sposobu korzystania i interpretowania treści wdrożenia TL za pomocą TSL. Te zwyczajowe zasady MUSZĄ być wspólne w odniesieniu do wszystkich zaufanych list państw członkowskich niezależnie od rodzaju usługi wymienionej na liście i niezależnie od systemu (systemów) nadzoru/akredytacji.

Tekst opisowy:

**„Participation in a scheme**

Each Member State must create a »Trusted List of supervised/accredited Certification Service Providers« providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

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

**Policy/rules for the assessment of the listed services**

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C1

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable »supervision« system (respectively »voluntary accreditation« system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art. 2.13, Art. 3.2, Art. 7.1(a), Art. 8.1, Art. 11).

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a »voluntary accreditation« system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined »recognised approval scheme« implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2.11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific »qualification« on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a »qualification« is likely to be limited solely to the national level.

**Interpretation of the TSL implementation of the Trusted List**

The general user guidelines for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision 2009/767/WE are as follows:

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

— indicates that from the »Service digital identifier« (»Sdi«) identified CA (similarly within the CA hierarchy starting from the »Sdi« identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) provided that it is claimed as such in the certificate through the use of appropriate ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C1

*Note:* if no »Sie«»Qualification« information is present or if an end-entity certificate that is claimed to be a QC is not »further identified« through a related »Sie« entry, then the »machine-processable« information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— and IF »Sie«»Qualification« information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this »Sie«»Qualification« entry, which is constructed on the principle of a sequence of »filters« further identifying a set of certificates, must be considered according to the associated »qualifiers« providing some additional information regarding »SSCD support« and/or »Legal person as subject« (e.g. those 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.). Those qualifiers are part of the following set of »qualifiers« used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

  — to indicate the nature of the SSCD support:

    — »QCWithSSCD« qualifier value meaning »QC supported by an SSCD«, or

    — »QCNoSSCD« qualifier value meaning »QC not supported by an SSCD«, or

    — »QCSSCDStatusAsInCert« qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the »Sdi«-»Sie« provided information in this CA/QC entry;

  AND/OR

  — to indicate issuance to Legal Person:

    — »QCForLegalPerson« qualifier value meaning »Certificate issued to a Legal Person«.

The general interpretation rule for any other »Sti« type entry is that the listed service named according to the »Sn« field value and uniquely identified by the »Sdi« field value has a current supervision/accreditation status according to the »Scs« 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 Technical specifications for a Common Template for the »Trusted List of supervised/accredited Certification Service Providers« in the Annex of Commission Decision 2009/767/EC for further details on the fields, description and meaning for the TSL implementation of the Member States' Trusted Lists".

▼C1

— 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/eSigDir-1999-93-EC-TrustedList/schemerules/CC

w którym CC = kod kraju zgodny z ISO 3166-1 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 dotyczący sposobu korzystania i interpretowania treści wdrożenia TSL zaufanej zaufania w odniesieniu do usług certyfikacyjnych niezwiązanych z wystawianiem QC. Można to wykorzystać do wskazania potencjalnej szczegółowości krajowych systemów nadzoru/akredytacji związanych z CSP niewystawiającymi QC oraz do wskazania sposobu wykorzystania do tego celu pól „Scheme service definition URI” (klauzula 5.5.6) i „Service information extension”.

Państwa członkowskie MOGĄ definiować dodatkowy URI na podstawie wskazanego powyżej szczególnego URI państwa członkowskiego (tzn. URI zdefiniowany na podstawie danego hierarchicznego określonego URI).

Scheme territory (klauzula 5.3.10)

W odniesieniu do niniejszej specyfikacji pole to jest WYMAGANE i MUSI określać kraj, w którym utworzono system (kod kraju według ISO 3166-1 alpha-2).

TSL policy/legal notice (klauzula 5.3.11)

W odniesieniu do niniejszej specyfikacji pole to jest WYMAGANE i MUSI określać politykę systemu lub podawać informacje o statusie prawnym systemu lub wymogach prawnych spełnionych przez system w ramach jurysdykcji, w której system ten utworzono lub wszelkich ograniczeniach i warunkach, zgodnie z którymi TL jest prowadzona i publikowana.

MUSI to być wielojęzyczny ciąg znaków (zwykły tekst) składający się z dwóch części:

— pierwszej obowiązkowej części wspólnej dla wszystkich TL państw członkowskich (w języku angielskim (EN) 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 the 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”.

▼C1

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 stanowi 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].”,

— drugiej fakultatywnej części określonej dla każdej TL (w języku angielskim (EN) 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 QC).

Historical information period (klauzula 5.3.12)

Pole to jest WYMAGANE i MUSI określać okres (liczba całkowita), odnośnie do którego przedstawiane są informacje historyczne w TSL. Ta wartość całkowita jest wyrażana w liczbie dni, a w odniesieniu do niniejszej specyfikacji MUSI być równa lub większa niż 3 653 (tzn. wdrożenie TSL zaufanej listy państw członkowskich MUSI obejmować informacje historyczne co najmniej z dziesięciu lat). Liczby o wyższej wartości powinny uwzględniać wymogi prawne dotyczące zatrzymywania danych w państwie członkowskim wskazanym w polu „Scheme Territory” (klauzula 5.3.10).

Pointers to other TSLs (klauzula 5.3.13)

W odniesieniu do niniejszej specyfikacji pole to jest WYMAGANE i MUSI obejmować, o ile jest to możliwe, odsyłacz do zbiorczego wykazu odsyłaczy (wskaźników) WE spełniającego wymagania ETSI TS 102231 do wszystkich wdrożeń TSL zaufanych list państw członkowskich. Specyfikacja zamieszczona w klauzuli 5.3.13 ETSI TS 102231 ma zastosowanie przy upoważnianiu do korzystania z fakultatywnej tożsamości cyfrowej reprezentującej wydawcę wskazanego TSL sformatowanego zgodnie z klauzulą 5.5.3.

*Uwaga:* Pola tego NIE MOŻNA wykorzystywać, dopóki nie zostanie wdrożony zgodnie z ETSI TS 102231 kompletny wykaz odsyłaczy WE do wdrożenia TSL zaufanych list państw członkowskich.

List issue date and time (klauzula 5.3.14)

Pole to jest WYMAGANE i MUSI określać datę i czas (czas UTC określany jako czas Zulu) wydania TSL za pomocą wartości data-czas określonej w klauzuli 5.1.4 ETSI TS 102231.

Next update (klauzula 5.3.15)

Pole to jest WYMAGANE i MUSI określać najpóźniejszą datę i godzinę (czas UTC czasem określany jako czas Zulu) wydania kolejnej TSL lub być puste, aby wskazać, że TSL jest zamknięta (stosując wartości data-godzina określone w klauzuli 5.1.4 ETSI TS 102231).

W przypadku braku zmian tymczasowego statusu dowolnej TSP lub usług określonych w systemie, TSL MUSI być ponownie wydana zanim przestanie obowiązywać ostatnia wydana TSL.

W odniesieniu do niniejszej specyfikacji różnica między datą i godziną między „Next update” oraz „List issue date and time” NIE MOŻE przekraczać sześciu (6) miesięcy.

▼C1

**Distribution points** (klauzula 5.3.16)

Pole to jest FAKULTATYWNE. W przypadku skorzystania z niego MUSI określać miejsce publikacji aktualnego wdrożenia TSL zaufanej listy, w którym znajdują się aktualizacje bieżącej TSL. Jeżeli wyznaczono wiele punktów dystrybucji, wówczas w każdym z nich MUSZĄ być wydawane identyczne kopie bieżącej TSL lub jej zaktualizowanej wersji. Jeżeli korzysta się z tego pola, jest ono sformatowane jako zapisana sekwencja łańcuchów, z których każdy jest zgodny z RFC 3986 ([1]).

Scheme extensions (klauzula 5.3.17)

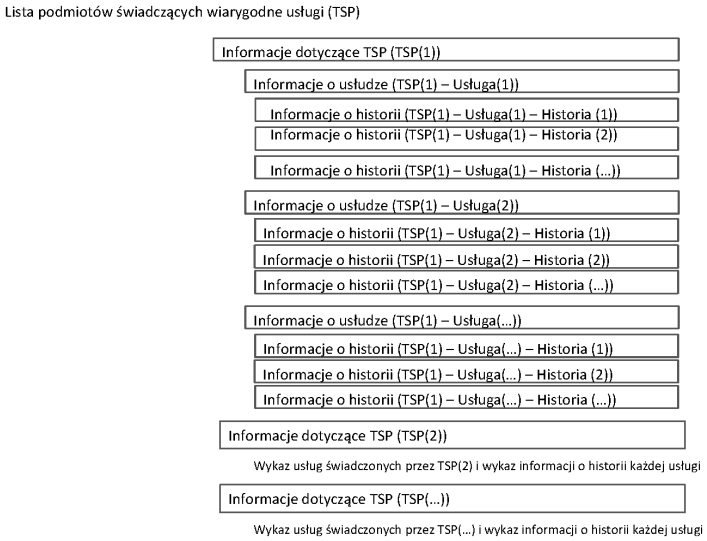
Pole to jest FAKULTATYWNE i nie jest stosowane w kontekście niniejszej specyfikacji.

*List of Trust Service Providers*

Pole to jest FAKULTATYWNE.

Pole to MUSI pozostać puste, jeżeli żaden CSP nie jest i nie był nadzorowany/akredytowany w odniesieniu do systemu w państwie członkowskim. Uzgodniono jednak, że państwa członkowskie MUSZĄ wdrożyć TSL z takim pustym polem, nawet jeżeli w państwie członkowskim żaden CSP nie jest nadzorowany ani akredytowany przez system. Brak na liście CSP MUSI oznaczać, że w kraju określonym w polu „Scheme Territory” nie ma nadzorowanych/akredytowanych CSP.

Jeżeli jedna lub większa liczba usług świadczonych przez CSP jest lub była nadzorowana/akredytowana na podstawie systemu, wówczas w polu MUSI znajdować się sekwencja identyfikująca każdy CSP świadczący jedną lub większą liczbę nadzorowanych/akredytowanych usług oraz szczegółowe informacje dotyczące statusu nadzoru/akredytacji i historii statusu każdej usługi świadczonej przez CSP (na poniższym schemacie TSP = CSP).




([1]) IETF RFC 3986: „Uniform Resource Identifiers (URI): Generic syntax”.

▼C1

Lista TSP jest zorganizowana w sposób wskazany na powyższym schemacie. W odniesieniu do każdego TSP istnieje sekwencja pól zawierających informacje dotyczące TSP („TSP Information”) poprzedzająca wykaz usług. W odniesieniu do każdej usługi wymienionej na liście istnieje sekwencja pól zawierających informacje o usłudze („Service Information”) i sekwencja pól dotycząca historii statusu zatwierdzenia usługi („Service approval history”).

**TSP Information**

*TSP (1)*

T S P n a m e (klauzula 5.4.1)

Pole to jest WYMAGANE i MUSI określać nazwę **osoby prawnej** odpowiedzialnej za usługi świadczone przez CSP, które są lub były nadzorowane lub akredytowane przez system. Nazwa składa się z sekwencji wielojęzycznych łańcuchów znaków (w języku angielskim (EN) jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych). MUSI to być nazwa wykorzystana podczas oficjalnej rejestracji i nazwa, na którą będą kierowane wszystkie oficjalne powiadomienia.

T S P t r a d e n a m e (klauzula 5.4.2)

Pole to jest FAKULTATYWNE. a jeżeli występuje, MUSI określać alternatywną nazwę identyfikującą CSP w szczególnym kontekście świadczenia tych usług, które znajdują się na danej TSL w polu wpisu „TSP name” (klauzula 5.4.1).

*Uwaga:* Jeżeli pojedyncza osoba prawna będąca CSP świadczy usługi certyfikacyjne pod różnymi nazwami handlowymi lub w różnych szczególnych kontekstach, liczba wpisów CSP może być równa liczbie szczególnych kontekstów (np. wpisy nazwy/nazwy handlowej). Alternatywnie można tylko raz wymienić w wykazie każdy CSP (osobę prawną) i przedstawić informacje dotyczące kontekstu świadczenia usługi. Operator systemu państwa członkowskiego decyduje o przedyskutowaniu i uzgodnieniu z CSP najbardziej odpowiedniego podejścia.

T S P a d d r e s s (klauzula 5.4.3)

Pole to jest WYMAGANE i MUSI określać adres osoby prawnej lub upoważnionej organizacji określonej w polu „TSP name” (klauzula 5.4.1) używany do przesyłania korespondencji pocztą i do łączności elektronicznej. MUSI zawierać zarówno „PostalAddress” (tj. ulicę, miejscowość, [stan lub prowincja], [kod pocztowy] i kod kraju zgodny z ISO 3166-1 alpha-2) zgodny z klauzulą 5.3.5.1 oraz „ElectronicAddress” (tj. e-mail: lub URI strony internetowej) zgodnie z klauzulą 5.3.5.2.

T S P i n f o r m a t i o n U R I (klauzula 5.4.4)

Pole to jest WYMAGANE i MUSI określać URI, gdzie użytkownicy (np. strony bazujące na danych informacjach) mogą uzyskać informacje dotyczące CSP. URI MUSI składać się z sekwencji wielojęzycznych wskaźników (w języku angielskim (EN) jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych). Przedmiotowy (przedmiotowe) URI MUSI zapewnić ścieżkę dostępu do informacji opisujących warunki ogólne dotyczące CSP, jego praktyk, kwestii prawnych, polityki obsługi klienta i innych ogólnych informacji mających zastosowanie do wszystkich usług świadczonych przez ten podmiot wymienionych w we wpisie CSP w TSL.

*Uwaga:* Jeżeli pojedyncza osoba prawna będąca CSP świadczy usługi pod różnymi nazwami handlowymi lub w różnych szczególnych kontekstach i znalazło to odzwierciedlenie w tylu wpisach TSP ile jest szczególnych kontekstów, pole to MUSI zawierać informacje dotyczące określonego zbioru usług wymienionych w szczególnym wpisie TSP/TradeName.

▼C1

TSP information extensions (klauzula 5.4.5)

Pole to jest FAKULTATYWNE, a jeżeli występuje MOŻE być wykorzystane przez operatora systemu zgodnie ze specyfikacją ETSI TS 102231 (klauzula 5.4.5) do przedstawienia szczególnych informacji podlegających interpretacji zgodnej z zasadami określonego systemu.

**List of Services**

Pole to jest WYMAGANE i MUSI zawierać sekwencję identyfikującą każdą uznaną usługę świadczoną przez CSP i status zatwierdzenia (oraz historię tego statusu) tej usługi. Na liście należy podać co najmniej jedną usługę (nawet jeżeli posiadane informacje są wyłącznie historyczne).

Przechowywanie informacji historycznych dotyczących usług wymienionych na liście jest WYMAGANE na podstawie niniejszej specyfikacji, więc informacje historyczne MUSZĄ być przechowywane, nawet jeżeli zgodnie z bieżącym statusem usługi nie musiałaby ona być co do zasady wymieniona na liście (np. wycofanie się ze świadczenia usługi). W związku z tym do celów zachowania informacji historycznych CSP MUSI być uwzględniony, nawet jeżeli jedyna wymieniona na liście usługa świadczona przez ten podmiot jest w stanie opisanym powyżej.

**Service Information**

*TSP(1) Service(1)*

Service type identifier (klauzula 5.5.1)

▼M1

Pole to jest WYMAGANE i MUSI określać identyfikator rodzaju usługi zgodnie z rodzajem aktualnej specyfikacji TSL (tj. „/eSigDir-1999-93-EC-TrustedList/TSLType/generic”).

▼C1

Jeżeli wymieniona na liście usługa jest związana z wystawianiem certyfikatów kwalifikowanych, cytowany URI MUSI być następujący http://uri.etsi.org/TrstSvc/Svctype/CA/QC (urząd certyfikacji wystawiający certyfikaty kwalifikowane).

Jeżeli wymieniona na liście usługa jest związana z wydawaniem tokenów usługi zaufania niebędących QC i nieobsługujących wystawiania QC, cytowanym URI MUSI być jeden z URI określonych w ETSI 102231 i wymienionych w klauzuli D.2 tego dokumentu dotyczącej tego pola. MUSI to mieć zastosowanie nawet do tokenów usługi zaufania nadzorowanych/akredytowanych pod względem spełnienia niektórych szczególnych kwalifikacji zgodnie z krajowymi przepisami państw członkowskich (np. tak zwanego kwalifikowanego tokena znacznika czasu w DE lub HU), cytowanym URI MUSI być jeden z URI określonych w ETSI 102231 i wymienionych w klauzuli D.2 tego dokumentu dotyczącej tego pola (np. TSA ds. określonych w prawie krajowym kwalifikowanych tokenów znacznika czasu). W stosownych przypadkach takie szczególne krajowe kwalifikacje tokenów usługi zaufania MOGĄ być przedstawione we wpisie usługi, i MUSI być do tego celu stosowane rozszerzenie additionalServiceInformation (klauzula 5.8.2) w klauzuli 5.5.9 („Service information extension”).

▼C1

Jako ogólna zasada domyślności każdemu certyfikatowi X.509v3 MUSI odpowiadać jeden wpis (np. w odniesieniu do usługi certyfikacyjnej CA/QC) w ramach wymienionych na liście usług certyfikacyjnych świadczonych przez wymienione na zaufanej liście CSP (np. urząd certyfikacji wystawiający (bezpośrednio) QC). W niektórych starannie przewidzianych okolicznościach i starannie zarządzanych i zatwierdzonych warunkach organ ds. nadzoru/organ ds. akredytacji państwa członkowskiego MOŻE zadecydować o wykorzystaniu certyfikatu X.509v3 głównego urzędu ds. certyfikacji lub urzędu ds. certyfikacji wyższego szczebla (np. urzędu ds. certyfikacji niewystawiającego bezpośrednio certyfikatów kwalifikowanych wierzchołka ścieżki, ale certyfikujących hierarchię urzędów ds. certyfikacji, łącznie z urzędami ds. certyfikacji wystawiającymi certyfikaty kwalifikowane wierzchołka ścieżki) jako „Sdi" pojedynczego wpisu na liście usług świadczonych przez wymieniony na liście CSP. Konsekwencje (zalety i wady) stosowania certyfikatu X.509v3 głównego urzędu ds. certyfikacji lub urzędu certyfikacji wyższego szczebla jako wartości „Sdi" wpisów usług TL muszą być dokładnie rozważone i zatwierdzone przez państwa członkowskie ([1]). Ponadto jeżeli państwo członkowskie stosuje dopuszczalne wyjątki od zasady domyślności, MUSI ono przedstawić niezbędne dokumenty ułatwiające tworzenie i weryfikację ścieżki certyfikatu.

*Uwaga:* TSP, takie jak respondery OCSP i wydawcy CRL stanowiące część usług certyfikacyjnych $CSP_{CQ}$ i korzystające z oddzielnych par kluczy przy podpisywaniu odpowiednio odpowiedzi OCSP i CRL MOGĄ być także wymienione w aktualnym wzorze TSL przez zastosowanie następującej kombinacji URI:

— wartość „Service type identifier" (klauzula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

połączona z następującą wartością „Service information extension" (klauzula 5.5.9) additionalServiceInformation (klauzula 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Opis: podmiot nadający status certyfikatu obsługujący serwer OCSP jako część usługi świadczonej przez CSP wystawiający certyfikaty kwalifikowane,

— wartość „Service type identifier" (klauzula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

połączona z następującą wartością „Service information extension" (klauzula 5.5.9) additionalServiceInformation (klauzula 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Opis: CSP obsługujący CRL jako część usługi świadczonej przez CSP wystawiający certyfikaty kwalifikowane,

— wartość „Service type identifier" (klauzula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

([1]) Stosowanie certyfikatu X.509v3 głównego urzędu certyfikacji jako wartości „Sdi" w odniesieniu do usługi wymienionej na liście zmusi operatora systemu do uznania całego zbioru usług certyfikacyjnych w ramach takiego głównego urzędu certyfikacji jako całości w odniesieniu do „statusu nadzoru/akredytacji". Np. wszelka zmiana statusu wymagana od pojedynczego urzędu certyfikacji na podstawie wykazanej hierarchii urzędów wymusi na całej hierarchii przyjęcie tej zmiany statusu.

▼C1

połączona z następującą wartością „Service information extension” (klauzula 5.5.9) additionalServiceInformation (klauzula 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Opis: główny urząd ds. certyfikacji, od którego można ustalić ścieżkę certyfikacji do urzędu ds. certyfikacji wystawiającego certyfikaty kwalifikowane,

— wartość „Service type identifier” (klauzula 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

połączona z następującą wartością „Service information extension” (klauzula 5.5.9) additionalServiceInformation (klauzula 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Opis: usługa znakowania czasem jako część usługi świadczonej przez podmiot świadczący usługi certyfikacyjne wystawiający certyfikaty kwalifikowane, w związku z którą wydaje się tokeny znacznika czasu wykorzystywane w procesie weryfikacji kwalifikowanego podpisu, by zapewnić i przedłużyć okres ważności podpisu, gdy dochodzi do wycofania lub wygaśnięcia certyfikatu kwalifikowanego.

Service name (klauzula 5.5.2)

Pole to jest WYMAGANE i MUSI określać nazwę, pod którą CSP zidentyfikowany w polu „TSP name” (klauzula 5.4.1) świadczy usługę zidentyfikowaną w polu „Service type identifier” (klauzula 5.5.1). Nazwa ta MUSI składać się z sekwencji wielojęzycznych łańcuchów znaków (w języku angielskim (EN) jako w języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych).

Service digital identity (klauzula 5.5.3)

Pole to jest WYMAGANE i MUSI określać co najmniej jedną formę niepowtarzalnego identyfikatora cyfrowego usługi, której rodzaj jest określony w polu „Service type identifier” (klauzula 5.5.1) pozwalającego na jednoznaczne zidentyfikowanie usługi.

W niniejszej specyfikacji identyfikatorem cyfrowym zastosowanym w tym polu MUSI być odpowiedni certyfikat X.509v3 stanowiący klucz publiczny (klucze publiczne) wykorzystywany przez CSP do świadczenia usługi, której rodzaj jest określony w polu „Service type identifier” (klauzula 5.5.1) (tzn. klucz wykorzystywany przez główny CA/QC, klucz wykorzystywany przy podpisywaniu certyfikatów ([1]) lub alternatywnie przy wydawaniu tokenów znacznika czasu, podpisywaniu CRL lub podpisywaniu odpowiedzi OCSP). Ten powiązany certyfikat X.509v3 MUSI być stosowany jako minimalny wymagany identyfikator cyfrowy (stanowiący klucz publiczny (klucze publiczne) wykorzystywany przez CSP do świadczenia usługi wymienionej na liście). Dodatkowe identyfikatory MOGĄ być stosowane w następujący sposób, ale wszystkie MUSZĄ odnosić się do tej samej tożsamości (tzn. powiązanego certyfikatu X.509v3):

([1]) Może to być certyfikat urzędu certyfikacji wystawiającego certyfikaty wierzchołka ścieżki (np. CA/PKC, CA/QC) **lub** certyfikat wiarygodnego głównego CA, od którego można ustalić ścieżkę prowadzącą do kwalifikowanych certyfikatów wierzchołka ścieżki. Zależnie od tego, czy dane informacje i informacje objęte każdym certyfikatem wierzchołka ścieżki wystawionym w ramach tego wiarygodnego systemu urzędów mogą być wykorzystane do jednoznacznego określenia odpowiedniej charakterystyki każdego certyfikatu kwalifikowanego, może istnieć potrzeba uzupełnienia tych informacji „Service digital identity” o dane z pola „Service information extensions” (zob. klauzulę 5.5.9).

▼C1

a) wyróżniona nazwa (DN) certyfikatu, którą można wykorzystać do weryfikacji podpisów elektronicznych usługi CSP określona w polu „Service type identifier” (klauzula 5.5.1);

b) powiązany identyfikator klucza publicznego (tzn. X.509v3 SubjectKeyIdentifier lub wartość SKI);

c) powiązany klucz publiczny.

Jako ogólna zasada domyślności identyfikator cyfrowy (tzn. powiązany certyfikat X.509v3) NIE MOŻE występować w oficjalnym wykazie więcej niż raz tzn. każdemu certyfikatowi X.509v3 MUSI odpowiadać jeden wpis usługi certyfikacyjnej zgodnie z wymienionymi na liście usługami certyfikacyjnymi świadczonymi przez wymienione na liście zaufania CSP. Z drugiej strony pojedynczy certyfikat X.509v3 MUSI być stosowany w pojedynczym wpisie usługi jako wartość „Sdi”.

*Uwaga (1):* Jedyną sytuacją, w której można nie stosować wskazanej powyżej ogólnej zasady domyślności, jest sytuacja, gdy pojedynczy certyfikat X.509v3 jest stosowany przy wydawaniu różnych rodzajów tokenów usług zaufania, do których stosuje się różne systemy nadzoru/akredytacji, przykładowo pojedynczy certyfikat X.509v3 jest wykorzystywany przez CSP z jednej strony przy wydawaniu QC zgodnie z odpowiednim systemem nadzoru, a z drugiej strony przy wydawaniu certyfikatów niekwalifikowanych zgodnie z innym statusem nadzoru/akredytacji. We wskazanej sytuacji i przykładzie zastosowano by dwa wpisy z różnymi wartościami „Sti” (np. w podanym przykładzie odpowiednio CA/QC i CA/PKC) i takimi samymi wartościami „Sdi” (powiązany certyfikat X.509v3).

Implementacje zależą od ASN.1 lub XML i MUSZĄ być zgodne ze specyfikacją zawartą w ETSI TS 102231 (w odniesieniu do ASN.1 zob. załącznik A do ETSI TS 102231, a w odniesieniu do XML zob. załącznik B do ETSI TS 102231).

*Uwaga (2):* Jeżeli należy przedstawić dodatkowe informacje dotyczące „kwalifikacji” w odniesieniu do wpisu zidentyfikowanej usługi, wówczas w stosownych przypadkach operator systemu MUSI rozważyć zastosowanie rozszerzenia „additionalServiceInformation” (klauzula 5.8.2) pola „Service information extension” (klauzula 5.5.9) zgodnie z celem przedstawiania takich dodatkowych informacji dotyczących „kwalifikacji”. Ponadto operator systemu może fakultatywnie zastosować klauzulę 5.5.6 („Scheme service definition URI”).

Service current status (klauzula 5.5.4)

Pole to jest WYMAGANE i MUSI określać identyfikator statusu usługi przez jeden z następujących URI:

▼C2

— **Under Supervision** (podlega nadzorowi) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision),

— **Supervision of Service in Cessation** (nadzór usługi w fazie wstrzymania) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionincessation),

— **Supervision Ceased** (nadzór wstrzymany) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased),

— **Supervision Revoked** (nadzór wycofany) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked),

— **Accredited** (objęta akredytacją) (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited),

— **Accreditation Ceased** (akredytacja wstrzymana) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased),

— **Accreditation Revoked** (akredytacja wycofana) (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

W odniesieniu do niniejszej specyfikacji oficjalnego wykazu powyższe statusy MUSZĄ być interpretowane w następujący sposób:

— ***podlega nadzorowi:*** Usługa określona w polu „Service digital identity" (klauzula 5.5.3) świadczona przez podmiot świadczący usługi certyfikacyjne (CSP) zidentyfikowany w polu „TSP name"å (klauzula 5.4.1) podlega aktualnie nadzorowi pod względem zgodności z przepisami dyrektywy 1999/93/WE sprawowanemu przez państwo członkowskie określone w polu „Scheme territory" (klauzula 5.3.10), w którym CSP ma siedzibę lub miejsce zamieszkania,

▼M1

— ***nadzór usługi w fazie wstrzymania:*** Usługa określona w polu „Service digital identity" (klauzula 5.5.3) świadczona przez CSP zidentyfikowany w polu „TSP name" (klauzula 5.4.1) jest aktualnie w fazie wstrzymania, ale wciąż podlega nadzorowi do czasu wstrzymania lub wycofania nadzoru. Jeżeli osoba prawna inna niż ta zidentyfikowana w polu „TSP name" przejmuje odpowiedzialność za fazę wstrzymania, wówczas identyfikacja tej nowej lub rezerwowej osoby prawnej (rezerwowy CSP) MUSI być zapewniona w polu „Scheme service definition URI" (klauzula 5.5.6) i w rozszerzeniu pola „TakenOverBy" (klauzula L.3.2) wpisu usługi.

▼C1

— ***nadzór wstrzymany:*** Ważność oceny nadzoru upłynęła bez ponownej oceny usługi określonej w polu „Service digital identity" (klauzula 5.5.3). Od dnia nadania bieżącego statusu usługa nie podlega już nadzorowi, ponieważ uznaje się, że zakończono jej świadczenie,

— ***nadzór wycofany:*** Uprzednio nadzorowana usługa CSP i ewentualnie także sam CSP nie spełnia już wymogów przepisów dyrektywy 1999/93/WE, co zostało stwierdzone przez państwo członkowskie określone w polu „Scheme territory" (klauzula 5.3.10), w którym to państwie CSP ma siedzibę lub miejsce zamieszkania. W związku z powyższym zażądano zakończenia świadczenia usługi i ze względów wskazanych powyżej musi być ona uznawana za zakończoną.

*Uwaga (1):* Wartość statusu „nadzór wycofany" może być statusem ostatecznym, nawet jeżeli CSP całkowicie kończy następnie swoją działalność. W takiej sytuacji migracja do „nadzór usługi w fazie wstrzymania" lub „nadzór wstrzymany" jest niepotrzebna. Jedynym sposobem na dokonanie zmiany statusu „nadzór wycofany" jest powrót do spełniania wymogów dyrektywy 1999/93/WE zgodnie z odpowiednim systemem nadzoru obowiązującym w państwie członkowskim prowadzącym zaufaną listę oraz odzyskanie statusu „podlega nadzorowi". Status „nadzór usługi w fazie wstrzymania" lub status „nadzór wstrzymany" występuje tylko, gdy CSP bezpośrednio kończy świadczenie powiązanych usług podlegających nadzorowi, a nie w sytuacji, gdy nadzór wycofano,

— ***objęta akredytacją:*** Oceny akredytacji dokonał organ ds. akredytacji w imieniu państwa członkowskiego określonego w polu „Scheme territory" (klauzula 5.3.10), a usługa określona w polu „Service digital identity" (klauzula 5.5.3) świadczona przez CSP ([1]) zidentyfikowany w polu „TSP name" (klauzula 5.4.1) została uznana za zgodną z przepisami dyrektywy 1999/93/WE.

([1]) Należy zauważyć, że ten akredytowany CSP może mieć siedzibę lub miejsce zamieszkania w innym państwie członkowskim niż państwo określone w polu „Scheme territory" wdrożenia TSL zaufanej listy lub w kraju trzecim (zob. art. 7 ust. 1 lit. a) dyrektywy 1999/93/WE).

▼C1

*Uwaga (2)*: Jeżeli dwa statusy „akredytacja wycofana” i „akredytacja wstrzymana” zostaną użyte w odniesieniu do CSP wystawiającego QC wskazanego w polu „Scheme territory” (klauzula 5.3.10) MUSZĄ być one uznane za „status przejściowy” i NIE WOLNO ich stosować jako wartości „bieżącego statusu usługi”, a jeżeli zostaną jako takie zastosowane, wówczas w polach „informacje o historii zatwierdzenia usługi” lub „bieżący status usługi” MUSZĄ bezpośrednio poprzedzać status „podlega nadzorowi”., który ewentualnie może być poprzedzony dowolnym innym statusem nadzoru określonym powyżej i zobrazowanym na schemacie 1. Statusy „akredytacja wycofana” i „akredytacja wstrzymana” MOGĄ być zastosowane jako wartość „bieżącego statusu usługi”, jeżeli zostaną użyte w odniesieniu do CSP niewystawiającego QC, gdy występuje tylko towarzyszący system „akredytacji dobrowolnej” bez towarzyszącego systemu nadzoru lub w odniesieniu do CSP wystawiającego QC, gdy CSP nie ma siedziby lub miejsca zamieszkania w polu „Scheme territory” (klauzula 5.3.10) (np. w kraju trzecim),

— ***akredytacja wstrzymana:*** Ważność oceny akredytacji upłynęła bez przeprowadzenia ponownej oceny usługi określonej w polu „Service digital identity” (klauzula 5.5.3),

— ***akredytacja wycofana:*** Uznana uprzednio za zgodną z kryteriami systemu usługa określona w polu „Service digital identity” (klauzula 5.5.3) świadczona przez podmiot świadczący usługi certyfikacyjne (CSP) zidentyfikowany w polu „TSP name” (klauzula 5.4.1) i ewentualnie sam CSP nie spełnia już wymogów przepisów dyrektywy 1999/93/WE.

*Uwaga (3):* Dokładnie takie same wartości statusu muszą być zastosowane w odniesieniu do CSP wystawiających QC i CSP niewystawiających QC (np. podmioty świadczące usługi znakowania czasem wydające tokeny znacznika czasu, CSP wystawiające certyfikaty niekwalifikowane itp.). Pole „Service Type identifier” (klauzula 5.5.1) stosuje się do rozróżnienia mających zastosowanie systemów nadzoru/akredytacji.

*Uwaga (4):* Dodatkowe informacje dotyczące „kwalifikacji” związanych ze statusem określone na poziomie krajowych systemów nadzoru/akredytacji w odniesieniu do CPS niewystawiających QC MOGĄ być w stosownych przypadkach i w razie potrzeby udostępniane na poziomie usług (np. aby umożliwić rozróżnienie kilku poziomów jakości/bezpieczeństwa). Operatorzy systemu MUSZĄ stosować rozszerzenie „additionalServiceInformation” (klauzula 5.8.2) pola „Service information extension” (klauzula 5.5.9) zgodnie z celem przedstawienia tych dodatkowych informacji o „kwalifikacji”. Ponadto operator systemu może fakultatywnie zastosować klauzulę 5.5.6 („Scheme service definition URI”).

Current status starting date and time (klauzula 5.5.5)

Pole to jest WYMAGANE i MUSI określać datę oraz godzinę wejścia w życie bieżącego statusu zatwierdzenia (wartości daty i godziny zgodnie z definicją zawartą w klauzuli 5.1.4 ETSI TS 102231).

Scheme service definition URI (klauzula 5.5.6)

Pole to jest FAKULTATYWNE i jeżeli występuje, MUSI określać URI, gdzie strony bazujące na informacjach mogą uzyskać określone informacje dotyczące usługi, zapewniane przez operatora systemu w postaci sekwencji wielojęzycznych odnośników (w języku angielskim (EN) jako języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych).

W przypadku korzystania z przedmiotowego lub przedmiotowych URI MUSZĄ one określać ścieżkę do informacji opisujących usługe określoną w systemie. W szczególności w stosownych przypadkach MOŻE to dotyczyć:

a) URI wskazującego tożsamość rezerwowego CSP w przypadku nadzoru usługi w fazie wstrzymania, z którą związany jest rezerwowy CSP (zob. „Service current status” – klauzula 5.5.4);

▼C1

b) URI prowadzących do dokumentów, które zapewniają dodatkowe informacje związane z wykorzystaniem określonej w prawie krajowym kwalifikacji do świadczenia nadzorowanych/akredytowanych usług tworzenia rezerw w ramach tokena usługi zaufania zgodnie z wykorzystaniem pola „Service information extension" (klauzula 5.5.9) z rozszerzeniem „additionalServiceInformation" określonym w klauzuli 5.8.2.

Service supply points (klauzula 5.5.7)

Pole to jest FAKULTATYWNE i jeżeli występuje, MUSI określać URI, gdzie strony bazujące na informacjach mają dostęp do usługi za pośrednictwem sekwencji łańcuchów znaków, których składnia MUSI być zgodna z RFC 3986.

TSP service definition URI (klauzula 5.5.8)

Pole to jest FAKULTATYWNE i jeżeli występuje, MUSI określać URI, gdzie strony bazujące na informacjach mogą uzyskać informacje dotyczące usługi zapewniane przez TSP w postaci sekwencji wielojęzycznych odnośników (w języku angielskim (EN) jako języku obowiązkowym i ewentualnie w jednym lub w większej liczbie języków krajowych). Przedmiotowy lub przedmiotowe URI MUSZĄ określić ścieżkę dostępu do informacji opisujących usługę określoną przez TSP.

Service information extensions (klauzula 5.5.9)

W odniesieniu do niniejszej specyfikacji pole to jest FAKULTATYWNE, jednak MUSI występować w przypadkach, w których informacje zawarte w polu „Service digital identity" (klauzula 5.5.3) nie wystarczają, aby jednoznacznie zidentyfikować certyfikaty kwalifikowane wystawiane w ramach tej usługi, lub informacje zawarte we właściwych certyfikatach kwalifikowanych nie pozwalają na automatyczną identyfikację faktów dotyczących ustalenia, czy QC jest obsługiwany przez SSCD ([1]).

W odniesieniu do niniejszej specyfikacji, w przypadku, w którym użycie pola jest WYMAGANE, np. do celów usług CA/QC, zgodnie z rozszerzeniem „kwalifikacje" określonym w załączniku L.3.1 do ETSI TS 102231 fakultatywne pole informacyjne „Service information extensions" („Sie") MUSI być stosowane i organizowane w formie sekwencji jednej lub większej liczby krotek, z których każda zawiera:

— (filtry) informacje wykorzystywane do dalszej identyfikacji – zgodnie z usługą certyfikacyjną zidentyfikowaną w polu „Sdi" – tej określonej usługi (tj. zbioru certyfikatów kwalifikowanych), w odniesieniu do której wymagane/udzielane są dodatkowe informacje dotyczące obsługi przez SSCD lub jej braku (lub wystawienia certyfikatu osobie prawnej), oraz

— informacje powiązane („kwalifikatory") pozwalające ustalić, czy dodatkowo zidentyfikowany zbiór usług w postaci certyfikatów kwalifikowanych, jest obsługiwany przez SSCD (jeżeli informacja ta ma postać „QCSSCDStatusAsInCert", oznacza to, że informacje powiązane stanowią część QC zgodnie ze znormalizowaną według ETSI formą nadającą się do przetwarzania automatycznego ([2]), lub informacji dotyczących faktu, że takie QC wystawiane są osobom prawnym (domyślnie uznaje się, że są wystawiane wyłącznie osobom fizycznym),

— QCWithSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD) oznacza, że CSP gwarantuje, a państwo członkowskie (odpowiednio organ ds. nadzoru lub organ ds. akredytacji) to kontroluje (model nadzoru) lub poddaje audytowi (model akredytacji), że wszelkie QC wystawione w ramach usługi (QCA) określonej w polu „Service digital identity" (klauzula 5.5.3) i dodatkowo zidentyfikowanej przez powyższe (filtry) informacje wykorzystywane do dalszej identyfikacji w ramach usługi certyfikacyjnej zidentyfikowanej w polu „Sdi" tego określonego zbioru certyfikatów kwalifikowanych, w odniesieniu do których wymagane są dodatkowe informacje dotyczące obsługi przez SSCD lub jej braku, SĄ obsługiwane przez SSCD (tj. że klucz prywatny związany z kluczem publicznym w certyfikacie jest przechowywany w bezpiecznym urządzeniu służącym do składania podpisu, zgodnie z załącznikiem III dyrektywy 1999/93/WE),

([1]) Zob. część 2.2 niniejszego dokumentu.

([2]) Dotyczy to właściwej kombinacji określonych w ETSI poświadczenia o zgodności certyfikatu kwalifikowanego, poświadczeń o wystawieniu certyfikatu kwalifikowanego z użyciem bezpiecznego urządzenia służącego do składania podpisu [ETSI TS 101 862] lub identyfikatorów obiektów QCP/QCP + określonych w ETSI [ETSI TS 101 456].

▼C1

— QCNoSSCD (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD) oznacza, że CSP gwarantuje, a państwo członkowskie (odpowiednio organ ds. nadzoru lub organ ds. akredytacji) to kontroluje (model nadzoru) lub poddaje audytowi (model akredytacji), że wszelkie QC wystawione w ramach usługi (RootCA/QC lub CA/QC) określonej w polu „Service digital identity" (klauzula 5.5.3) i dodatkowo zidentyfikowanej przez powyższe (filtry) informacje wykorzystywane do dalszej identyfikacji w ramach usługi certyfikacyjnej zidentyfikowanej w polu „Sdi" określonego zbioru certyfikatów kwalifikowanych, w odniesieniu do których wymagane są dodatkowe informacje dotyczące obsługi przez SSCD lub jej braku, NIE SĄ obsługiwane przez SSCD (tj. że klucz prywatny związany z kluczem publicznym w certyfikacie nie jest przechowywany w bezpiecznym urządzeniu służącym do składania podpisu, zgodnie z załącznikiem III dyrektywy 1999/93/WE),

— QCSSCDStatusAsInCert (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert) oznacza, że CSP gwarantuje, a państwo członkowskie (odpowiednio organ ds. nadzoru lub organ ds. akredytacji) to kontroluje (model nadzoru) lub poddaje audytowi (model akredytacji), że wszelkie QC wystawione w ramach usługi (CA/QC) określonej w polu „Service digital identity" (klauzula 5.5.3) i dodatkowo zidentyfikowanej przez powyższe (filtry) informacje wykorzystywane do dalszej identyfikacji w ramach usługi certyfikacyjnej zidentyfikowanej w polu „Sdi" określonego zbioru certyfikatów kwalifikowanych, w odniesieniu do których wymagane są dodatkowe informacje dotyczące obsługi przez SSCD lub jej braku, MUSI zawierać informacje nadające się do automatycznego przetwarzania, które wskazują, czy certyfikat kwalifikowany jest obsługiwany przez SSCD,

— QCForLegalPerson (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): oznacza, że CSP gwarantuje, a państwo członkowskie (odpowiednio organ ds. nadzoru lub organ ds. akredytacji) kontroluje (model nadzoru) lub poddaje audytowi (model akredytacji), że wszelkie QC wystawione w ramach usługi (QCA) określonej w polu „Service digital identity" (klauzula 5.5.3) i dodatkowo zidentyfikowanej przez powyższe (filtry) informacje wykorzystywane do dalszej identyfikacji w ramach usługi certyfikacyjnej zidentyfikowanej w polu „Sdi" określonego zbioru certyfikatów kwalifikowanych, w odniesieniu do których wymagane są dodatkowe informacje dotyczące wystawienia certyfikatu osobie prawnej, SĄ wystawiane osobom prawnym.

Kwalifikatory te można wykorzystywać jako rozszerzenia wyłącznie w przypadku, w którym rodzajem usługi jest http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Pole to jest zależne od implementacji (ASN.1 lub XML) i MUSI spełniać wymagania specyfikacji określonej w załączniku L.3.1 do ETSI TS 102231.

▼M1

W odniesieniu do implementacji XML charakterystyczna treść dodatkowych informacji musi być kodowana przy pomocy plików xsd zamieszczonych w załączniku C do ETSI TS 102 231.

▼C1

**Service Approval History**

Pole to jest FAKULTATYWNE, ale MUSI występować, jeżeli pole „Historical information period" (klauzula 5.3.12) jest niezerowe. W kontekście niniejszej specyfikacji system MUSI zatem zachowywać informacje historyczne. W przypadku, w którym informacje historyczne mają być zachowane, ale usługa nie zawiera historii sprzed bieżącego statusu (tj. pierwszego zapisanego statusu lub informacji historycznej, które nie zostały zachowane przez operatora systemu), pole to MUSI być puste. W przeciwnym wypadku dla każdej zmiany w bieżącym statusie usługi podmiotu świadczącego usługi zaufania, która zaszła w trakcie okresu informacji historycznych zgodnie z ETSI TS 102231, klauzula 5.3.12, informacje dotyczące wcześniejszych statusów zatwierdzeń MUSZĄ być podane w porządku malejącym według daty i godziny zmiany statusu (tj. data i godzina, w których wchodzi w życie kolejny status zatwierdzania).

▼C1

Sekwencja informacji historycznych MUSI mieć formę określoną poniżej.

***TSP(1) Service(1) History(1)***

Service type identifier (klauzula 5.6.1)

Pole to jest WYMAGANE i MUSI określać identyfikator rodzaju usługi razem z formatem i znaczeniem zastosowanymi w polu „TSP Service Information – Service type identifier" (klauzula 5.5.1).

Service name (klauzula 5.6.2)

Pole to jest WYMAGANE i MUSI określać nazwę, w ramach której CSP świadczył usługi określone w polu „TSP Service Information – Service type identifier" (klauzula 5.5.1), razem z formatem i znaczeniem zastosowanymi w polu „TSP Service Information – Service name" (klauzula 5.5.2). Klauzula ta nie wymaga, by nazwa była identyczna z nazwą określoną w klauzuli 5.5.2. Zmiana nazwy MOŻE być jedną z okoliczności wymagających nowego statusu.

▼M1

Service digital identity (klauzula 5.6.3)

Pole to jest WYMAGANE i MUSI określać co najmniej jedną reprezentację identyfikatora cyfrowego (tj. certyfikat X.509v3) stosowanego w polu „TSP Service Information – Service digital identity" (klauzula 5.5.3) w formacie i ze znaczeniem określonymi w ETSI TS 102 231, klauzula 5.5.3.

Uwaga: W przypadku wartości certyfikatu X.509v3 stosowanej w klauzuli 5.5.3 „Sdi" usługi, na zaufanej liście może być tylko pojedynczy wpis usługi dla wartości „Sti:Sie/additionalServiceInformation". Informacja „Sdi" (klauzula 5.6.3) stosowana w informacjach o historii zatwierdzenia usługi powiązana z wpisem usługi i informacja „Sdi" (klauzula 5.5.3) stosowana w tym wpisie usługi MUSZĄ odnosić się do tej samej wartości certyfikatu X.509v3. Gdy usługa wymieniona na liście zmienia swoje „Sdi" (tj. odnowienie lub ponowne wprowadzenie certyfikatu X.509v3 dla np. CA/PKC lub CA/QC) lub tworzy nowe „Sdi" dla danej usługi, nawet w przypadku identycznych wartości dla powiązanych „Sti", „Sn" i [„Sie"], oznacza to, że Scheme Operator MUSI stworzyć wpis usługi inny niż poprzedni wpis.

▼C1

Service previous status (klauzula 5.6.4)

Pole to jest WYMAGANE i MUSI określać identyfikator wcześniejszego statusu usługi razem z formatem i znaczeniem zastosowanymi w polu „TSP Service Information – Service current status" (klauzula 5.5.4).

Previous status starting date and time (klauzula 5.6.5)

Pole to jest WYMAGANE i MUSI określać datę oraz godzinę wejścia w życie określonego wcześniejszego statusu razem w formatem i znaczeniem zastosowanymi w polu „TSP Service Information – Service current status starting date and time" (klauzula 5.5.5).

Service information extensions (klauzula 5.6.6)

Pole to jest FAKULTATYWNE i MOŻE być wykorzystane przez operatorów systemu w celu zapewnienia informacji związanych z usługą razem z formatem i znaczeniem zastosowanymi w polu „TSP Service Information – Service information extensions" (klauzula 5.5.9).

▼C1

***TSP(1) Service(1) History(2)***

To samo dla: TSP(1) Service(1) History(2) (przed History 1)

…

*TSP(1) Service(2)*

To samo dla: TSP(1) Service 2 (odpowiednio)

TSP(1) Service(2) History(1)

…

*TSP(2) Information*

To samo dla: TSP 2 (odpowiednio)

To samo dla: TSP 2 Service 1

To samo dla: TSP 2 Service 1 History 1

…

▼M1

**Signed TSL**

Czytelna dla człowieka postać wdrożenia TLS zaufanej listy ustanowiona zgodnie z niniejszą specyfikacją, a w szczególności z rozdziałem IV, POWINNA zostać podpisana przez „Scheme operator name" (klauzula 5.3.4) w celu zapewnienia jej autentyczności oraz integralności ([1]). Format podpisu POWINIEN mieć postać PAdES part 3 (ETSI TS 102 778-3 ([2])), jednak MOŻE mieć postać PAdES part 2 (ETSI TS 102 778-2 ([3])) w kontekście szczegółowego modelu zaufania ustanowionego poprzez publikację certyfikatów stosowanych do podpisywania zaufanych list.

Przetwarzalna maszynowo wersja wdrożenia TSL zaufanej listy ustanowiona zgodnie z niniejszą specyfikacją MUSI zostać podpisana przez „Scheme operator name" (klauzula 5.3.4) w celu zapewnienia jej autentyczności oraz integralności. Format przetwarzalnej maszynowo wersji wdrożenia TSL zaufanej listy ustanowiony zgodnie z niniejszą specyfikacją MUSI mieć postać XML i MUSI być zgodny ze specyfikacją zawartą w załącznikach B i C do ETSI TS 102 231.

Format podpisu MUSI mieć postać XAdES BES lub EPES zgodnie ze specyfikacją ETSI TS 101 903 dla implementacji XML. Tego rodzaju implementacja podpisu elektronicznego MUSI spełniać wymogi zawarte w załączniku B do ETSI TS 102 231 ([4]). Dodatkowe ogólne wymogi dotyczące przedmiotowego podpisu zostały określone w następujących częściach.

▼C1

Scheme identification (klauzula 5.7.2)

Pole to jest WYMAGANE i MUSI określać odniesienie przydzielone przez operatora systemu, które jednoznacznie identyfikuje system opisany w niniejszej specyfikacji i w ustanowionej TSL, oraz MUSI być uwzględnione przy obliczaniu podpisu. Oczekuje się, że będzie to ciąg znaków lub ciąg bitów.

([1]) W przypadku, w którym czytelna dla człowieka wersja wdrożenia TSL zaufanej listy nie jest podpisana, jej autentyczność oraz integralność MUSI być zagwarantowana przez odpowiedni kanał komunikacyjny o równoważnym poziomie bezpieczeństwa. W tym celu zaleca się stosowanie TLS (IETF RFC 5246: „The Transport Layer Security (TLS) Protocol Version 1.2"), a państwo członkowskie MUSI użytkownikom TSL udostępnić z pasma unikalny identyfikator certyfikatu kanału TLS.

([2]) ETSI TS 102 778-3 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 – Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000-1.

([4]) Ochrona operatora systemu podpisującego certyfikat z użyciem podpisu w jeden ze sposobów określonych w ETSI TS 101 903 jest obowiązkowa, a ds:keyInfo powinien zawierać w stosownych przypadkach odpowiedni łańcuch certyfikatów.

▼M1

W odniesieniu do niniejszej specyfikacji przydzielone odniesienia MUSZĄ obejmować pola „TSL type” (klauzula 5.3.3), „Scheme name” (klauzula 5.3.6) oraz wartości rozszerzenia SubjectKeyIdentifier certyfikatu używanego przez operatora systemu do złożenia podpisu elektronicznego na TSL.

▼C1

Signature algorithm identifier (klauzula 5.7.3)

Pole to jest wymagane i MUSI określać algorytm kryptograficzny, którego użyto do utworzenia podpisu. Pole to MOŻE wymagać dodatkowych parametrów, w zależności od użytego algorytmu. Pole to MUSI zostać uwzględnione przy obliczaniu podpisu.

Signature value (klauzula 5.7.4)

Pole to jest WYMAGANE i MUSI zawierać rzeczywistą wartość podpisu cyfrowego. Wszystkie pola TSL (z wyjątkiem samej wartości podpisu) MUSZĄ zostać uwzględnione przy obliczaniu podpisu.

TSL extensions (klauzula 5.8)

Rozszerzenie **expiredCertsRevocationInfo** (klauzula 5.8.1)

Rozszerzenie to jest FAKULTATYWNE. Jeżeli jest używane, MUSI spełniać wymagania specyfikacji ETSI TS 102231, klauzula 5.8.1.

Roezszerzenie **additionalServiceInformation** (klauzula 5.8.2)

Jest to rozszerzenie FAKULTATYWNE, które, jeżeli jest używane, MUSI być stosowane wyłącznie na poziomie usług i wyłącznie w polu określonym w klauzuli 5.5.9 („Service information extension”). Rozszerzenie to jest używane w celu zapewnienia dodatkowych informacji dotyczących usługi. MUSI to być sekwencja jednej lub większej liczby krotek, z których każda zawiera:

a) URI określający dodatkowe informacje, np.:

   — URI wskazujący niektóre szczególne, określone w prawie krajowym kwalifikacje do świadczenia nadzorowanych/akredytowanych usług tworzenia rezerw w ramach tokena usługi zaufania, np.:

      — szczególny poziom rozdrobnienia ochrony/jakości w odniesieniu do systemu krajowego nadzoru/akredytacji dla CSP niewystawiających QC (np. RGS */**/*** w FR, szczególny status „nadzorczy” ustanowiony przez prawodawstwo krajowe w odniesieniu do szczególnych CSP wystawiających QC w DE), zob. uwaga (4) do „Service current status” – klauzula 5.5.4,

      — lub szczególny status prawny dla świadczenia nadzorowanych/akredytowanych usług tworzenia rezerw w ramach tokena usługi zaufania (np. określony w prawie krajowym kwalifikowany TST, jak ma to miejsce w przypadku DE lub HU),

      — lub znaczenie szczególnego identyfikatora polityki występującego w przypadku certyfikatu X.509v3 określonego w polu „Sdi”,

   — lub zarejestrowany URI określony w polu „Service type identifier”, klauzula 5.5.1, w celu dalszego określenia uczestnictwa usługi zidentyfikowanej w polu „Sti” jako usługi składowej w ramach podmiotu świadczącego usługi certyfikacyjne wystawiającego QC (np. OCSP-QC, CRL-QC i RootCA-QC);

b) fakultatywny łańcuch zawierający wartość serviceInformation, znaczenie określone w systemie (np. *, ** lub ***);

c) jakiekolwiek fakultatywne dodatkowe informacje podane w formacie właściwym dla systemu.

▼M1

Odwołanie URI POWINNO prowadzić do informacji czytelnych dla człowieka (minimum w języku angielskim i ewentualnie w jednym lub więcej języku narodowym), które uznano za właściwe i wystarczające do zrozumienia rozszerzenia przez stronę ufającą, a w szczególności które wyjaśniają znaczenie danych URIs, określając możliwe wartości dla serviceInformation i znaczenie dla każdej wartości.

Qualifications Extension (klauzula L.3.1)

Opis: Pole to jest FAKULTATYWNE, ale MUSI występować w przypadkach, w których jego użycie jest WYMAGANE, np. dla usług RootCA/QC lub CA/QC, oraz jeżeli:

— informacje zawarte w polu „Service digital identity" nie są wystarczające, by jednoznacznie zidentyfikować certyfikaty kwalifikowane wystawiane przez daną usługę,

— informacje zawarte we właściwych certyfikatach kwalifikowanych nie pozwalają na automatyczną identyfikację faktów dotyczących ustalenia, czy QC jest obsługiwany przez SSCD.

Jeżeli dane rozszerzenie poziomu usługi jest używane, MUSI być używane tylko w polu określonym w polu „Service information extension" (klauzula 5.5.9) i MUSI być zgodne ze specyfikacjami określonymi w załączniku L.3.1 do ETSI TS 102 231.

TakenOverBy Extension (klauzula L.3.2)

Opis: Rozszerzenie to jest FAKULTATYWNE, ale MUSI występować w przypadkach, w których usługa, za którą odpowiedzialność prawną ponosił kiedyś CSP, zostaje przejęta przez inny TSP i ma stwierdzać formalnie odpowiedzialność prawną za usługę oraz umożliwiać oprogramowaniu weryfikującemu pokazywanie użytkownikowi niektórych szczegółów prawnych. Informacje przedstawione w niniejszym rozszerzeniu MUSZĄ być spójne z powiązanym stosowaniem klauzuli 5.5.6 i MUSZĄ być zgodne ze specyfikacjami w załączniku L.3.2 do ETSI TS 102 231.

▼M1

ROZDZIAŁ II

Ustanawiając zaufane listy, państwa członkowskie będą stosowały:

kody języka małymi literami i kody krajów dużymi literami;

kody języka i kraju zgodnie z tabelą zamieszczoną poniżej;

Jeżeli występuje alfabet łaciński (z właściwym kodem języka), dodaje się transliterację w alfabecie łacińskim wraz z powiązanymi kodami języka określonymi w poniższej tabeli.

| Nazwa skrócona (w języku źródłowym) | Nazwa skrócona (w języku angielskim) | Kod kraju | Kod języka | Uwagi | Transliteracja łacińska |
|---|---|---|---|---|---|
| Belgique/België | Belgium | BE | nl, fr, de | | |
| България (*) | Bulgaria | BG | bg | | bg-Latn |
| Česká republika | Czech Republic | CZ | cs | | |
| Danmark | Denmark | DK | da | | |
| Deutschland | Germany | DE | de | | |
| Eesti | Estonia | EE | et | | |
| Éire/Ireland | Ireland | IE | ga, en | | |
| Ελλάδα (*) | Greece | EL | el | Kod kraju zalecany przez UE | el-Latn |
| España | Spain | ES | es | również kataloński (ca), baskijski (eu), galicyjski (gl) | |
| France | France | FR | fr | | |

▼M2

| | | | | | |
|---|---|---|---|---|---|
| Hrvatska | Croatia | HR | hr | | |

▼M1

| | | | | | |
|---|---|---|---|---|---|
| Italia | Italy | IT | it | | |
| Κύπρος/Kıbrıs (*) | Cyprus | CY | el, tr | | el-Latn |
| Latvija | Latvia | LV | lv | | |
| Lietuva | Lithuania | LT | lt | | |
| Luxembourg | Luxembourg | LU | fr, de, lb | | |
| Magyarország | Hungary | HU | hu | | |
| Malta | Malta | MT | mt, en | | |
| Nederland | Netherlands | NL | nl | | |
| Österreich | Austria | AT | de | | |
| Polska | Poland | PL | pl | | |
| Portugal | Portugal | PT | pt | | |
| România | Romania | RO | ro | | |

▼**M1**

| Nazwa skrócona (w języku źródłowym) | Nazwa skrócona (w języku angielskim) | Kod kraju | Kod języka | Uwagi | Transliteracja łacińska |
|---|---|---|---|---|---|
| Slovenija | Slovenia | SI | sl | | |
| Slovensko | Slovakia | SK | sk | | |
| Suomi/Finland | Finland | FI | fi, sv | | |
| Sverige | Sweden | SE | sv | | |
| United Kingdom | United Kingdom | UK | en | Kod kraju zalecany przez UE | |
| Ísland | Iceland | IS | is | | |
| Liechtenstein | Liechtenstein | LI | de | | |
| Norge/Noreg | Norway | NO | no, nb, nn | | |

(*) transliteracja łacińska: България = Bulgaria; Ελλάδα = Elláda; Κύπρος = Kýpros.

———————

▼C1

ROZDZIAŁ IV

**SPECYFIKACJA CZYTELNEJ DLA CZŁOWIEKA POSTACI WDROŻENIA TSL ZAUFANEJ LISTY**

Czytelna dla człowieka postać wdrożenia TSL zaufanej listy MUSI być dostępna powszechnie oraz dostępna drogą elektroniczną. POWINNA być udostępniona w postaci dokumentu w formacie PDF zgodnie z ISO 32000, a dokument ten MUSI być sformatowany zgodnie z profilem PDF/A (ISO 19005).

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

▼M1

— tytuł zaufanych list w postaci czytelnej dla człowieka musi być tworzony jako konkatenacja następujących elementów:

  — fakultatywnie symbol flagi państwowej państwa członkowskiego,

  — pusta przestrzeń,

  — skrócona nazwa kraju w języku źródłowym (językach źródłowych) (jak przedstawiono w pierwszej kolumnie tabeli w rozdziale II),

  — pusta przestrzeń,

  — „(”;

  — skrócona nazwa kraju w języku angielskim (jak przedstawiono w drugiej kolumnie tabeli w rozdziale II) w nawiasach okrągłych,

  — „):” jako nawias zamykający i znak rozdzielający,

  — pusta przestrzeń,

  — „Trusted List”,

  — fakultatywnie logo operatora systemu państwa członkowskiego,

▼C1

— struktura czytelnej dla człowieka formy POWINNA odzwierciedlać model logiczny opisany w części 5.1.2 ETSI TS 102231,

— każde pole POWINNO być widoczne i POWINNO zawierać:

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

  — wartość pola (np. „CA/QC”),

  — znaczenie (opis) wartości pola w stosownych przypadkach oraz w szczególności zgodnie z postanowieniami załącznika D do ETSI TS 102231 lub zgodnie z niniejszą specyfikacją dla zarejestrowanych URI (np. „urząd certyfikacji wystawiający certyfikaty kluczy publicznych”),

  — w stosownych przypadkach liczne wersje języków naturalnych zgodnie z wdrożeniem TSL zaufanej listy,

— 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,

  — numer seryjny,

  — algorytm podpisu,

  — wydawca,

  — ważne od,

  — ważne do,

  — podmiot,

▼C1

— klucz publiczny,

— polityka certyfikacji,

— identyfikator klucza podmiotu,

— punkty dystrybucji CRL,

— identyfikator klucza urzędu,

— użycie klucza,

— podstawowe warunki ograniczające,

— algorytm odcisku palca,

— odcisk palca,

— postać czytelna dla człowieka POWINNA być łatwa do wydrukowania,

— postać czytelna dla człowieka MOŻE być podpisywana za pomocą podpisu elektronicznego. Jeżeli jest podpisywana, MUSI zostać podpisana przez operatora systemu zgodnie z taką samą specyfikacją podpisu, jak w przypadku wdrożenia TSL zaufanej listy.