

UNIZETO



**POWSZECHNE
CENTRUM CERTYFIKACJI**

Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM

**Załącznik nr 3: Wskazówki dotyczące
wydawania certyfikatów o podwyższonej
wiarygodności Extended Validation SSL**

Wersja 3.2

Data: 9 luty 2011

Status: poprzedni

Unizeto Technologies S.A.
„CERTUM – Powszechne Centrum Certyfikacji”
21 Królowej Korony Polskiej, street
70-486 Szczecin
<http://www.certum.pl>

Spis treści

| | |
|---|-----------|
| A. WPROWADZENIE..... | 1 |
| 1. Wprowadzenie..... | 1 |
| B. PODSTAWOWE ZAŁOŻENIA CERTYFIKATU EV SSL | 2 |
| 2. Zastosowanie certyfikatów EV SSL | 2 |
| 3. Gwarancje i oświadczenia | 3 |
| C. ŚRODOWISKO I ZASTOSOWANIE | 6 |
| 4. Wydawanie certyfikatów EV SSL | 6 |
| 5. Otrzymanie certyfikatu EV SSL | 7 |
| D. ZAWARTOŚĆ I PROFIL CERTYFIKATU EV SSL | 11 |
| 6. Wymagania dotyczące zawartości certyfikatu EV SSL | 11 |
| 7. Wymagania dotyczące polityki certyfikatów EV SSL..... | 13 |
| 8. Maksymalny okres ważności | 14 |
| 9. Pozostałe wymagania techniczne dla certyfikatów EV SSL | 15 |
| E. WYMAGANIA DOTYCZĄCE ZAMÓWIENIA CERTYFIKATU EV SSL | 16 |
| 10. Wymagania ogólne..... | 16 |
| 11. Wymagania dotyczące Wniosku o wydanie certyfikatu EV SSL..... | 17 |
| 12. Wymagania dotyczące Umowy z Subskrybentem | 18 |
| F. WYMAGANIA DOTYCZĄCE WERYFIKACJI INFORMACJI..... | 20 |
| 13. Wymagania ogólne..... | 20 |
| 14. Weryfikacja formy prawnej oraz tożsamości Subskrybenta..... | 21 |
| 15. Weryfikacja adresu Zamawiającego..... | 23 |
| 16. Weryfikacja działalności gospodarczej Zamawiającego..... | 25 |
| 17. Weryfikacja domeny Subskrybenta..... | 25 |
| 18. Weryfikacja tożsamości, charakteru piastowanych stanowisk oraz upoważnień udzielonych Osobie Podpisującej Umowę i Osobie Zatwierdzającej Certyfikat | 27 |
| 19. Weryfikacja podpisu pod Umową z Subskrybentem i Wnioskiem o wydanie certyfikatu EV SSL..... | 30 |
| 20. Weryfikacja zatwierdzenia Wniosku o wydanie certyfikatu EV SSL | 31 |
| 21. Weryfikacja Źródeł Informacji Pewnej..... | 32 |
| 22. Pozostałe wymagania dotyczące weryfikacji..... | 37 |
| 23. Podwójna weryfikacja | 38 |
| 24. Wymagania dotyczące odnowień certyfikatów EV SSL | 38 |
| G. STATUS ORAZ UNIEWAŻNIENIE CERTYFIKATU EV SSL..... | 39 |
| 25. Sprawdzenie statusu certyfikatu EV SSL..... | 39 |
| 26. Unieważnianie certyfikatów EV SSL | 40 |
| 27. Zgłaszanie problemów z certyfikatami EV SSL | 41 |
| H. PRACOWNICY I STRONY TRZECIE..... | 42 |
| 28. Wiarygodność i kompetencje..... | 42 |
| 29. Punkty Rejestracji oraz podwykonawcy | 42 |
| I. DOKUMENTACJA I ARCHIWIZACJA DANYCH | 44 |
| 30. Dokumentacja zdarzeń na potrzeby audytu | 44 |
| 31. Przechowywanie dokumentacji | 45 |

| | |
|---|-----------|
| 32. Ponowne użycie oraz aktualizacja informacji i dokumentacji związanych z certyfikatami EV SSL..... | 45 |
| 33. Bezpieczeństwo danych | 46 |
| J. ZGODNOŚĆ Z WYMAGANIAMI MIĘDZYNARODOWYCH STANDARDÓW DOTYCZĄCYCH CERTYFIKATÓW EV SSL..... | 47 |
| 34. Wymagania audytowe | 47 |
| K. POZOSTAŁE WYMAGANIA KONTRAKTOWE | 50 |
| 35. Polityka prywatności | 50 |
| 36. Odpowiedzialność | 50 |
| Odniesienia | 52 |
| Słownik pojęć | 53 |

A. WPROWADZENIE

1. Wprowadzenie

Niniejszy Załącznik nr 3 (zwany dalej Załącznikiem) stanowi uzupełnienie aktualnego Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM o informacje na temat postępowania jakie obowiązuje CERTUM w trakcie wydawania certyfikatów Extended Validation (zwanymi dalej EV SSL) zgodnie z terminami i w kategoriach określonych w aktualnej wersji dokumentu **CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates** (zwanym dalej **EV Guidelines**), który jest publikowany jest na stronie <http://www.cabforum.org/>. Dokument EV Guidelines powstał za sprawą grupy **CA/Browser Forum** zrzeszającej szereg urzędów certyfikacji oraz dostawców oprogramowania, których wspólnym celem jest tworzenie i rozwijanie standardów Infrastruktury Klucza Publicznego. W dokumencie EV Guidelines określa się podstawowe wymagania, jakie spełniać musi urząd certyfikacji, aby mógł wydawać certyfikaty EV SSL oraz charakterystykę subskrybenta CERTUM, który może ubiegać się o certyfikat EV SSL. Informacja o właścicielu strony zamieszczona w certyfikacie EV SSL może zostać wyświetlona w specjalnie wyróżniony sposób przez odpowiednie oprogramowanie (np. przeglądarkę internetową).. Dzięki certyfikatowi EV SSL użytkownik oprogramowania zyskuje pewność odnośnie autentyczności strony WWW, którą odwiedza.

B. PODSTAWOWE ZAŁOŻENIA CERTYFIKATU EV SSL

2. Zastosowanie certyfikatów EV SSL

Certyfikaty EV SSL przeznaczone są dla systemów sieciowej wymiany informacji, które korzystają z protokołów TLS/SSL.

(a) Zastosowania podstawowe

W pierwszym rzędzie certyfikat EV SSL stosuje się do:

- (1) **identyfikacji oraz uwierzytelnienia podmiotu, do którego należy strona WWW zabezpieczona certyfikatem EV SSL**, zapewniając użytkownika przeglądarki internetowej, że strona, do której uzyskuje dostęp jest zarządzana przez właściciela, którego dane takie jak nazwa, adres, podstawa prawna funkcjonowania, numer wpisu do rejestru publicznego oraz inne dane pozwalające na jednoznaczne potwierdzenie jego tożsamości zawarte są w certyfikacie EV SSL;
- (2) **szyfrowania danych podczas komunikacji ze stroną WWW**, ułatwiając wymianę kluczy kryptograficznych i co za tym idzie, umożliwiając kodowanie danych transmitowanych między przeglądarką użytkownika a stroną WWW.

(b) Pozostałe zastosowania

Certyfikaty EV SSL mogą pomóc użytkownikowi sieci Web w ustaleniu czy strona WWW zarządzana jest legalnie przez podmiot do tego uprawniony oraz może stanowić narzędzie wspierające rozwiązywanie problemów z adresowaniem stron WWW takich jak ataki typu *phishing* i inne formy oszustw internetowych. Dostarczając wiarygodne – niezależnie potwierdzone – informacje, dotyczące właściciela strony, certyfikaty EV SSL mogą pomóc w:

- (3) znacznym utrudnieniu dokonywania ataków typu *phishing* oraz ograniczeniu skuteczności podobnych ataków, wykorzystujących różne formy fałszowania tożsamości;
- (4) ochronie firm narażonych na podobne ataki, dostarczając narzędzia umożliwiającego ich wzajemną identyfikację oraz identyfikację przez użytkownika;

- (5) dostarczeniu wsparcia w przypadku prowadzonego dochodzenia w sprawie ataków typu *phishing* lub innych form fałszowania tożsamości. Wsparcie obejmuje: kontakt, uczestnictwo w dochodzeniu lub podjęcie czynności prawnych przeciwko sprawcy.

(c) Zastosowania nie objęte gwarancją

Informacje, jakie zawierają certyfikaty EV SSL, dotyczą tylko tożsamości **Podmiotu certyfikatu EV SSL** (zwanego dalej **Podmiotem**) i nie odnoszą się do jego działań. Certyfikaty EV SSL nie dostarczają pewności, na podstawie której CERTUM gwarantowałoby, że:

- (6) Podmiot, którego nazwa występuje w certyfikacie EV SSL prowadzi aktualnie działalność gospodarczą;
- (7) Podmiot, którego nazwa występuje w certyfikacie EV SSL stosuje się do obowiązującego prawa;
- (8) Podmiot, którego nazwa występuje w certyfikacie jest godny zaufania, uczciwy, o nieposzlakowanej opinii oraz, że
- (9) prowadzenie wymiany handlowej z Podmiotem, którego nazwa występuje w certyfikacie, uważane jest za „bezpieczne”.

3. Gwarancje i oświadczenia

(a) Ze strony CERTUM

Beneficjentami certyfikatów EV SSL mogą być:

- (1) **Subskrybenci** zawierający z CERTUM **Umowę z Subskrybentem certyfikatu EV SSL** (zwaną dalej **Umową z Subskrybentem**);
- (2) Podmiot, którego nazwa występuje w certyfikacie EV SSL;
- (3) wszyscy **dostawcy oprogramowania**, którzy na podstawie zawartej z Unizeto S.A. umowy umieszczają w swoich produktach certyfikat główny urzędu **Certum Trusted Network CA**.
- (4) wszystkie **Strony Ufające**, czyli osoby i podmioty polegające na wydanym certyfikacie EV SSL w trakcie trwania okresu jego ważności.

CERTUM wydając certyfikat EV SSL oświadcza i gwarantuje swoim beneficjentom, że w okresie, w którym certyfikat EV SSL jest ważny, postępowanie CERTUM wobec

certyfikatu (proces wydania oraz weryfikacji danych w nim zawartych) jest zgodne z wymaganiami przedstawionymi w EV Guidelines. Zakres powyższej gwarancji, nie ograniczając się tylko do poniższych kwestii, obejmuje następujące zagadnienia:

- (1) **Forma prawna**: CERTUM potwierdza, na podstawie informacji uzyskanych za pośrednictwem właściwego urzędu, że w dniu wydania certyfikatu Subskrybent posiadał określoną formę prawną nadaną mu przez ten urząd oraz, że jego status w rejestrach urzędu nie widniał jako nieważny, nieaktualny, wykreślony z rejestru itp;
- (2) **Tożsamość**: CERTUM potwierdza, że w dniu wydania certyfikatu, oficjalna nazwa podmiotu, która występuje w certyfikacie EV SSL jest tożsama z nazwą zawartą w oficjalnych dokumentach urzędu rejestracji właściwego dla miejsca prowadzenia przez podmiot deklarowanej działalności;
- (3) **Prawo do nazwy domeny**: CERTUM podejmuje wszelkie wymagane przez EV Guidelines kroki niezbędne, aby potwierdzić, że Podmiot, którego nazwę zawiera certyfikat EV SSL posiadał, w dniu wydania certyfikatu, wyłączne prawo do posługiwania się nazwą domeny zawartą w certyfikacie;
- (4) **Upoważnienie**: CERTUM podejmuje wszelkie wymagane przez EV Guidelines czynności niezbędne do uzyskania pewnej wiedzy o tym, czy Podmiot wydał stosowne upoważnienia osobom ubiegającym się w jego imieniu o certyfikat EV SSL;
- (5) **Prawdziwość informacji**: CERTUM podejmuje czynności niezbędne do uzyskania pewności odnośnie tego, że w dniu wystawienia certyfikatu wszystkie pozostałe informacje zawarte w certyfikacie są dokładne i prawdziwe;
- (6) **Umowę z Subskrybentem**: CERTUM zapewnia, że Podmiot, którego nazwa występuje w certyfikacie EV SSL przystąpił do podpisania z CERTUM ważnej Umowy z Subskrybentem, zaś Umowa ta spełnia wymagania określone w dokumencie EV Guidelines;
- (7) **Status**: CERTUM, w zgodzie z wymaganiami EV Guidelines v1.2, zapewnia, że repozytorium zawierające informacje na temat aktualnego statusu certyfikatu EV SSL jest dostępne publicznie przez 24 godziny, 7 dni w tygodniu;
- (8) **Unieważnienie**: CERTUM, w zgodzie z niniejszym Załącznikiem oraz wymaganiami EV Guidelines, unieważnia certyfikat niezwłocznie po otrzymaniu sygnałów świadczących o tym, że miały miejsce zdarzenia uprawniające CERTUM do podjęcia takich czynności.

(b) Ze strony Subskrybenta

CERTUM będzie wymagać, jako strona Umowy z Subskrybentem, aby Subskrybent wywiązywał się ze swoich zobowiązań i gwarancji wobec CERTUM oraz beneficjentów certyfikatu EV SSL, stosownie do wymagań przedstawionych w rozdziale Wymagania dotyczące Umowy z Subskrybentem niniejszego Załącznika.

C. ŚRODOWISKO I ZASTOSOWANIE

4. Wydawanie certyfikatów EV SSL

Wydając certyfikaty EV SSL, CERTUM spełnia następujące wymagania:

(a) Zgodność

CERTUM świadczy usługi:

- (1) w zgodzie z prawem obowiązującym na obszarze Rzeczypospolitej Polskiej na którym CERTUM wydaje certyfikaty;
- (2) w zgodzie z wymaganiami aktualnej wersji dokumentu EV Guidelines;
- (3) w zgodzie z wymaganiami AICPA/CICA WebTrust Program for Certification Authorities Version 1.0 zweryfikowanymi przez licencjonowanych audytorów WebTrust lub w zgodzie z wymaganiami standardu ETSI TS 102 042 V2.1.1 (lub późniejszy);
- (4) w zgodzie z otrzymanymi uprawnieniami, niezbędnymi do świadczenia usług certyfikacyjnych.

(b) Polityki EV SSL

- (1) Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM wraz z niniejszym Załącznikiem:
 - (A) realizuje wymagania EV Guidelines zawsze, gdy tylko zostaną w nim opublikowane jakiegokolwiek zmiany;
 - (B) realizuje aktualne wymagania (i) WebTrust Program for Certification Authorities oraz (ii) WebTrust for Certification Authorities -Extended Validation Audit Criteria lub ETSI TS 102 042 V2.1.1 (lub późniejszy),
 - (C) określa ścieżkę certyfikacji w ramach hierarchicznej struktury urzędów podległych głównemu urzędowi CERTUM odpowiedzialnych za weryfikację autentyczności wydawanych certyfikatów EV SSL
- (2) CERTUM udostępnia publicznie własną politykę certyfikacji za pośrednictwem Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM,

który znajduje się w repozytorium dostępnym online, 24 godziny przez 7 dni w tygodniu. Kodeks Postępowania Certyfikacyjnego sporządzony jest zgodnie z polityką RFC 3647.

- (3) CERTUM spełnia kryteria wskazane w aktualnej wersji CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates (EV Guidelines) opublikowanym na stronie: <http://www.cabforum.org> W przypadku jakichkolwiek rozbieżności pomiędzy niniejszym Załącznikiem a EV Guidelines, treść dokumentu EV Guidelines jest nadrzędna wobec Załącznika.

Dodatkowo CERTUM zapewnia, że powyższa klauzula dotycząca gwarancji zgodności postępowania CERTUM z wymaganiami EV Guidelines dotyczy (bezpośrednio lub przez odniesienie) każdej umowy zawartej z podległymi urzędami, punktami rejestracji oraz podwykonawcami, którzy związani są z procesem wydawania i obsługi certyfikatów EV SSL. CERTUM wymaga od w/w podmiotów przestrzegania wymagań stawianych przez EV Guidelines.

(c) Ubezpieczenie

CERTUM posiada następujące wymagane ubezpieczenia:

- (A) Ubezpieczenie odpowiedzialności cywilnej na kwotę przynajmniej 2 mln dolarów;
- (B) Ubezpieczenie odpowiedzialności cywilnej w zakresie prowadzonej działalności na kwotę przynajmniej 5 mln dolarów obejmujące odszkodowanie za (i) błędy, szkody powstałe w wyniku zaniechania, nieświadomego naruszenia umowy, lub zaniedbania obowiązków służbowych dotyczących wydawania i obsługi certyfikatów EV SSL, oraz (ii) odszkodowania za szkody powstałe w wyniku naruszenia prawa własności którejkolwiek ze stron trzecich (z wyłączeniem praw autorskich oraz praw do znaku towarowego), naruszenia prywatności i dobrego imienia.

5. Otrzymanie certyfikatu EV SSL

Zgodnie z wymaganiami EV Guidelines, certyfikaty EV SSL mogą być wydawane organizacjom i przedsiębiorstwom posiadającym osobowość prawną, przedsiębiorstwom i organizacjom nie posiadającym osobowości prawnej a także podmiotom administracji publicznej oraz organizacjom międzynarodowym o charakterze niekomercyjnym, które spełniają następujące warunki:

(a) Organizacje i przedsiębiorstwa posiadające osobowość prawną¹

CERTUM może wydać certyfikat EV SSL każdej organizacji/przedsiębiorstwu spełniającej następujące warunki:

- (1) Organizacja/przedsiębiorstwo musi być prawnie rozpoznawalnym podmiotem, który został powołany do istnienia poprzez wpisanie do rejestru (lub akt powołania) przez urząd (sąd) właściwy ze względu na miejsce prowadzenia przez podmiot działalności;
- (2) Wpis do rejestru musi zawierać nazwę organizacji/przedsiębiorstwa;
- (3) Status organizacji/przedsiębiorstwa w rejestrze stosownego organu władzy (sądu) dokonującego wpisu nie może pozostawać jako nieważny, nieaktualny, wykreślony z rejestru itp;
- (4) Organizacja/przedsiębiorstwo musi posiadać potwierdzony adres oraz zweryfikowaną obecność na rynku;
- (5) Miejscem zarejestrowania organizacji/przedsiębiorstwa oraz miejscem, w którym prowadzi ona działalność nie może być terytorium kraju, z którym prawo Rzeczypospolitej Polskiej zabrania prowadzenia wymiany handlowej, a w szczególności świadczenia usług certyfikacyjnych;
- (6) Organizacja/przedsiębiorstwo nie może znajdować się na rządowych listach podmiotów objętych zakazem wykonywania czynności prawnych lub publicznie, na mocy prawa, wskazanych jako posiadające zobowiązania finansowe wobec innych

¹ W oryginalnym brzmieniu dokumentu **Guidelines for Extended Validation Certificates v 1.2** subskrybenci tej grupy nazywani są **Private Organization Subjects**. Z kolei podmioty, które - dla potrzeb niniejszego dokumentu - nazwiemy *Przedsiębiorstwami oraz organizacjami nie posiadającymi osobowości prawnej*, określa się nazwą **Business Entity Subjects**. O ile dokument EV Guidelines definiuje podmioty drugiego rodzaju jako organizacje związane tylko w celach gospodarczych, o tyle niniejszy Załącznik, będąc odzwierciedleniem treści EV Guidelines w warunkach polskich koncentruje się na podziale przyszłych subskrybentów certyfikatów EV ze względu na formę prawną jaką przyjmuje prowadzona przez nich działalność nie zaś na rodzaj prowadzonej przez nich działalności. Dlatego pojęciu **Private Organization** odpowiadać będzie zarówno przedsiębiorstwo jak i organizacja, które łączy fakt posiadania osobowości prawnej. Analogicznie, pojęciu **Business Entity** przypisuje się, w wersji polskiej Załącznika, zarówno przedsiębiorstwa jak i organizacje nie prowadzące działalności gospodarczej, które nie posiadają osobowości prawnej, są jednak zarejestrowane przez stosowną instytucję charakterystyczną ze względu na rodzaj prowadzonej przez nich działalności. Autorzy niniejszego Załącznika będąc świadomi, że nie sposób jest przenieść istniejącego w dokumencie EV Guidelines podziału grup subskrybentów na grunt polski zachowując przy tym tożsamość znaczeniową tłumaczonych pojęć uważają, że jest możliwe znalezienie wspólnego mianownika jakim można połączyć obie wersje koncepcji podziału subskrybentów certyfikatu EV odnosząc się do istnienia pojęcia formy prawnej i, co za tym idzie rodzaju ponoszonej odpowiedzialności, która wprowadza podział między przyszłymi subskrybentami certyfikatów bardzo podobny do tego jaki sugeruje dokument Guidelines for Extended Validation Certificates v 1.2.

osób, firm, organizacji etc. Organizacja/przedsiębiorstwo nie może być podmiotem prawa w państwie, z którym prawo Rzeczypospolitej Polskiej zabrania prowadzenia wymiany handlowej.

(b) Organizacje i przedsiębiorstwa nie posiadające osobowości prawnej

CERTUM może wydać certyfikat EV SSL podmiotom nie odpowiadającym charakterystyce opisanej w rozdziale 5(a) spełniającym jednak następujące wymagania:

- (1) Przedsiębiorstwo lub organizacja musi być porównie rozpoznawalnym podmiotem, którego powstanie wymagało wydania bądź akceptacji przez dany urząd właściwy ze względu na miejsce prowadzenia przez podmiot działalności takich dokumentów jak statut, certyfikat, licencja;
- (2) Można zweryfikować adres podmiotu i prowadzoną przez niego działalność;
- (3) Musi zostać zidentyfikowana i zweryfikowana tożsamość przynajmniej jednej z osób reprezentujących Subskrybenta np. właściciel, współwłaściciel, członek zarządu;
- (4) Osoba reprezentująca Subskrybenta musi poświadczyć upoważnienia wydane innym przedstawicielom występującym w imieniu przedsiębiorstwa;
- (5) Podmiot i osoba reprezentująca Subskrybenta nie mogą pozostawać na rządowych listach podmiotów i/lub osób objętych zakazem wykonywania czynności prawnych lub publicznie, na mocy prawa, wskazanych jako posiadające zobowiązania finansowe wobec innych osób, firm, lub organizacji;
- (6) Podmiot nie może prowadzić działalności na terytorium kraju, z którym prawo Rzeczypospolitej Polskiej zabrania prowadzenia wymiany handlowej, w szczególności świadczenia usług certyfikacyjnych.

(c) Podmioty administracji publicznej

CERTUM może wydać certyfikat EV SSL każdemu podmiotowi administracji publicznej, który spełnia następujące warunki:

- (1) Podstawą prawną istnienia podmiotu administracji publicznej jest jego ukonstytuowanie się na podstawie właściwych rozporządzeń, uchwał lub innych aktów legislacyjnych wydanych przez stosowny urząd, ministerstwo, parlament itp.

- (2) Podmiot administracji publicznej nie może być podmiotem prawa na terytorium kraju, z którym prawo Rzeczypospolitej Polskiej zabrania prowadzenia wymiany handlowej, w szczególności świadczenia usług certyfikacyjnych;
- (3) Podmiot administracji publicznej nie może pozostawać na rządowych listach podmiotów objętych zakazem wykonywania czynności prawnych lub publicznie, na mocy prawa, wskazanych jako posiadające zobowiązania finansowe wobec innych osób, firm, organizacji etc.

(d) Organizacje międzynarodowe (niekomercyjne)

CERTUM może wydać certyfikat EV SSL każdej niekomercyjnej organizacji międzynarodowej, która spełnia następujące warunki:

- (1) Zamawiający jest międzynarodową organizacją powstałą na podstawie statusu, traktatu, konwencji lub innego równoważnego dokumentu, który został podpisany przez, lub w imieniu więcej niż jednego państwa.
- (2) Organizacja nie może prowadzić działalności na terytorium kraju, z którym prawo Rzeczypospolitej Polskiej zabrania prowadzenia wymiany handlowej, w szczególności świadczenia usług certyfikacyjnych.
- (3) Organizacja nie może pozostawać na rządowych listach podmiotów objętych zakazem prowadzenia wymiany handlowej z podmiotami prawa Rzeczypospolitej Polskiej (np. embargo)

D. ZAWARTOŚĆ I PROFIL CERTYFIKATU EV SSL

6. Wymagania dotyczące zawartości certyfikatu EV SSL

Niniejszy rozdział określa minimalne wymagania dotyczące zawartości certyfikatu EV SSL, związane z charakterystyką podmiotów certyfikatu EV SSL. Będąc przedmiotem wymagań, jakie opisuje niniejszy Załącznik certyfikat EV SSL zawiera następujące informacje dotyczące podmiotu certyfikatu EV SSL, które wyszczególnione są w kolejnych polach certyfikatu EV SSL:

- (1) **Nazwa Organizacji** (ang. Organization Name)

Pole certyfikatu:

subject:organizationName (OID 2.5.4.10)

Wymagane/Opcjonalne: Wymagane

Zawartość: Pole musi zawierać pełną nazwę **Zamawiającego certyfikat EV SSL** (zwanego dalej **Zamawiającym**), którą zarejestrowano w stosownym urzędzie. Jeśli pełna nazwa przekracza liczbę 64 znaków, to CERTUM może dokonać skrócenia nazwy zgodnie z obowiązującymi standardami języka prawniczego i urzędowego.

- (2) **Nazwa domeny** (ang. Domain Name)

Pole certyfikatu:

subject:commonName (OID 2.5.4.3) lub

SubjectAlternativeName:dNSName

Wymagane/Opcjonalne: Wymagane

Zawartość: Pole musi zawierać jedną lub więcej nazw domenowych posiadanych lub kontrolowanych przez Podmiot, związanych z publicznie dostępnym serwerem Podmiotu. Serwer taki może być własnością lub może być administrowany przez Podmiot lub inną jednostkę (np. firmę hostingową). Nazwy wieloznaczne (ang. Wildcard) nie mogą być stosowane w przypadku Certyfikatów EV SSL.

(3) **Rodzaj działalności** (ang. Business Category)

Pole certyfikatu:

subject: businessCategory (OID 2.5.4.15)

Wymagane/Opcjonalne: Wymagane

Zawartość: Pole zawiera następujące wpisy: 'V1.0, Clause 5.(b)', 'V1.0, Clause 5.(c)', 'V1.0, Clause 5.(d)' or 'V1.0, Clause 5.(e)' w zależności od tego do jakiej kategorii podmiotów, opisanych kolejno w punktach 5(b), 5(c), 5(d) oraz 5(e) EV Guidelines, należy właściciel certyfikatu EV.

(4) **Miejsce zarejestrowania** (ang. Jurisdiction of Incorporation)

Pola certyfikatu:

Miejscowość (jeśli dotyczy):

subject:jurisdictionOfIncorporationLocalityName

(OID 1.3.6.1.4.1.311.60.2.1.1)

ASN.1 - X520LocalityName jak określono w 5280

Jednostka podziału administracyjnego (jeśli dotyczy):

subject:jurisdictionOfIncorporationStateOrProvinceName

(OID 1.3.6.1.4.1.311.60.2.1.2)

ASN.1 - X520StateOrProvinceName jak określono w RFC 5280

Kraj:

subject:jurisdictionOfIncorporationCountryName

(OID 1.3.6.1.4.1.311.60.2.1.3)

ASN.1 - X520countryName jak określono w RFC 5280

Wymagane/Opcjonalne: Wymagane

Zawartość: Pole nie może zawierać informacji o miejscu zarejestrowania nieadekwatnej do faktycznego obszaru w jakim administruje dany urząd – np. miejsce zarejestrowania dla urzędu o krajowym zasięgu oddziaływania będzie zawierać nazwę kraju, nie będzie jednak zawierać województwa lub miasta. Miejsce zarejestrowania dla urzędu na poziomie województwa będzie zawierać nazwę kraju i nazwę województwa, nie będzie jednak zawierać nazwy miasta, itd. Informacja o kraju musi

być określona zgodnie z systemem kodowania ISO. Nazwa województwa oraz nazwa miasta musi być określona pełnymi nazwami.

(5) **Numer wpisu do rejestru:** (ang. Registration Number)

Pole certyfikatu:

Subject:serialNumber (OID 2.5.4.5)

Wymagane/Opcjonalne: Wymagane

Zawartość: Pole musi zawierać unikalny identyfikator przyznany Podmiotowi przez stosowny urząd. Jeśli urząd dokonujący rejestracji Podmiotu nie dostarcza takiego identyfikatora, wówczas pole zawierać musi datę zarejestrowania Podmiotu.

(6) **Adres miejsca prowadzenia działalności:** (ang. Physical Address of Place of Business)

Pola certyfikatu:

Numer lokalu i ulica (opcjonalne) subject:streetAddress (OID 2.5.4.9)

Miejscowość subject:localityName (OID 2.5.4.7)

Województwo (jeśli istnieje) subject:stateOrProvinceName (OID 2.5.4.6)

Kraj subject:countryName (OID 2.5.4.6)

Kod pocztowy (opcjonalne) subject:postalCode (OID 2.5.4.17)

Wymagane/Opcjonalne: Miejscowość, jednostka podziału administracyjnego oraz kraj – Wymagane; Ulica oraz kod pocztowy – Opcjonalne.

Zawartość: Pole MUSI zawierać adres miejsca, w którym Podmiot prowadzi działalność.

7. Wymagania dotyczące polityki certyfikatów EV SSL

(a) Certyfikaty subskrybentów

Każdy certyfikat EV SSL wydany przez CERTUM musi zawierać w rozszerzeniu certificatePolicies identyfikator OID, który wskazuje politykę CERTUM odnoszącą się do danego certyfikatu. Numer OID stosownej polityki dla certyfikatu EV SSL wydawanych przez CERTUM to 1.2.616.1.113527.2.5.1.1

(b) Certyfikaty EV SSL urzędów podległych CERTUM

Certyfikaty wydane urzędom pośrednim będącym pod kontrolą urzędu Certum Trusted Network CA (np. Certum Extended Validation CA) mogą, w polu anyPolicy, zawierać specjalny OID (2.5.29.32.0).

(c) Certyfikat Główny urzędu CERTUM

Certyfikatem głównym urzędu dla certyfikatów EV SSL jest certyfikat urzędu Certum Trusted Network CA. Certyfikat główny nie zawiera pól: certificatePolicies oraz extendedKeyUsage.

8. Maksymalny okres ważności

(a) Dla certyfikatów EV SSL

Maksymalny okres ważności dla Certyfikatów EV SSL może wynosić 27 miesięcy.

(b) Dla weryfikowanych informacji

Maksymalny okres ważności informacji dotyczących Subskrybenta, wykorzystywanych przez CERTUM w procesie wydawania certyfikatów EV SSL (zanim koniecznym stanie się ponowne złożenie dokumentów) wynosi:

- Forma prawna oraz tożsamość – trzynaście (13) miesięcy;
- Adres miejsca, w którym prowadzona jest działalność – trzynaście (13) miesięcy;
- Numer telefonu właściwy dla miejsca prowadzenia działalności – trzynaście (13) miesięcy;
- Weryfikacja konta bankowego – trzynaście (13) miesięcy;
- Nazwa domeny – trzynaście (13) miesięcy;
- Tożsamość i upoważnienie **Osoby Zatwierdzającej Certyfikat** – trzynaście (13) miesięcy, o ile pomiędzy podmiotem a CERTUM nie została zawarta umowa określająca inny termin – w takim przypadku wiążące są postanowienia takiej umowy. Dla przykładu – umowa może określać okres ważności uprawnień Osoby Zatwierdzającej Certyfikat do czasu ich odwołania, wygaśnięcia lub zerwania samej umowy.

9. Pozostałe wymagania techniczne dla certyfikatów EV SSL

Pozostałe wymagania techniczne opisane są w załącznikach nr 4 i 5 do Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM.

E. WYMAGANIA DOTYCZĄCE ZAMÓWIENIA CERTYFIKATU EV SSL

10. Wymagania ogólne

(a) Wymagane dokumenty

Przed wydaniem certyfikatu EV SSL CERTUM musi uzyskać od Zamawiającego następujące dokumenty, określone przez niniejszy Załącznik:

- **Wniosek o wydanie certyfikatu EV SSL**
- **Umowa z Subskrybentem**
- Dodatkowe dokumenty wymagane przez CERTUM w celu poprawnej i zgodnej z niniejszym Załącznikiem weryfikacji podmiotu.

(b) Wymagania dotyczące osób reprezentujących Subskrybenta certyfikatu EV SSL

Wydanie certyfikatu EV SSL wymaga, aby osoby, które występują w imieniu Zamawiającego spełniały następujące wymagania:

- **Wnioskodawca certyfikatu EV SSL** (ang. *Certificate Requester*), zwany dalej **Wnioskodawcą** – Osoba fizyczna reprezentująca Zamawiającego, pracownik zatrudniony przez Zamawiającego, autoryzowany przedstawiciel Zamawiającego lub strona trzecia (np. dostawcy usług internetowych) reprezentująca Zamawiającego i upoważniona do złożenia w CERTUM podpisanego Wniosku o wydanie certyfikatu EV SSL.
- **Osoba Zatwierdzająca Certyfikat** (ang. *Certificate Approver*) – Osoba fizyczna reprezentująca Zamawiającego, pracownik zatrudniony przez Zamawiającego lub autoryzowany przedstawiciel Zamawiającego (i) posiadający wyraźne pełnomocnictwo do występowania samemu jako Wnioskodawca lub udzielania innym pracownikom Zamawiającego lub stronom trzecim takiego pełnomocnictwa, a także (ii) do zatwierdzania Wniosków o wydanie certyfikatu EV SSL składanych przez innych Wnioskodawców.
- **Osoba Podpisująca Umowę** (ang. *Contract Signer*) – Osoba fizyczna reprezentująca Zamawiającego, pracownik zatrudniony przez Zamawiającego lub

autoryzowany przedstawiciel Zamawiającego posiadający wyraźne pełnomocnictwo do reprezentowania Zamawiającego, w tym upoważnienie do podpisywania w jego imieniu Umowy z Subskrybentem.

Zamawiający może upoważnić tylko jedną osobę do pełnienia dwóch lub więcej ról wymienionych powyżej, lecz może także upoważnić więcej niż jedną osobę do zajmowania którejkolwiek ze wspomnianych ról.

11. Wymagania dotyczące Wniosku o wydanie certyfikatu EV SSL

(a) Ogólne

Przed wydaniem certyfikatu EV SSL, CERTUM musi uzyskać od Zamawiającego (za pośrednictwem Wnioskodawcy upoważnionego do działania w imieniu Zamawiającego) poprawnie wypełniony i podpisany Wniosek o wydanie certyfikatu EV SSL, w formie określonej przez CERTUM, spełniając przy tym wymagania niniejszego Załącznika. Jeden Wniosek o wydanie certyfikatu EV SSL może być podstawą wydania wielu certyfikatów EV SSL dla danego Zamawiającego w danym czasie.

(b) Wniosek i oświadczenie

Wniosek o wydanie certyfikatu EV SSL musi zostać złożony przez, lub w imieniu Zamawiającego oraz musi zawierać oświadczenie złożone przez, lub w imieniu Zamawiającego, że zawarte we Wniosku informacje są prawdziwe i poprawne.

(c) Informacje zawarte we Wniosku o wydanie certyfikatu EV

Wniosek o wydanie certyfikatu EV SSL musi zawierać wszystkie informacje o Zamawiającym, które zostaną umieszczone w certyfikacie EV SSL oraz informacje dodatkowe, wymagane przez CERTUM, aby wydanie certyfikatu odbyło się w zgodzie z wymaganiami niniejszego Załącznika. W przypadku, gdy Wniosek o wydaniu certyfikatu EV SSL nie zawiera wszystkich niezbędnych informacji o Zamawiającym, CERTUM zobowiązane jest otrzymać brakujące dane od Osoby Zatwierdzającej Certyfikat lub Osoby Podpisującej Umowę. Wniosek o wydaniu certyfikatu EV SSL powinien zawierać co najmniej następujące informacje:

- o **Nazwa Organizacji**: Formalna nazwa organizacji lub przedsiębiorstwa Zamawiającego, która zostanie zamieszczona w certyfikacie EV SSL, zgodna z nazwą zarejestrowaną w stosownym urzędzie;

- **Nazwa Domeny:** Nazwa domeny będącej przedmiotem certyfikatu EV SSL;
- **Miejsce wpisania do rejestru:** Miejsce zarejestrowania działalności Subskrybenta
 - (a) Miasto (jeśli wymagane),
 - (b) Jednostka podziału administracyjnego (jeśli wymagane)
 - (c) Kraj
- **Urząd rejestracji:** Nazwa urzędu, który dokonał rejestracji Zamawiającego
- **Numer wpisu do rejestru publicznego:** Unikalny numer identyfikacyjny przyznany Zamawiającemu przez urząd odpowiedzialny za jego rejestrację, który zostanie zawarty w certyfikacie EV SSL;
- **Adres:** Adres miejsca, w którym Zamawiający prowadzi działalność:
 - (a) Ulica i numer lokalu,
 - (b) Miasto,
 - (c) Jednostka podziału administracyjnego (jeśli wymagane),
 - (d) Kraj,
 - (e) Kod pocztowy,
 - (f) Główny numer telefonu.
- **Osoba Zatwierdzająca Certyfikat:** Nazwisko, imię oraz dane kontaktowe Osoby Zatwierdzającej Certyfikat, składającej i podpisującej lub upoważniającej Wnioskodawcę do złożenia i podpisania Wniosku o wydanie certyfikatu EV SSL w imieniu Zamawiającego.
- **Wnioskodawca:** Nazwisko, imię oraz dane kontaktowe Wnioskodawcy składającego Wniosek o wydanie certyfikatu EV SSL w imieniu Zamawiającego, jeśli Wnioskodawca jest osobą różną od Osoby Zatwierdzającej Certyfikat.

12. Wymagania dotyczące Umowy z Subskrybentem

(a) Ogólne

Przed wydaniem Certyfikatu EV SSL, CERTUM musi otrzymać od Zamawiającego podpisaną Umowę z Subskrybentem. Umowa ta musi być podpisana przez upoważnioną do tego Osobę Podpisującą Umowę działającą w imieniu Zamawiającego i musi odnosić się do certyfikatu EV SSL, który ma zostać wydany na podstawie Wniosku o wydanie certyfikatu EV SSL. Osobna Umowa z Subskrybentem może odnosić się do każdego z

kolejnych Wniosków o wydanie certyfikatu EV SSL lub jedna Umowa z Subskrybentem może dotyczyć kilku (również przyszłych) Wniosków o wydanie certyfikatu EV SSL pod warunkiem, że każdy z certyfikatów EV SSL, który ma zostać wydany będzie uwzględniony w danej Umowie z Subskrybentem.

(b) Wymagania

Umowa z Subskrybentem dotyczy Zamawiającego oraz Osoby Podpisującej Umowę. Minimalne wymagania dotyczące zawartości Umowy z Subskrybentem określają jakie treści powinna zawierać Umowa z Subskrybentem odnośnie obowiązków oraz gwarancji CERTUM oraz Zamawiającego:

- Prawdziwość informacji: Zamawiający ma obowiązek udzielania CERTUM prawdziwych i ścisłych informacji dotyczących podmiotu certyfikatu EV SSL przez cały okres ważności certyfikatu,
- Ochrona klucza prywatnego: Subskrybent certyfikatu EV SSL zobowiązuje się kontrolować użycie klucza prywatnego związanego z kluczem publicznym umieszczonym w certyfikacie oraz chronić wszelkie informacje z nim związane (np. hasło),
- Akceptacja certyfikatu EV SSL: CERTUM zobowiązuje się nie wydawać certyfikatu EV SSL zanim nie zostaną pomyślnie zweryfikowane dane w nim zawarte,
- Stosowanie certyfikatu: Subskrybent certyfikatu EV SSL zobowiązuje się do używania certyfikatu wyłącznie zgodnie z zasadami określonymi prawem, używania certyfikatu wyłącznie przez uprawniony do tego Podmiot, używania certyfikatu zgodnie z Umową z Subskrybentem oraz instalacji certyfikatu tylko na serwerze związanym z nazwą domeny, będącą przedmiotem certyfikatu EV SSL,
- Zgłaszanie problemów i unieważnienie: Subskrybent certyfikatu EV SSL zobowiązuje się do niezwłocznego zaprzestania używania certyfikatu EV SSL i związanego z nim klucza prywatnego oraz niezwłocznego zgłoszenia do CERTUM woli unieważnienia certyfikatu w następujących przypadkach: (a) gdy informacja zawarta w certyfikacie okazuje się nieprawdziwa lub niepoprawna lub (b) gdy nastąpiło podejrzenie nadużycia lub niewłaściwego wykorzystania certyfikatu EV SSL lub kompromitacji klucza prywatnego,
- Ograniczenia w stosowaniu certyfikatu EV SSL: Subskrybent certyfikatu EV SSL jest zobowiązany do niezwłocznego zaprzestania używania klucza prywatnego powiązanego z kluczem publicznym umieszczonym w certyfikacie EV SSL w chwili wygaśnięcia jego ważności lub jego unieważnienia.

F. WYMAGANIA DOTYCZĄCE WERYFIKACJI INFORMACJI

13. Wymagania ogólne

Niniejsza część Załącznika określa wymagania jakie stawiane są przez dokument EV Guidelines procedurze weryfikacji informacji otrzymanych od Zamawiającego

(a) Wymagania

Przed wydaniem Certyfikatu EV SSL, CERTUM musi upewnić się, że wszystkie informacje o organizacji lub przedsiębiorstwie ubiegającym się o certyfikat EV SSL, które będą zamieszczone w certyfikacie EV SSL zostały zweryfikowane zgodnie z niniejszymi Załącznikiem oraz zgadzają się z informacjami potwierdzonymi i udokumentowanymi przez CERTUM w wyniku procesu weryfikacji. Obowiązkiem CERTUM jest weryfikacja następujących informacji:

- (1) Weryfikacja cech indywidualnych Zamawiającego:
 - (A) Forma prawna i tożsamość;
 - (B) Adres miejsca prowadzenia działalności;
 - (C) Działalność gospodarcza
- (2) Weryfikacja praw Zamawiającego do posługiwania się nazwą domeny wymienionej w certyfikacie EV SSL:
- (3) Weryfikacja osób reprezentujących Zamawiającego:
 - (A) Tożsamość, charakter piastowanych stanowisk oraz pełnomocnictwa udzielone Osobie Podpisującej Umowę, Osobie Zatwierdzającej Certyfikat oraz Wnioskodawcy;
 - (B) Podpis na Umowie z Subskrybentem;
 - (C) Akceptacja Wniosku przez Osobę Zatwierdzającą Certyfikat.

(b) Akceptowane metody weryfikacji

Przyjmuje się zasadę ogólną, że CERTUM jest odpowiedzialne za podjęcie wszelkich niezbędnych kroków, aby zweryfikować informacje wymienione powyżej. Akceptowane metody weryfikacji, opisane w rozdziałach 14 oraz 24 (zazwyczaj zakładających różne

alternatywy) uznawane są za minimalny akceptowany poziom polityki weryfikacji realizowanej przez CERTUM. W każdym przypadku CERTUM jest zobowiązane do podjęcia wszelkich innych działań, których mogą wymagać zapisy w niniejszym Załączniku.

14. Weryfikacja formy prawnej oraz tożsamości

Subskrybenta

Aby zweryfikować formę prawną i tożsamość Zamawiającego, CERTUM musi wykonać poniższe działania:

- (1) Organizacje i przedsiębiorstwa posiadające osobowość prawną:
 - **Forma prawna:** CERTUM sprawdza czy Zamawiający jest faktycznie istniejącym i poprawnie zarejestrowanym (np. jako spółka) podmiotem, którego kształt prawny zdefiniowany jest przepisami prawa. Urząd rejestrujący działalność Zamawiającego jest urzędem właściwym ze względu na miejsce działalności Zamawiającego, zaś status Zamawiającego w rejestrach urzędu nie jest określony jako „nieważny”, „nieaktualny”, „wykreślony z rejestru” itp..
 - **Nazwa organizacji:** CERTUM sprawdza czy formalna nazwa Zamawiającego zarejestrowana w stosownym urzędzie właściwym ze względu na miejsce działalności Zamawiającego jest zgodna z nazwą umieszczoną we Wniosku o wydanie certyfikatu EV SSL.
 - **Numer wpisu do rejestru:** CERTUM musi otrzymać unikalny identyfikator przyznany Zamawiającemu przez stosowny urząd właściwy ze względu na miejsce działalności Zamawiającego.
 - **Podmiot rejestrujący:** CERTUM musi zidentyfikować właściwy urząd, w którym dokonano rejestracji Zamawiającego, uzyskując adres tego urzędu.
- (2) Podmioty administracji publicznej
 - **Forma prawna:** CERTUM musi sprawdzić czy Zamawiający jest prawnie rozpoznawanym podmiotem administracji publicznej, podległym organom administracyjnym właściwym ze względu na obszar działania (np. Urząd Wojewódzki etc.).
 - **Nazwa podmiotu:** CERTUM musi sprawdzić, czy nazwa formalna Zamawiającego, zarejestrowana w stosownym urzędzie właściwym ze względu

na miejsce działalności Zamawiającego jest zgodna z nazwą umieszczoną we Wniosku o wydanie certyfikatu EV SSL.

- **Numer wpisu do rejestru:** CERTUM musi uzyskać unikalny identyfikator przyznany Zamawiającemu przez stosowny urząd właściwy ze względu na miejsce działalności Zamawiającego lub otrzymać dokumenty ustaw, uchwał lub innych aktów legislacyjnych, na podstawie których dany podmiot powołany został do pełnienia swoich funkcji. Jeśli pozyskanie niniejszych informacji okazuje się niemożliwe CERTUM stosuje inne środki w celu weryfikacji Zamawiającego.
- (3) Przedsiębiorstwa oraz organizacje nie posiadające osobowości prawnej
- **Forma prawna:** CERTUM musi sprawdzić czy Zamawiający prowadzi działalność pod nazwą, którą podał we Wniosku o wydanie certyfikatu EV SSL.
 - **Nazwa podmiotu:** CERTUM musi sprawdzić czy formalna nazwa Zamawiającego, zarejestrowana w stosownym urzędzie rejestracyjnym właściwym ze względu na miejsce działalności Zamawiającego jest zgodna z nazwą umieszczoną we Wniosku o wydanie certyfikatu EV SSL.
 - **Numer wpisu do rejestru:** CERTUM musi uzyskać unikalny numer identyfikacyjny przyznany Zamawiającemu przez stosowny urząd właściwy ze względu na miejsce działalności Zamawiającego. Jeśli dany urząd nie przypisał Zamawiającemu żadnego identyfikatora CERTUM musi otrzymać datę dokonania rejestracji Zamawiającego.
 - **Osoba reprezentująca Subskrybenta:** CERTUM musi zweryfikować tożsamość osoby fizycznej związanej z podmiotem certyfikatu EV SSL, która jest upoważniona przez Zamawiającego do podejmowania czynności związanych z wydaniem i użytkowaniem certyfikatu EV SSL.
- (4) Organizacje międzynarodowe (niekomercyjne)
- **Forma prawna:** CERTUM musi zweryfikować czy Zamawiający jest prawnie rozpoznawalnym podmiotem będącym organizacją międzynarodową.
 - **Nazwa organizacji:** CERTUM musi zweryfikować czy formalna nazwa Zamawiającego jest identyczna z nazwą podaną we Wniosku o wydanie certyfikatu EV SSL.

- **Numer wpisu do rejestru:** CERTUM musi zweryfikować datę utworzenia organizacji lub stosowny identyfikator nadany przez jednostkę powołującą do istnienia daną organizację. Jeśli pozyskanie niniejszych informacji okazuje się niemożliwe CERTUM stosuje inne środki w celu weryfikacji Subskrybenta.

Organizacje międzynarodowe weryfikowane są poprzez:

- odniesienie do dokumentów konstytuujących ich działalność,
- bezpośrednio uzyskane potwierdzenie od jednostek rządowych podpisujących w/w dokumenty. Potwierdzenie takie można uzyskać od właściwej jednostki administracji państwowej lub jednostki reprezentującej prawodawstwo danego kraju lub dokonując weryfikacji tej jednostki, która reprezentuje daną organizację zgodnie z własnym statutem,
- na podstawie listy właściwych podmiotów prowadzonej przez CABForum na stronie www.cabforum.org,
- jeśli dana organizacja (niekomercyjna) jest jednostką podległą innej organizacji międzynarodowej, CERTUM może zweryfikować daną jednostkę na podstawie weryfikacji organizacji zwierzchniej, której częścią jest organizacja Subskrybenta.

15. Weryfikacja adresu Zamawiającego

(a) Adres miejsca prowadzenia działalności

CERTUM musi sprawdzić czy adres podany przez Zamawiającego jest adresem, pod którym Zamawiający faktycznie prowadzi działalność gospodarczą (tzn. nie jest to punkt przyjmowania poczty lub skrzynka pocztowa).

- (1) Jeśli adres prowadzonej działalności nie jest taki sam jak w **Kwalifikowanym Rządowym Źródle Informacji**, na podstawie którego CERTUM potwierdziło tożsamość oraz formę prawną Zamawiającego:
 - (A) Wobec Zamawiających, których adres prowadzonej działalności znajduje się przynajmniej w jeszcze jednym aktualnym **Kwalifikowanym Rządowym Źródle Informacji** lub **Kwalifikowanym, Niezależnym Źródle Informacji**, CERTUM akceptuje oświadczenie Zamawiającego, że adres, wskazany we Wniosku o wydanie Certyfikatu EV SSL, jest aktualnym adresem prowadzonej przez niego działalności;

(B) Wobec Zamawiających, którzy nie prowadzą działalności w miejscu potwierdzonym w przynajmniej jednym Kwalifikowanym Niezależnym Źródle Informacji, CERTUM weryfikuje adres Zamawiającego na podstawie wizyty kontrolnej, którą składa Zamawiającemu pracownik firmy/organizacji odpowiedzialnej za przeprowadzenie takiej kontroli lub pracownik CERTUM.

Na podstawie takiej wizyty przygotowany jest raport z wizyty, w trakcie której:

- zweryfikowano adres Zamawiającego;
- zweryfikowano czy obiekt mieszczący siedzibę Zamawiającego jest stałą jego rezydencją;
- wskazano czy w miejscu prowadzenia działalności istnieje stałe, nieusuwalne oznaczenie/logo Zamawiającego;
- wskazano czy istnieją dowody na to, że Zamawiający prowadzi w tamtym miejscu nieprzerwana działalność;
- załączono zdjęcia przedstawiające widok zewnętrzny miejsca prowadzenia działalności (wraz z widniejącym nań stałym, nieusuwalnym oznaczeniem zawierającym nazwę Zamawiającego oraz, jeśli to możliwe, z uwidocznionym adresem ulicy) oraz widok wewnętrzny miejsca pracy Subskrybenta.

(2) Wobec Zamawiających, którzy nie prowadzą działalności w tym samym kraju gdzie dokonano rejestracji, CERTUM polega na weryfikacji dostarczonej **Opinii Prawnej**, która wskazuje na adres prowadzonej przez Zamawiającego działalności oraz potwierdza faktyczną jego obecność w wymienionym miejscu.

(b) Numer telefonu w miejscu prowadzenia działalności

CERTUM musi sprawdzić, czy numer telefonu podany przez Zamawiającego jest jego głównym numerem telefonu właściwym dla miejsca działalności Zamawiającego.

Aby zweryfikować numer telefonu Zamawiającego, CERTUM musi wykonać działania opisane w punkcie (1) oraz jedno z działań z punktów (2) lub (3) poniżej:

(1) CERTUM musi zweryfikować numer telefonu Zamawiającego poprzez nawiązanie z nim połączenia i uzyskanie odpowiedzi pozwalającej potwierdzić, że Zamawiający jest dostępny pod danym numerem telefonu,

- (2) CERTUM musi potwierdzić w bazach danych właściwej firmy telekomunikacyjnej np. <http://www.pkt.pl/> lub co najmniej jednego Kwalifikowanego Niezależnego Źródła Informacji, że numer telefonu podany przez Zamawiającego jest przypisany do adresu miejsca prowadzonej przez niego działalności,
- (3) CERTUM musi uzyskać potwierdzoną Opinię Prawną gwarantującą, że podany przez Zamawiającego numer telefonu jest głównym numerem telefonu w miejscu prowadzonej przez niego działalności.

16. Weryfikacja działalności gospodarczej

Zamawiającego

Jeśli wpis do stosownego rejestru właściwego urzędu świadczy o tym, że Zamawiający prowadzi działalność gospodarczą przez okres krótszy niż trzy lata oraz nie figuruje w co najmniej jednym Kwalifikowanym Niezależnym Źródle Informacji, CERTUM musi sprawdzić, czy Zamawiający jest w stanie prowadzić działalność gospodarczą.

- (1) CERTUM musi sprawdzić czy Zamawiający posiada aktywny rachunek rozliczeniowy w zarejestrowanej instytucji finansowej (np. konto w banku). W tym celu CERTUM otrzymuje od osoby reprezentującej Zamawiającego dokumenty bankowe gwarantujące, że Zamawiający posiada aktywne konto bankowe w instytucji o uregulowanej pozycji finansowej (np. kopia umowy rachunku bankowego).
- (2) CERTUM może polegać na Opinii Prawnej zawierającej stosowne zapewnienie, że Zamawiający jest w stanie prowadzić działalność handlową będąc właścicielem aktywnego konta bankowego.

17. Weryfikacja domeny Subskrybenta

(a) Wymagania

CERTUM, aby potwierdzić, że Zamawiający jest właścicielem nazwy domeny będącej przedmiotem certyfikatu EV SSL lub posiada prawa do wyłączności w użytkowaniu domeny, musi zweryfikować, czy każda z nazw domenowych spełnia następujące wymagania:

- (1) Nazwa domeny zarejestrowana jest przez podmiot identyfikowany przez organizację Internet Corporation for Assigned Names and Numbers (ICANN) lub widnieje w rejestrach organizacji Internet Assigned Numbers Authority (IANA);

- (2) Informacje o domenie dostępne w bazie WHOIS powinny zawierać nazwę, adres fizyczny oraz dane kontaktowe organizacji;
- (3) Zamawiający jest zarejestrowanym właścicielem domeny lub posiada do niej wyłączone prawo, przyznane mu przez właściciela domeny.

(b) Akceptowane metody weryfikacji

- (1) Jeśli Subskrybent jest właścicielem domeny:
 - (A) CERTUM może sprawdzić informacje o domenie korzystając z bazy WHOIS w celu potwierdzenia praw Zamawiającego do posługiwania się nazwą domenową, lub
 - (B) CERTUM może nawiązać kontakt z osobą wymienioną w bazie WHOIS w celu potwierdzenia, że Zamawiający jest właścicielem nazwy domenowej lub, ewentualnie, uzgodnienia z osobą kontaktową aktualizacji danych w bazie WHOIS,
 - (C) CERTUM może, w przypadku gdy informacja o rejestracji domeny nie jest publicznie dostępna, nawiązać kontakt z rejestratorem domeny za pomocą poczty elektronicznej lub tradycyjnej.
- (2) Jeśli Zamawiający nie jest właścicielem domeny, CERTUM weryfikuje jego uprawnienia do posługiwania się domeną:
 - (A) CERTUM może polegać na Opinii Prawnej, która wskazuje na Zamawiającego jako posiadającego wyłączność na użytkowanie nazwy domeny lub
 - (B) CERTUM może polegać na uwierzytelnionym oświadczeniu złożonym przez Osobę Podpisującą Umowę lub Osobę Zatwierdzającą Certyfikat w połączeniu z demonstracją kontroli nad domeną poprzez dokonanie uprzednio uzgodnionej modyfikacji informacji zawartej na stronie WWW o określonym adresie URL w domenie FQDN subskrybenta;

CERTUM może upewnić się czy Zamawiający jest świadomy posiadanych przez siebie praw do domeny. W tym celu CERTUM kontaktuje się z jedną z osób reprezentujących Zamawiającego prosząc o potwierdzenie tego faktu.

18. Weryfikacja tożsamości, charakteru piastowanych stanowisk oraz upoważnień udzielonych Osobie Podpisującej Umowę i Osobie Zatwierdzającej Certyfikat

CERTUM weryfikuje następujące informacje:

- (1) **Dane osobowe, stanowisko oraz sposób reprezentacji Zamawiającego** – CERTUM musi zweryfikować nazwisko i tytuł Osoby Podpisującej Umowę oraz Osoby Zatwierdzającej Certyfikat. CERTUM musi również potwierdzić, że powyższe osoby reprezentują Zamawiającego .
- (2) **Upoważnienie Osoby Podpisującej Umowę** – CERTUM musi zweryfikować, poprzez źródło inne niż Osoba Podpisująca Umowę, że została ona wyraźnie upoważniona przez Zamawiającego do zawarcia Umowy z Subskrybentem (oraz każdego innego dwustronnego porozumienia).
- (3) **Upoważnienie Osoby Zatwierdzającej Certyfikat** – CERTUM musi zweryfikować, poprzez źródło inne niż sama Osoba Zatwierdzająca Certyfikat, że została ona wyraźnie upoważniona przez Zamawiającego do wykonania poniższych działań:
 - o złożenia lub – jeśli dotyczy – upoważnienia Wnioskodawcy do złożenia Wniosku o wydanie certyfikatu EV SSL w imieniu Zamawiającego oraz
 - o dostarczenia lub – jeśli dotyczy – upoważnienia Wnioskodawcy do dostarczenia informacji wymaganych od Zamawiającego w celu wydania certyfikatu EV SSL oraz
 - o zatwierdzenia Wniosku o wydanie certyfikatu EV SSL złożonego przez Wnioskodawcę.

Akceptowane metody weryfikacji danych osobowych, stanowisk oraz sposobu reprezentacji Subskrybenta przez Osobę Podpisującą Umowę oraz Osobę Zatwierdzającą Certyfikat:

- (1) **Dane osobowe i stanowisko** – CERTUM może zweryfikować nazwisko i tytuł Osoby Podpisującej Umowę i Osoby Zatwierdzającej Certyfikat za pomocą dowolnej metody zapewniającej wystarczającą pewność, że osoba weryfikowana jest w istocie

osobą wyznaczoną do działania w danej roli.

- (2) **Sposób reprezentacji Subskrybenta** – CERTUM może zweryfikować charakter, w jakim dane osoby występują w imieniu Zamawiającego poprzez:
- o nawiązanie kontaktu z działem kadr Zamawiającego (korespondencyjnie lub telefonicznie – kierując się danymi adresowymi, jakie przypisane są do miejsca prowadzenia działalności przez Zamawiającego i pozyskane zostały zgodnie ze wskazaniami niniejszego Załącznika) i uzyskanie potwierdzenia, że Osoba Podpisująca Umowę i/lub Osoba Zatwierdzająca Certyfikat są pracownikami Zamawiającego, lub
 - o uzyskanie oświadczenia Zamawiającego lub potwierdzonej **Opinii Prawnej** zaświadczających, że Osoba Podpisująca Umowę i/lub Osoba Zatwierdzająca Certyfikat są pracownikami Zamawiającego lub zostali przez niego upoważnieni do działania w jego imieniu.

CERTUM może również zweryfikować upoważnienie, jakie otrzymała Osoba Zatwierdzająca Certyfikat poprzez uzyskanie stosownego oświadczenia od Osoby Podpisującej Umowę (oświadczenie takie może być również elementem Umowy między Subskrybentem a CERTUM), pod warunkiem, że status Osoby Podpisującej Umowę został już uprzednio w pełni zweryfikowany.

Akceptowane metody weryfikacji upoważnień otrzymanych przez Osobę Podpisującą Umowę oraz Osobę Zatwierdzającą Certyfikat obejmują:

- (1) **Opinia Prawna** – Upoważnienie w/w osób do występowania w imieniu Subskrybenta może zostać zweryfikowane w oparciu o potwierdzoną Opinię Prawną.
- (2) **Zarządzenie firmy lub organizacji** – Upoważnienie w/w osób do występowania w imieniu Zamawiającego może zostać zweryfikowane w oparciu o prawidłowo potwierdzone zarządzenie, które nadaje takie upoważnienia, pod warunkiem, że zarządzenie jest (i) poświadczone przez upoważnionego pracownika firmy lub organizacji (np. sekretarza) oraz (ii) CERTUM może bez wątpliwości potwierdzić, że poświadczenie zostało złożone przez taką właśnie osobę, której atrybuty wskazują na posiadanie przez nią roli decyzyjnej w organizacji lub firmie.
- (3) **Oświadczenie Zamawiającego** – Upoważnienie może zostać zweryfikowane na podstawie otrzymanego przez CERTUM oświadczenia Zamawiającego.
- (4) **Umowa między CERTUM a Subskrybentem** – Upoważnienie Osoby

Zatwierdzającej Certyfikat może być częścią umowy pomiędzy CERTUM a Subskrybentem, której treść wskazuje na Osobę Zatwierdzającą Certyfikat jako posiadającą prawo do występowania w imieniu Subskrybenta, pod warunkiem, że umowa ta została podpisana przez Osobę Podpisującą Umowę, której status został już uprzednio w pełni zweryfikowany.

- (5) **Wcześniejsze upoważnienie** – Jeśli nie wcześniej niż 90 dni przed złożeniem zamówienia na certyfikat EV SSL została zawarta przez Subskrybenta umowa na świadczenie na jego rzecz przez CERTUM usług certyfikacyjnych (jednak wyłącznie odnośnie certyfikatów SSL) zaś umowie tej towarzyszyło upoważnienie w/w osób do występowania w imieniu Zamawiającego oraz umowa ta została podpisana przez Osobę Podpisującą Umowę lub Osobę Zatwierdzającą Certyfikat to CERTUM może na podstawie takiego upoważnienia pozytywnie zweryfikować w/w osoby jako uprawnione do występowania w imieniu Subskrybenta. Elementy wcześniejszej umowy jakie CERTUM weryfikuje to m. in.:

- Tytuł umowy
- Data zawarcia umowy
- Numer umowy
- Miejsce zawarcia umowy

Wcześniejsze upoważnienie może służyć jako podstawa weryfikacji także wówczas gdy CERTUM posiada oświadczenie Osoby Zatwierdzającej Certyfikat lub zweryfikowane upoważnienie Osoby Zatwierdzającej Certyfikat, która:

- na podstawie zawartej z CERTUM umowy, świadczy wobec Zamawiającego usługi Punktu Rejestracji
- zatwierdziła już jeden lub więcej certyfikatów SSL wydanych przez CERTUM Zamawiającemu. W takim przypadku CERTUM musi skontaktować się telefonicznie z Osobą Zatwierdzającą Certyfikat korzystając z uprzednio zweryfikowanego numeru telefonu.

- (6) **Długoterminowe upoważnienie Osoby Zatwierdzającej Certyfikat** – W przypadku, gdy CERTUM i Subskrybent zakładają wielokrotne składanie Wniosków o wydanie certyfikatu EV SSL i wielokrotne wydawanie certyfikatów EV SSL oraz gdy:

- CERTUM zweryfikowało status Osoby Podpisującej Umowę i
- CERTUM zweryfikowało uprawnienia Osoby Podpisującej Umowę do

występowania w imieniu Subskrybenta, wówczas

CERTUM oraz Zamawiający mogą zawrzeć pisemną umowę, podpisaną przez Osobę Podpisującą Umowę w imieniu Zamawiającego, na mocy której przez wskazany okres czasu Zamawiający udzieli jednej lub kilku Osobom Zatwierdzającym Certyfikat wskazanym w umowie upoważnienia do składania w przyszłości kolejnych Wniosków o wydanie certyfikatu EV SSL.

Umowa taka musi zapewniać, że Zamawiający będzie uznawał wszystkie Wnioski o wydanie certyfikatów EV SSL, złożone lub zatwierdzone przez Osobę Zatwierdzającą Certyfikat do czasu odwołania udzielonego jej upoważnienia. Umowa musi dotyczyć (i) uwierzytelnienia Osoby Zatwierdzającej Certyfikat, gdy ta zatwierdza Wnioski o wydanie certyfikatu EV SSL, (ii) okresowego nadania upoważnienia Osobie Zatwierdzającej Certyfikat, (iii) bezpiecznej procedury powiadamiania CERTUM przez Zamawiającego o wycofaniu upoważnienia dla Osoby Zatwierdzającej Certyfikat oraz (iv) innych wymaganych sytuacją środków ostrożności.

19. Weryfikacja podpisu pod Umową z Subskrybentem i Wnioskiem o wydanie certyfikatu EV SSL

Umowa z Subskrybentem oraz każdy Wniosek o wydanie certyfikatu EV SSL muszą być podpisane. Umowa musi być podpisana przez upoważnioną Osobę Podpisującą Umowę. Wniosek o wydanie certyfikatu EV SSL musi być podpisany przez Wnioskodawcę. Jeśli Wnioskodawca nie jest jednocześnie Osobą Zatwierdzającą Certyfikat, upoważniona Osoba Zatwierdzająca Certyfikat musi niezależnie potwierdzić Wniosek o wydanie certyfikatu EV SSL. We wszystkich przypadkach podpis musi być ważnym podpisem odręcznym lub pieczęcią (dla papierowych Umów i Wniosków), lub ważnym podpisem elektronicznym (dla Umowy i Wniosku elektronicznego) wiążącym Zamawiającego z treścią obu dokumentów.

(a) Wymagania dotyczące weryfikacji

- (1) **Podpis:** CERTUM musi sprawdzić podpis Osoby Podpisującej się pod Umową z Subskrybentem oraz podpis Wnioskodawcy pod każdym Wnioskiem o wydanie certyfikatu EV SSL w sposób gwarantujący pewność, że osoba wymieniona jako podpisująca dany dokument jest w istocie osobą, która podpisała dokument w

imieniu Zamawiającego.

- (2) **Alternatywa:** W przypadku, gdy Wniosek o wydanie certyfikatu EV SSL jest podpisany przez Wnioskodawcę, który nie jest jednocześnie Osobą Zatwierdzającą Certyfikat, zatwierdzenie Wniosku przez Osobę Zatwierdzającą Certyfikat, zgodnie z postanowieniami opisanymi w rozdziale 18, może zastąpić konieczność weryfikacji podpisu samego Wnioskodawcy.

(b) Akceptowane metody weryfikacji

- (1) CERTUM może przeprowadzić z przedstawicielem Subskrybenta rozmowę telefoniczną, nawiązując połączenie z numerem telefonu potwierdzonym zgodnie z niniejszym Załącznikiem, podczas której prosi się o rozmowę z Wnioskodawcą lub Osobą Podpisującą Umowę (w zależności od sytuacji). Osoba, która przedstawi się jako Wnioskodawca lub Osoba Podpisująca Umowę powinna potwierdzić, że podpisała i złożyła badany dokument w imieniu Zamawiającego.
- (2) CERTUM może zwrócić się listownie do Zamawiającego lub jego przedstawiciela – list adresowany jest wówczas do Wnioskodawcy lub Osoby Podpisującej Umowę – z prośbą o informację zwrotną potwierdzającą, że dana osoba podpisała i złożyła dany dokument w imieniu Zamawiającego.
- (3) CERTUM może zastosować inny sposób weryfikacji nazwiska i tytułu/stanowiska osoby podpisującej dany dokument. CERTUM może wykorzystać do tego celu szyfrowany kanał komunikacyjny, który pozwala na identyfikację osoby podpisującej dokument poprzez użycie podpisów elektronicznych weryfikowanych za pomocą stosownych certyfikatów.
- (4) CERTUM może polegać na notarialnym poświadczeniu podpisów pod warunkiem, że sprawdzi, czy dany notariusz jest upoważnionym do świadczenia usług notarialnych na terytorium, gdzie prowadzona jest działalność Zamawiającego.

20. Weryfikacja zatwierdzenia Wniosku o wydanie certyfikatu EV SSL

W przypadku, gdy Wniosek o wydanie certyfikatu EV SSL został złożony przez Wnioskodawcę, który pozostaje różny od Osoby Zatwierdzającej Certyfikat, CERTUM przed wydaniem

żądanego Certyfikatu musi potwierdzić, że upoważniona Osoba Zatwierdzająca Certyfikat przejrzała i zatwierdziła Wniosek. W tym celu:

- (1) CERTUM nawiązuje kontakt z Osobą Zatwierdzającą Certyfikat telefonując na zweryfikowany już numer telefonu lub wysyłając list na adres pocztowy Zamawiającego w celu uzyskania ustnego lub pisemnego potwierdzenia, że Osoba Zatwierdzająca Certyfikat przejrzała i zaakceptowała Wniosek o wydanie certyfikatu EV SSL;
- (2) CERTUM powiadamia Osobę Zatwierdzającą Certyfikat, że jeden lub więcej Wniosków o wydanie certyfikatu EV SSL jest dostępnych do przejrzenia i zatwierdzenia poprzez dedykowaną, zabezpieczoną stronę WWW. Osoba Zatwierdzająca Certyfikat powinna zalogować się na wskazanej stronie i wyrazić akceptację Wniosku w sposób wymagany przez mechanizm strony.

21. Weryfikacja Źródeł Informacji Pewnej

(a) Zweryfikowana Opinia Prawna

Przed akceptacją jakiegokolwiek opinii prawnej, CERTUM musi zweryfikować następujące elementy:

- (A) **Status autora** – CERTUM musi zweryfikować, czy Opinia Prawna jest autorstwa niezależnego prawnika, reprezentującego Zamawiającego (np. prawnika zatrudnionego przez Zamawiającego) będącego:
 - (1) prawnikiem (notariuszem, adwokatem, etc.), uprawnionym do świadczenia usług prawnych w kraju, w którym Zamawiający prowadzi działalność lub kraju, w którym Zamawiający posiada biuro lub inną siedzibę;
 - (2) notariuszem, będącym członkiem Międzynarodowej Unii Notariuszy (*International Union of Latin Notaries*) uprawnionym do świadczenia usług notarialnych w kraju w którym Zamawiający prowadzi działalność lub kraju, w którym Zamawiający posiada biuro lub inną siedzibę.
- (B) **Podstawa Opinii** – CERTUM musi zweryfikować, czy autor opinii działa w imieniu Zamawiającego oraz czy potwierdzona przez niego Opinia Prawna jest oparta na znajomości przez niego faktów, których dotyczy Opinia Prawna oraz czy wiedza ta

poparta jest zawodowym doświadczeniem i właściwie wykonaną ekspertyzą. Opinia może również zawierać zwyczajowe w danym prawodawstwie klauzule i ograniczenia pod warunkiem, że zakres odpowiedzialności autora opinii nie pozwala na to, aby potencjalne błędy lub zaniechania w wydanej Opinii Prawnej nie powodowały żadnych konsekwencji (finansowych, zawodowych lub reputacji) dla prawnika sporządzającego Opinię.

- (C) **Autentyczność** – CERTUM musi potwierdzić autentyczność Opinii Prawnej, nawiązując połączenie telefoniczne z jej autorem lub wysyłając kopię Opinii Prawnej na adres, telefon, faks lub adres email, które muszą być potwierdzone w jednostce odpowiedzialnej za rejestrację i licencjonowanie osób świadczących usługi prawne na terytorium danego kraju. Wysyłając kopię Opinii Prawnej CERTUM zwraca się z prośbą o potwierdzenie przez autora Opinii lub jego asystenta, że przedłożona Opinia jest autentyczna. Jeśli dane kontaktowe prawnika nie mogą być pozyskane ze źródła odpowiedzialnego za jego rejestrację i/lub licencjonowanie CERTUM może skorzystać z informacji zawartych w Kwalifikowanych Niezależnych Źródłach Informacji lub **Kwalifikowanych Rządowych Źródłach Informacji**.

(b) Weryfikacja autentyczności bezpośredniego spotkania

Przed akceptacją jakichkolwiek dokumentów otrzymanych od strony trzeciej przeprowadzającej weryfikację Zamawiającego (prawnik, rewident etc.), CERTUM sprawdza czy strona trzecia spełnia następujące warunki:

- (A) **Kwalifikacje strony trzeciej** – CERTUM w sposób niezależny weryfikuje czy strona trzecia jest kwalifikowanym notariuszem, prawnikiem lub biegłym księgowym (rewidentem) zarejestrowanym w miejscu, w którym świadczy on swoje usługi..
- (B) **Dokumenty** – CERTUM upewnia się, że strona trzecia widziała dostarczone jej przez osobę reprezentującą Zamawiającego dokumenty aplikacyjne.
- (C) **Oświadczenie** – Jeśli strona trzecia nie jest notariuszem prawa łacińskiego, CERTUM weryfikuje oświadczenie strony trzeciej, że przesłane przez nią dokumenty zostały zweryfikowane i są w pełni autentyczne. W tym celu CERTUM kontaktuje się telefonicznie ze stroną trzecią z prośbą o potwierdzenie przez osobę dokonującą weryfikacji lub jej asystenta, że przedłożone dokumenty dostarczone zostały stronie trzeciej w trakcie bezpośredniego spotkania z osobą/osobami reprezentującymi Zamawiającego. Informacje otrzymane przez CERTUM od strony trzeciej wykorzystywane są wyłącznie dla celów weryfikacji Subskrybenta. W przypadku, gdy

potwierdzenie podpisane jest elektronicznie w sposób gwarantujący jego autentyczność, weryfikacja opisana powyżej nie jest wymagana.

(c) Weryfikacja Oświadczenia Zamawiającego

Oświadczenie Zamawiającego jest formą uwierzytelnienia konkretnego faktu (np. wiedzy o wyłącznej kontroli nad domeną, potwierdzeniem statusu zatrudnienia Osoby Podpisującej Umowę lub Osoby Zatwierdzającej Certyfikat, potwierdzeniem upoważnienia dla w/w osób etc). Elementy, które charakteryzują takie Oświadczenie są następujące:

- (i) CERTUM otrzymuje Oświadczenie Zamawiającego od osoby zatrudnionej przez Zamawiającego (innej niż weryfikowana osoba), posiadającej stosowne upoważnienia do potwierdzania faktów nazywaną w niniejszym Załączniku **Osobą Potwierdzającą**,
- (ii) CERTUM otrzymuje Oświadczenie Zamawiającego w sposób umożliwiający autoryzację i weryfikację źródła z jakiego pochodzi oświadczenie oraz
- (iii) Oświadczenie Zamawiającego jest wiążące dla Zamawiającego

CERTUM otrzymuje Oświadczenie Zamawiającego w następujący sposób:

- (1) CERTUM musi zainicjować nawiązanie kontaktu z Zamawiającym w celu uzyskania od niego potwierdzenia danych faktów lub w celu zdobycia dodatkowych informacji:
 - (A) **Adres** – Prośba CERTUM musi być skierowana do:
 - (i) osoby piastującej w organizacji lub firmie Zamawiającego stanowisko kwalifikujące ją do bycia Osobą Potwierdzającą (np. sekretarz, prezes, właściciel, współwłaściciel, członek zarządu, dyrektor etc), która określona jest z imienia i nazwiska oraz stanowiska w aktualnym Kwalifikowanym Rządowym Źródle Informacji (np. Krajowy Rejestr Sądowy), Kwalifikowanym Niezależnym Źródle Informacji, potwierdzonej Opinii Prawnej, Opinii Biegłego Rewidenta lub jej tożsamość została zweryfikowana telefonicznie lub listownie w dziale kadr organizacji lub firmy Zamawiającego lub
 - (ii) urzędu, który zarejestrował działalność Zamawiającego, z prośbą o uzyskanie kontaktu do właściwej Osoby Potwierdzającej bądź przekierowanie do niej sformułowanej przez CERTUM prośby.

(iii) osoby będącej przełożonym Osoby Podpisującej Umowę lub Osoby Zatwierdzającej Certyfikat. Kontakt do w/w osoby powinien być pozyskany za pośrednictwem działu kadr organizacji/firmy Zamawiającego (pod warunkiem, że numer telefonu został zweryfikowany zgodnie z wymaganiami niniejszego Załącznika)

(B) **Sposoby komunikacji** – Prośba CERTUM musi być skierowana do Osoby Zatwierdzającej Certyfikat w sposób umożliwiający dotarcie do niej wysłanej prośby. Akceptowane formy komunikacji obejmują:

(i) List tradycyjny, wysyłany do Osoby Potwierdzającej:

(a) na adres miejsca działalności Zamawiającego, zweryfikowany zgodnie z niniejszym Załącznikiem lub

(b) na adres służbowy Osoby Potwierdzającej, określony w aktualnym Kwalifikowanym Rządowym Źródle Informacji, Kwalifikowanym Niezależnym Źródle Informacji, potwierdzonej Opinii Prawnej, potwierdzonej opinii biegłego rewidenta lub

(c) na adres urzędu, który zarejestrował działalność Zamawiającego, z prośbą o uzyskanie kontaktu do właściwej Osoby Potwierdzającej bądź przekierowanie do niej sformułowanej przez CERTUM prośby.

(ii) Poczta elektroniczna adresowana do Osoby Potwierdzającej na jej adres służbowy, określony w aktualnym Kwalifikowanym Rządowym Źródle Informacji, Kwalifikowanym Niezależnym Źródle Informacji, potwierdzonej Opinii Prawnej lub potwierdzonej Opinii Biegłego Rewidenta lub

(iii) Rozmowa telefoniczna z Osobą Potwierdzającą, przy założeniu, że telefon wykonuje się na główny numer Zamawiającego (zweryfikowany zgodnie z niniejszymi Załącznikami), po czym następuje przełączenie do Osoby Potwierdzającej, zaś osoba do której rozmowa zostanie przełączona potwierdzi własną tożsamość lub

(iv) Faks kierowany do Osoby Potwierdzającej w miejscu działalności Zamawiającego. Numer faksu musi być ujęty w aktualnym Kwalifikowanym Rządowym Źródle Informacji, Kwalifikowanym

Niezależnym Źródle Informacji, potwierdzonej Opinii Prawnej lub potwierdzonej Opinii Biegłego Rewidenta. Strona tytułowa musi wyraźnie wskazywać, że faks jest adresowany do Osoby Potwierdzającej.

- (2) CERTUM musi otrzymać odpowiedź na złożoną prośbę od Osoby Potwierdzającej Certyfikat, która potwierdzi weryfikowane informacje. Odpowiedź może mieć formę rozmowy telefonicznej, wiadomości poczty elektronicznej lub listu tradycyjnego pod warunkiem, że CERTUM będzie w stanie zweryfikować, że została ona udzielona przez właściwą Osobę Potwierdzającą.

(d) Kwalifikowane Niezależne Źródło Informacji

Kwalifikowane Niezależne Źródło Informacji to regularnie aktualizowana, publicznie dostępna baza danych, ogólnie rozpoznawana jako niezawodne źródło informacji, którym może być komercyjna baza danych, jeśli spełnia następujące warunki:

- (1) Informacje w niej zawarte zostały zweryfikowane także przez inne niezależne źródła informacji;
- (2) Baza danych wyraźnie odróżnia informacje pozyskane we własnym zakresie od informacji otrzymanych od innych niezależnych źródeł informacji;
- (3) Dostawca, właściciel, zarządzający bazą informuje jak często ma miejsce aktualizacja danych;
- (4) Zmiany zachodzące w danych znajdują odzwierciedlenie w bazie nie później niż w przeciągu 12 miesięcy;
- (5) Dostawca, zarządzający bazą korzysta z wiarygodnych źródeł informacji niezwiązanych z podmiotem, którego dotyczą lub korzysta z wielu potwierdzających się wzajemnie źródeł.

(e) Kwalifikowane Rządowe Źródło Informacji

Kwalifikowane Rządowe Źródło Informacji to regularnie aktualizowana, publicznie dostępna baza danych stworzona w celu umożliwienia pozyskania dokładnej informacji, ogólnie rozpoznawana jako niezawodne jej źródło, które utrzymywane jest przez organ administracji państwowej. Ten publikuje informacje obligatoryjnie, zaś zgłoszenie i/lub

publikacja danych nieprawdziwych jest zagrożone karą kodeksu karnego lub cywilnego.

22. Pozostałe wymagania dotyczące weryfikacji

(a) Status wysokiego ryzyka

CERTUM musi wskazać i zweryfikować Zamawiających, których znamionuje wysokie ryzyko bycia obiektem ataków typu *phishing* lub innych form oszustw internetowych, wobec których CERTUM podejmuje takie dodatkowe kroki weryfikacji, które gwarantują prawidłowe i rzetelne zweryfikowanie Zamawiającego zgodnie z niniejszym Załącznikiem. CERTUM może identyfikować **Zamawiających Wysokiego Ryzyka** poprzez sprawdzenie stosownych list organizacji/przedsiębiorstw, będących najczęstszymi obiektami ataków typu *phishing* lub innych nieuczciwych działań. Certyfikaty EV SSL wydawane takim podmiotom powinny być automatycznie oznaczone jako certyfikaty wysokiego ryzyka i powinny podlegać dalszym czynnościom sprawdzającym. Przykładami takich list są:

- (1) listy obiektów będących celem ataków typu *phishing*, publikowane przez Anti-Phishing Work Group (APWG), oraz
- (2) wewnętrzne bazy danych, prowadzone przez CERTUM, zawierające certyfikaty EV SSL oraz Wnioski o wydanie certyfikatów EV SSL unieważnione lub odrzucone z uwagi na podejrzenie *phishingu* lub innych form oszustw internetowych

(b) Listy odmowne oraz „czarne listy”

CERTUM nie wydaje certyfikatów EV SSL Zamawiającemu, jeśli Zamawiający, osoby reprezentujące Zamawiającego lub kraj, w którym jest zarejestrowany albo działa Zamawiający odpowiadają poniższej charakterystyce:

- (1) Zamawiający figuruje na listach firm/organizacji, z którymi prowadzenie wymiany handlowej jest zabronione lub na listach osób objętych zakazem wykonywania czynności prawnych lub publicznie, na mocy prawa, wskazane są jako osoby lub podmioty posiadające zobowiązania finansowe wobec innych osób, firm, organizacji etc.
- (2) Zamawiający działa na terytorium kraju, z którym prawo Rzeczypospolitej Polskiej

zakazuje prowadzenia wymiany handlowej.

CERTUM sprawdza następujące rodzaje informacji:

- (1) Stosowne rejestry osób fizycznych
- (2) Stosowne rejestry podmiotów gospodarczych, organizacji, stowarzyszeń etc.
- (3) Regulacje prawne dotyczące ograniczeń eksportowych obowiązujących na terytorium Rzeczypospolitej Polskiej.

23. Podwójna weryfikacja

Rezultaty procesu weryfikacji i realizacji procedur opisanych w niniejszym Załączniku powinny być rozpatrywane zarówno indywidualnie jak i grupowo. Dlatego też, po zakończeniu procesu weryfikacji, CERTUM musi przy pomocy osoby nie będącej odpowiedzialną za proces pozyskiwania informacji, dokonać raz jeszcze analizy wszystkich dokumentów oraz danych w nich zawartych, jakie CERTUM otrzymało w związku z procedurą wydania certyfikatu EV SSL. Korelacja dokumentów ma na celu wykrycie ewentualnych rozbieżności, które wymagałyby dalszych wyjaśnień. Zgromadzenie możliwie największej ilości informacji dotyczących Zamawiającego oraz przeprowadzanie na ich podstawie dokładnej weryfikacji Wniosku o wydanie certyfikatu EV SSL gwarantuje, że postępowanie certyfikacyjne CERTUM wyczerpuje znamiona działania z należytą starannością.

24. Wymagania dotyczące odnowień certyfikatów EV SSL

Przed odnowieniem certyfikatu EV SSL CERTUM musi przeprowadzić pełną weryfikację Zamawiającego, jakiej wymaga niniejszy Załącznik, aby upewnić się, że żądanie odnowienia zostało w sposób właściwy potwierdzone przez Zamawiającego a wszystkie informacje publikowane w certyfikacie EV SSL są nadal ważne i aktualne.

G. STATUS ORAZ UNIEWAŻNIENIE CERTYFIKATU EV SSL

25. Sprawdzenie statusu certyfikatu EV SSL

CERTUM zapewnia, że repozytorium, za pomocą którego przeglądarki internetowe będą mogły automatycznie, w czasie rzeczywistym, sprawdzać aktualny status certyfikatów, jest publicznie dostępne przez 24 godziny 7 dni w tygodniu.

- (1) Dla certyfikatów EV SSL
 - (A) CRL: (Listy Certyfikatów Unieważnionych) muszą być aktualizowane co najmniej raz na 7 dni, zaś okres ich ważności to maksymalnie 10 dni lub
 - (B) OCSP: Począwszy od Stycznia 2011 urząd **Certum Extended Validation CA** dostarcza informacje dotyczące unieważnień za pomocą protokołu Online Certificate Status Protocol (OCSP) aktualizując odpowiedzi OCSP nie rzadziej niż raz na 4 dni, z maksymalnym okresem ważności odpowiedzi 10 dni.
- (2) Dla certyfikatów urzędów pośrednich głównego urzędu **Certum Trusted Network CA**:
 - (A) CRL: Listy Certyfikatów Unieważnionych są aktualizowane, co najmniej raz na 12 miesięcy, z maksymalnym okresem ważności 12 miesięcy; lub
 - (B) OCSP: Począwszy od Stycznia 2011 urząd **Certum Trusted Network CA** dostarcza informacje dotyczące unieważnień za pomocą protokołu Online Certificate Status Protocol (OCSP) aktualizując odpowiedzi OCSP nie rzadziej niż raz na 12 miesięcy, z maksymalnym okresem ważności odpowiedzi 12 miesięcy.

CERTUM świadcząc usługi CRL i/lub OCSP zapewnia wystarczająco krótki czas odpowiedzi dla zapytań generowanych dla wszystkich certyfikatów EV SSL. CERTUM zapewnia możliwość pobrania wszystkich list CRL dla całej ścieżki certyfikatu EV SSL w ciągu trzech sekund za pomocą analogowej linii telefonicznej przy normalnym obciążeniu sieci.

Zapisy dotyczące unieważnień, czy to w CRL, czy w usłudze OCSP nie mogą być usunięte do czasu upłynięcia pierwotnych okresów ważności unieważnionych certyfikatów EV SSL.

26. Unieważnianie certyfikatów EV SSL

CERTUM zobowiązuje się unieważnić certyfikat EV SSL, jeśli nastąpiło którekolwiek z poniższych wydarzeń:

- (1) Subskrybent zażądał unieważnienia swojego certyfikatu EV SSL;
- (2) Subskrybent zgłosił, że Wniosek o wydanie certyfikatu EV SSL nie został autoryzowany i nie udziela mu takiej autoryzacji;
- (3) Zachodzi uzasadnione podejrzenie, że klucz prywatny Subskrybenta (związany z kluczem publicznym certyfikatu EV SSL) został ujawniony lub certyfikat EV SSL został użyty niezgodnie z przeznaczeniem;
- (4) CERTUM otrzyma zgłoszenie lub uzyska informację, że Subskrybent naruszył istotne postanowienia Umowy z Subskrybentem;
- (5) CERTUM otrzyma zgłoszenie lub uzyska informację, że sąd lub uprawniony do tego podmiot odebrał Subskrybentowi prawo do posługiwania się nazwą domenową zawartą w Certyfikacie EV SSL lub Subskrybent nie odnowił swoich praw względem nazwy domeny;
- (6) CERTUM otrzyma zgłoszenie lub uzyska informację o istotnej zmianie informacji zawartych w certyfikacie EV SSL;
- (7) CERTUM uzna, że certyfikat EV SSL nie został wydany zgodnie z warunkami i ograniczeniami niniejszego Załącznika lub polityk EV;
- (8) CERTUM ustali, że jakkolwiek informacja zawarta w certyfikacie EV SSL jest nieaktualna;
- (9) CERTUM zaprzestanie świadczenia usług i nie przekaze swoich zobowiązań innemu urzędowi, który będzie świadczył usługi unieważniania;
- (10) Prawa jakie posiada CERTUM do wydawania certyfikatów EV SSL zostaną mu odebrane lub wygasną (chyba, że CERTUM przekaze obowiązki związane ze świadczeniem usług CRL/OCSP innemu urzędowi);
- (11) Klucz prywatny CERTUM, używany do podpisywania certyfikatów EV SSL zostanie unieważniony;
- (12) Nastąpiło jakiegokolwiek inne zdarzenie wymienione w opublikowanych politykach dotyczących certyfikatów EV SSL lub

- (13) CERTUM otrzyma zgłoszenie lub uzyska informacje o umieszczeniu Subskrybenta na liście odmownej lub *Czarnej Liście* lub otrzyma informacje o działalności Subskrybenta w kraju objętym ograniczeniami eksportowymi z punktu widzenia prawodawstwa Rzeczypospolitej Polskiej.

27. Zgłaszanie problemów z certyfikatami EV SSL

CERTUM dostarcza Subskrybentom, Stronom Ufającym, **Dostawcom Oprogramowania** i innym stronom trzecim, jasnych instrukcji dotyczących zgłaszania skarg lub podejrzeń ujawnienia kluczy prywatnych certyfikatów EV SSL, niewłaściwego użycia certyfikatów EV SSL oraz różnego rodzaju nadużyć lub nieprawidłowości związanych z certyfikatami EV SSL. Zarazem CERTUM gwarantuje, że jest zdolne do obsługi takich zgłoszeń 24 godziny na dobę przez 7 dni w tygodniu, udostępniając w tym celu stronę:

http://www.certum.pl/certum/cert,kontakt_pomoc24h.xml

CERTUM zobowiązuje się rozpocząć badanie wszystkich zgłoszonych problemów z certyfikatem EV SSL w ciągu 24 godzin od przyjęcia zgłoszenia i podjąć decyzję o unieważnieniu lub innym niezbędnym działaniu na podstawie:

- (i) natury zgłaszanego problemu,
- (ii) ilości zgłoszeń otrzymanych w związku z danym certyfikatem EV SSL lub witryną WWW zabezpieczoną takim certyfikatem,
- (iii) tożsamością zgłaszającego (np. zgłoszenie od przedstawiciela organów ścigania, że strona zaangażowana jest w nielegalne działania ma wyższą wagę niż zgłoszenie reklamacyjne),
- (iv) stosownych przepisów prawa.

CERTUM posiada zdolność reagowania na zgłoszone problemy z certyfikatem EV SSL przez 24 godziny 7 dni w tygodniu oraz – kiedy to wymagane – dalszego kierowania takich problemów do organów ścigania i/lub unieważnienia certyfikatu EV SSL danego podmiotu.

H. PRACOWNICY I STRONY TRZECIE

28. Wiarygodność i kompetencje

Przed upoważnieniem danej osoby do wykonywania pracy związanej z obsługą certyfikatów EV SSL, czy to jako pracownika CERTUM, czy niezależnego podwykonawcy, CERTUM weryfikuje tożsamość oraz wiarygodność takiej osoby:

- (1) poprzez osobiste stawiennictwo danej osoby przed pracownikiem CERTUM pełniącym jedną z zaufanych ról² lub pracownikiem działu kadr Unizeto Technologies S.A oraz
- (2) weryfikację przynajmniej jednego z dokumentów ze zdjęciem danej osoby identyfikującym jej tożsamość (np. paszport i/lub prawa jazdy).

CERTUM weryfikuje następujące informacje:

- (1) potwierdzenie poprzedniego zatrudnienia danej osoby,
- (2) sprawdzenie referencji zawodowych danej osoby,
- (3) potwierdzenie wykształcenia danej osoby,
- (4) sprawdzenie danej osoby w rejestrze skazanych.

CERTUM wymaga od swoich pracowników wykonujących czynności weryfikacyjne zdania wewnętrznych egzaminów sprawdzających znajomość wymagań jakie stawia niniejszy Załącznik wobec postępowania z Wnioskami o wydanie certyfikatu EV SSL.

29. Punkty Rejestracji oraz podwykonawcy

CERTUM może przekazać realizację części lub wszystkich wymagań opisanych w niniejszym Załączniku Punktom Rejestracji (zwanym dalej PR) lub podwykonawcom pod warunkiem, że część ostateczna (druga) procesu certyfikacji opisana w rozdziale 23 pozostanie w gestii CERTUM.

Podwykonawców oraz Punkty Rejestracji obowiązują wymagania opisane w rozdziale 28.

CERTUM może upoważnić podmiot ważnego certyfikatu EV SSL do pełnienia funkcji Punktu Rejestracji a także upoważnić inne urzędy do wydawania dodatkowych certyfikatów EV SSL dla domen trzeciego lub wyższego poziomu w obrębie głównej domeny przynależnej do głównego certyfikatu EV SSL danego podmiotu (zwanego również

² Patrz rozdział 5.2.1 Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM.

„**Certyfikatem EV SSL typu Enterprise**”). W takiej sytuacji, podmiot będzie uznawany za **Punkt Rejestracji typu Enterprise** i zastosowanie znajdą poniższe zapisy:

- (i) Żaden PR typu Enterprise nie może upoważnić CERTUM do wydania certyfikatu EV SSL typu Enterprise trzeciego lub wyższego poziomu domenowego podmiotowi innemu niż PR typu Enterprise lub organizacji będącej pod bezpośrednią kontrolą PR Enterprise;
- (ii) We wszystkich przypadkach podmiotem certyfikatu EV SSL typu Enterprise musi być organizacja zweryfikowana przez CERTUM zgodnie z niniejszym Załącznikiem;
- (iii) CERTUM musi wymóc powyższe ograniczenia jako zapisy kontraktowe oraz monitorować zgodność postępowania z nimi PR Enterprise;
- (iv) Zasada podwójnej weryfikacji opisana w rozdziale 23 niniejszego załącznika może być realizowana przez osobę reprezentującą PR Enterprise.

We wszystkich przypadkach Punkty Rejestracji oraz inni podwykonawcy współpracujący z CERTUM zobowiązują się na podstawie umowy zawartej z CERTUM do przestrzegania wymagań opisanych w niniejszym Załączniku oraz stosować się do nich w sposób, w jak robi to CERTUM.

I. DOKUMENTACJA I ARCHIWIZACJA DANYCH

30. Dokumentacja zdarzeń na potrzeby audytu

CERTUM dokumentuje szczegółowo wszystkie działania podjęte w celu obsługi Wniosku o wydanie certyfikatu EV SSL i wydania certyfikatu EV SSL, włączając w to wszelkie informacje utworzone lub otrzymane w związku z żądaniem przez subskrybenta wydania certyfikatu EV SSL oraz wszystkie działania podjęte w celu przetworzenia takiego żądania – w tym: czas, datę i personel zaangażowany w realizację zadania. Wymagania dotyczące tworzenia i udostępniania zapisów na potrzeby audytu dotyczą również wszystkich PR oraz podwykonawców i obejmują, między innymi, następujące zdarzenia:

- (i) Zdarzenia związane z zarządzaniem cyklem życia klucza CERTUM:
 - (a) Tworzenie klucza, tworzenie kopii zapasowej klucza, przechowywanie, odzyskiwanie, archiwizacja i zniszczenie klucza;
 - (b) Zdarzenia związane z zarządzaniem cyklem życia urządzeń kryptograficznych.
- (ii) Zdarzenia związane z zarządzaniem cyklem życia certyfikatu EV SSL subskrybenta i certyfikatu CERTUM:
 - (a) Wnioski o wydanie certyfikatu EV SSL, żądania odnowień, aktualizacji kluczy i unieważnienia;
 - (b) Czynności weryfikacyjne wymagane przez niniejszy Załącznik;
 - (c) Daty, czas, numery telefonów, dane osób kontaktowych i rezultaty telefonicznych weryfikacji;
 - (d) Akceptacja i odrzucenie Wniosków o wydanie certyfikatu EV SSL;
 - (e) Wydanie certyfikatu EV SSL;
 - (f) Tworzenie list CRL rekordów OCSP dla certyfikatów EV SSL.
- (iii) Zdarzenia związane z bezpieczeństwem:
 - (a) Udane i nieudane próby dostępu do systemów PKI;
 - (b) Działania administracyjne w systemie PKI i systemie bezpieczeństwa;
 - (c) Zmiany profili bezpieczeństwa;
 - (d) Awarie systemu, sprzętu i inne anomalie;
 - (e) Aktywność routerów i firewalli;
 - (f) Wejścia i wyjścia do siedziby CERTUM.

- (iv) Zapisy zdarzeń zawierają następujące informacje:
 - (a) Datę i czas zapisu;
 - (b) Tożsamość osoby dokonującej zapisu;
 - (c) Opis rekordu.

31. Przechowywanie dokumentacji

Zapisy są dostępne na żądanie niezależnych audytorów. Zapisy powinny być przechowywane przez co najmniej 7 lat. CERTUM przechowuje wszelką dokumentację związaną z Wnioskiem o wydanie certyfikatu EV SSL i jego weryfikacją oraz certyfikatem EV SSL i jego unieważnieniem przez co najmniej 7 lat od wygaśnięcia ważności danego certyfikatu EV SSL. Dodatkowo CERTUM utrzymuje aktualną wewnętrzną bazę wszystkich unieważnionych certyfikatów EV SSL i odrzuconych Wniosków o wydanie certyfikatu EV SSL, dla których powodem odrzucenia lub unieważnienia było podejrzenie *phishingu* lub innych działań nieuczciwych. Informacje o tak scharakteryzowanych zamówieniach służą następnie do identyfikacji oraz oznaczania kolejnych, mogących budzić podejrzenia Wniosków o wydanie certyfikatu EV SSL.

32. Ponowne użycie oraz aktualizacja informacji i dokumentacji związanych z certyfikatami EV SSL

(a) Zastosowanie dokumentacji przy powtarzających się Wnioskach o wydanie certyfikatu EV SSL

CERTUM może wydać wiele certyfikatów EV SSL zawierających dane jednego podmiotu, w oparciu o pojedynczy Wniosek o wydanie certyfikatu EV SSL pod warunkiem, że spełnione zostaną wymagania opisane poniżej:

(b) Zastosowanie istniejącej dokumentacji lub informacji

- (1) Każdy certyfikat EV SSL wydany przez CERTUM musi być poparty ważnym i aktualnym Wnioskiem o wydanie certyfikatu EV SSL oraz Umową z Subskrybentem, podpisanymi przez przedstawiciela działającego w imieniu Subskrybenta.
- (2) Okres ważności dla informacji wykorzystywanej przez CERTUM do weryfikacji Wniosków o wydanie certyfikatu EV SSL nie może przekraczać maksymalnego

okresu ważności dla danej informacji, opisanego w rozdziale 8 niniejszego Załącznika. Punktem odniesienia powinna być data otrzymania informacji (np. data potwierdzenia telefonicznego) lub ostatniej jej aktualizacji w stosownym źródle (np. w przypadku, gdy baza danych została sprawdzona przez CERTUM 1 czerwca, jednak zawierała dane ostatnio uaktualniane przez dostawcę 1 lutego, wtedy datą uzyskania informacji będzie 1 luty).

- (3) W przypadku informacji przeterminowanych CERTUM musi powtórzyć proces weryfikacji zgodnie z niniejszym Załącznikiem.

33. Bezpieczeństwo danych

Polityka CERTUM odnośnie bezpieczeństwa danych została opisana w rozdziałach 5 oraz 6 Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM.

J. ZGODNOŚĆ Z WYMAGANIAMI MIĘDZYNARODOWYCH STANDARDÓW DOTYCZĄCYCH CERTYFIKATÓW EV SSL

34. Wymagania audytowe

(a) Audyt wstępny

Przed wydaniem certyfikatu EV SSL, CERTUM musi pomyślnie zakończyć przeprowadzony przez niezależnych audytorów (i) audyt zgodności postępowania CERTUM z WebTrust Program for Certification Authorities oraz (ii) WebTrust for Certification Authorities -Extended Validation Audit Criteria lub ETSI TS 102 042 V2.1.1 (lub późniejszy)..

(b) Regularny audyt wewnętrzny

CERTUM, przez okres w którym wydaje certyfikaty EV SSL, musi kontrolować jakość swoich usług przeprowadzając regularne audyty wewnętrzne na losowej próbie danych, stanowiących co najmniej 3% wydanych certyfikatów EV SSL. Audyt ma charakter cykliczny i następuje zaraz po zakończeniu badania ostatniej próby.

(c) Coroczny audyt zewnętrzny

CERTUM, przez okres w którym wydaje certyfikaty EV SSL musi poddawać się corocznym audytom dotyczącym (i) zgodności postępowania CERTUM z WebTrust Program for Certification Authorities oraz (ii) WebTrust for Certification Authorities - Extended Validation Audit Criteria lub ETSI TS 102 042 V2.1.1 (lub późniejszy). Audyt obejmuje wszystkie obowiązki CERTUM wyszczególnione w niniejszym Załączniku oraz EV Guidelines, niezależnie od tego, czy są one wykonywane bezpośrednio przez CERTUM czy przez PR lub podwykonawców współpracujących z CERTUM.

Wyniki audytów są publicznie dostępne.

(d) Kwalifikacje audytora

Wszystkie audyty jakich wymaga niniejszy Załącznik muszą być wykonywane przez kwalifikowanego audytora. Kwalifikowany audytor musi spełniać następujące wymagania:

- (1) audytor jest niezależną firmą zajmującą się audytem przedsiębiorstw, posiadającą doświadczenie w zakresie oceny technologii PKI, technologii informatycznych, narzędzi i technik bezpieczeństwa informacji oraz oceny podmiotów pełniących role stron trzecich. Audytor musi posiadać aktualną licencję do przeprowadzania audytów WebTrust for CA Program i WebTrust EV Program lub stosowną licencję – wymaganą przez prawo, któremu podlega CERTUM – dla podmiotów spełniających wyżej wymienione wymagania, oraz
- (2) audytor musi być członkiem organizacji **American Institute of Certified Public Accountants** AICPA lub jej odpowiednika (poza granicami Stanów Zjednoczonych Ameryki), który wymaga od audytora aby świadczone przez niego usługi spełniały określone standardy, które zakładają: posiadanie przez audytora stosownych umiejętności gwarantujących wysoką jakość przeprowadzonej oceny, regularne przeprowadzanie testów kompetencji audytora, właściwy podział obowiązków i zadań w firmie audytora oraz wymóg ciągłego szkolenia zawodowego osób przeprowadzających audyt, oraz
- (3) audytor musi posiadać ubezpieczenie odpowiedzialności cywilnej oraz odpowiedzialności cywilnej w zakresie prowadzonej działalności na kwotę ubezpieczenia nie mniejszą niż jeden (1) milion dolarów USD.

(e) Tworzenie klucza głównego urzędu

Kwalifikowany audytor musi uczestniczyć w ceremonii tworzenia kluczy głównych CERTUM jeśli są one generowane po opublikowaniu dokumentu EV Guidelines. Celem uczestnictwa audytora jest przeprowadzenie przez niego kontroli integralności i poufności procesu tworzenia klucza głównego CERTUM. Kwalifikowany audytor musi stworzyć raport zawierający informacje odnośnie następujących wymagań, które spełniać musi CERTUM w trakcie tworzenia swojego klucza głównego:

- (1) CERTUM udokumentowało procedury tworzenia i ochrony swojego klucza głównego w swojej Polityce Certyfikacji oraz Kodeksie Postępowania Certyfikacyjnego;
- (2) CERTUM ujęło w swoich procedurach szczegółowy opis działań, jakie należy podjąć w celu utworzenia pary kluczy głównych CERTUM;
- (3) CERTUM zapewniło ochronę oraz właściwy nadzór nad procesem tworzenia kluczy głównych CERTUM zgodnie z procedurami opisanymi w Polityce Certyfikacji Niekwalifikowanych Usług CERTUM i Kodeksie Postępowania Certyfikacyjnego

Niekwalifikowanych Usług CERTUM oraz zgodnie ze skrytem tworzącym klucze oraz;

- (4) Utworzenie kluczy głównych CERTUM nastąpiło zgodnie z własnym skrytem tworzącym klucze..
- (5) Ceremonia tworzenia kluczy powinna zostać zarejestrowana w formie zapisu video.

K. POZOSTAŁE WYMAGANIA KONTRAKTOWE

35. Polityka prywatności

CERTUM musi spełniać wszystkie stosowne wymagania prawne związane z ochroną prywatności, jak również z własną polityką prywatności odnośnie pozyskiwania, stosowania i ujawnienia informacji prywatnych podczas weryfikacji danych niezbędnych do wydania certyfikatu EV SSL.

36. Odpowiedzialność

(a) Odpowiedzialność CERTUM

- (1) **Subskrybenci i strony ufające.** CERTUM wydając i zarządzając certyfikatem EV SSL zgodnie z niniejszym Załącznikiem, Kodeksem Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM oraz Polityką Certyfikacji Niekwalifikowanych Usług CERTUM, nie będzie odpowiadało przed beneficjentami certyfikatów EV SSL lub inną stroną trzecią certyfikatu EV SSL za jakiegokolwiek szkody powstałe w wyniku użycia lub udzielenia zaufania certyfikatowi poza warunkami określonymi w niniejszym Załączniku, Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM oraz Polityce Certyfikacji Niekwalifikowanych Usług CERTUM W przypadkach, gdy CERTUM wydało lub zarządzało certyfikatem EV SSL niezgodnie z wymaganiami niniejszego Załącznika, Kodeksem Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM lub Polityką Certyfikacji Niekwalifikowanych Usług CERTUM, może wówczas starać się, za pomocą dowolnych metod, ograniczyć – względem Subskrybentów lub stron ufających – swoją odpowiedzialność za straty lub szkody powstałe w związku z użyciem lub udzieleniem zaufania takiemu certyfikatowi EV SSL. Sytuacje, wobec zaistnienia których CERTUM zastrzega sobie prawo do ograniczenia własnej odpowiedzialność wyszczególnione zostały w niniejszym Załączniku, Kodeksie Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM oraz Polityce Certyfikacji Niekwalifikowanych Usług CERTUM, przy czym CERTUM nie może starać się ograniczyć swojej odpowiedzialności wobec Subskrybentów i stron ufających certyfikatu EV SSL.

poniżej kwoty odszkodowania mniejszej niż dwa tysiące (2000) dolarów USD wobec każdego Subskrybenta lub strony ufającej. CERTUM przyjmuje na siebie ryzyko związane z tym, czy ograniczenia odpowiedzialności, jakie sobie zastrzega, są prawnie wykonalne.

- (2) **Dostawcy oprogramowania.** Pomimo wszystkich ograniczeń odpowiedzialności w stosunku do Subskrybentów i stron ufających, CERTUM przyjmuje do wiadomości i potwierdza, że dostawców oprogramowania, którzy związani są z CERTUM umową dystrybucyjną dla certyfikatów EV SSL, nie dotyczą obowiązki lub odpowiedzialność opisane w niniejszym Załączniku ani też nie dotyczą ich obowiązki i odpowiedzialność związane z wydawaniem i zarządzaniem certyfikatami EV SSL. Dostawców oprogramowania nie obejmują także obowiązki i odpowiedzialność, które są wiążące dla beneficjentów certyfikatów EV SSL oraz innych stron darzących zaufaniem, certyfikaty EV SSL wydane przez CERTUM.

CERTUM zabezpiecza i chroni dostawców oprogramowania od wszelkich roszczeń związanych z certyfikatami EV SSL wydanymi przez CERTUM. CERTUM zwalnia także wszystkich dostawców oprogramowania od odpowiedzialności za wszelkie zniszczenia i straty powstałe w związku ze stosowaniem certyfikatu EV SSL wydanego przez CERTUM bez względu na faktyczną przyczynę zaistniałych szkód. Powyższe zastrzeżenie nie odnosi się jednak do roszczeń wobec dostawcy oprogramowania oraz szkód i strat poniesionych przez danego dostawcę oprogramowania w związku z certyfikatem EV SSL wydanym przez CERTUM, jeśli dane roszczenie, szkoda lub strata była bezpośrednio spowodowana przez oprogramowanie samego dostawcy oprogramowania, wyświetlającego ważny certyfikat EV SSL jako nie zaufany lub wyświetlający jako godny zaufania certyfikat EV SSL (i) który jest przeterminowany lub (ii) unieważniony (pod warunkiem, że status certyfikatu EV SSL jest dostępny online w CERTUM natomiast pobranie przez przeglądarkę internetową strony ufającej informacji dotyczącej statusu certyfikatu nie powiodło się lub informacja taka została zignorowana)

Odniesienia

1. CA/BROWSER FORUM Guidelines for the issuance and Management of Extended Validation Certificates, Version 1.2, 1 Oct 2009
2. VeriSign CPS – VeriSign Certification Practice Statement, ver.3.8, June 01, 2008, <http://www.verisign.com>

Słownik pojęć

Certyfikat EV SSL – elektroniczne zaświadczenie, wydane zgodnie z wymaganiami określonymi w dokumencie Guidelines for the issuance and management of extended validation certificates (v 1.1), służące do zabezpieczania transmisji danych między użytkownikiem sieci globalnej a witryną Internetową, do której przyporządkowany jest certyfikat EV SSL oraz umożliwiające identyfikację właściciela tej witryny.

Dostawca oprogramowania (ang. Application Software Vendor) – właściciel i/lub dostawca oprogramowania używającego certyfikatów EV SSL, w którym certyfikaty EV SSL oraz certyfikaty główne urzędu certyfikacji prezentowane są stronom ufającym.

Działalność gospodarcza (ang. Operational Existence) – zdolność finansowa Zamawiającego do prowadzenia działalności handlowej, weryfikowana tylko wówczas, gdy działalność Zamawiającego nie przekracza trzech lat.

Forma prawna (ang. Legal Existence) – Organizacje i przedsiębiorstwa posiadające osobowość prawną lub przedsiębiorstwa i organizacje nie posiadające osobowości prawnej posiadają określoną formę prawną, jeśli zostały powołane w sposób przewidziany w ustawodawstwie danego kraju i nie zakończyły działalności, nie uległy rozwiązaniu etc.

Guidelines for the Issuance and Management of Extended Validation Certificates v 1.1 (nazwa skrócona EV Guidelines) – dokument stworzony przez CA/Browser Forum, konsorcjum opiniotwórcze o charakterze non-profit zrzeszającym szereg urzędów certyfikacji oraz twórców przeglądarek internetowych. W dokumencie określone zostały standardy dotyczące charakterystyki certyfikatów EV SSL oraz wymagań, jakie muszą spełniać urzędy certyfikacji chcące wydawać certyfikaty EV SSL. Dokument w aktualnej wersji dostępny jest na stronie <http://www.cabforum.org>.

Kwalifikowane Niezależne Źródło informacji (ang. Qualified Independent Information Sources) – [opisano w Rozdziale 21(e)]

Kwalifikowane Rządowe Źródło Informacji (ang. Qualified Government Information Source) – [opisano w Rozdziale 21(d)]

Oświadczenie Zamawiającego (ang. Independent Confirmation From Applicant) – [opisano w Rozdziale 21(c)].

Opinia Prawna (*ang. Legal Opinion*) – pismo sporządzone przez stronę trzecią (kancelarię prawną lub notarialną) potwierdzające autentyczność podstawowych danych dostarczonych przez Zamawiającego w złożonym Wniosku o wydanie certyfikatu EV SSL. Przykładowy Formularz Opinii Prawnej dostępny jest w formie załącznika do EV Guidelines³

Organizacje i przedsiębiorstwa posiadające osobowość prawną – podmioty ukierunkowane na osiąganie celów gospodarczych lub niegospodarczych, które uzyskują osobowość prawną z chwilą zarejestrowania w stosownym urzędzie. Ich odpowiedzialność jest ograniczona stosownie wobec posiadanej osobowości prawnej.

Osoba reprezentująca Subskrybenta (*ang. Principal Individual*) – osoba fizyczna związana z podmiotem certyfikatu EV SSL będąca właścicielem, współwłaścicielem, członkiem Zarządu, dyrektorem lub pracownikiem, pracownikiem kontraktowym, a także reprezentantem Subskrybenta upoważnionym przez Subskrybenta do podejmowania czynności związanych z wydaniem i użytkowaniem certyfikatu EV SSL.

Osoba Potwierdzająca (*ang. Confirming Person*) – osoba podpisująca się pod Oświadczeniem Zamawiającego. Jest to osoba piastująca wysokie stanowisko w organizacji lub firmie np. Sekretarz, Prezydent, Prezes, Dyrektor Generalny, Dyrektor Finansowy etc., której imię, nazwisko oraz nazwa zajmowanego stanowiska widnieją w aktualnych źródłach informacji takich jak: Kwalifikowane Rządowe Źródła Informacji, Kwalifikowane Niezależne Źródła Informacji, Kwalifikowane Rządowe Źródła Informacji Podatkowej oraz zweryfikowana Opinia Prawna. Ewentualnie CERTUM może kontaktować się z Zamawiającym (np. z działem kadr (Human Resources Department) firmy lub organizacji Subskrybenta) w celu zweryfikowania tożsamości Osoby Potwierdzającej.

Osoba Zatwierdzająca Certyfikat (*ang. Certificate Approver*) – [opisano w Rozdziale 10]

Osoba Podpisująca Umowę (*ang. Contract Signer*) – [opisano w Rozdziale 10]

Przedsiębiorstwa oraz organizacje nie posiadające osobowości prawnej – podmioty ukierunkowane na osiąganie celów gospodarczych lub nie gospodarczych, nie posiadające osobowości prawnej, których działalność zarejestrowana jest w stosownym urzędzie.

Punkt Rejestracji – miejsce, gdzie świadczone są usługi w zakresie weryfikacji i potwierdzania tożsamości osób ubiegających się o certyfikat, ich funkcją jest kompleksowa obsługa subskrybentów w zakresie świadczenia usług certyfikacyjnych.

³ EV Certificate Guidelines, v1.2 Appendix D

Punkt Rejestracji typu Enterprise – podmiot ważnego certyfikatu EV SSL, który jest upoważniony przez CERTUM do pełnienia funkcji Punktu Rejestracji oraz może być upoważniony także do wydawania certyfikatów EV SSL dla subdomen domeny głównej będącej już przedmiotem certyfikatu EV SSL.

Strona Ufająca (*ang. Reling Party*) – każda osoba (fizyczna lub prawna), która polega na certyfikacie EV SSL wystawionym przez CERTUM. Dostawca Oprogramowania nie jest uznawany za Stronę Ufającą, gdy dostarczane przez niego oprogramowanie jedynie wyświetla informacje o Certyfikacie EV SSL.

Subskrybent certyfikatu EV SSL – subskrybent jest właścicielem bądź wyłącznym użytkownikiem nazwy domeny będącej przedmiotem certyfikatu EV SSL, który składa do CERTUM zamówienie na certyfikat EV SSL. Subskrybentem może być osoba prawna lub jednostka organizacyjna nie posiadająca osobowości prawnej, która jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej jednostce, w polu Subject:organizationName certyfikatu EV SSL wydanego zgodnie z niniejszym Załącznikiem. Subskrybent posiada klucz prywatny związany z kluczem publicznym umieszczonym w certyfikacie EV SSL, a zatem tożsamość subskrybenta jest bezsprzecznie związana z kluczem publicznym zawartym w tym certyfikacie.

Umowa z Subskrybentem certyfikatu EV SSL (*ang. Subscriber Agreement*) – umowa zawarta między CERTUM i Zamawiającym, w której określa się ich prawa i obowiązki według kryteriów wyznaczonych i opublikowanych w EV Guidelines.

Uwierzytelnienie – mechanizm zabezpieczeń, którego zadaniem jest zapewnienie wiarygodności przesyłanych danych, wiadomości lub nadawcy, albo mechanizmy weryfikowania autoryzacji osoby przed otrzymaniem przez nią określonych kategorii informacji.

Użytkownik certyfikatu, (*ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Wniosek (*ang. Certificate Request*) – wniosek o wydanie certyfikatu EV SSL.

Wnioskodawca certyfikatu EV SSL (*ang. Certificate Requester*) – [opisano w Rozdziale 10]

Zamawiający (*ang. Applicant*) – Organizacja lub przedsiębiorstwo posiadające osobowość prawną, organizacja lub przedsiębiorstwo nie posiadające osobowości prawnej, podmiot administracji publicznej lub organizacja międzynarodowa (niekomercyjna), która ubiega się o wydanie certyfikatu EV SSL (lub jego odnowienie).

Zamawiający Wysokiego Ryzyka (*ang. High Risk Applicant*) – [opisano w Rozdziale 22]

Źródła Informacji Pewnej (*ang. Certain Information Sources*) – źródła informacji, w oparciu o które CERTUM weryfikuje dane otrzymane we Wniosku o wydanie certyfikatu EV SSL.

EV Guidelines wyróżnia następujące Źródła Informacji Pewnej:

- zweryfikowana Opinia Prawna
- bezpośrednie spotkanie
- Niezależne Potwierdzenie Zamawiającego
- Kwalifikowane Niezależne Źródło Informacji
- Kwalifikowane Rządowe Źródło Informacji
- Kwalifikowane Rządowe Źródło Informacji Podatkowej