# DECYZJA KOMISJI

## z dnia 28 lipca 2010 r.

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

*(notyfikowana jako dokument nr C(2010) 5063)*

**(Tekst mający znaczenie dla EOG)**

(2010/425/UE)

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

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

a także mając na uwadze, co następuje:

(1) Transgraniczne stosowanie zaawansowanych podpisów elektronicznych weryfikowanych certyfikatem kwalifikowanym stworzonych z użyciem lub bez użycia bezpiecznego urządzenia służącego do składania podpisu elektronicznego zostało ułatwione dzięki decyzji Komisji 2009/767/WE z dnia 16 października 2009 r. ustanawiającej środki ułatwiające korzystanie z procedur realizowanych drogą elektroniczną poprzez pojedyncze punkty kontaktowe zgodnie z dyrektywą 2006/123/WE Parlamentu Europejskiego i Rady dotyczącą usług na rynku wewnętrznym [2], która to decyzja 2009/767/WE zobowiązuje państwa członkowskie do udostępnienia informacji niezbędnych do weryfikacji takich podpisów elektronicznych. Państwa członkowskie muszą w szczególności udostępnić na swoich tak zwanych „zaufanych listach" informacje dotyczące nadzorowanych/akredytowanych przez nie podmiotów świadczących usługi certyfikacyjne i powszechnie wystawiających certyfikaty kwalifikowane zgodnie z dyrektywą Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych [3] oraz informacje dotyczące usług świadczonych przez te podmioty.

(2) W Europejskim Instytucie Norm Telekomunikacyjnych zorganizowano szereg badań praktycznych mających na celu umożliwienie państwom członkowskim sprawdzenia zgodności ich zaufanych list ze specyfikacjami określonymi w załączniku do decyzji 2009/767/WE. Przedmiotowe badania wykazały, że konieczne jest wprowadzenie pewnych zmian technicznych w specyfikacjach technicznych znajdujących się w załączniku do decyzji 2009/767/WE w celu zapewnienia funkcjonujących i interoperacyjnych zaufanych list.

(3) Powyższe badania potwierdziły również potrzebę publicznego udostępnienia przez państwa członkowskie nie tylko zaufanych list w wersji czytelnej dla człowieka, zgodnie z wymogiem przewidzianym w decyzji 2009/767/WE, ale również list w wersji przetwarzalnej maszynowo. Ręczne korzystanie z zaufanych list w wersji czytelnej dla człowieka może być stosunkowo skomplikowane i czasochłonne, jeżeli w państwach członkowskich istnieje wiele podmiotów świadczących usługi certyfikacyjne. Publikowanie zaufanych list w wersji przetwarzalnej maszynowo ułatwi ich stosowanie poprzez umożliwienie automatycznego przetwarzania list, a tym samym zwiększy zakres ich stosowania w publicznych usługach elektronicznych.

(4) W celu ułatwienia dostępu do krajowych zaufanych list państwa członkowskie powinny przekazać Komisji informacje dotyczące umiejscowienia i ochrony ich zaufanych list. Komisja powinna udostępnić te informacje pozostałym państwom członkowskim w bezpieczny sposób.

(5) W celu umożliwienia automatycznego stosowania list i ułatwienia dostępu do nich należy uwzględnić wyniki wspomnianych badań praktycznych dotyczących zaufanych list państw członkowskich.

(6) Należy zatem odpowiednio zmienić decyzję 2009/767/WE.

(7) W celu umożliwienia państwom członkowskim przeprowadzenia wymaganych zmian technicznych w aktualnych zaufanych listach niniejszą decyzję należy stosować od dnia 1 grudnia 2010 r.

(8) Środki przewidziane w niniejszej decyzji są zgodne z opinią komitetu ds. dyrektywy o usługach,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

*Artykuł 1*

**Zmiany w decyzji 2009/767/WE**

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

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

1) w art. 2 wprowadza się następujące zmiany:

a) ust. 2 otrzymuje brzmienie:

„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.";

b) wprowadza się ust. 2a w brzmieniu:

„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.";

c) ust. 3 otrzymuje brzmienie:

„3. Państwa członkowskie przekazują Komisji informacje o:

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

d) dodaje się ust. 4 w brzmieniu:

„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.";

2) w załączniku wprowadza się zmiany określone w załączniku do niniejszej decyzji.

*Artykuł 2*

**Stosowanie**

Niniejszą decyzję stosuje się od dnia 1 grudnia 2010 r.

*Artykuł 3*

**Adresaci**

Niniejsza decyzja skierowana jest do państw członkowskich.

Sporządzono w Brukseli dnia 28 lipca 2010 r.

*W imieniu Komisji*

Michel BARNIER

*Członek Komisji*

*ZAŁĄCZNIK*

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

1) w rozdziale I wprowadza się następujące zmiany:

a) akapit drugi, zdanie pierwsze i drugie otrzymują brzmienie:

„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.";

b) skreśla się akapit drugi sekcji „TSL tag (klauzula 5.2.1)";

c) akapit po tytule sekcji „TSL sequence number (klauzula 5.3.2)" otrzymuje brzmienie:

„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.«";

d) akapit pierwszy po tytule sekcji „TSL type (klauzula 5.3.3)" otrzymuje brzmienie:

„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).";

e) akapit trzeci po tytule sekcji „TSL type (klauzula 5.3.3)" otrzymuje brzmienie:

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

f) akapit drugi, zdanie drugie po tytule sekcji „Scheme operator name (klauzula 5.3.4)" otrzymuje brzmienie:

„Wyznaczenie Scheme operator wdrożenia TSL zaufanej listy w państwie członkowskim jest sprawą tego państwa.";

g) akapit czwarty po tytule sekcji „Scheme operator name (klauzula 5.3.4)" otrzymuje brzmienie:

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

h) tiret czwarte po tytule sekcji „Scheme name (klauzula 5.3.6)" otrzymuje brzmienie:

„»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;"

i) akapit pierwszy po tytule sekcji „Service type identifier (klauzula 5.5.1)" otrzymuje brzmienie:

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

j) tiret piąte po tytule sekcji „Service current status (klauzula 5.5.4)" otrzymuje brzmienie:

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

k) tiret dziewiąte po tytule sekcji „Service current status (klauzula 5.5.4)" otrzymuje brzmienie:

„— **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.";

l) akapit piąty po tytule sekcji „Service information extensions (klauzula 5.5.9)" otrzymuje brzmienie:

„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.";

m) sekcja zatytułowana „Service digital identity (klauzula 5.6.3)" otrzymuje brzmienie:

„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.";

n) sekcja zatytułowana „Signed TSL" otrzymuje brzmienie:

„**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 (*). Format podpisu POWINIEN mieć postać PAdES part 3 (ETSI TS 102 778-3 (**)), jednak MOŻE mieć postać PAdES part 2 (ETSI TS 102 778-2 (***)) 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 (****). Dodatkowe ogólne wymogi dotyczące przedmiotowego podpisu zostały określone w następujących częściach.

---

(*) 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.

(**) 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.

(***) 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.

(****) 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.";

o) akapit drugi po tytule sekcji „Scheme identification (klauzula 5.7.2)" otrzymuje brzmienie:

„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.";

p) akapit drugi po tytule sekcji „additionalServiceInformation Extension (klauzula 5.8.2)" otrzymuje brzmienie:

„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.";

q) sekcja zatytułowana „Qualifications Extension (klauzula L.3.1)" otrzymuje brzmienie:

„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.";

r) po sekcji Qualifications Extension (klauzula L.3.1) wprowadza się sekcję TakenOverBy Extension (klauzula L 3.2) w brzmieniu:

„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.";

2) rozdział II otrzymuje brzmienie:

„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 | | |
| Italia | Italy | IT | it | | |
| Κύπρος/Kıbrıs (*) | Cyprus | CY | el, tr | | el-Latn |
| Latvija | Latvia | LV | lv | | |

| Nazwa skrócona (w języku źródłowym) | Nazwa skrócona (w języku angielskim) | Kod kraju | Kod języka | Uwagi | Transliteracja łacińska |
|---|---|---|---|---|---|
| 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 | | |
| 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.";

3) skreśla się rozdział III;

4) w rozdziale IV po zdaniu wprowadzającym „Zawartość opartej na pliku PDF/A czytelnej dla człowieka postaci wdrożenia TSL zaufanej listy POWINNA spełniać następujące wymogi:" wprowadza się tiret w brzmieniu:

„— 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;".