Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM

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

Wersja 3.0

Data: 5 października 2009

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. Wprowadzenie

Niniejsze procedury stanowią uzupełnienie do aktualnego Kodeksu Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM uwzględniając reguły postępowania obowiązujące przy wystawianiu certyfikatów Extended Validation zgodnie z terminami i w kategoriach określonych w dokumencie Guidelines for Extended Validation Certificates v 1.1 (zwanym dalej EV Guidelines), który publikowany jest na stronie http://www.cabforum.org/. Dokument ten powstał za sprawą konsorcjum opiniotwórczego CA/Browser Forum o charakterze niekomercyjnym, zrzeszającego szereg urzędów certyfikacji oraz twórców przeglądarek internetowych.
W dokumencie EV Guidelines określa się podstawowe wymagania, jakie spełniać musi urząd certyfikacji, aby mógł wystawiać certyfikaty EV SSL oraz charakterystykę Subskrybenta, który może ubiegać się o certyfikat EV SSL. Dzięki certyfikatowi EV SSL użytkownik uzyskuje pewność odnośnie autentyczności strony WWW, którą odwiedza. Informacja o właścicielu strony zamieszczona w certyfikacie EV SSL może zostać wyświetlona w specjalnie wyróżniony sposób przez odpowiednie oprogramowanie (np. przeglądarkę internetową).

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: 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 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 wymienianych między przeglądarką użytkownika a stroną WWW.

(b) Pozostałe zastosowania

Kolejnym zastosowaniem certyfikatu EV SSL jest pomoc użytkownikowi w ustaleniu czy strona WWW zarządzana jest legalnie przez podmiot do tego uprawniony oraz dostarczenie narzędzia wspierającego rozwiązywanie problemów z adresowaniem stron WWW takich jak *phishing* i inne formy oszustw internetowych. Dostarczając wiarygodne – niezależnie potwierdzone – informacje, dotyczące właściciela strony, certyfikaty EV SSL mogą pomóc w:

(1) znacznym utrudnieniu dokonywania aktów *phishingu* i innych form fałszerstwa tożsamości;

(2) ochronie firm narażonych na podobne ataki, dostarczając narzędzia umożliwiającego ich wzajemną identyfikację oraz identyfikację przez użytkownika;

(3) dostarczeniu wsparcia w przypadku prowadzonego dochodzenia w sprawie *phishingu* lub innych form fałszerstwa tożsamości. Wsparcie obejmuje: kontakt, uczestnictwo w dochodzeniu lub podjęcie czynności prawnych przeciwko sprawcy.

(c) Cele nie objęte gwarancją

Informacje, jakie zawierają certyfikaty EV SSL dotyczą tylko tożsamości Subskrybenta certyfikatu EV SSL i nie odnoszą się do jego działań. Certyfikaty EV SSL nie dostarczają pewności na podstawie której CERTUM gwarantowałoby, że:

(1) podmiot, którego nazwa występuje w certyfikacie prowadzi aktualnie działalność gospodarczą;

(2) podmiot, którego nazwa występuje w certyfikacie stosuje się do obowiązującego prawa;

(3) podmiot, którego nazwa występuje w certyfikacie jest godny zaufania, uczciwy i o nieposzlakowanej opinii oraz, że

(4) prowadzenie wymiany handlowej z Subskrybentem, którego nazwa występuje w certyfikacie jest „bezpieczne".

3. Gwarancje i oświadczenia

(a) Ze strony CERTUM

Beneficjentami certyfikatów EV SSL mogą być:

(1) subskrybent zawierający Umowę z Subskrybentem certyfikatu EV SSL;

(2) podmiot, którego nazwa występuje w certyfikacie EV SSL;

(3) wszyscy dostawcy oprogramowania, którzy na podstawie zawartej z CERTUM 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, jego postępowanie wobec certyfikatu (proces wydania oraz weryfikacji danych w nim zawartych) jest zgodne z wymaganiami przedstawionymi w EV Guidelines. Powyższa gwarancja, nie ograniczając się tylko do poniższych kwestii, w szczególności obejmuje:

(1) **Podstawę Prawną**: CERTUM potwierdza we właściwym urzędzie, że w dniu wydania certyfikatu Subskrybent certyfikatu EV SSL posiadał osobowość prawną nadaną mu przez urząd oraz, że jego status w rejestrach urzędu widniał jako ważny;

(2) **Tożsamość**: CERTUM potwierdza, że w dniu wydania certyfikatu oficjalna oraz skrócona nazwa Subskrybenta występująca w certyfikacie są tożsame z nazwami zawartymi w oficjalnych rejestrach urzędu właściwego dla miejsca prowadzenia przez Subskrybenta działalności;

(3) **Prawo do nazwy Domeny**: CERTUM podejmuje wszelkie wymagane przez EV Guidelines kroki niezbędne, aby potwierdzić, że Subskrybent, którego nazwę zawiera certyfikat EV SSL w dniu wydania certyfikatu posiadał wyłączne prawo do posługiwania się nazwą domeny zawartą w certyfikacie;

(4) **Upoważnienie**: CERTUM podejmuje, w zgodzie z EV Guidelines, czynności niezbędne do zweryfikowania czy Subskrybent certyfikatu EV SSL wyraził stosowne upoważnienia osobom ubiegającym się w jego imieniu o certyfikat EV SSL;

(5) **Prawdziwość informacji**: CERTUM podejmuje czynności niezbędne do zweryfikowania, że w dniu wystawienia certyfikatu wszystkie pozostałe informacje zawarte w certyfikacie są dokładne i prawdziwe;

(6) **Umowę z Subskrybentem**: Podmiot ubiegający się o certyfikat EV SSL przystąpił do podpisania z CERTUM ważnej prawnie Umowy z Subskrybentem na warunkach wskazanych w EV Guidelines;

(7) **Status**: CERTUM, w zgodzie z wymaganiami EV Guidelines v1.1, 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 wymaganiami EV Guidelines oraz niniejszym Załącznikiem, dokonuje unieważnienia certyfikatu 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 występująca w Umowie z Subskrybentem, aby Subskrybent wywiązywał się ze swoich zobowiązań i korzystał z udzielonych beneficjentom CERTUM oraz beneficjentom certyfikatu EV SSL gwarancji stosownie do zapisów w dokumencie EV Guidelines oraz niniejszym Załączniku do Kodeksu Postępowania Certyfikacyjnego.

C. ŚRODOWISKO I ZASTOSOWANIE

4. Wydawanie certyfikatów EV SSL

Podczas wydawania certyfikatów EV SSL, CERTUM spełnia następujące wymagania:

(a) Wymagania dotyczące zgodności z obowiązującymi politykami EV

CERTUM działa:

(1) w zgodzie z prawem obowiązującym na danym obszarze, na którym CERTUM wydaje certyfikaty;

(2) w zgodzie z wymaganiami EV Guidelines;

(3) w zgodzie z wymaganiami określonymi w programach (i) WebTrust Program for Certification Authorities oraz (ii) WebTrust EV Program lub ekwiwalentem obydwu, jeśli jest zaakceptowany przez CA/Browser Forum oraz;

(4) w zgodzie z otrzymanymi uprawnieniami, jakie posiada, niezbędnymi do świadczenia przez nie usług certyfikacyjnych.

(b) Polityki EV

(1) **Realizacja**. Kodeks Postępowania Certyfikacyjnego CERTUM wraz z niniejszym Załącznikiem:

(A) realizuje wymagania EV Guidelines zawsze, gdy tylko zostaną w nim opublikowane jakiekolwiek zmiany;

(B) realizuje aktualne wymagania (i) WebTrust Program for Certification Authorities oraz (ii) WebTrust EV Program lub ich ekwiwalentu, jeśli jest on zaakceptowany przez CA/Browser Forum;

(C) określa ścieżkę certyfikacji w ramach hierarchicznej struktury urzędów podległych głównemu urzędowi CERTUM odpowiedzialnych za weryfikację autentyczności wydawanych certyfikatów EV SSL

(2) **Udostępnianie**. CERTUM udostępnia publicznie własną politykę certyfikacji za pośrednictwem Kodeksu Postępowania Certyfikacyjnego, 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) **Gwarancja zgodności z EV Guidelines.** 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 stosownymi wymaganiami określonymi przez dokument EV Guidelines objęte są (bezpośrednio lub przez odniesienie) wszystkie umowy zawarte 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 od odpowiedzialności cywilnej na kwotę przynajmniej 2 mln dolarów;

(B) Ubezpieczenie przed skutkami błędów i zaniechania 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. Uzyskanie certyfikatu EV SSL

W myśl wymagań określonych w EV Guidelines, certyfikaty EV SSL mogą być wydawane jedynie Przedsiębiorstwom, Organizacjom prywatnym oraz Podmiotom państwowym, które spełniają następujące warunki:

(a) Organizacje prywatne

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

(1) Organizacja musi być prawnie rozpoznanym podmiotem, który został powołany do istnienia poprzez wpisanie do rejestru (lub akt powołania) przez organ władzy właściwy ze względu na miejsce prowadzenia przez podmiot działalności;

(2) Wpis do rejestru musi zawierać nazwę Organizacji;

(3) Organizacja nie może figurować w rejestrze stosownego organu władzy dokonującego wpisu jako „nieaktywna", „nieważna" lub „nieaktualna" etc;

(4) Organizacja musi posiadać potwierdzony adres oraz zweryfikowaną obecność na rynku;

(5) Miejscem zarejestrowania Organizacji oraz miejscem, w którym prowadzi ona działalność nie może być terytorium kraju, z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej, a w szczególności świadczenia usług certyfikacyjnych;

(6) Organizacja nie może figurować 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. Organizacja nie może być podmiotem prawa w państwie, z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej.

(b) Przedsiębiorstwa

(1) Przedsiębiorstwo musi być prawnie rozpoznanym podmiotem, które został powołany do istnienia poprzez wpisanie do rejestru (lub akt powołania) przez organ władzy właściwy ze względu na miejsce prowadzenia przez podmiot działalności;

(2) Przedsiębiorstwo musi posiadać potwierdzony adres oraz zweryfikowaną obecność na rynku;

(3) Musi zostać zidentyfikowana i zweryfikowana tożsamość przynajmniej jednej z osób dysponujących ostateczną lub znaczącą władzą wykonawczą w firmie (Osoba Decyzyjna) np. Sekretarz, Prezydent, Prezes, Dyrektor Generalny, Dyrektor Finansowy etc., której imię, nazwisko oraz nazwa zajmowanego stanowiska widnieją w aktualnym dokumencie KRS lub innym,.

(4) Osoba Decyzyjna musi posiadać uprawnienia pozwalające na upoważnienie innych przedstawicieli Subskrybenta do działania w jego imieniu, w szczególności do podpisania Umowy z Subskrybentem.

(5) W przypadku, gdy Przedsiębiorstwo działa pod nazwą skróconą CERTUM musi zweryfikować czy użycie nazwy skróconej przez Przedsiębiorstwo jest zgodne z zapisami sekcji 15 niniejszego Załącznika.

(6) Przedsiębiorstwo i Osoba Decyzyjna nie mogą figurować 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.

(7) Miejscem, w którym Przedsiębiorstwo prowadzi działalność nie może być terytorium kraju z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej, w szczególności świadczenia usług certyfikacyjnych;

(c) Podmioty państwowe

CERTUM może wydać certyfikat EV SSL każdemu Podmiotowi państwowemu, który spełnia następujące warunki:

(1) Podstawą prawną istnienia Podmiotu państwowego jest jego ukonstytuowanie się na podstawie właściwych rozporządzeń, uchwał lub innych aktów legislacyjnych wydanych przez stosowny urząd państwa.

(2) Podmiot państwowy nie jest podmiotem prawa na terytorium kraju, z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej, w szczególności świadczenia usług certyfikacyjnych;

(3) Podmiot państwowy nie może figurować 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. ZAWARTOŚĆ I PROFIL CERTYFIKATU EV SSL

6. Wymagania dotyczące zawartości certyfikatu EV SSL

Niniejsza sekcja określa minimalne wymagania dotyczące zawartości certyfikatu EV SSL, związane z charakterystyką podmiotów certyfikatu EV SSL.
Będąc przedmiotem wymagań niniejszego Załącznika certyfikat EV SSL zawiera następujące informacje dotyczące podmiotu, jakie 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, prawnie zarejestrowana nazwę organizacji podmiotu, pod jaką dokonano rejestracji podmiotu w stosownym urzędzie. Dodatkowo, nazwa skrócona lub inna nazwa (d/b/a – doing business as – działający jako) Podmiotu MOŻE zostać zawarta na początku pola, pod warunkiem, że po niej zostanie zamieszczona w nawiasach pełna, prawnie zarejestrowana nazwa. Jeśli nazwa pełna przekracza limit 64 znaków CERTUM może dokonać skrótu nazwy

zgodnie z obowiązującymi standardami języka prawnego i urzędowego. Jeśli połączenie nazwy skróconej lub d/b/a oraz nazwy pełnej przekracza 64 znaki, jak określono w RFC 5280, CERTUM POWINNO użyć jedynie nazwy pełnej. Jeśli dokonanie skrótu lub wyróżnienie tylko jednej nazwy – przy czym dwie nie mogą występować łącznie – jest niemożliwe, CERTUM nie wydaje certyfikatu EV SSL.

(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 czy charakterystyka Podmiotu odpowiada cechom opisanym w sekcjach 5b, 5c,5d or 5e EV Guidelines.

(4) **Miejsce rejestracji** (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

Pole MUSI zawierać informacje właściwe ze względu na miejsce rejestracji podmiotu – np.: Miejsce zarejestrowania dla urzędu o zasięgu krajowym 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 ze stosowanymi kodami ISO. Nazwa województwa oraz nazwa miasta MUSI być określona pełnymi nazwami.

Zgodność z Europejskimi Standardami dla Certyfikatów Kwalifikowanych: dodatkowo, CA MOŻE dołączyć rozszerzenie qcStatements, określone w RFC 3739. OID dla qcStatement: qcStatement:statementId (1.3.6.1.4.1.311.60.2.1).

Numer Rejestracyjny: (ang. Registration Number)

Pole certyfikatu: Subject:serialNumber (OID 2.5.4.5)

Wymagane/Opcjonalne: Wymagane

Pole MUSI zawierać unikalny numer rejestracyjny przyznany Podmiotowi przez stosowny urząd.

(5) **Adres miejsca prowadzenia działalności** (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 EV SSL subskrybentów

Każdy Certyfikat EV SSL wydawany przez CERTUM Subskrybentom MUSI zawierać w rozszerzeniu certificatePolicies, OID określony przez CERTUM, który wskazuje jaka polityka CERTUM odnosi się do danego certyfikatu. Numer OID stosownej polityki dla certyfikatu EV SSL CERTUM to 1.2.616.1.113527.2.5.1.1

(b) Certyfikaty EV SSL urzędów podległych CERTUM

Certyfikat wydany dla urzędu podległego CERTUM (np. Certum Extended Validation) jest kontrolowany przez główny urząd certyfikacji CERTUM. Certyfikaty urzędów podległych mogą zawierać specjalny OID (2.5.29.32.0) w polu anyPolicy.

(c) Certyfikat Główny urzędu

Certyfikatem głównym urzędu CERTUM dla certyfikatów EV SSL jest certyfikat 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 wynosi 27 miesięcy.

(b) Dla weryfikowanych informacji

Maksymalny okres ważności dla danych dotyczących podmiotu certtyfikatu EV SSL, używanych w procesie wydawania certyfikatu EV SSL (zanim koniecznym stanie się ponowne złożenie dokumentów) jest następujący:

- Podstawa prawna oraz tożsamość – trzynaście (13) miesięcy;
- Dodatkowa nazwa – trzynaście (13) miesięcy;
- Adres miejsca prowadzonej działalności – 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, chyba, że pomiędzy Podmiotem a CERTUM została zawarta umowa określająca inny termin – w takim przypadku górę biorą postanowienia umowy. Dla przykładu – umowa może zawierać klauzule o kontynuowaniu uprawnień Osoby Zatwierdzającej Certyfikat do czasu ich odwołania lub wygaśnięcia lub zerwania umowy.

9. Pozostałe wymagania techniczne dla certyfikatów EV SSL

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

E. WYMAGANIA DOTYCZĄCE ZAMÓWIENIA CERTYFIKATU EV SSL

10. Wymagania ogólne

(a) Wymagane dokumenty

Przed wydaniem Certyfikatu EV SSL CA MUSI uzyskać od Podmiotu następujące dokumenty, określone przez niniejsze 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 Podmiot certyfikatu EV SSL

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

- **Wnioskodawca** (ang. Certificate Requester) – Osoba fizyczna reprezentująca Subskrybenta; pracownik zatrudniony przez Subskrybenta lub autoryzowany przedstawiciel Subskrybenta lub strona trzeciej (np. dostawcy usług internetowych)

upoważniony do złożenia podpisanego Wniosku o wydanie certyfikatu EV SSL do CERTUM

- **Osoba Zatwierdzająca Certyfikat** (ang. Certificate Approver) – Osoba fizyczna reprezentująca Subskrybenta; pracownik zatrudniony przez Subskrybenta lub autoryzowany przedstawiciel Subskrybenta, (i) posiadający wyraźne pełnomocnictwo do występowania samemu jako Wnioskodawca oraz udzielania innym pracownikom Subskrybenta lub stronom trzecim takiego pełnomocnictwa, a także (ii) do zatwierdzania Wniosków składanych przez innych Wnioskodawców.
- **Osoba Podpisująca Umowę** (ang. Contract Signer) – Osoba fizyczna reprezentująca Subskrybenta; pracownik zatrudniony przez Subskrybenta lub autoryzowany przedstawiciel Subskrybenta posiadający wyraźne pełnomocnictwo do reprezentowania Subskrybenta, w tym upoważnienie do podpisywania w jego imieniu Umowy z Subskrybentem.

Jedna osoba MOŻE być upoważniona przez Subskrybenta do pełnienia jednej, dwóch lub wszystkich trzech powyższych ról pod warunkiem jednak, że jest ona pracownikiem Subskrybenta. Podobnie kilka osób może być upoważnionych do pełnienia jednej roli.

11. Wymagania dotyczące Wniosku o wydanie certyfikatu EV SSL

(a) Ogólne

Przed wydaniem Certyfikatu EV SSL, CERUM MUSI uzyskać od Subskrybenta (za pośrednictwem Wnioskodawcy upoważnionego do działania w imieniu Subskrybenta) 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 Subskrybenta w danym czasie.

(b) Wniosek i oświadczenie

Wniosek o wydanie certyfikatu EV SSL MUSI być złożony w imieniu Subskrybenta oraz zawierać oświadczenie, że zawarte w nim informacje są prawdziwe i poprawne.

(c) Informacje zawarte we Wniosku

Wniosek o wydanie certyfikatu EV SSL zawiera wszystkie rzeczywiste informacje o Subskrybencie, które zostaną umieszczone w certyfikacie EV SSL oraz informacje dodatkowe, wymagane przez CERTUM, aby wydanie certyfikatu miało miejsce w zgodzie z niniejszym Załącznikiem. W przypadku, gdy Wniosek nie zawiera wszystkich niezbędnych informacji o Subskrybencie, CERTUM uzyskuje pozostałe wymagane informacje od Osoby Zatwierdzającej Certyfikat lub Osoby Podpisującej Umowę. Informacje o Subskrybencie powinny zawierać, lecz nie powinny być ograniczone do:

- **Nazwa Organizacji**: Formalna nazwa organizacji lub przedsiębiorstwa, która zostanie zamieszczona w certyfikacie EV SSL, zgodna z nazwą zarejestrowaną w stosownym urzędzie;
- **Nazwa skrócona (opcjonalnie):** Nazwa dodatkowa (skrócona), która zarejestrowana jest w stosownym urzędzie jako nazwa skrócona;
- **Nazwa Domeny**: Nazwa domeny będącej przedmiotem certyfikatu EV SSL

- **Miejsce wpisu do rejestru**: Miejsce zarejestrowania działalności Subskrybenta
  (a) Miasto (jeśli wymagane),
  (b) Jednostka podziału administracyjnego (jeśli wymagane), oraz
  (c) Kraj.
- **Urząd rejestracji**: Nazwa urzędu, który dokonał rejestracji Subskrybenta
- **Numer rejestracji:** unikalny numer rejestracyjny przyznawany Subskrybentowi przez urząd odpowiedzialny za rejestrację, który zostanie zwarty w certyfikacie EV SSL (jedynie dla Organizacji i Przedsiębiorstw);
- **Adres**: Adres prowadzenia działalności przez Subskrybenta –
  (a) Ulica i numer lokalu,
  (b) Miasto,
  (c) Jednostka podziału administracyjnego (jeśli wymagane),
  (d) Kraj,
  (e) Kod pocztowy, oraz
  (f) Główny numer telefonu.
- **Osoba Zatwierdzająca Certyfikat:** Nazwisko i imię oraz dane kontaktowe Zatwierdzającego Certyfikat składającego i podpisującego lub upoważniającego Wnioskodawcę do złożenia i podpisania Wniosku o wydanie certyfikatu EV SSL w imieniu Subskrybenta
- **Wnioskodawca**: Nazwisko i imię oraz dane kontaktowe Wnioskodawcy składającego Wniosek o wydanie certyfikatu EV SSL w imieniu Subskrybenta jeśli jest osobą różną od Zatwierdzającego Certyfikat.

12. Wymagania dotyczące Umowy z Subskrybentem

(a) Ogólne

Przed wydaniem Certyfikatu EV SSL, CERTUM MUSI uzyskać prawnie obowiązującą Umowę z Subskrybentem. Umowa z Subskrybentem musi być podpisana przez upoważnioną do tego Osobę Podpisującą Umowę, działającą w imieniu Subskrybenta zgodnie z wymaganiami sekcji 20 niniejszego Załącznika i musi odnosić się do certyfikatu EV SSL, który ma zostać wydany na podstawie Wniosku o wydanie certyfikatu EV SSL. Osobna Umowa może zostać użyta dla każdego z Wniosków o wydanie certyfikatu EV SSL lub jedna Umowa może obejmować kilka (również przyszłych) Wniosków i wynikających z nich certyfikatów EV SSL pod warunkiem, że każdy certyfikat EV SSL wydany przez CERTUM jest objęty i określony w tej Umowie.

(b) Wymagania

Umowa z Subskrybentem dotyczy Subskrybenta oraz Osoby Podpisującej Umowę.
Minimalne wymagania dotyczące zawartości Umowy obejmują zapisy nakładające na Subskrybenta określone obowiązki a także dające mu gwarancje odnośnie:

- obowiązku prawdziwości i ścisłości udzielanych CERTUM informacji dotyczących danych podmiotu przez cały okres ważności certyfikatu;

- ochrony klucza prywatnego – podmiot certyfikatu zobowiązuje się kontrolować użycie klucza prywatnego, powiązanego z kluczem publicznym umieszczonym w certyfikacie oraz chronić wszelkie informacje z nim związane (np. hasło)

- terminu uzyskania przez Subskrybenta certyfikatu nie prędzej niż zostaną pomyślnie zweryfikowane dane w nim zawarte;

- używania certyfikatu zgodnie z prawami określonymi we wcześniejszych etapach certyfikacji – instalacji certyfikatu tylko na serwerze związanym z nazwą domeny, używania certyfikatu zgodnie z prawem, używania certyfikatu wyłącznie przez uprawniony do tego podmiot oraz u używania certyfikatu w zgodzie z zapisami w Umowie z Subskrybentem;

- niezwłocznego zaprzestania używania certyfikatu i, związanego z nim, klucza prywatnego oraz niezwłocznego zgłoszenia do CERTUM woli unieważnienia certyfikatu w następujących przypadkach:

    - nieprawidłowej lub nieprawdziwej informacji zawartej w certyfikacie;

    - podejrzeń nadużycia lub niewłaściwego wykorzystania certyfikatu – kompromitacji klucza prywatnego;

- ograniczeń czasowych w użytkowaniu certyfikatu – niezwłocznego zaprzestania używania klucza prywatnego powiązanego z kluczem publicznym umieszczonym w certyfikacie w chwili wygaśnięcia jego ważności certyfikatu lub jego unieważnienia.

F. WYMAGANIA DOTYCZĄCE WERYFIKACJI INFORMACJI

13. Wymagania ogólne

Niniejsza część Załącznika określa wymagania, jakie stawiane są procedurze weryfikacji informacji otrzymanych od Subskrybenta.

(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. CERTUM zobowiązane jest zweryfikować:

(A) Weryfikacja cech charakterystycznych; materialnych oraz formalnych Subskrybenta:

(1) Podstawa prawna i tożsamość;

(2) Istnienie fizyczne;

(3) Stan działalności handlowej (zdolność biznesowa)

(B) Weryfikacja prawa Subskrybenta do posługiwania się nazwą domeny wymienionej w certyfikacie EV SSL:

(1) Rejestracja domeny;

(2) Prawo Subskrybenta do domeny.

(C) Weryfikacja osób reprezentujących Subskrybenta w trakcie ubiegania się o certyfikat EV SSL:

(1) Tożsamość, charakter piastowanych stanowisk oraz pełnomocnictwa udzielone Osobie Podpisującej Umowę, Osobie Zatwierdzającej Certyfikat oraz Wnioskodawcy;

(2) Podpis na Umowie z Subskrybentem;

(3) Akceptacja Wniosku przez Osobę Zatwierdzającą Certyfikat.

(b) Akceptowane metody weryfikacji

Przyjmuje się zasadę ogólną, że CERTUM jest odpowiedzialne za podjęcie wszelkich niezbędnych kroków, aby spełnić wymagania dla weryfikacji opisanych powyżej. Akceptowalne metody weryfikacji, opisane w rozdziałach 14 do 25 poniżej (zazwyczaj zakładających różne alternatywy) uznawane są za minimalny akceptowalny poziom polityki weryfikacji realizowanej przez CERTUM. We wszystkich jednak przypadkach CERTUM jest zobowiązane do podjęcia wszelkich innych działań, które mogą być wymagane przez zapisy w niniejszym Załączniku.

14. Weryfikacja podstawy prawnej oraz tożsamości Subskrybenta

Aby zweryfikować istnienie prawne i tożsamość Subskrybenta, CERTUM MUSI wykonać poniższe działania:

(1) Organizacje prywatne

- **Istnienie prawne**: Sprawdzić, czy Subskrybent jest prawnie rozpoznawanym podmiotem, istniejącym i właściwie zarejestrowanym (np. jako spółka) w stosownym urzędzie właściwym ze względu na miejsce działalności Subskrybenta i nie figuruje w żadnych urzędowych rejestrach jako „nieaktywny", „nieważny", „nieaktualny" lub podobne;
- **Nazwa organizacji**: Sprawdzić, czy formalna nazwa prawna Subskrybenta, zarejestrowana w stosownym urzędzie właściwym ze względu na miejsce działalności Subskrybenta jest zgodna z nazwą umieszczoną we Wniosku o wydanie certyfikatu EV SSL.
- **Numer wpisu do rejestru**: Uzyskać unikalny numer rejestracyjny przyznany Subskrybentowi przez stosowny urząd właściwy ze względu na miejsce działalności Subskrybenta
- **Urząd rejestrujący**: Zidentyfikować właściwy urząd, w którym dokonano rejestracji Subskrybenta, uzyskując adres tego urzędu

(2) Podmioty państwowe:

- **Istnienie prawne**: Sprawdzić czy Subskrybent jest prawnie rozpoznawanym podmiotem państwowym podległym jednostce władzy centralnej właściwej ze względu na obszar działania (np. Urząd Wojewódzki etc.)
- **Nazwa podmiotu**: Sprawdzić, czy formalna nazwa prawna Subskrybenta, zarejestrowana w stosownym urzędzie właściwym ze względu na miejsce działalności Subskrybenta jest zgodna z nazwą umieszczoną we Wniosku o wydanie certyfikatu EV SSL.
- **Numer rejestracji:** Uzyskać unikalny numer rejestracyjny przyznany Subskrybentowi przez stosowny urząd właściwy ze względu na miejsce działalności Subskrybenta lub otrzymać dokumenty Ustaw, Uchwał, wszelkich 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 Subskrybenta jako podmiotu państwowego.

(3) Przedsiębiorstwa

- **Istnienie prawne**: Sprawdzić czy Subskrybent prowadzi działalność pod nazwą, którą podał we Wniosku o wydanie certyfikatu EV SSL;
- **Nazwa przedsiębiorstwa**: Sprawdzić czy formalna nazwa prawna Subskrybenta, zarejestrowana w stosownym urzędzie właściwym ze względu na miejsce działalności Subskrybenta jest zgodna z nazwą umieszczoną we Wniosku o wydanie certyfikatu EV SSL.

- **Numer rejestracji:** Uzyskać unikalny numer rejestracyjny przyznany Subskrybentowi przez stosowny urząd właściwy ze względu na miejsce działalności Subskrybenta. Jeśli dany urząd nie przypisał przedsiębiorstwu żadnego identyfikatora CERTUM musi otrzymać datę rejestracji przedsiębiorstwa.

(4) Organizacje międzynarodowe (niekomercyjne)

- **Istnienie prawne:** Zweryfikować czy Subskrybent jest prawnie rozpoznawalnym podmiotem będącym organizacją międzynarodową
- **Nazwa organizacji:** Zweryfikować czy prawnie zarejestrowana nazwa Subskrybenta jest identyczna z nazwą podaną we Wniosku o wydanie certyfikatu EV SSL
- **Numer rejestracji:** Uzyskać 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 jako organizacji międzynarodowej.

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 na zasadzie działań statutowych.
- Na podstawie listy właściwych podmiotów prowadzonej przez CABForum na stronie www.cabforum.org.
- Jeśli dana organizacja (niekomercyjna) jest tylko częścią, jednostką podległą innej organizacji międzynarodowej. CERTUM może zweryfikować daną jednostkę na podstawie weryfikacji organizacji zwierzchniej, której częścią jest organizacja Subskrybenta.

15. Weryfikacja podstawy prawnej oraz tożsamości Subskrybenta – Nazwa Skrócona

Jeśli poza formalną nazwą prawną Subskrybenta, zarejestrowanego w stosownym urzędzie, certyfikat EV SSL zawiera również nazwę skróconą lub inną (znaną również jako „doing business as", „DBA" lub „d/b/a" w US oraz „trading as" w UK), pod która Subskrybent prowadzi działalność, CERTUM MUSI zweryfikować, że (i) Subskrybent zarejestrował nazwę skróconą lub inną w urzędzie właściwym ze względu na miejsce prowadzenia przez Subskrybenta działalności. (weryfikowane zgodnie z niniejszym Załącznikiem) oraz, że (ii) dany wpis do rejestru jest nadal aktualny.

CERTUM może zweryfikować nazwę skróconą lub inną poprzez Kwalifikowane Rządowe Źródło Informacji, obsługiwane przez lub w imieniu stosowanej jednostki państwowej właściwej ze względu na miejsce prowadzenia przez Subskrybenta działalności lub poprzez bezpośredni kontakt z taką jednostką – osobiście, poprzez pocztę, pocztę elektroniczną, formularz WWW lub telefonicznie; lub może zweryfikować nazwę przybraną lub inną poprzez Kwalifikowane Niezależne Źródło Informacji pod warunkiem, że takie Źródło zweryfikowało nazwę we właściwym urzędzie. Ewentualnie CERTUM może polegać na potwierdzonej Opinii Prawnej lub

potwierdzonym Liście Księgowym, które wskażą nazwę skróconą lub inną Subskrybenta, urząd, który nazwę zarejestrował oraz zawierać będą oświadczenie, że informacja ta pozostaje ważna.

16. Weryfikacja adresu Subskrybenta

(a) Adres miejsca prowadzenia działalności

Aby zweryfikować fizyczne istnienie Subskrybenta CERTUM MUSI sprawdzić, czy adres fizyczny, podany przez Subskrybenta jest adresem, pod którym Subskrybent faktycznie prowadzi działalność gospodarczą (tzn. nie jest to punkt zbierania poczty lub skrzynka pocztowa).

(A) Wobec Subskrybentów, którzy prowadzą działalność w tym samym kraju, w którym są zarejestrowani:

(1) Wobec Subskrybentów, których adres prowadzonej działalności jest taki sam w przynajmniej jednym (1) aktualnym Kwalifikowanym Niezależnym Źródle Informacji, CERTUM potwierdza, że adres Subskrybenta wykazany we Wniosku o wydanie Certyfikatu EV SSL jest ważnym adresem Subskrybenta poprzez odniesienie do danego Źródła Informacji i może polegać na oświadczeniu Subskrybenta, że dany adres jest jego faktycznym miejscem działalności;

(2) Wobec Subskrybentów, którzy nie prowadzą działalności w miejscu potwierdzonym w przynajmniej jednym Kwalifikowanym Niezależnym Źródle Informacji CERTUM potwierdza adres Zamawiającego na podstawie wizyty kontrolnej, którą składa Subskrybentowi pracownik CERTUM. Na podstawie takiej wizyty przygotowywany jest raport z wizyty, w trakcie której:

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

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

(b) Numer telefonu w miejscu prowadzenia działalności

Aby w najwyższym stopniu zweryfikować autentyczność atrybutów Subskrybenta, CERTUM MUSI sprawdzić, czy numer telefonu dostarczony przez Subskrybenta jest głównym numerem telefonu dla miejsca działalności Subskrybenta.

Aby zweryfikować numer telefonu Subskrybenta, CERTUM MUSI wykonać działania opisane w punkcie A oraz jedno z działań z punktów B lub C:

(A) Potwierdzić numer telefonu Subskrybenta poprzez nawiązanie z nim połączenia i uzyskanie odpowiedzi pozwalającej potwierdzić, że Subskrybent jest dostępny pod danym numerem telefonu; oraz

(B) 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 Subskrybenta jest przypisany do adresu miejsca prowadzonej przez niego działalności;

(C) Uzyskać potwierdzoną Opinię Prawną gwarantującą, że podany przez Subskrybenta numer telefonu jest głównym numerem telefonu dla miejsca działalności Subskrybenta.

17. Weryfikacja zdolności biznesowej Subskrybenta

Jeśli wpis do stosownego rejestru świadczy o tym, że Subskrybent prowadzi działalność handlową przez mniej niż trzy lata oraz nie jest ujęty w, co najmniej jednym Kwalifikowanym Niezależnym Źródle Informacji, CERTUM MUSI zweryfikować, że Subskrybent jest w stanie prowadzić działalność biznesową.

(A) W celu weryfikacji zdolności biznesowej Subskrybenta CERTUM sprawdza czy Subskrybent posiada aktywny rachunek rozliczeniowy w zarejestrowanej instytucji finansowej. W tym celu CERTUM otrzymuje od osoby reprezentującej Subskrybenta dokumenty bankowe gwarantujące, że Subskrybent posiada aktywne konto bankowe w instytucji o uregulowanej pozycji finansowej (np. kopia Umowy o Prowadzenie Rachunku Bankowego).

(B) Ewentualnie CERTUM może polegać na Opinii Prawnej zawierającej stosowne zapewnienie, że Podmiot jest w stanie prowadzić działalność handlową będąc właścicielem aktywnego konta bankowego.

18. Weryfikacja domeny Subskrybenta

(a) Wymagania

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

(1) Nazwa domeny zarejestrowana jest przez jednostkę rejestrującą akceptowaną przez Internet Corporation for Assigned Names and Numbers (ICANN) lub widnieje w rejestrach Internet Assigned Numbers Authority (IANA);

(2) Informacje o rejestracji domeny w bazie WHOIS POWINNY być publiczne i POWINNY zawierać nazwę, adres fizyczny raz kontakt administracyjny organizacji;

(3) Subskrybent jest zarejestrowanym właścicielem domeny lub posiada wyłączne prawo do posługiwania się nią przyznane mu przez właściciela domeny;

(b) Metody weryfikacji

(A) Jeśli Subskrybent jest właścicielem domeny:

(1) Wykonanie zapytania do bazy WHOIS dla nazwy domenowej podanej przez Subskrybenta i otrzymanie odpowiedzi potwierdzającej prawa Subskrybenta do posługiwania się nazwą domenową; lub

(2) Nawiązanie kontaktu z osobą wymienioną w zapisie WHOIS w celu potwierdzenia, że Subskrybent jest właścicielem nazwy domenowej i uzgodnienia z osobą kontaktową aktualizacji danych w zapisie WHOIS;

(3) W przypadku, gdy informacja o rejestracji domeny nie jest publiczna, CERTUM może nawiązać kontakt z rejestratorem domeny za pomocą poczty elektronicznej lub tradycyjnej.

(B) Jeśli Subskrybent nie jest właścicielem domeny CERTUM weryfikuje jego uprawnienia do posługiwania się domeną

(1) CERTUM polega na Opinii Prawnej, która wskazuje na Subskrybenta jako posiadającego wyłączność na użytkowanie nazwy domeny; lub

(2) CERTUM polega na 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 chcieć upewnić się czy Subskrybent jest świadomy posiadanych przez siebie praw do domeny. W tym celu CERTUM kontaktuje się z jedną z osób reprezentujących Subskrybenta prosząc o potwierdzenie tego faktu.

19. 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 Subskrybenta** – CERTUM MUSI zweryfikować nazwisko i tytuł Osoby Podpisującej Umowę jak i Osoby Zatwierdzającej Certyfikat. CERTUM MUSI również potwierdzić, że powyższe osoby występują w imieniu Subskrybenta.

(2) **Upoważnienie Osoby Podpisującej Umowę** – CERTUM MUSI zweryfikować, poprzez źródło inne niż sam podpisujący, że został on wyraźnie upoważniony przez Subskrybenta do zawarcia Umowy z Subskrybentem (oraz każdego innego dwustronnego porozumienia) w imieniu Subskrybenta, włączając umowę, na podstawie której wskazuje się jedną lub więcej osób mogących zatwierdzić certyfikat w imieniu Subskrybenta („Upoważnienie do Podpisywania").

(3) **Upoważnienie Osoby Zatwierdzającej Certyfikat** – CERTUM musi zweryfikować, poprzez źródło inne niż sama Osoba Zatwierdzająca Certyfikat, że została ona wyraźnie upoważniona przez Subskrybenta do wykonania poniższych działań:

- Złożenia lub – jeśli dotyczy – upoważnienia Wnioskodawcy do złożenia Wniosku o wydanie certyfikatu EV SSL w imieniu Subskrybenta; oraz

- Dostarczenia lub – jeśli dotyczy – upoważnienia Wnioskodawcy Certyfikatu do dostarczenia informacji wymaganych od Subskrybenta w celu wydania Certyfikatu EV SSL; oraz
- Zatwierdzenia Wniosku o wydanie certyfikatu EV SSL złożonego przez Wnioskodawcę..

(A) 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 powyższe osoby występują w imieniu Subskrybenta poprzez:

- Nawiązanie kontaktu z działem kadr Subskrybenta (korespondencyjnie lub telefonicznie – kierując się danymi adresowymi, jakie przypisane są do miejsca prowadzenia działalności przez Subskrybenta i pozyskane zostały zgodnie z e wskazaniami niniejszego Załącznika) i uzyskanie potwierdzenia, że Osoba Podpisująca Umowę i/lub Osoba Zatwierdzająca Certyfikat są pracownikami Subskrybenta, lub
- Uzyskanie Niezależnego Potwierdzenia od Subskrybenta, potwierdzonej Opinii Prawnej (opisanych w sekcji 22(a)) lub potwierdzonego Listu Księgowego zaświadczających, że Osoba Podpisująca Umowę i/lub Osoba Zatwierdzająca Certyfikat są pracownikami Subskrybenta 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.

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

(1) **Opinię Prawną** – Upoważnienia do występowania w imieniu Subskrybenta przez w/w osoby mogą zostać zweryfikowane w oparciu o potwierdzoną Opinię Prawną;

(2) **Zarządzenie firmy lub organizacji** – Upoważnienia do występowania w imieniu Subskrybenta przez w/w osoby mogą 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) i (ii) CERTUM może bez wątpliwości potwierdzić, że poświadczenie zostało złożone przez taką właśnie

osobę, której atrybuty wskazują na posiadanie przez nią władzy wykonawczej w organizacji lub firmie.

(3) **Niezależne Potwierdzenie przez Subskrybenta –** Upoważnienie może zostać zweryfikowane w oparciu o fakt Niezależnego Potwierdzenia przez Subskrybenta

(4) **Umowa między CERTUM a Subskrybentem** – Upoważnienie Osoby Zatwierdzającej Certyfikat może zostać potwierdzone poprzez zapisy umowy pomiędzy CERTUM a Subskrybentem wskazujące na Osobę Zatwierdzającą Certyfikat i przyznające jej prawo do występowania w imieniu Subskrybenta, pod warunkiem, że umowa została podpisana przez Osobę Podpisującą Umowę, której status został już uprzednio w pełni zweryfikowany.

(5) **Wcześniejsza umowa między CERTUM a Subskrybentem** – Jeśli nie wcześniej niż 90 dni przed złożeniem zamówienia na certyfikat EV SSL została przez Subskrybenta zawarta umowa na świadczenie na jego rzecz przez CERTUM usług certyfikacyjnych (jednak wyłącznie odnośnie certyfikatów SSL) oraz umowa ta została podpisana przez Osobę Podpisującą Umowę lub Osobę Zatwierdzającą Certyfikat to CERTUM może na tej podstawie pozytywnie zweryfikować w/w osoby jako uprawnione do występowania w imieniu Subskrybenta

(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, oraz
- CERTUM zweryfikowało uprawnienia Osoby Podpisującej Umowę do występowania w imieniu Subskrybenta, wówczas:

CERTUM i Subskrybent mogą zawrzeć pisemną umowę, podpisaną przez Osobę Podpisującą Umowę w imieniu Subskrybenta, na mocy której, przez wskazany okres czasu, Subskrybent 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 Subskrybent będzie uznawał wszystkie Wnioski o wydanie certyfikatów EV SSL, złożone przez lub zatwierdzone przez Osobę Zatwierdzającą Certyfikat do czasu odwołania upoważnienia. Umowa MUSI zawierać obustronnie zgodę wobec (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 Subskrybenta o wycofaniu upoważnienia dla Osoby Zatwierdzającej Certyfikat oraz (iv) innych wymaganych sytuacją środków ostrożności.

20. 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 prawnie ważnym podpisem odręcznym lub pieczęcią (dla papierowych Umów i Wniosków) lub prawnie ważnym podpisem elektronicznym (dla Umowy i Wniosku elektronicznego), wiążącym Subskrybenta 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 Subskrybenta.

(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 sekcji 19, może zastąpić konieczność weryfikacji podpisu samego Wnioskodawcy.

(b) Akceptowane metody weryfikacji

(1) Rozmowa telefoniczna z przedstawicielem Subskrybenta, nawiązana z numerem telefonu potwierdzonym zgodnie z niniejszym Załącznikiem, podczas której prosi się o przełączenie do Wnioskodawcy lub Osoby Podpisującej 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 Subskrybenta.

(2) List wysłany na zweryfikowany zgodnie z niniejszym Załącznikiem adres Subskrybenta lub jego przedstawiciela, adresowany wówczas do – odpowiednio – Wnioskodawcy lub Osoby Podpisującej Umowę, w odpowiedzi na który osoba przedstawiająca się jako Wnioskodawca lub Osoba Podpisująca Umowę oddzwania lub odsyła list, potwierdzający, że dana osoba podpisała i złożyła badany dokument w imieniu Subskrybenta.

(3) Zastosowanie procesu podpisywania, który potwierdzi nazwisko i tytuł podpisującego dokument w bezpieczny sposób, np. poprzez szyfrowany kanał komunikacyjny (np. logowanie), który pozwala na identyfikację podpisującego przez złożeniem podpisu lub poprzez użycie podpisów elektronicznych weryfikowanych za pomocą stosowanych certyfikatów.

(4) Notarialne poświadczenie podpisów, pod warunkiem, że CERTUM niezależnie

potwierdzi, że dany notariusz jest upoważnionym do świadczenia usług notarialnych na terytorium, gdzie prowadzona jest działalność Subskrybenta.

21. Weryfikacja zatwierdzenia Wniosku o wydanie certyfikatu EV SSL

W przypadku, gdy Wniosek o wydanie certyfikatu EV SSL został złożony przez Wnioskodawcę, CERTUM przed wydaniem żądanego Certyfikatu MUSI potwierdzić, że upoważniona Osoba Zatwierdzająca Certyfikat przejrzała i zatwierdziła Wniosek za pomocą następujących metod:

(1) CERTUM nawiązuje kontakt z Osobą Zatwierdzającą Certyfikat telefonując na zweryfikowany już numer telefonu lub wysyłając list na adres pocztowy 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 akceptacje Wniosku w sposób wymagany przez mechanizm strony; lub

(3) CERTUM weryfikuje podpis Wnioskodawcy

22. Weryfikacja Źródeł Informacji Pewnej

(a) Weryfikacja Opinii Prawnej

Przed akceptacją jakiejkolwiek opinii prawnej złożonej w CERTUM, CERTUM MUSI upewnić się, że spełnia one następujące wymagania:

(A) **Status autora** – CERTUM MUSI zweryfikować, czy Opinia Prawna jest autorstwa niezależnego praktyka prawa, reprezentującego Subskrybenta (lub prawnika zatrudnionego przez Subskrybenta) będącego:

(1) Prawnikiem (lub notariuszem, adwokatem, obrońcą etc.), uprawnionym do świadczenia usług prawnych w kraju prowadzenia działalności przez Subskrybenta lub kraju, w którym Subskrybent utrzymuje biuro lub inną siedzibę.

(2) Notariuszem, będącym członkiem Międzynarodowej Unii Notariuszy Łacińskich uprawnionym do świadczenia usług notarialnych w kraju Subskrybenta lub kraju, w którym Subskrybent utrzymuje biuro lub inną siedzibę.

(B) **Podstawa Opinii** – CERTUM MUSI zweryfikować, czy autor opinii działa w imieniu Subskrybenta oraz czy zapisy potwierdzonej Opinii Prawnej są oparte na znajomości przez niego potwierdzanych faktów oraz czy znajomość ta poparta jest zawodowym doświadczeniem i dokonaną ekspertyzą. Opinia może również zawierać

zwyczajowe w danym prawodawstwie klauzule i ograniczenia pod warunkiem, że zakres ograniczanej odpowiedzialności nie jest na tyle duży, że potencjalne błędy lub zaniechania w Opinii nie będą niosły żadnych konsekwencji (finansowych, zawodowych lub reputacji) dla prawnika.

(C) **Autentyczność** – Aby potwierdzić autentyczność opinii prawnej, CERTUM MUSI nawiązać połączenie telefoniczne z autorem Opinii lub wysłać kopię Opinii zwrotnie do prawnika 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. CERTUM zwraca się z prośbą o potwierdzenie przez autora Opinii lub jego asystenta, że przedłożona Opinia jest autentyczna. Jeśli dane teleadresowe 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.

(b) List księgowy

Przed akceptacją jakiegokolwiek listu księgowego złożonego w CERTUM, CERTUM MUSI zweryfikować, że list taki spełnia następujące wymagania:

(A) **Status autora** – CERTUM MUSI zweryfikować, czy List Księgowy jest autorstwa niezależnego biegłego rewidenta działającego w imieniu Subskrybenta (lub będącego jego pracownikiem), który jest dyplomowanym księgowym publicznym, księgowym zawodowym etc, licencjonowanym przez pełnoprawnego członka Międzynarodowej Federacji Księgowych (IFAC) do wykonywania swojego zawodu w miejscu rejestracji Subskrybenta lub w kraju, w którym Subskrybent utrzymuje swoje biuro lub inną siedzibę.

(B) **Podstawa opinii** – CERTUM MUSI potwierdzić, że rewident działa w imieniu Subskrybenta a treść Listu jest oparta na znajomości przez rewidenta potwierdzanych faktów oraz poparta jest profesjonalnym doświadczeniem i ekspertyzą rewidenta. List może również zawierać zwyczajowe w danym prawodawstwie klauzule i ograniczenia pod warunkiem, że zakres ograniczanej odpowiedzialności nie jest na tyle duży, że potencjalne błędy lub zaniechania w Liście nie będą niosły żadnych konsekwencji (finansowych, zawodowych lub reputacji) dla rewidenta.

(C) **Autentyczność –** Aby potwierdzić autentyczność Listu, CERTUM MUSI nawiązać połączenie telefoniczne z autorem Listu lub wysłać kopię Listu zwrotnie do rewidenta na adres, telefon, faks lub adres email, które muszą być potwierdzone w jednostce odpowiedzialnej za rejestrację i licencjonowanie osób świadczących usługi księgowe na terytorium danego kraju. CERTUM zwraca się z prośbą o potwierdzenie przez autora Listu lub jego asystenta, że przedłożony List jest autentyczny. Jeśli dane teleadresowe rewidenta nie mogą być pozyskane ze źródła odpowiedzialnego za jego rejestrację i/lub licencjonowanie CERTUM może skorzystać z informacji zawartych w Kwalifikowanych Niezależnych Źródłach Informacji

(c) Weryfikacja bezpośrednia

Przed akceptacją jakichkolwiek dokumentów otrzymanych od Strony Trzeciej, która dokonała weryfikacji Subskrybenta CERTUM sprawdza czy Strona Trzecia Weryfikacji (zwana dalej Stroną Trzecią) spełnia następujące warunki:

Kwalifikacje Strony Trzeciej – CERTUM w sposób niezależny weryfikuje czy Strona Trzecia jest kwalifikowanym notariuszem, prawnikiem lub biegłym księgowym (rewidentem) właściwym dla miejsca, w którym prowadzi działalność.

Dokumenty – CERTUM upewnia się, że Strona Trzecia widziała dostarczone jej przez osobę reprezentującą Subskrybenta dokumenty aplikacyjne;
Potwierdzenie – Jeśli Strona Trzecia nie jest notariuszem prawa łacińskiego, CERTUM potwierdza autentyczność otrzymanych za pośrednictwem Strony Trzeciej dokumentów. W tym celu CERTUM wykonuje telefon do Strony Trzeciej 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 Subskrybenta. 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.

(d) Niezależne Potwierdzenie Zamawiającego

Niezależnie Potwierdzenie Subskrybenta 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)

(i) Niezależnie Potwierdzenie Subskrybenta CERTUM otrzymuje od osoby zatrudnionej przez Subskrybenta (innej niż sprawdzana osoba), posiadającej stosowane upoważnienia do potwierdzania faktów („Osoba Potwierdzająca"),

(ii) Niezależnie Potwierdzenie Subskrybenta CERTUM otrzymuje w sposób umożliwiający autoryzacje i weryfikację źródła informacji; oraz

(iii) Niezależnie Potwierdzenie Subskrybenta jest wiążące dla Subskrybenta

Niezależne Potwierdzenie Subskrybenta może zostać pozyskane za pomocą następującej procedury:

(1) CERTUM MUSI zainicjować komunikację z Subskrybentem w celu uzyskania od niego potwierdzenia danych faktów lub informacji:

(A) **Adresat** – Prośba o potwierdzenie MUSI być skierowana do:

(i) Osoby piastującej w organizacji lub firmie Subskrybenta stanowisko kwalifikujące ją do bycia Osobą Potwierdzającą (np. sekretarz, prezes, CEO, CFO, COO, CIO, CSO, Dyrektor etc), która określona jest z imienia i nazwiska oraz stanowiska w aktualnym Kwalifikowanym Rządowym Źródle Informacji (np. rejestr giełdy i papierów wartościowych), Kwalifikowanym Niezależnym Źródle Informacji, Potwierdzonej Opinii Prawnej lub potwierdzone znajduje w Dziale Kadr Subskrybenta, z którym nawiązano kontakt telefoniczny lub listowny (pod zweryfikowanym zgodnie z niniejszymi Załącznikiem numerem telefonu lub adresem Subskrybenta); lub

(ii) Urzędu rejestrującego działalność Subskrybenta, z prośbą o przekazanie do właściwej Osoby Potwierdzającej.

(B) **Środki komunikacji** – Prośba o potwierdzenie MUSI być skierowana do Osoby Zatwierdzającej Certyfikat w sposób umożliwiający dotarcie prośby do danej osoby. Akceptowane formy komunikacji obejmują:

(i) List tradycyjny, adresowany do Osoby Potwierdzającej skierowany na adres:

(a) miejsca działalności Subskrybenta, zweryfikowany zgodnie z niniejszym Załącznikiem; lub

(b) adres służbowy Osoby Potwierdzającej, określony w aktualnym Kwalifikowanym Rządowym Źródle Informacji, Kwalifikowanym Niezależnym Źródle Informacji, Potwierdzonej Opinii Prawnej lub;

(c) adres urzędu rejestrującego działalność Subskrybenta, z prośbą o przekazanie do właściwej Osoby Potwierdzającej.

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

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

(iv) Faks, kierowany do Osoby Potwierdzającej w miejscu działalności Subskrybenta. Numer faksu musi być ujęty w aktualnym Kwalifikowanym Rządowym Źródle Informacji, Kwalifikowanym Niezależnym Źródle Informacji lub potwierdzonej Opinii Prawnej. Strona tytułowa musi wyraźnie wskazywać na adresowanie faksu do Osoby Potwierdzającej.

(2) CERTUM MUSI otrzymać odpowiedź na prośbę o potwierdzenie od Osoby Zatwierdzającej 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 Zatwierdzającą Certyfikat.

(e) 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 tylko, 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.

(f) Kwalifikowane Rządowe Źródło Informacji

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 karami kodeksu karnego lub cywilnego.

23. Pozostałe wymagania dotyczące weryfikacji

(a) Status wysokiego ryzyka

CERTUM MUSI wyszukiwać i identyfikować Subskrybentów, których znamionuje wysokie ryzyko bycia obiektem ataków typu *phishing* lub innych form oszustw internetowych, wobec których podejmuje takie dodatkowe kroki weryfikacji, które gwarantują prawidłowe i pewne zweryfikowanie Subskrybenta zgodnie z niniejszym Załącznikiem.

CERTUM może identyfikować Subskrybentów Wysokiego Ryzyka poprzez sprawdzanie stosownych list organizacji, 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:

(A) Listy obiektów ataków typu *phishing*, publikowane przez Anti-Phishing Work Group (APWG); oraz

(B) 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 Subskrybentowi, jeśli Subskrybent, Osoba Podpisująca Umowę, Osoba Zatwierdzająca Certyfikat lub kraj, w którym jest zarejestrowany lub działa Subskrybent odpowiadają poniższej charakterystyce:

(A) Figurują na rządowych listach podmiotów lub 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.

(B) Figurują na listach firm, organizacji oraz osób, którym zakazana jest lub ograniczona działalność na terenie objętym prawem, pod które podlega wystawiający certyfikat urząd CERTUM.

CERTUM dokonuje sprawdzenia następujących rejestrów:

(A) Rejestr odmowny dla osób fizycznych

(B) Rejestr odmowny dla podmiotów

(C) Rejestr dotyczący ograniczeń eksportowych Rzeczypospolitej Polskiej

24. Podwójna weryfikacja oraz zasada Due Diligence

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 niebędącej 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. Ostateczna korelacja dokumentów ma na celu wykrycie ewentualnych rozbieżności, które wymagałyby dalszych wyjaśnień. W ten sposób, poddając należytemu sprawdzeniu możliwie największą ilość informacji, CERTUM w swoim postępowaniu kieruje się zasadą Due Diligence.

25. Wymagania dotyczące odnowień certyfikatów EV SSL

Przed odnowieniem certyfikatu EV SSL CERTUM musi wykonać wszystkie etapy weryfikacji wymagane przez niniejszy Załącznik, aby upewnić się, że żądanie odnowienia zostało właściwie potwierdzone przez Subskrybenta a wszystkie informacje publikowane w certyfikacie EV SSL są nadal ważne i aktualne.

G. STATUS CERTYFIKATU EV SSL ORAZ JEGO UNIEWAŻNIENIE

26. Sprawdzenie statusu certyfikatu EV SSL

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

(1) Dla certyfikatów EV SSL

(A) CRL: (Listy Certyfikatów Unieważnionych) MUSZĄ być aktualizowane co najmniej raz na 7 dni, z maksymalnym okresem ważności 10 dni; lub

(B) OCSP: Począwszy od Stycznia 2010 **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 podległych Certum Extended Validation:

(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 2010 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 dostarcza swoje usługi CRL i/lub OCSP zapewniając wystarczająco krótki czas odpowiedzi dla zapytań generowanych dla wszystkich certyfikatów EV SSL. CERTUM zapewnia możliwość pobrania wszystkich 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 lub w usłudze OCSP NIE MOGĄ być usuwane do czasu upłynięcia pierwotnych okresów ważności unieważnionych certyfikatów EV SSL.

27. 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 informacje, że Subskrybent naruszył istotne postanowienia Umowy z Subskrybentem;

(5) CERTUM otrzyma zgłoszenie lub uzyska informacje, że sąd lub właściwy 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 informacje 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 jakakolwiek informacja zawarta w certyfikacie EV SSL jest nieaktualna;

(9) CERTUM zaprzestanie świadczenia usług i nie przekaże swoich zobowiązań innemu urzędowi, który będzie świadczył usługi unieważniania;

(10) Prawa CERTUM do wydawania certyfikatów EV SSL zgodnych z niniejszym Załącznikiem wygasną, zostaną unieważnione lub zakończone [chyba, że CERTUM przekaże obowiązki związane ze świadczeniem usług CRL/OCSP innemu urzędowi];

(11) Klucz prywatny CERTUM, używany do podpisywania certyfikatów EV SSL zostanie

unieważniony;

(12) Jakichkolwiek innych wydarzeń ujętych w politykach EV; lub

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

28. Zgłaszanie problemów z certyfikatami EV SSL i możliwości odpowiedzi ze strony CERTUM

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 innych typów nadużyć, lub nieprawidłowości związanych z certyfikatami EV SSL. Zarazem CERTUM gwarantuje, że jest zdolne do przyjmowania i potwierdzania takich zgłoszeń 24 godziny na dobę przez 7 dni w tygodniu, udostępniając w tym celu stronę: www.certum.pl/repository.
CERTUM zobowiązuje się rozpocząć badanie wszystkich zgłoszonych problemów z certyfikatem EV SSL w ciągu 24 godzin od przyjęcia zgłoszenie i podjąć decyzję o unieważnieniu lub innym niezbędnym działaniu na podstawie co najmniej następujących kryteriów:

(i) Natury zgłaszanego problemu;
(ii) Ilości zgłoszeń otrzymanych w związku z danym certyfikatem EV SSL lub witryną www zabezpieczoną takim certyfikatem;
(iii) Tożsamością zgłaszającego (dla przykładu, zgłoszenie od przedstawiciela organów ścigania, że strona zaangażowana jest w nielegalne działania ma wyższą wagę niż zgłoszenie klienta, twierdzącego, że nie otrzymał zamawianych towarów); oraz
(iv) Stosownych obowiązujących uwarunkowań prawnych

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

H. PRACOWNICY I STRONY TRZECIE

29. 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:

(A) Przez osobiste stawiennictwo danej osoby przed zaufaną osobą pełniącą funkcje kadrowe lub bezpieczeństwa, oraz

(B) Weryfikację powszechnie rozpoznawanych, wydawanych przez administrację rządową dokumentów ze zdjęciem (np. paszport i/lub prawa jazdy); oraz

(C) Potwierdzenie poprzedniego zatrudnienia;

(D) Sprawdzenie referencji zawodowych

(E) Potwierdzenie wykształcenia

(F) Sprawdzenie rejestru skazanych

CERTUM wymaga od swoich pracowników wykonujących czynności weryfikacyjne zdania wewnętrznych egzaminów związanych z kryteriami postępowania z Wnioskami o wydanie certyfikatu EV SSL w zgodzie z niniejszym Załącznikiem.

.

30. Punkty Rejestracji oraz podwykonawcy

CERTUM może przekazać realizację części lub wszystkich wymagań opisanych w niniejszym Załączniku Punktowi Rejestracji (zwanym dalej PR) lub podwykonawcy. Wyjątek stanowią wymagania końcowej weryfikacji opisane w sekcji 23.

CERTUM może upoważnić podmiot ważnego certyfikatu EV SSL do pełnienia funkcji Punktu Rejestracji a także upoważnić inne urzędy do wydawania dodatkowych certyfikatów EV SSL na trzecim lub wyższym poziomie domenowym, zawartym w domenie ujętej w oryginalnym certyfikacie EV SSL CERTUM (zwanym również „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) Weryfikacja krzyżowa może być realizowana przez osobę reprezentującą PR Enterprise.

We wszystkich przypadkach CERTUM musi kontraktowo zobligować każdy PR, podwykonawcę i PR typu Enterprise do spełniania stosownych wymagań niniejszego Załącznika i realizować je tak, jak robi to CERTUM.

I. DOKUMENTACJA I ARCHIWIZACJA DANYCH

31. Dokumentacja zdarzeń na potrzeby audytu

CERTUM dokumentuje w szczegółach wszystkie działania podjęte w celu obsługi Wniosku o wydanie certyfikatu EV SSL i wydania certyfikatu EV SSL, włączając wszelkie informacje utworzone lub otrzymane w związku z żądaniem certyfikatu EV SSL oraz wszystkie działania podjęte do jego przetworzenia – w tym czas, datę i personel zaangażowany w realizację zadania. Zapisy te są udostępniane audytorom jako dowody praktyk CERTUM. Zapisy poniżej dotyczą również wszystkich PR i podwykonawców. Wymagane zapisy obejmują lecz nie są ograniczone do rejestracji następujących zdarzeń:

(i) Zdarzeń związanych z zarządzaniem cyklem życia klucza CERTUM, włączając:

(a) Tworzenie, utworzenie kopii zapasowej, przechowywanie, odzyskiwanie, archiwizację i zniszczenie klucza;

(b) Zdarzenia związane z zarządzaniem cyklem życia urządzeń kryptograficznych

(ii) Zdarzeń związanych z zarządzaniem cyklem życia certyfikatu EV SSL Subskrybenta i certyfikatu CERTUM, włączając:
   (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; oraz
   (f) Tworzenie list CRL dla certyfikatów EV SSL oraz rekordów OCSP.

(iii) Zdarzeń związanych z bezpieczeństwem, włączając:
   (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, oraz
   (f) Wejścia i wyjścia do siedziby CERTUM.

(iv) Zapisy zdarzeń zawieraj następujące informacje:
   (a) Datę i czas zapisu;
   (b) Tożsamość osoby lub podmiotu dokonującego zapisu, oraz
   (c) Opis rekordu.

32. Przechowywanie dokumentacji

Zapisy są dostępne na żądanie niezależnych audytorów. Zapisy audytowe powinny być przechowywane przez co najmniej 7 lat. CERTUM MUSI przechowywać 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 MUSI również utrzymywać aktualną wewnętrzną bazę wszystkich unieważnionych certyfikatów EV SSL i odrzuconych Wniosków, dla których powodem odrzucenia lub unieważnienia było podejrzenie *phishingu* lub innych działań nieuczciwych. Informacja taka powinna być używana do oznaczenia podejrzanych Wniosków.

33. 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 pod warunkiem zachowania wymagań opisanych w punkcie (b) poniżej.

(b) Użycie istniejącej dokumentacji lub informacji

(1) Każdy certyfikat EV SSL wydany przez CERTUM MUSI być poparty ważnym i aktualnym Wnioskiem o wydanie certyfikatu EV SSL i Umową z Subskrybentem, podpisanymi przez przedstawiciela działającego w imieniu

Subskrybenta.

(2) Okres ważności dla informacji używanej przez CERTUM do weryfikacji takich Wniosków NIE MOŻE przekraczać maksymalnego okresu ważności dla danej informacji, opisanego w sekcji 8 niniejszego Załącznika. Punktem odniesienia powinna być wcześniejsza z dat: otrzymania informacji (np. data potwierdzenia telefonicznego) lub ostatniej jej aktualizacji przez źródło (np. w przypadku, gdy baza danych została sprawdzona przez CERTUM 1 czerwca, jednak zawierała dane ostatnio uaktualniane przez dostawcę 1 lutego, wtedy data uzyskania informacji będzie 1 luty).

(3) W przypadku informacji przeterminowanych CERTUM MUSI powtórzyć proces weryfikacji zgodny z niniejszym Załącznikiem.

34. Bezpieczeństwo danych

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

J. ZGODNOŚĆ Z WYMAGANIAMI MIĘDZYNARODOWYCH STANDARDÓW DOTYCZĄCYCH CERTYFIKATÓW EV SSL

35. Wymagania audytowe

(a) Audyt wstępny

Przed wydaniem certyfikatu EV SSL CERTUM MUSI pomyślnie zakończyć: (i) audyt za zgodność z Programem WebTrust for CA oraz (ii) audyt za zgodność z Programem WebTrust EV Program, lub ich odpowiedniki, jeśli są one zaakceptowane przez CA/Browser Forum.

(b) Regularny audyt wewnętrzny

Przez cały okres, w którym CERTUM wydaje certyfikaty EV SSL, MUSI ściśle kontrolować jakość swoich usług poprzez realizację audytów wewnętrznych na losowej próbce 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

Przez cały okres wydawania certyfikatów EV SSL, CERTUM MUSI poddawać się corocznym audytom za zgodność z (i) WebTrust for CA Program (ii) WebTrust EV Program lub odpowiednikiem obydwu, jeśli został zaakceptowany przez CA/Browser Forum. Audyt taki MUSI objąć wszystkie obowiązki CERTUM wyszczególnione w niniejszym Załączniku, niezależnie od tego, czy są one wykonywane bezpośrednio przez CERTUM czy przez PR lub podwykonawców.

Wyniki audytu są udostępnione publicznie przez CERTUM

(d) Kwalifikacje audytora

Wszystkie audyty wymagane przez niniejszy Załącznik MUSZĄ być wykonywane przez Kwalifikowanego Audytora. Kwalifikowany Audytor MUSI:

(1) Być niezależną publiczną firmą, posiadającą doświadczenie w badaniu technologii PKI, narzędziach i technikach bezpieczeństwa informacji, audytowaniu bezpieczeństwa i IT oraz oceny podmiotów będących stronami trzecimi oraz posiadać aktualną licencje do przeprowadzania audytów WebTrust for CA Program i WebTrust EV Program lub odpowiadających im audytów zaakceptowanych przez CA/Browser Forum; oraz

(2) Być członkiem AICPA lub odpowiadającego mu podmiotu zlokalizowanego poza USA, wymagającego, aby audyty przeprowadzać według ustalonych standardów, zakładających posiadanie stosownych umiejętności, środków zapewnienia jakości takich jak przeglądy badawcze, testy kompetencji, standardy właściwego podziału obowiązków i zadań oraz spełniających wymagania odnośnie ciągłego szkolenia zawodowego; *oraz*

(3) Posiadać ubezpieczenie Odpowiedzialności Zawodowej/Błędów i Zaniechań z kwotą ubezpieczenia, co najmniej 1 miliona USD.

(e) Tworzenie klucza głównego urzędu

Dla kluczy głównych CERTUM tworzonych po wydaniu niniejszego Załącznika, Kwalifikowany Audytor CERTUM POWINIEN być świadkiem ceremonii tworzenia klucza głównego CERTUM w celu obserwacji procesu i kontroli integralności i poufności utworzonego klucza głównego CERTUM. Kwalifikowany Audytor MUSI w takiej sytuacji utworzyć raport wskazujący, że CERTUM podczas procesu tworzenia swojego klucza głównego:

- Udokumentowało procedury tworzenia i ochrony swojego klucza głównego w swoich Politykach Certyfikacji oraz Kodeksie Postępowania Certyfikacyjnego;
- W swoich procedurach ujęło szczegółowy opis procesu, jaki należy zrealizować w celu utworzenia pary kluczy głównych CERTUM;
- Utrzymywało właściwy nadzór, aby zapewnić tworzenie i ochronę klucza głównego CERTUM w zgodzie z procedurami opisanymi w Polityce i Kodeksie oraz Skrypcie Tworzenia Kluczy Głównych; oraz
- Wykonało, podczas tworzenia klucza głównego, wszystkie procedury wymagane przez Skrypt Tworzenia Kluczy Głównych.

Z przebiegu całej ceremonii tworzenia kluczy powinien zostać wykonany zapis video dla celów audytowych..

K. POZOSTAŁE WYMAGANIA KONTRAKTOWE

36. Polityka prywatności

CERTUM MUSI spełniać wszystkie stosowne wymagania prawne związane z ochroną prywatności, jak również własną polityką prywatności, w trakcie zbierania, używaniu i ujawnienia informacji prywatnych w trackie procesu weryfikacji danych do certyfikatu EV SSL.

37. Ograniczenia odpowiedzialności

(a) Odpowiedzialność CERTUM

(1) Subskrybenci i strony ufające. W przypadku, gdy CERTUM wydało i zarządzało certyfikatem EV SSL zgodnie z niniejszym Załącznikiem i swoimi Politykami EV, nie będzie odpowiadało przed beneficjentami certyfikatów EV SSL lub innymi przedstawicielami strony trzeciej za jakiekolwiek szkody powstałe w wyniku użycia lub udzieleniu zaufania certyfikatowi poza odpowiedzialnością określoną w swoich Politykach EV. W przypadkach, gdy CERTUM *nie* wydało lub zarządzało certyfikatem EV SSL w pełnej zgodności z niniejszym Załącznikiem i swoimi Politykami EV, CERTUM może starać się ograniczyć swoja odpowiedzialność względem Subskrybentów lub Stron Trzecich certyfikatu EV SSL, za wydarzenia lub działania prawne związane z roszczeniami, stratami lub szkodami wynikającymi z użycia lub udzielenia zaufania certyfikatowi EV SSL za pomocą dowolnych metod. Wszystkie takie ograniczenia odpowiedzialności CERTUM MUSZĄ być również ujęte w Politykach EV. Dodatkowo, CERTUM nie może starać się ograniczyć swojej odpowiedzialności wobec Subskrybentów i Stron Trzecich certyfikatu EV SSL dla prawnie uznanych roszczeń do kwoty mniejszej niż 2000 USD na każdego Subskrybenta lub Strony Trzeciej certyfikatu EV SSL. CERTUM bierze na siebie ryzyko związane z prawną zasadnością ograniczeń odpowiedzialności.

(2) **Ochrona Dostawców Oprogramowania.** Pomimo wszystkich ograniczeń odpowiedzialności w stosunku do Subskrybentów i stron ufających, CERTUM przyjmuje do wiadomości i potwierdza, że Dostawca Oprogramowania, który podpisał z CERTUM umowę dystrybucyjną dla certyfikatów EV SSL, nie podejmuje żadnych zobowiązań lub odpowiedzialności, spoczywających na CERTUM w ramach niniejszego Załącznika, lub istniejących z uwagi na wydawanie i zarządzanie certyfikatami EV SSL lub powierzone zaufanie beneficjentom certyfikatu EV SSL lub innych podmiotów. Z tego też względu CERTUM będzie bronił, ochraniał i ostrzegał każdego Dostawcę Oprogramowania przed wszelkimi roszczeniami, szkodami i stratami, które może ponieść dany Dostawca Oprogramowania w związku z certyfikatami EV SSL wydanymi przez CERTUM, bez względu na przyczynę działań i ich podstawy prawne. Powyższe zastrzeżenie nie odnosi się jednakże do roszczeń, 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 niegodny zaufania lub wyświetlający jako godny zaufania certyfikat EV SSL (i) który jest przeterminowany lub (ii) unieważniony (tylko w przypadku, gdy status unieważnienia jest dostępny online w CERTUM a przeglądarka internetowa nie potrafiła go pobrać lub zignorowała wskazanie takiego statusu).

Odniesienia

1. CA/BROWSER FORUM Guidelines for the issuance and Management of Extended Validation Certificates, Version 1.1, 10 April 2008
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 miedzy użytkownikiem sieci globalnej a witryną Internetową, do której przyporządkowany jest certyfikat EV SSL oraz umożliwiające identyfikację właściciela tej witryny.

Guidelines for the Issuance and Management of Extended Validation Certificates v 1.1 (zwany dalej 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.

Organizacja Prywatna (*ang. Private Organization*) – organizacja pozarządowa posiadająca osobowość prawną, której właścicielem może być osoba prywatna lub spółka. Zarejestrowana w Krajowym Rejestrze Sądowym.

Przedsiębiorstwo (*ang. Business Entity*) – podmiot prowadzący działalność gospodarczą, który nie jest ani Organizacją Prywatną ani Podmiotem Państwowym. Przedsiębiorstwem mogą być na przykład: spółki, korporacje, osoby prowadzące indywidualną działalność gospodarczą etc.

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

Umowa Subskrybencka (*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.

Zamawiający (*ang. Applicant*) – Organizacja Prywatna, Podmiot Państwowy lub Przedsiębiorstwo, które ubiega się o wydanie certyfikatu EV SSL (lub jego odnowienie). Podmiot certyfikatu.EV SSL. Właściciel bądź wyłączny użytkownik nazwy domeny będącej przedmiotem certyfikatu EV SSL, który składa zamówienie na usługi certyfikacyjne CERTUM

Wnioskodawca (*ang. Certificate Requester*) – osoba fizyczna, którą może być pracownik zatrudniony przez Subskrybenta, autoryzowany przedstawiciel Subskrybenta lub strona trzecia (np. dostawca usługi internetu) upoważniona do złożenia podpisanego Wniosku o wydanie certyfikatu EV SSL do CERTUM.

Osoba Zatwierdzająca Certyfikat (*ang. Certificate Approver*) – osoba fizyczna, którą może być pracownik zatrudniony przez Subskrybenta lub autoryzowany przedstawiciel Subskrybenta (i) posiadający wyraźne pełnomocnictwo do występowania samemu jako Wnioskodawca oraz udzielania innym pracownikom Subskrybenta lub stronom trzecim takiego pełnomocnictwa, a także (ii) do zatwierdzania Wniosków składanych przez innych Wnioskodawców.

Osoba Podpisująca Umowę (*ang. Contract Signer*) – osoba fizyczna, którą może być pracownik zatrudniony przez Subskrybenta lub autoryzowany przedstawiciel Subskrybenta posiadający wyraźne pełnomocnictwo do reprezentowania Zamawiającego, w tym upoważnienie do podpisywania w jego imieniu Umów z Subskrybentem.

Podstawa Prawna (*ang. Legal Existence*) – Organizacja Prywatna lub Przedsiębiorstwo posiada Podstawę Prawną, jeśli zostało powołane w sposób prawomocny i nie zakończyło działalności, nie uległo rozwiązaniu etc.

Istnienie Fizyczne (Physical Existence) – ważny adres, pod którym Subskrybent prowadzi działalność.

Stan Działalności Handlowej, zdolność biznesowa (*ang. Operational Existence*) – zdolność finansowa Subskrybenta do prowadzenia działalności handlowej, weryfikowana tylko wówczas, gdy działalność Subskrybenta nie przekracza trzech lat.

Niezależne Potwierdzenie Zamawiającego (*ang. Independent Confirmation From Applicant*) – zdarzenia, poprzez które potwierdza się pewien konkretny fakt (np. że Subskrybent jest właścicielem domeny lub któraś z osób podpisujących dokumenty jest pracownikiem bądź upoważnionym reprezentantem Subskrybenta). Niezależne Potwierdzenie CERTUM otrzymuje od osoby zatrudnionej przez Subskrybenta. W niniejszych procedurach Niezależne Potwierdzenie występuje jako dokument równoważny Upoważnieniu.

Osoba Potwierdzająca (*ang. Confirming Person*) – osoba podpisująca się pod Niezależnym Potwierdzeniem Zamawiającego. Jest to osoba dysponująca ostateczną lub znaczącą władzą wykonawczą 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 CA może kontaktować się w celu zweryfikowania tożsamości Osoby Potwierdzającej z działem kadr (Human Resources Department) firmy lub organizacji Subskrybenta.

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

Opinia Prawna (*ang. Legal Opinion*) – pismo sporządzone przez stronę trzecią (notariusza) 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 Guidelines[1]

Subskrybent – Subskrybentem może być osoba prawna, 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. Subskrybent jest także właścicielem bądź wyłącznym użytkownikiem nazwy domeny będącej przedmiotem certyfikatu EV SSL, który składa zamówienie na usługi certyfikacyjne CERTUM.

Kwalifikowane Niezależne Źródło informacji (*ang. Qualified Independent Information Sources*) – regularnie aktualizowana, publicznie dostępna baza danych, ogólnie rozpoznawana jako niezawodne źródło informacji, którym może być komercyjna baza danych tylko, jeśli spełnia następujące warunki:

- informacje w niej zawarte zostały zweryfikowane także przez inne niezależne źródła informacji;

1 EV Certificate Guidelines, v1.1 Appendix D s. 65

- baza danych wyraźnie odróżnia informacje pozyskane we własnym zakresie od informacji otrzymanych od innych niezależnych źródeł informacji;
- dostawca, właściciel, zarządzający bazą informuje jak często ma miejsce aktualizacja danych;
- zmiany zachodzące w danych znajdują odzwierciedlenie w bazie nie później niż w przeciągu 12 miesięcy;
- dostawca, zarządzający bazą korzysta z wiarygodnych źródeł informacji nie związanych z podmiotem, którego dotyczą lub korzysta z wielu potwierdzających się wzajemnie źródeł.

Kwalifikowane Rządowe Źródło Informacji (*ang. Qualified Government Information Source*) – regularnie aktualizowana, publicznie dostępna baza danych stworzona w celu umożliwienia pozyskania dokładnej informacji, ogólnie rozpoznawana jako niezawodne jej źródło, które utrzymywane jest przez Podmiot Państwowy. Ten publikuje informacje obligatoryjnie zaś zgłoszenie i/lub publikacja danych nieprawdziwych jest karane w myśl KPK lub KPC.

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

Zamawiający Wysokiego Ryzyka (*ang. High Risk Applicant*) – Zamawiający, wobec którego istnieją uzasadnione obawy, że jest on szczególnie narażony na ataki ze strony oszustów internetowych. Z drugiej strony, choć EV Guidelines nie określa tego jednoznacznie, Zamawiający, wobec którego istnieją uzasadnione podejrzenia, że sam prowadzi nieuczciwą działalność także kwalifikuje się do grupy Wysokiego Ryzyka, jeśli rozumiemy przez to taką grupę podmiotów, które wymagają szczególnej uwagi, w tym podjęcia dodatkowych działań weryfikacyjnych.

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.

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.

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.