Polityka Certyfikacji i Kodeks Postepowania Certyfikacyjnego Niekwalifikowanych Usług EuroCert

Wersja 2

Zatwierdził
Prezes Zarządu
Łukasz Konikiewicz .....

Data zatwierdzenia 02.06.2020

EuroCert Sp. z o.o. „CENTRUM EUROCERT”
ul. Puławska 474
02-884 Warszawa
https://eurocert.pl

SPIS TREŚCI

1 Wstęp

1. Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług EuroCert (zwane dalej Polityką) określa ogólne zasady stosowane przez EuroCert Sp. z o.o. (zwaną dalej EuroCert) w trakcie świadczenia niekwalifikowanych usług zaufania. Niniejszy dokument pełni także rolę Polityki certyfikacji dla każdego z rodzajów niekwalifikowanych certyfikatów (zwanych dalej „certyfikatami").

2. Powyższe usługi świadczone są zgodnie z:
   a) Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. poz. 1579), zwaną dalej „Ustawą o usługach zaufania" oraz Rozporządzeniem Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania (Dz. U. poz. 1632),
   b) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) Nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz decyzjami wykonawczymi do niniejszego rozporządzenia, zwanym dalej „eIDAS".

3. Struktura Polityki została stworzona na podstawie zaleceń: *RFC 3647* "*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework*[1]".

1.1 Wprowadzenie

1. Polityka określa zasady świadczenia niekwalifikowanych usług zaufania, szczegóły ich realizacji, działania jakie są realizowane przez urząd certyfikacji, punkty rejestracji oraz subskrybentów i strony ufające. Wydawanie certyfikatów zgodnie z niniejszą Polityką odbywa się niezależnie od świadczenia kwalifikowanych usług zaufania.

2. EuroCert jest kwalifikowanym dostawcą usług zaufania, w myśl Ustawy o usługach zaufania i eIDAS, wpisanym do rejestru kwalifikowanych dostawców usług zaufania pod numerem 13.

3. EuroCert świadczy niekwalifikowane usługi zaufania w zakresie wydawania certyfikatów, w ramach których dokonuje następujących czynności:
   a) rejestruje subskrybentów,
   b) generuje klucze i certyfikaty,
   c) dostarcza informacje o statusie certyfikatu w oparciu o listy CRL,
   d) unieważnia lub zawiesza certyfikaty.

4. Wydawanie certyfikatów przez EuroCert odbywa się za pośrednictwem głównego urzędu certyfikacji EUROCERT COMMERCIAL, który wydaje certyfikaty dla samego siebie (tzw. certyfikat samopodpisany) oraz certyfikaty dla subskrybentów służące do realizacji usług informatycznych wymagających podpisu lub pieczęci elektronicznej, uwierzytelnienia lub szyfrowania

5. Certyfikaty wydawane zgodnie z niniejszą Polityką zawierają jej identyfikator, który umożliwia stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Identyfikator ten umieszczany jest w rozszerzeniu *CertificatePolicies* (patrz pkt 7.1.2) każdego certyfikatu.

[1] https://www.ietf.org/rfc/rfc3647.txt

1.2 Identyfikator i nazwa dokumentu

1. Polityce przypisuje się następujący zarejestrowany identyfikator obiektu (ang. Object Identifier – OID): 1.2.616.1.113791.2.1.
2. Wszystkie wersje Polityki są dostępne w postaci elektronicznej na stronie internetowej https://www.eurocert.pl/repozytorium.

1.3 Elementy infrastruktury PKI

1. Infrastruktura EuroCert służąca do świadczenia niekwalifikowanych usług zaufania składa się z następujących elementów:
   a) główny urząd certyfikacji: EUROCERT COMMERCIAL,
   b) punkty rejestracji, notariusze i inne osoby potwierdzające tożsamość subskrybentów,
   c) zamawiający,
   d) subskrybenci,
   e) strony ufające.

1.3.1 EUROCERT COMMERCIAL

1. Urząd certyfikacji – EUROCERT ROOT – jest głównym urzędem certyfikacji, który wydaje certyfikaty dla samego siebie (tzw. certyfikat samopodpisany) oraz subskrybentów oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów.

1.3.2 Punkty Rejestracji

1. Realizując swoje zadania, EuroCert może działać samodzielnie lub za pośrednictwem punktów rejestracji. Punktami rejestracji mogą osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, po podpisaniu stosownej umowy z EuroCert o współpracy w zakresie świadczenia usług zaufania. Podległe EuroCert punkty rejestracji nie mogą akredytować innych punktów rejestracji ani przyjmować i realizować wniosków o unieważnienie lub zawieszenie certyfikatu – leży to w wyłącznej gestii EuroCert.
2. Punkty rejestracji reprezentują urząd certyfikacji w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez urząd certyfikacji uprawnień w zakresie:
   a) przyjmowania wniosków o wydanie certyfikatu,
   b) potwierdzania tożsamości subskrybentów,
   c) podpisywania umów z subskrybentami,
   d) tworzenia zgłoszeń certyfikacyjnych,
   e) generowania kluczy i certyfikatów subskrybentom,
   f) przekazywania certyfikatów subskrybentom,
   g) udzielania informacji o warunkach korzystania z usługa zaufania, w tym o skutkach jakie wywołują,
   h) sprzedaży usług zaufania EuroCert.
3. Szczegółowy zakres obowiązków punktów rejestracji określany jest przez umowę pomiędzy EuroCert a danym punktem rejestracji.
4. Kompetencje punktów rejestracji nie mogą obejmować w szczególności posługiwania się kluczem prywatnym służącym do generowania certyfikatów i list CRL.

5. Lista aktualnych autoryzowanych punktów rejestracji dostępna jest na stronie internetowej https://sklep.eurocert.pl/pl/i/Mapa-Punktow-Partnerskich/14. Żaden z tych punktów nie jest jednostką organizacyjną EuroCert.

1.3.3 Subskrybenci

1. Subskrybentem może być każda osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej której dane zostaną umieszczone w polu *podmiot* (ang. subject) certyfikatu i która sama dalej nie wydaje certyfikatów innym podmiotom.
2. W przypadku certyfikatów wydawanych innym podmiotom niż osoba fizyczna czynności przewidziane w Polityce dla subskrybenta, w tym potwierdzenie odbioru certyfikatu, potwierdzenie posiadania klucza prywatnego, akceptację treści certyfikatu, ustalenie kodów PIN i PUK lub haseł do żądania unieważniania i zawieszenia certyfikatu, wykonuje osoba upoważniona przez zamawiającego. Na osobie tej ciążą także obowiązki związane z ochroną klucza prywatnego.

1.3.4 Strony ufające

1. Strona ufająca jest podmiotem, który posługuje się certyfikatem innego podmiotu w celu zweryfikowania jego podpisu elektronicznego.
2. Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta (patrz pkt 4.5.2). Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego. Informacje zawarte w certyfikacie (m.in. *CertificatePolicies*, *KeyUsage*) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.3.5 Zamawiający

1. Osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej lub organ władzy publicznej, którego dane zostały umieszczone w certyfikacie, w imieniu której działa subskrybent posługując się certyfikatem. Sponsor certyfikatu finansuje usługi certyfikacyjne świadczone na rzecz danego subskrybenta. Ma on prawo unieważnić certyfikat jeśli jego dane znajdują się w certyfikacie.

1.4 Zakres stosowania certyfikatów

1. Certyfikaty wydane zgodnie z Polityką mogą być używane do zapewnienia usług integralności, identyfikacji, poufności i niezaprzeczalności nadania danych (ang. nonRepudiation).

Tab. 1. Rodzaje certyfikatów i ich zastosowanie

Certyfikat	Zalecane obszary zastosowań
Standard	Ochrona informacji przesyłanych drogą elektroniczną, głównie pocztą e-mail, autoryzacja dostępu do systemów, uwierzytelnianie klienta w połączeniach SSL, podpisywanie i szyfrowanie danych w postaci elektronicznej oraz uwierzytelnianie subskrybentów.
Testowy	Testowanie współpracy certyfikatu z rozwiązaniami wykorzystywanymi lub tworzonymi przez zamawiających lub subskrybenta. Certyfikaty te nie zapewniają żadnej gwarancji co do identyfikacji subskrybenta posługującego się takim certyfikatem.

2. Przed wydaniem certyfikatów o których mowa w tab. 1 subskrybent musi zaakceptować postanowienia niniejszej Polityki, a następnie podpisać umowę z EuroCert o świadczenie usług zaufania.

3. W szczególnych przypadkach (wydzielony projekt) dopuszcza się wydawanie certyfikatu bez zawarcia umów z poszczególnymi subskrybentami. Warunkiem jest zawarcie Umowy głównej, której zapis przenosi pełną odpowiedzialność za: weryfikację tożsamości osób odbierających certyfikat, poprawność danych zawartych w certyfikatach oraz prawidłowość procesu wydania certyfikatu, na zamawiającego.

1.4.1 Dozwolone obszary użycia certyfikatów

1. Certyfikaty kluczy weryfikujących podpisy, wydawane zgodnie z Polityką stanowią certyfikaty niekwalifikowane podpisów elektronicznych. Podpis elektroniczny weryfikowany przy pomocy tych certyfikatów nie wywołuje skutków prawnych równorzędnych podpisowi własnoręcznemu.

2. Certyfikaty mogą zawierać dane i służyć do identyfikacji innych podmiotów niż osoby fizyczne.

3. Certyfikaty powinny być używane w aplikacjach odpowiednio do tego przystosowanych, spełniających przynajmniej niżej określone wymagania:
   a) właściwe zabezpieczenie kodu źródłowego i praca w bezpiecznym środowisku operacyjnym,
   b) prawidłowa obsługa algorytmów kryptograficznych, funkcji skrótu,
   c) odpowiednie zarządzanie certyfikatami, kluczami publicznymi i prywatnymi,
   d) weryfikacja statusów i ważności certyfikatów,
   e) właściwy sposób informowania użytkownika o stanie aplikacji, statusie certyfikatów, weryfikacji podpisów elektronicznych/pieczęci elektronicznych.

1.4.2 Zakazane obszary użycia certyfikatów

1. Certyfikatów nie wolno używać niezgodnie z przeznaczeniem oraz bez przestrzegania ewentualnych ograniczeń zastosowania danego certyfikatu zapisanych w certyfikacie.
2. Zakazane jest również używanie certyfikatów przez osoby do tego nieupoważnione.

1.5 Zarządzanie dokumentem

1. Każda zmiana Polityki, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymaga utworzenia nowej wersji i zatwierdzenia jej przez Zarząd EuroCert. Nowa wersja wskazuje nowy kolejny numer wersji oraz datę zatwierdzenia.
2. Polityka jest publikowana w repozytorium (patrz pkt 2) niezwłocznie po zatwierdzeniu otrzymując status obowiązująca.
3. Każda z wersji Polityki jest aktualna do czasu zatwierdzenia i opublikowania ze statusem obowiązująca kolejnej wersji.
4. Subskrybenci oraz pozostałe zainteresowane strony (wymienione w pkt 1.3) zobowiązani są stosować się wyłącznie do aktualnie obowiązującej Polityki.

1.5.1 Odpowiedzialność za zarządzanie dokumentem

1. Podmiotem odpowiedzialnym za zarządzanie Polityką (w tym zatwierdzania zmian itd.), jest EuroCert Sp. z o.o.

1.5.2 Dane kontaktowe

1. Wszelkie pytania dotyczące usług i działalności EuroCert należy kierować na poniższy adres:

EuroCert Sp. z o.o.
Centrum EuroCert
ul. Puławska 474
02-884 Warszawa
+48 22 490 36 45
biuro@eurocert.pl

1.5.3 Odpowiedzialność za aktualność zasad określonych w Polityce

1. Za ocenę aktualności i przydatności niniejszego dokumentu oraz innych dokumentów dotyczących usług zaufania świadczonych przez EuroCert, a także za zgodność między wymienionymi dokumentami, odpowiada kadra wykwalifikowanych pracowników EuroCert (patrz pkt 5.2.1) oraz Zarząd EuroCert.

1.5.4 Procedury zatwierdzania dokumentu

1. Polityka jest zatwierdzana przez Zarząd EuroCert i otrzymuje status *zatwierdzona*.
2. Opublikowanie Polityki w repozytorium ze statusem obowiązująca następuje niezwłocznie po zatwierdzeniu.

1.6 Słownik używanych terminów, skrótów i skrótowców

1. Terminy , skróty i skrótowce wykorzystywane w Polityce, a niezdefiniowane poniżej należy interpretować zgodnie z definicjami zawartymi w Ustawie o usługach zaufania i eIDAS.

Tab. 2. Terminy, skróty i skrótowce używane w Polityce

Termin/akronim	Opis
Urząd certyfikacji	EuroCert Commercial
Punkt Rejestracji	jednostka organizacyjna działająca w imieniu EuroCert Sp. z o.o., wykonująca zgodnie z niniejszą Polityką niektóre funkcje związane ze świadczeniem usług zaufania.
DN	Identyfikator DN – Distinguished Name – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500.
CRL	Lista unieważnionych certyfikatów (Certificate Revocation List).
PKI	Public Key Infrastructure – infrastruktura klucza publicznego – system obejmujący Centra Certyfikacji Kluczy, Punkty Rejestracji oraz użytkowników końcowych, służący do dystrybucji certyfikatów klucza publicznego oraz zapewnienia możliwości ich wiarygodnej weryfikacji.
HSM	Hardware Security Module – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego do generowania podpisów/pieczęci elektronicznych (np. przy wystawianiu certyfikatów, list CRL).
Klucz prywatny	Dane służące do składania podpisu elektronicznego.
Klucz publiczny	Dane służące do weryfikacji podpisu elektronicznego, zazwyczaj dystrybuowane w postaci certyfikatu.
Ustawa o usługach zaufania	Ustawy o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. poz. 1579).
eIDAS	Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r., w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.
Ustawa o ochronie danych osobowych	ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)
Zgłoszenie certyfikacyjne	plik w formacie PKCS#10 zawierający między innymi nazwę wyróżniającą Subskrybenta oraz dane służące do walidacji.

2 Odpowiedzialność za publikację i repozytorium

2.1 Repozytorium

1. Repozytorium EuroCert znajduje się na stronie internetowej: https://eurocert.pl/repozytorium.
2. Repozytorium dostępne jest 24 godziny na dobę, przez 7 dni w tygodniu. Maksymalny czas niedostępności repozytorium nie może przekroczyć 1 godziny.

2.2 Informacje publikowane w repozytorium

1. W repozytorium publikowane są między innymi następujące informacje:
   a) aktualne certyfikaty głównego urzędu certyfikacji EUROCERT COMMERCIAL,
   b) aktualną listę CRL dla certyfikatów wydanych przez EUROCERT COMMERCIAL,
   c) wszystkie wersje niniejszego dokumentu,
   d) wzory umów i zamówień,
   e) opisy procedur uzyskiwania, odnawiania, zawieszania i unieważniania certyfikatów,
   f) raporty z audytów przeprowadzonych przez zewnętrzne instytucje.
2. EuroCert nie publikuje certyfikatów subskrybentów.

2.3 Częstotliwość publikowania

1. Częstotliwość publikowania poszczególnych dokumentów i danych przedstawia poniższa tabela.

Tab. 3. Częstotliwość publikacji dokumentów w repozytorium

Rodzaj dokumentu	Częstotliwość publikacji
Certyfikaty urzędów certyfikacji	Każdorazowo i niezwłocznie, gdy zostaną wygenerowane
Listy CRL	Dla EuroCert COMMERCIAL – nie rzadziej niż co 8 dni lub w ciągu 24 godzin od żądania zawieszenia lub unieważnienia certyfikatu.
Polityka Certyfikacji i Kodeks Postepowania Certyfikacyjnego Niekwalifikowanych Usług EuroCert	Zgodnie z pkt 1.5 oraz 9.10 i 9.12
raporty z audytów przeprowadzonych przez zewnętrzne instytucje	Każdorazowo po przejściu audytu i otrzymaniu raportu
Pozostałe informacje	Każdorazowo po zmianie lub uaktualnieniu

2.4 Kontrola dostępu do repozytorium

1. Wszystkie informacje publikowane w repozytorium są publicznie dostępne. Informacje te są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem oraz są przechowywane z zachowaniem kopii zapasowych.

3 Identyfikacja i uwierzytelnianie

1. Niniejszy rozdział przedstawia zasady weryfikacji tożsamości potencjalnych subskrybentów przy wydawaniu, zawieszaniu lub unieważnianiu certyfikatów.
2. Zasady te zawierają środki które należy przedsięwziąć w celu uzyskania pewności, że informacje przekazane przez potencjalnego subskrybenta we wniosku o wydanie certyfikatu są dokładne i wiarygodne w momencie wydania certyfikatu.
3. Wiarygodność certyfikatu zależy od przyjętej procedury weryfikacji tożsamości subskrybenta i wysiłku włożonego przez EuroCert w sprawdzenie danych przesłanych przez subskrybenta we wniosku rejestracyjnym. Im więcej informacji należy zweryfikować, a więc im bardziej procedura ta jest złożona, tym bardziej wiarygodny jest certyfikat.

3.1 Nazewnictwo używane w certyfikatach

1. Identyfikacja każdego subskrybenta odbywa się w oparciu o dane umieszczone w polu identyfikatora podmiotu (tj. pole *subject*). Dane te tworzą łącznie nazwę wyróżniającą (ang. Distinguished Name – DN), zgodnie z tabelą w pkt 3.1.2.

3.1.1 Rodzaje nazw

1. Profil nazwy DN subskrybenta oraz wystawcy certyfikatu jest zgodny z normą: ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part: 1,2,5 oraz zaleceniami ITU z serii X.500.

3.1.2 Konieczność używania nazw znaczących

1. Nazwa subskrybenta jest tworzona w oparciu o podzbiór poniższych atrybutów (tab. 4).

Tab. 4. Profil nazwy subskrybenta

Pole	Znaczenie
C	międzynarodowy dwuliterowy skrót nazwy kraju (dla Polski – PL)
G	imię (imiona) subskrybenta
S	nazwisko subskrybenta plus ewentualnie nazwisko rodowe
SN	numer paszportu, numer dowodu osobistego, PESEL, NIP, numer identyfikacji podatkowej subskrybenta lub lokalny identyfikator subskrybenta specyficzny dla danego kraju notyfikowany i rozpoznawalny na poziomie Unii Europejskiej
O	nazwa organizacji, w której pracuje subskrybent lub ją reprezentuje
T	nazwa stanowiska pracy pełnionego przez subskrybenta w danej organizacji
ST	województwo
L	miejscowość
A	adres pocztowy
mailAddress	adres poczty elektronicznej (e-mail)

2. Subskrybent może posiadać dowolną liczbę certyfikatów zawierających ten sam identyfikator DN.
3. W przypadku subskrybenta identyfikującego się numerem PESEL atrybut Numer seryjny występuje w formacie „PNOPL-XXXXXXXXXX” zgodnie z normą ETSI EN 319 412-2.

4. Dane adresowe (województwo, miejscowość, adres pocztowy) podmiotu, którego nazwa widnieje w atrybucie O (*Organizacja)* są zgodne z wpisem w odpowiednim rejestrze, ewidencji, statucie lub innym dokumencie tego typu odpowiednim dla rodzaju podmiotu i powinny być w takiej postaci, w jakiej są umieszczane na przesyłkach.

3.1.3 Anonimowość subskrybentów

1. EuroCert nie wystawia certyfikatów zapewniających anonimowość.

3.1.4 Zasady interpretacji różnych form nazw

1. Interpretacja nazw pól umieszczanych przez EuroCert w wydawanych przez siebie certyfikatach jest zgodna z profilem certyfikatów opisanym w ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part: 1,2,5.

3.1.5 Unikalność nazw

1. EuroCert gwarantuje unikalność identyfikatora DN, przydzielonego podmiotowi certyfikatu. Każdy wydany certyfikat posiada unikalny w ramach urzędu certyfikacji numer seryjny. Łącznie z identyfikatorem DN subskrybenta gwarantuje jednoznaczną identyfikację certyfikatu.

3.1.6 Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

1. Identyfikator DN powinien zawierać wyłącznie nazwy, do których subskrybent ma prawo.
2. EuroCert nie sprawdza prawa do posługiwania się zastrzeżonymi znakami towarowymi, nie odpowiada za nieuprawnione wykorzystywanie znaków towarowych i nie jest stroną w przypadku tego typu sporów.
3. W przypadku utraty przez subskrybenta prawa do posługiwania się daną nazwą lub innym oznaczeniem zamieszczonym w certyfikacie, jest on zobowiązany do zgłoszenia tego faktu celem unieważnienia certyfikatu z powodu nieaktualności danych zawartych w certyfikacie.

3.2 Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu

1. Procedura weryfikacji tożsamości potencjalnego subskrybenta przeprowadzana jest przez operatora punktu rejestracji, inspektora rejestracji, notariusza lub inną osobę weryfikującą tożsamość. Polega ona na szczegółowej weryfikacji wniosku oraz dokumentów okazanych przez subskrybenta oraz opcjonalnie na zweryfikowaniu poprawności nazwy DN.
2. Potencjalny subskrybent, obok podania danych będących treścią nazwy wyróżniającej certyfikatu (patrz pkt 3.1.2), jest zobowiązany udzielić dodatkowych informacji pozwalających na jego identyfikację, w tym:
   a) cechy dokumentu tożsamości,
   b) datę i miejsce urodzenia,
   c) dane kontaktowe.
3. Potwierdzenie tych danych w sytuacji, gdy potencjalny subskrybent nie posiada ważnego certyfikatu kwalifikowanego wydanego przez kwalifikowanego dostawcę usług zaufania następuje przez jego fizyczną obecność w punkcie rejestracji lub osobisty kontakt operatora punktu rejestracji z potencjalnym subskrybentem w innym miejscu.

4. EuroCert może również stwierdzić tożsamość osoby ubiegającej się o certyfikat bez jej osobistego stawiennictwa w punkcie rejestracji, na podstawie notarialnego potwierdzenia tożsamości.

5. EuroCert dopuszcza dla wybranych typów certyfikatów, aby wnioski o ich wydanie mogły być przesyłane za pośrednictwem zwykłej poczty, poczty elektronicznej, witryny stron typu WWW itp., zaś ich rozpatrywanie nie wymaga fizycznego kontaktu z wnioskodawcą.

3.2.1 Udowodnienie posiadania klucza prywatnego

Nie dotyczy.

3.2.2 Identyfikacja i uwierzytelnianie osób prawnych

1. W przypadku gdy certyfikat ma zawierać dane dotyczące zamawiającego (podmiotu niebędącego osobą fizyczną), takie jak nazwa organizacji i jej adres, EuroCert przed wydaniem certyfikatu sprawdza na podstawie informacji pozyskanych z legalnych, wiarygodnych, publicznie dostępnych źródeł, w tym dostępnych rejestrów prowadzonych przez organy publiczne, czy taki podmiot istnieje, czy dane wskazane przez zamawiającego są zgodne z danymi prezentowanymi w wykorzystywanym rejestrze oraz czy osoby występujące w imieniu zamawiającego są do tego upoważnione. Adres organizacji może być również zweryfikowany w trakcie wizyty upoważnionej przez EuroCert osoby fizycznej zajmującej się weryfikacją tożsamości subskrybentów i/ lub przyjmowaniem wniosków o wydanie certyfikatu, zwanej dalej Operatorem Punktu Rejestracji, w siedzibie zamawiającego.

2. W przypadku, gdy certyfikat ma służyć do zabezpieczania poczty elektronicznej przeprowadzana jest weryfikacja adresu poczty elektronicznej. Weryfikacja polega na sprawdzeniu, czy adres poczty elektronicznej wskazany w zamówieniu należy do subskrybenta. Sprawdzenie może się odbywać poprzez potwierdzenie odebrania przez subskrybenta danych uwierzytelniających wysłanych na adres poczty elektronicznej podany w zamówieniu. Sprawdzenie ma na celu ustalenie, że adres pocztowy jest legalnie wykorzystywany przez subskrybenta.

3.2.3 Identyfikacja i uwierzytelnianie osób fizycznych

1. EuroCert weryfikuje tożsamość i, w stosownym przypadku, wszelkie specjalne atrybuty osoby fizycznej, prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej, której wydaje kwalifikowany certyfikat:

   a) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej; lub

   b) zdalnie, przy użyciu środka identyfikacji elektronicznej, w przypadku którego przed wydaniem kwalifikowanego certyfikatu zapewniono fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej i który spełnia wymogi określone w art. 8 eIDAS w odniesieniu do średniego lub wysokiego poziomu bezpieczeństwa; lub

   c) zdalnie, przy użyciu wideo-weryfikacji; lub

   d) za pomocą certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a), b) lub c) powyżej.

2. W procesie potwierdzania tożsamości, EuroCert może również korzystać z notarialnego potwierdzenia tożsamości.

3. Weryfikacja tożsamości osób fizycznych dokonywana jest na podstawie ważnego dowodu osobistego lub paszportu.

4. W przypadku użycia systemu wideo weryfikacji (lit. c powyżej), Subskrybent składa wniosek o certyfikat wyłącznie poprzez elektroniczny formularz. Przed inicjacją sesji wideo z operatorem weryfikującym tożsamość Subskrybent jest zobowiązany zapoznać się z postanowieniami niniejszej Polityki i zaakceptować je.

5. Wideo weryfikacja odbywa się poprzez wideokonferencję. Polega ona na obecności osoby fizycznej w tej samej sesji wideo co operator weryfikujący tożsamość. Wideokonferencja zastępuje osobistą (fizyczną) obecność osoby podlegającej weryfikacji. Jest rejestrowana w celach dowodowych.

6. System ten dla osób fizycznych zapewnia pewność równoważną, pod względem wiarygodności, fizycznej obecności zgodnie z art. 24.1 lit. d rozporządzenia eIDAS. Równoważna pewność została potwierdzona przez jednostkę oceniającą zgodność.

7. Operator przeprowadza wideo weryfikację na podstawie okazanego elektronicznie dokumentu tożsamości.

8. Operator weryfikuje ważność i autentyczność dokumentu tożsamości wnioskodawcy oraz sprawdza czy dane na dokumencie odpowiadają tym wprowadzonym w elektronicznym wniosku o certyfikat.

9. Powyższy proces weryfikacji przeprowadzany jest ponownie przez drugiego operatora.

10. Weryfikacja kończy się powodzeniem tylko wtedy gdy obaj potwierdzą tożsamość pozytywnie.

11. Jeżeli weryfikacja tożsamości zakończy się powodzeniem Punkt Rejestracji udostępnia EuroCert dane z procesu weryfikacji tożsamości oraz przesyła Żądanie Certyfikacyjne (pkcs#10).

12. Żądania certyfikacyjne przekazywane są do EuroCert, do systemu CA, w postaci elektronicznej. Poufność transmisji zgłoszeń certyfikacyjnych jest zapewniona poprzez zestawienie szyfrowanego kanału w protokole TLS.

13. EuroCert automatycznie pobiera dane z procesu weryfikacji tożsamości, które zostały udostępnione EuroCert przez Punkt Rejestracji.

14. EuroCert weryfikuje, czy Żądanie Certyfikacyjne pochodzi z zaufanego Punktu Rejestracji poprzez uwierzytelnienie kanału komunikacyjnego.

15. Żądanie Certyfikacyjne zostaje opatrzone podpisem elektronicznym Inspektora ds. Rejestracji, który je zatwierdził.

16. EuroCert generuje klucze Subskrybenta i Certyfikat; kluczem prywatnym zarządza EuroCert w imieniu Subskrybenta, przy czym Subskrybent ma wyłączną kontrolę nad nim; autoryzacja dostępu do klucza prywatnego odbywa się z wykorzystaniem loginu i hasła oraz OTP.

17. EuroCert przekazuje Subskrybentowi informacje zwrotne z danymi uwierzytelniającymi i autoryzacyjnymi.

18. Punkt Rejestracji udostępnia EuroCert wszystkie dane, zawierające potwierdzenie tożsamości Subskrybenta, które EuroCert może pobrać w terminie 7 dni, po upływie tego czasu dane zostają usunięte przez Punkt Rejestracji.

19. Podczas wymiany danych elektronicznie pomiędzy Punktem Rejestracji do EuroCert zapewniony jest odpowiedni poziom ochrony tych danych, zapewniający poufność danych (poprzez szyfrowanie) oraz autentyczność i integralność (poprzez zastosowanie elektronicznego podpisu),

20. Przed wydaniem certyfikatu Subskrybent zobowiązuje się do zapoznania się z niniejszą Polityką.

21. Subskrybent jest zobowiązany potwierdzić zapoznanie się z Polityką poprzez zaakceptowanie tej Polityki.

22. W przypadku gdy w certyfikacie dla osoby fizycznej ma zostać umieszczony adres poczty elektronicznej, wówczas sprawdzenie podanego na zamówieniu adresu odbywa się analogicznie jak w pkt 3.2.2.

23. W szczególnych przypadkach (wydzielony projekt) dopuszcza się wydawanie certyfikatu bez zawarcia umów z poszczególnymi subskrybentami. Warunkiem jest zawarcie Umowy głównej, której zapis przenosi pełną odpowiedzialność na zamawiającego za:
    a) weryfikację tożsamości osób odbierających certyfikat,
    b) poprawność danych zawartych w certyfikatach,
    c) prawidłowość procesu wydania certyfikatu.

3.2.4 Dane subskrybenta niepodlegające weryfikacji

Patrz pkt 3.1.6.

3.2.5 Sprawdzanie praw do otrzymania certyfikatu

1. Przed przekazaniem certyfikatu subskrybentowi lub osobie upoważnionej do otrzymania certyfikatu EuroCert sprawdza tożsamość tej osoby na podstawie okazanego przez nią dokumentu tożsamości, a w przypadku certyfikatu testowego na podstawie przekazanych danych, takich jak imię, nazwisko oraz numer i seria dokumentu tożsamości.

3.2.6 Kryteria interoperacyjności

Nie dotyczy.

3.3 Identyfikacja i uwierzytelnianie przy wydawaniu kolejnego certyfikatu

1. Weryfikacja danych, które mają być umieszczone w nowym certyfikacie, przebiega zgodnie z opisem w pkt 3.2 lub pkt 3.3.1 lub za pomocą certyfikatu kwalifikowanego podpisu elektronicznego, zgodnie z art. 24 ust. 1 lit. c) eIDAS.

3.3.1 Wydawanie kolejnego certyfikatu w okresie ważności obecnego certyfikatu

1. Weryfikacja danych, które mają być umieszczone w certyfikacie, przebiega zgodnie z opisem w pkt 3.2.2 i 3.2.3. Uwierzytelnienie subskrybenta może być także zrealizowane w oparciu o informacje zawarte w bazach danych EuroCert i polega na zweryfikowaniu podpisu elektronicznego złożonego pod wnioskiem o certyfikat oraz potwierdzeniu autentyczności związanego z podpisem certyfikatu (w oparciu o tzw. ścieżkę certyfikacji).

3.3.2 Wydanie kolejnego certyfikatu po wygaśnięciu/unieważnieniu obecnego certyfikatu

1. W przypadku, gdy dotychczasowy certyfikat uległ przeterminowaniu lub unieważnieniu oraz w przypadku zmiany jakichkolwiek danych identyfikacyjnych zawartych w certyfikacie należy postępować według zasad przewidzianych dla wydawania pierwszego certyfikatu (patrz pkt 3.2).

3.4 Identyfikacja i uwierzytelnianie przy unieważnianiu certyfikatu

1. Unieważnienie certyfikatu może nastąpić:
   a) na wniosek subskrybenta,
   b) na wniosek zamawiającego (organizacji reprezentowanej przez subskrybenta), którego dane zostały zawarte w certyfikacie,
   c) na wniosek osoby reprezentującej zamawiającego (subskrybenta nie będącego osobą fizyczną),
   d) z inicjatywy EuroCert.
2. Unieważnienia certyfikatu można dokonać w następujący sposób:
   a) osobiście w EuroCert (adres podano w pkt 1.5.2), w godzinach pracy tj. od 9.00 do 17.00, po potwierdzeniu tożsamości osoby występującej o unieważnienie przez Inspektora rejestracji na zasadach opisanych w pkt 3.2,
   b) telefonicznie (numer infolinii: 22 490 49 86), w ciągu całej doby, na podstawie danych osobowych podanych przy wydawaniu certyfikatu oraz numeru seryjnego certyfikatu,
   c) drogą elektroniczną pod adresem uniewaznienia@eurocert.pl podając dane osobowe podane podczas wydawania certyfikat wraz z danymi kontaktowymi oraz numeru seryjnego certyfikatu.
3. W przypadku opisanym w p. 2 lit. c Inspektor rejestracji dzwoni pod wskazany we wniosku numer telefonu, sprawdza dane z certyfikatu i weryfikuje z danymi we wniosku o unieważnienie.

4. W przypadku niezgodności weryfikowanych danych certyfikat zostaje zawieszony do czasu wyjaśnienia powstałych niezgodności lub wniosek o unieważnienie zostaje odrzucony.
5. Identyfikacja i uwierzytelnienie podmiotu trzeciego, którego dane zawarte są w certyfikacie przebiega na zasadach opisanych w pkt 3.2. Podstawą przyjęcia wniosku w tym przypadku jest pozytywna weryfikacja prawa podmiotu trzeciego do występowania o unieważnienie certyfikatu.
6. Warunki zawieszenia, uchylenia zawieszenia oraz unieważnienia certyfikatu w szczególności na wniosek zamawiającego lub subskrybenta określone zostały w pkt 4.9.

4 Wymagania funkcjonalne

1. Podstawą do składania zamówień na certyfikaty i ich wydawania przez EuroCert jest zawarcie Umowy o świadczenie usług zaufania. Umowa może zostać zawarta z osobą fizyczną, osobą prawną lub jednostką organizacyjną nieposiadającą osobowości prawnej. Na podstawie Umowy zamawiający wskazuje subskrybentów, dla których zamawia certyfikaty lub którzy będą odpowiedzialni za odbiór certyfikatów.
2. Zawarcie Umowy nie jest wymagane w przypadku certyfikatów testowych.

4.1 Wniosek o certyfikat

1. Wniosek o wydanie certyfikatu składany jest w EuroCert w formie zamówienia. Może być złożony przez dedykowany formularz zamówienia dostępny na stronie internetowej EuroCert. Wnioskodawca oświadcza we wniosku, że wszystkie przedstawione przez niego dane niezbędne do wydania certyfikatu są prawdziwe oraz oświadcza, że zapoznał się z dokumentami (w tym z niniejszą Polityką) określającymi warunki użycia certyfikatu, zawierającym między innymi:
   a) sposoby rozstrzygania skarg i sporów,
   b) zakres i ograniczenia stosowania certyfikatów,
   c) skutki prawne składania podpisów elektronicznych weryfikowanych przy użyciu certyfikatów,
   d) informację o systemie dobrowolnej rejestracji dostawców usług zaufania i ich znaczeniu.

4.1.1 Kto składa wniosek o certyfikat

1. O wydanie certyfikatu mogą się ubiegać osoby fizyczne , prawne i jednostki organizacyjne nieposiadające osobowości prawnej. Wnioski, czyli zamówienia mogą składać w EuroCert osoby uprawnione do reprezentowania subskrybenta lub pełnomocnicy wskazani w umowie lub odrębnych pełnomocnictwach.

4.1.2 Rejestracja wniosku

1. Rejestracji wniosków dokonują operatorzy punktów rejestracji lub są one automatycznie rejestrowane w przypadku gdy zostały złożone drogą elektroniczną. Rejestracja wniosków w formie papierowej polega na wprowadzeniu danych wnioskodawcy, po uprzedniej weryfikacji (metodami opisanymi w pkt 3.2 lub pkt 3.3) do systemu EuroCert.

4.2 Przetwarzanie wniosku

1. Po otrzymaniu zamówienia na certyfikat EuroCert przystępuje do weryfikacji danych zawartych we wniosku, a następnie – w przypadku pomyślnej weryfikacji – do rejestracji lub zatwierdzenia wniosku w systemie i wygenerowania certyfikatu.

2. Wnioski (zamówienia) prawidłowo wypełnione z danymi uwierzytelnionymi w sposób opisany w rozdziale 3 są przyjmowane do realizacji. Operator, który dokonuje weryfikacji wniosku, musi dokonać następujących czynności:
   a) przypisać wniosek do odpowiedniej umowy o świadczenie usług zaufania,
   b) sprawdzić uprawnienia do składania zamówień osoby, która podpisała wniosek o certyfikat,
   c) zweryfikować dane wprowadzone do systemu obsługi klienta prowadzonego przez EuroCert podczas rejestracji wniosku z danymi dostępnymi w bazach EuroCert lub innych dostępnych mu bazach,
   d) dokonać porównania danych wpisanych do wniosku z danymi wynikającymi z dostarczonych dokumentów.

3. Część z wyżej opisanych czynności może zostać dokonana automatycznie.

4. Jeśli sprawdzenie przebiegło pozytywnie i wszystkie dane zawarte we wniosku zostaną zweryfikowane prawidłowo, Operator rozpoczyna realizację wniosku i generowanie certyfikatu.

4.2.1 Wykonywanie funkcji identyfikacji i uwierzytelniania

1. Operator punktu rejestracji dokonuje uwierzytelnienia potencjalnego subskrybenta na podstawie danych zawartych we wniosku oraz dokumentów dołączonych do wniosku, niezbędnych do jednoznacznej identyfikacji wnioskodawcy, zgodnie z postanowieniami pkt 3.2 lub pkt 3.3. Następnie generuje zgłoszenie certyfikacyjne, zawierające wszystkie dane niezbędne do wystawienia certyfikatu, zgodnie z profilem certyfikatu zawartym w pkt 7.1.

4.2.2 Przyjęcie/odrzucenie wniosku

1. Wniosek o wydanie certyfikatu może zostać odrzucony, w przypadku gdy:
   a) nazwa subskrybenta (DN) ubiegającego się o wydanie certyfikatu pokrywa się z nazwą innego subskrybenta,
   b) istnieje uzasadnione podejrzenie, że subskrybent sfałszował lub podał nieprawdziwe dane we wniosku,
   c) wnioskodawca nie dostarczył kompletu wymaganych dokumentów,
   d) z innych ważnych nie wymienionych powyżej przyczyn, po uprzednim uzgodnieniu odmowy z Inspektorem bezpieczeństwa.

2. EuroCert może odmówić wydania certyfikatu dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą wskutek poniesionych przez wnioskodawcę (w wyniku odmowy) strat lub kosztów. EuroCert zwraca w takim przypadku wnioskodawcy wniesioną przez niego opłatę za wydanie certyfikatu (jeśli dokonał stosownej przedpłaty), chyba że wnioskodawca we wniosku o wydanie certyfikatu umieścił sfałszowane lub nieprawdziwe dane.

3. Informacja o odmowie wydania certyfikatu przesyłana jest wnioskodawcy w postaci odpowiedniej decyzji z uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do EuroCert w terminie 14 dni od daty otrzymania decyzji.

4.2.3 Okres oczekiwania na przetworzenie wniosku

1. Jeśli nie wystąpią przyczyny niezależne od EuroCert, czas przetwarzania wniosków o certyfikat nie powinien przekroczyć 7 dni od momentu złożenia zamówienia, chyba że podpisana umowa pomiędzy EuroCert a zamawiającym przewiduje dłuższy okres.

4.3 Wydawanie certyfikatu

1. EuroCert generuje parę kluczy na nośniku wybranym w zamówieniu, dedykowanym dla subskrybenta. EuroCert, wydając certyfikat, opatruje pieczęcią elektroniczną klucz publiczny wraz z danymi o subskrybencie.
2. Proces wydawania kolejnego certyfikatu po unieważnieniu poprzedniego lub wydawania kolejnego certyfikatu w przypadku, gdy upłynął okres ważności posiadanego przez subskrybenta certyfikatu, przebiega analogicznie jak proces wydawania pierwszego certyfikatu. Jeżeli powodem unieważnienia certyfikatu nie była konieczność zmiany identyfikatora subskrybenta, wówczas nowy certyfikat może zawierać nadany wcześniej identyfikator.

4.3.1 Czynności urzędu certyfikacji podczas wydawania certyfikatu

1. Certyfikaty wydawane są przez EuroCert osobiście subskrybentowi lub mogą być przekazane subskrybentowi zdalnie, np. za pośrednictwem poczty elektronicznej na adres podany w zamówieniu i zweryfikowanych zgodnie z pkt 3.2.2. Podczas procesu osobistego wydawania certyfikatu Operator wykonuje następujące czynności:
   a) sprawdza kompletność zrealizowanego zamówienia z wnioskiem składanym przez zamawiającego,
   b) porównuje dane zawarte na potwierdzeniu certyfikatu z danymi z wniosku,
   c) weryfikuje tożsamość i uprawnienia subskrybenta,
   d) w przypadku, gdy zostanie stwierdzona zgodność danych i nastąpi poprawna weryfikacja tożsamości – przekazuje certyfikat.

4.3.2 Informowanie subskrybenta o wydaniu certyfikatu

1. Certyfikat jest gotowy do odbioru w terminie wskazanym w zamówieniu.

4.4 Akceptacja certyfikatu

1. Po odebraniu certyfikatu subskrybent jest zobowiązany do niezwłocznego sprawdzenia jego zawartości, nie później niż przed pierwszym użyciem klucza prywatnego związanego z certyfikatem. W przypadku nieprawdziwości danych zawartych w certyfikacie, jest on zobowiązany do niezwłocznego zgłoszenia tego faktu EuroCert, celem unieważnienia certyfikatu zgodnie z obowiązującymi procedurami (patrz pkt 3.4 i pkt 4.9) i otrzymania nowego certyfikatu, zawierającego poprawne dane. Posługiwanie się certyfikatem zawierającym nieprawdziwe dane naraża subskrybenta na odpowiedzialność karną określoną w art. 42 ust. 2 Ustawy o usługach zaufania.

2. Wstępna akceptacja certyfikatu jest wykonywana przez operatora punktu rejestracji niezwłocznie po wystawieniu certyfikatu przez urząd certyfikacji, a przed nagraniem go na jakikolwiek nośnik. Punkt rejestracji sprawdza, czy dane zawarte w certyfikacie są prawidłowe. Jeśli zawiera on jakiekolwiek wady, to powinien zostać niezwłocznie unieważniony, a na jego miejsce wydany nowy pozbawiony błędów bez obciążania subskrybenta kosztami za tę operacje. W takiej sytuacji nie wymaga się podpisania umowy i /lub dostarczenia dodatkowych dokumentów.

4.4.1 Potwierdzenie akceptacji certyfikatu

1. Certyfikat jest akceptowany przez subskrybenta poprzez poświadczenie potwierdzenia odbioru certyfikatu, które zawiera dane otrzymanego certyfikatu. Potwierdzenie to opatrzone własnoręcznym podpisem subskrybenta jest przechowywane przez EuroCert. Drugi egzemplarz otrzymuje subskrybent.
2. W przypadku certyfikatów wydawanych online (patrz pkt 4.7) akceptacja certyfikatu przez subskrybenta następuje poprzez pobranie go z systemu EuroCert.

4.4.2 Publikacja certyfikatu

1. Certyfikaty nie są publikowane poza siecią wewnętrzną EuroCert.

4.4.3 Poinformowanie innych podmiotów o wydaniu certyfikatu

1. EuroCert może informować o wydaniu certyfikatu inne podmioty, o ile certyfikat ich dotyczył lub zawierał ich dane (np. podmiot reprezentowany przez subskrybenta w przypadku certyfikatów firmowych).

4.5 Korzystanie z pary kluczy i certyfikatu

W tym punkcie przedstawiono zobowiązania subskrybentów, stron ufających oraz zamawiających związane z korzystaniem z pary kluczy i certyfikatu.

4.5.1 Zobowiązania subskrybenta

1. Subskrybent zobowiązuje się do:
   a) przestrzegania postanowień umowy podpisanej z EuroCert,
   b) przekazywania do EuroCert wyłącznie prawdziwych i kompletnych danych w zakresie wymaganym przez umowę lub wniosek o wydanie certyfikatu,
   c) dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku i umowie,
   d) informowania EuroCert o wszelkich zmianach informacji zawartych w jego certyfikacie, w celu unieważnienia certyfikatu i ewentualnie wystawienia nowego, zawierającego poprawne dane,
   e) sprawdzenia poprawności danych zawartych w certyfikacie niezwłocznie po jego otrzymaniu; w przypadku wystąpienia jakichkolwiek nieprawidłowości, w szczególności nieprawidłowych wartości pól określających tożsamość subskrybenta, jest on zobowiązany do niezwłocznego zgłoszenia tego faktu EuroCert celem unieważnienia certyfikatu i wygenerowania nowego certyfikatu z prawidłowymi danymi,
   f) niezwłocznego poinformowania EuroCert o wszelkich okolicznościach, w wyniku których jego klucz prywatny został ujawniony osobom trzecim lub w wyniku których subskrybent

może podejrzewać, że klucz prywatny mógł ulec ujawnieniu osobom trzecim (np. utraty klucza prywatnego),

g) niezwłocznego przystąpienia do procedury unieważnienia certyfikatu w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego,
h) traktowania utraty lub ujawnienia (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,
i) podjęcia wszelkich środków ostrożności w celu bezpiecznego przechowywania klucza prywatnego, włączając w to:
   - kontrolę i zabezpieczenie dostępu do urządzeń zawierających jego klucze prywatne,
   - nie przechowywanie nośnika zawierającego klucz prywatny razem z osobistym numerem identyfikacyjnym (PIN),
   - nie udostępnianie i nie przekazywanie swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim,
j) nie składania podpisu elektronicznego przy pomocy należącego do niego klucza prywatnego, jeżeli certyfikat ten jest przeterminowany (minął jego okres ważności), jest unieważniony lub zawieszony,
k) używania kluczy prywatnych i certyfikatów zgodnie z ich przeznaczeniem określonym w pkt 1.4 oraz wskazanym w certyfikacie (w polu *keyUsage*, patrz pkt 6.1.7),
l) niezwłocznego zgłoszenia EuroCert żądania unieważnienia certyfikatu w przypadkach przewidzianych w pkt 4.9.1.

4.5.2 Zobowiązania strony ufającej

1. Strony ufające są zobowiązane do:
   a) zaufania tylko tym certyfikatom, które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca,
   b) używania kluczy publicznych i certyfikatów tylko po zweryfikowaniu ich statusu oraz ważności pieczęci elektronicznej urzędu certyfikacji, który wystawił certyfikat,
   c) weryfikowania podpisu elektronicznego z wykorzystaniem listy zawieszonych i unieważnionych certyfikatów i właściwej ścieżki certyfikacji,
   d) informowania EuroCert o wszelkich przypadkach użycia certyfikatu przez osoby nieupoważnione lub podejrzeniach, że certyfikat został wydany niewłaściwemu podmiotowi,
   e) sprawdzenia, czy identyfikatory polityk certyfikacji, umieszczone w certyfikatach zawartych w ścieżce znajdują się w określonym przez weryfikującego zbiorze identyfikatorów dopuszczalnych,
   f) uznania podpisu za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis jest ważny lub uzyskany wynik weryfikacji jest negatywny,
   g) sprawdzenia rodzaju certyfikatu i polityki, według której został wydany; w przypadku wątpliwości, czy dany certyfikat został wydany poprawnie oraz czy jest używany przez upoważniony do tego podmiot strona ufająca jest zobowiązana do zgłoszenia wątpliwości do EuroCert,

h) używania kluczy prywatnych i certyfikatów zgodnie z ich przeznaczeniem określonym w pkt 1.4 oraz wskazanym w certyfikacie (w polu *keyUsage*, patrz pkt 6.1.7).

4.5.3 Obowiązki zamawiającego

1. Obowiązki zamawiającego określa umowa zawarta pomiędzy zamawiającym a EuroCert.

4.6 Odnowienie certyfikatu

1. Nie ma możliwości odnowienia certyfikatu subskrybenta. EuroCert wydaje certyfikaty za każdym razem generując nową parę kluczy. Jeśli subskrybent posiada ważny certyfikat, może ubiegać się o wystawienie nowego certyfikatu i wygenerowania nowej pary kluczy według uproszczonej procedury (patrz pkt 4.7).

4.7 Wystawienie kolejnego certyfikatu

1. Wystawienie kolejnego certyfikatu ma miejsce zawsze wtedy, gdy subskrybent występuje z wnioskiem o dodatkowy certyfikat posiadanego typu dla nowej pary kluczy w okresie ważności obecnego certyfikatu.
2. Wystawienie kolejnego certyfikatu może być realizowane przez subskrybenta okresowo, w oparciu o parametry wskazanego certyfikatu, będącego już w posiadaniu subskrybenta. W efekcie tworzony jest nowy certyfikat, którego parametry są takie same jak wskazanego we wniosku certyfikatu, poza zawartym w nim nowym kluczem publicznym, numerem seryjnym certyfikatu i innym okresem jego ważności.
3. Nowy certyfikat będzie zawierał identyfikator DN użytkownika taki sam, jaki znajduje się w certyfikacie subskrybenta, który jest wykorzystywany do weryfikacji podpisu elektronicznego subskrybenta złożonego pod wnioskiem o wydanie certyfikatu.
4. Proces wydawania kolejnego certyfikatu po unieważnieniu poprzedniego lub wydawania kolejnego certyfikatu w przypadku, gdy upłynął okres ważności posiadanego przez subskrybenta certyfikatu, przebiega analogicznie jak proces wydawania pierwszego certyfikatu.

4.7.1 Warunki wystawienia kolejnego certyfikatu

1. Subskrybent w każdej chwili może wystąpić z wnioskiem o wystawienie nowego certyfikatu, np. wtedy, gdy obecny certyfikat traci ważność.
2. Wydanie kolejnego certyfikatu musi być poprzedzone złożeniem niezbędnych dokumentów formalnych w postaci elektronicznej, podpisanych (uwierzytelnionych) przy użyciu ważnego klucza prywatnego, związanego z nieprzeterminowanym certyfikatem. Certyfikat ten nie jest unieważniany.
3. Weryfikacja tożsamości subskrybenta w tym przypadku realizowana jest na podstawie podpisu elektronicznego, złożonego pod wnioskiem o wydanie certyfikatu.

4.7.2 Kto może żądać wydania kolejnego certyfikatu?

1. Wydanie nowego certyfikatu następuje z inicjatywy subskrybenta posiadającego ważny certyfikat.

4.7.3 Przetwarzanie wniosku o wydanie kolejnego certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.7.4 Informowanie podmiotu o wydaniu certyfikatu

1. Informacja o wygenerowaniu certyfikatu jest przekazywana do subskrybenta elektronicznie.

4.7.5 Akceptacja certyfikatu

1. Akceptacja certyfikatu przez subskrybenta następuje poprzez pobranie go z systemu.

4.7.6 Publikacja certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.7.7 Powiadomienie innych podmiotów o wydaniu certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8 Modyfikacja certyfikatu

1. Zmiana treści certyfikatu wymaga wydania nowego certyfikatu.
2. Wydanie certyfikatu dla zmienionych danych przebiega tak samo jak w przypadku wydawania pierwszego certyfikatu. Dotychczasowy certyfikat – o ile dane w nim zawarte stały się nieaktualne i zawierają nieprawdziwą informację o subskrybencie – jest unieważniany.

4.8.1 Warunki modyfikacji certyfikatu

1. Modyfikacja certyfikatu:
   - odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o wydanie nowego certyfikatu,
   - może dotyczyć tylko certyfikatu, którego okres ważności nie minął lub nie został wcześniej unieważniony.
2. Nowy certyfikat posiada nowy klucz publiczny, nowy numer seryjny i różni się zawartością przynajmniej jednego z pozostałych pól certyfikatu. Modyfikacji nie może ulec identyfikator polityki certyfikacji, według której certyfikat został wystawiony.

4.8.2 Kto może żądać zmiany danych w certyfikacie?

1. Za zgłoszenie potrzeby aktualizacji danych zawartych w certyfikacie oraz za określenie, czy zmiana danych pociąga za sobą konieczność unieważnienia certyfikatu dotychczasowego, odpowiedzialny jest subskrybent (patrz pkt 4.5.1).

4.8.3 Przetwarzanie wniosku o modyfikację certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.4 Informowanie podmiotu o wydaniu zmodyfikowanego certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.5 Akceptacja certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.6 Publikacja certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.7 Powiadomienie innych podmiotów o wydaniu certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.9 Unieważnienie i zawieszenie certyfikatu

1. Zgodnie z art. 16 ust. 4 ustawy o usługach zaufania EuroCert zapewnia możliwość całodobowego zgłaszania żądań unieważnienia/ zawieszenia certyfikatu.

4.9.1 Okoliczności unieważnienia certyfikatu

1. Unieważnienie certyfikatu może wynikać z następujących okoliczności:
   a) dane zawarte w certyfikacie przestały być aktualne lub są nieprawdziwe,
   b) na każde żądanie subskrybenta lub – w przypadku zgłoszenia unieważnienia certyfikatu firmowego – na żądanie upoważnionego przedstawiciela reprezentowanego podmiotu lub innej upoważnionej osoby,
   c) klucz prywatny subskrybenta powiązany z kluczem publicznym w certyfikacie został skompromitowany, lub istnieje uzasadnione podejrzenie, iż fakt taki mógł mieć miejsce, (np. w wyniku utraty klucza prywatnego, nieuprawnionego dostępu lub podejrzenia nieuprawnionego dostępu do klucza prywatnego, zagubienia lub podejrzenia zagubienia klucza prywatnego, kradzieży lub podejrzenia kradzieży klucza prywatnego, przypadkowego zniszczenie klucza prywatnego),
   d) ustąpiły okoliczności uzasadniające zamieszczenie danych organizacji w certyfikacie (np. zwolnienie pracownika, zmiana zakresu obowiązków itd.),
   e) przez wystawcę certyfikatu, tzn. przez EuroCert, np. wskutek rażącego naruszenia przez subskrybenta zasad Polityki, w szczególności obowiązków określonych w pkt 4.5.1,
   f) EuroCert zaprzestaje świadczenia usług w zakresie usług zaufania i żaden podmiot nie przejmuje prowadzenia usługi udostępniania informacji o statusie certyfikatu,
   g) EuroCert otrzyma dowód, że certyfikat był wykorzystany niezgodnie z przeznaczeniem,
   h) z wyłącznej inicjatywy EuroCert w wyniku uzasadnionego podejrzenia, iż certyfikat wraz z parą kluczy zagraża bezpieczeństwu subskrybenta,
   i) certyfikat był wydany niezgodnie z Polityką,
   j) klucz prywatny operacyjnego urzędu certyfikacji lub głównego urzędu certyfikacji został skompromitowany lub EuroCert pozyska informację, że mógł zostać skompromitowany.

4.9.2 Kto może żądać unieważnienia certyfikatu

1. Z żądaniem unieważnienia certyfikatu subskrybenta mogą występować następujące podmioty:
   a) subskrybent będący podmiotem unieważnianego certyfikatu,
   b) upoważniony przedstawiciel zamawiającego, którego dane występują w certyfikacie ,
   c) inspektor bezpieczeństwa,
   d) organ nadrzędny organizacji, w imieniu której występuje subskrybent,
   e) osoba fizyczna udzielająca pełnomocnictwa do reprezentowania jej interesów,

f) operator punktu rejestracji, Inspektor rejestracji, którzy mogą wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli są w posiadaniu informacji uzasadniającej unieważnienie certyfikatu.

2. EuroCert zachowuje szczególną ostrożność przy rozpatrywaniu wniosków o unieważnienie certyfikatu, których autorem nie jest subskrybent i honoruje tylko te, które obejmują przypadki wymienione w pkt 4.9.1 oraz gdy ryzyko utraty zaufania do kwestionowanego certyfikatu przewyższa niedogodności i potencjalne straty subskrybenta, powstałe w wyniku unieważnienia.

3. Jeśli wnioskujący o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu (subskrybentem), to urząd certyfikacji:
   - sprawdza, czy dany wnioskodawca może żądać unieważnienia certyfikatu,
   - wysyła powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

4.9.3 Procedura unieważniania certyfikatu

1. Certyfikat jest unieważniany po pomyślnej weryfikacji wniosku o unieważnienie przez Inspektora rejestracji zgodnie z zasadami w pkt 3.4.

2. W przypadku, gdy istnieją przesłanki do unieważnienia certyfikatu, jednakże Inspektor rejestracji nie jest w stanie w ciągu 24 godzin od momentu otrzymania kompletnego wniosku wyjaśnić wszystkich wątpliwości dotyczących unieważnienia, certyfikat jest zawieszany.

3. Informacja o unieważnieniu certyfikatu jest umieszczana na liście CRL (patrz pkt 4.9.7 oraz 7.2). EuroCert przekazuje subskrybentowi certyfikatu oraz stronie ubiegającej się o unieważnienie za pośrednictwem poczty elektronicznej potwierdzenie unieważnienia lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy.

4. Unieważniany certyfikat i komplementarny z nim klucz prywatny, przechowywane na nośniku, powinny być w sposób nieodwracalny usunięte z tego nośnika. Operacji tej dokonuje właściciel nośnika – osoba fizyczna lub przedstawiciel działający z upoważnienia osoby prawnej.

4.9.4 Dopuszczalny okres zwłoki w unieważnieniu certyfikatu

1. EuroCert gwarantuje unieważnienie certyfikatu w ciągu 24 godziny od otrzymania kompletnego wniosku z zastrzeżeniem p. 4.9.3 pkt 2.

4.9.5 Maksymalny czas przetwarzanie wniosku o unieważnienie

1. Maksymalny dopuszczalny czas na przetworzenie wniosku o unieważnienie certyfikatu wynosi 24 godziny od momentu wpłynięcia kompletnego wniosku z zastrzeżeniem p. 4.9.3 pkt 2.

4.9.6 Obowiązek sprawdzania unieważnień przez stronę ufającą

1. Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem opublikowanej listy CRL w ciągu 24 godzin od wpłynięcia wniosku o unieważnienie certyfikatu.

2. Strona ufająca danym umieszczonym w certyfikacie wydanym przez EuroCert jest zobowiązana do każdorazowego sprawdzania, czy certyfikat nie został umieszczony na liście CRL przed jego wykorzystaniem do weryfikacji podpisu elektronicznego.

4.9.7 Częstotliwość publikacji CRL

1. Listy CRL dla certyfikatów wystawionych przez główny urząd certyfikacji EUROCERT COMMERCIAL są publikowane niezwłocznie po zawieszeniu lub unieważnieniu certyfikatu, nie rzadziej jednak niż co 8 dni. Listy CRL są dostępne na stronie internetowej EuroCert w trybie 24x7x365. EuroCert sprawdza co najmniej raz dziennie dostępność list CRL.

4.9.8 Maksymalne opóźnienie w publikowaniu list CRL

1. Listy CRL są publikowane, niezwłocznie po ich utworzeniu, nie później niż w ciągu 1 godziny od potwierdzenia żądania unieważnienia certyfikatu.

4.9.9 Dostępność weryfikacji statusu certyfikatu on-line

1. Dla certyfikatów wystawionych zgodnie z niniejszą Polityką nie udostępnia się usługi weryfikacji statusu certyfikatów w czasie rzeczywistym.

4.9.10 Obowiązek sprawdzenia unieważnień w trybie on-line

Polityka nie określa żadnych wymagań w tym zakresie.

4.9.11 Inne formy ogłaszania unieważnień certyfikatów

1. W przypadku naruszenia ochrony (ujawnienia) klucza prywatnego urzędu certyfikacji funkcjonującego w ramach EuroCert informacja o tym jest umieszczana natychmiast na listach CRL oraz obligatoryjnie przesłana za pośrednictwem poczty elektronicznej do wszystkich subskrybentów urzędu certyfikacji. Informowani są wszyscy subskrybenci, których interesy mogą być w jakikolwiek sposób (bezpośredni lub pośredni) zagrożone.

4.9.12 Specjalne obowiązki w przypadku kompromitacji klucza

1. Obowiązkiem EuroCert w przypadku kompromitacji klucza urzędu certyfikacji jest jak najszybsze poinformowanie subskrybentów i stron ufających o tym fakcie poprzez publikację na stronie internetowej EuroCert oraz jeśli to możliwe w środkach masowego przekazu.

4.9.13 Okoliczności zawieszenia certyfikatu

1. Zawieszenie certyfikatu następuje niezwłocznie po powzięciu uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu wskazane w pkt 4.9.1, w szczególności na wniosek złożony przez subskrybenta lub zamawiającego.
2. Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:
   a) dane zawarte w elektronicznym lub papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,
   b) wniosek o unieważnienie został przekazany telefonicznie i nie można w ciągu 24 godzin, liczonej od chwili otrzymania wniosku potwierdzić tożsamości wnioskodawcy, ale też zanegować słuszności złożonego wniosku,
   c) istnieje podejrzenie, że osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,

d) EuroCert może niezwłocznie zawiesić certyfikat w przypadku uzasadnionego podejrzenia, że certyfikat wydano bez przestrzegania postanowień niniejszej Polityki; certyfikat może pozostać zawieszony do czasu aż EuroCert znajdzie podstawy do unieważnienia certyfikatu, nie dłużej jednak jak 7 dni,
e) innych okoliczności wymagających wyjaśnień ze strony subskrybenta lub wnioskodawcy.

3. Wniosek o zawieszenie certyfikatu zawiera podobne informacje jak w przypadku wniosku o unieważnienie.

4.9.14 Kto może żądać zawieszenia certyfikatu

1. Zawieszenie certyfikatu następuje z inicjatywy EuroCert w przypadku uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu wskazane w pkt 4.9.1, w szczególności na wniosek subskrybenta lub zamawiającego (patrz pkt 3.4).

4.9.15 Procedura zawieszenia i odwieszenia certyfikatu

1. Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu. Po pomyślnej weryfikacji wniosku o zawieszenie przez Inspektora rejestracji przebiegającej jak w pkt 3.4 zmienia on status certyfikatu na zawieszony i umieszcza go na liście CRL (z przyczyną unieważnienia: *certificateHold*).

2. W przypadku niepotwierdzenia się przesłanek uzasadniających zawieszenie certyfikatu, o których mowa w pkt 4.9.13 EuroCert uchyla zawieszenie certyfikatu. W przypadku potwierdzenia podejrzenia oraz w przypadku, gdy EuroCert nie jest w stanie wyjaśnić wątpliwości dotyczących zawieszenia certyfikatu w terminie 7 dni od zawieszenia certyfikatu, certyfikat zostaje unieważniony.

3. Odwieszenie może nastąpić wyłącznie z inicjatywy EuroCert. Po odwieszeniu certyfikatu, informacja o takim certyfikacie jest usuwana z listy CRL.

4. Jeżeli unieważnienie certyfikatu następuje po jego uprzednim zawieszeniu, wówczas data unieważnienia certyfikatu jest tożsama z datą zawieszenia certyfikatu.

4.9.16 Ograniczenie czasowe zawieszenia

1. Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia). Ewentualne odwieszenie certyfikatu musi jednakże nastąpić nie później niż 7 dni od daty zawieszenia (w przeciwnym przypadku certyfikat zostaje unieważniony).

4.10 Weryfikacja statusu certyfikatu

1. Weryfikacji statusu certyfikatów wydanych przez EuroCert można dokonać na podstawie list CRL. Status certyfikatu wydanego przez EuroCert można również zweryfikować korzystając z usługi OCSP, o ile taka informacja jest umieszczona w wydanym certyfikacie.

2. W przypadku gdy w certyfikacie został umieszczony adres usługi OCSP oznacza to, że dla tego certyfikatu jest udostępniania usługa OCSP.

4.11 Rezygnacja z usług

1. Umowa o świadczenie usług certyfikacyjnych pomiędzy EuroCert a Subskrybentem, kończy się wraz z upłynięciem terminu ważności certyfikatu. Subskrybent może ponadto zakończyć umowę w każdym czasie, poprzez unieważnienie certyfikatu. Samo rozwiązanie Umowy nie skutkuje unieważnieniem lub zawieszeniem certyfikatów wydanych na jej podstawie.

4.12 Odzyskiwanie i przechowywanie kluczy prywatnych

1. EuroCert nie świadczy usług deponowania i przechowywania kluczy prywatnych subskrybentów. Nie powierza również swojego klucza prywatnego innym podmiotom.

5 Zabezpieczenia organizacyjne, operacyjne i fizyczne

W rozdziale opisano wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w EuroCert m.in. podczas generowania kluczy i certyfikatów, uwierzytelniania podmiotów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych.

5.1 Zabezpieczenia fizyczne

1. Pomieszczenia, w których odbywa się przetwarzanie danych związanych z wydawaniem, zawieszaniem lub unieważnianiem certyfikatów, oraz w których odbywa się generowanie, zawieszanie i unieważnianie certyfikatów, podlegają ochronie fizycznej zgodnie z wymaganiami dla kwalifikowanych dostawców usług zaufania oraz ustawą o ochronie danych osobowych.

5.1.1 Lokalizacja i budynki

1. Systemy teleinformatyczne wykorzystywane do świadczenia usług zaufania mieszczą się w dwóch niezależnych lokalizacjach (centrum podstawowym i centrum zapasowym) oddalonych od siebie na odległość wykluczającą jednoczesne wystąpienie tych samych zagrożeń dla obu lokalizacji.

5.1.2 Dostęp fizyczny

1. Fizyczny dostęp do budynków oraz pomieszczeń EuroCert jest kontrolowany oraz nadzorowany przez zintegrowane systemy alarmowe.
2. Budynki i pomieszczenia z których korzysta EuroCert objęte są kontrolą dostępu która funkcjonuje 24 godziny na dobę.
3. Pomieszczenia serwerowni z których korzysta EuroCert w których zainstalowane są systemy usług zaufania, w tym bezpieczne moduły kryptograficzne z pozostającymi w nich kluczami urzędu certyfikacji, wyposażone są w systemy kontroli dostępu do pomieszczeń, systemy sygnalizacji włamania i napadu.
4. Dostęp do pomieszczeń EuroCert posiadają tylko osoby upoważnione będące pracownikami EuroCert, dostęp do serwerowni posiadają wybrani pracownicy stanowiący zaufany personel EuroCert.

5. Nadzorowanie praw dostępu realizowane z wykorzystaniem systemu kontroli dostępu w oparciu o posiadane przez pracowników EuroCert spersonalizowane i zarejestrowane w tym systemie karty dostępu do pomieszczeń.

5.1.3 Zasilanie i klimatyzacja

1. Systemy informatyczne EuroCert są chronione przed zanikiem zasilania z sieci energetycznej poprzez automatyczne przełączenie na zasilanie awaryjne podtrzymywane przez UPS.
2. Środowisko pracy w pomieszczeniach systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń.
3. Wszystkie pomieszczenia są klimatyzowane, serwerownie posiadają osobne systemy klimatyzacji.

5.1.4 Zagrożenie powodziowe, ochrona przed zalaniem

1. Budynki i pomieszczenia z których korzysta EuroCert nie znajdują się w zasięgu zagrożenia wezbraniem lub powodzią.
2. Czujniki zalania są zainstalowane w pomieszczeniach serwerowni. Alarmy o zalaniu przekazywane są do ochrony i administratora budynku, którzy zawiadamiają odpowiednie służby miejskie, Inspektora bezpieczeństwa oraz Administratora systemu.

5.1.5 Ochrona przeciwpożarowa

1. System ochrony przeciwpożarowej, zainstalowany w pomieszczeniach systemu komputerowego, spełnia wymogi stosownych przepisów i norm przeciwpożarowych.
2. W serwerowi zainstalowano urządzenia tłumienia ognia (gazowe), które załączają się automatycznie w przypadku wykrycia pożaru w chronionym obszarze.

5.1.6 Nośniki informacji

1. Nośniki, na których przechowywane są archiwa oraz bieżące kopie danych składowane są w sejfach ognioodpornych zlokalizowanych w centrum podstawowym.
2. Dostęp do sejfów mają pracownicy wykonujący funkcję Inspektora bezpieczeństwa oraz Inspektora audytu.

5.1.7 Niszczenie informacji

1. Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo EuroCert po upływie okresu przechowywania (patrz pkt 5.4.3 i 5.5.2) niszczone są w specjalnych urządzeniach niszczących.
2. W przypadku kluczy kryptograficznych oraz numerów PIN nośniki, na których informacje te były przechowywane są niszczone w urządzeniach klasy DIN-3 (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji i ich ponowne użycie do tych samych lub innych celów).

5.1.8 Kopie bezpieczeństwa i centrum zapasowe

1. W wypadku niedostępności lokalizacji podstawowej, uniemożliwiającej świadczenie usług zaufania, wykorzystywane są systemy awaryjne zlokalizowane w centrum zapasowym.

2. W przypadku niedostępności systemów podstawowych utrzymanie ciągłości działania jest zapewnione przez systemy z centrum zapasowym w zakresie unieważniania, zawieszania certyfikatów i publikacji list CRL.

3. Dane istotne dla bezpieczeństwa EuroCert i świadczonych usług (w szczególności kopie haseł, numerów PIN oraz bezpieczne nośniki z kluczami kryptograficznymi stosowanymi w systemie EuroCert, archiwa, kopie danych bieżących, pełna wersja instalacyjna oprogramowania) są przechowywane w centrum podstawowym w sejfach ognioodpornych.

5.2 Zabezpieczenia organizacyjne

1. EuroCert zapewnia realizację zabezpieczeń organizacyjnych poprzez określenie, między innymi:
   a) zaufanych ról, które mogą być pełnione przez jedną lub więcej osób w urzędzie certyfikacji,
   b) łączenia określonych ról,
   c) zakresu obowiązków i odpowiedzialności osób pełniących określone role,
   d) liczby osób koniecznych do realizacji poszczególnych zadań,
   e) identyfikacji oraz uwierzytelniania personelu.

5.2.1 Kadra

1. Osoby sprawujące nadzór nad systemem wykorzystywanym do świadczenia usług zaufania w EuroCert pełnią określone role, jak pokazano w tab. 5. Przedstawiony podział ról jest zgodny z wymogami: ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Tab. 5. Zaufane role

Rola	Zakres obowiązków
Inspektor bezpieczeństwa	nadzorowanie wdrożeń i stosowania wszystkich procedur bezpieczeństwa eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług zaufania, kierowanie administratorami systemu, inicjowanie i nadzór nad procesem generowania kluczy oraz sekretów współdzielonych, przydzielanie uprawnienia w zakresie zabezpieczeń oraz prawa dostępu użytkownikom, przydzielanie haseł nowym kontom, nadzorowanie prac serwisowych.
Administrator systemu	instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia usług zaufania, zarządzanie uprawnieniami dla operatorów systemu.
Operator system	stała obsługa system teleinformatycznego, w tym wykonywanie kopii zapasowych, zarządzanie uprawnieniami Inspektorów rejestracji.
Inspektor rejestracji	podpisywanie zgłoszeń certyfikacyjnych oraz przyjmowanie wniosków o zawieszenie, unieważnienie lub odwieszenie certyfikatów i tworzenie nowych list CRL.

Rola	Zakres obowiązków
Inspektor audytu	analizowanie zapisów rejestrów zdarzeń mających miejsce w systemach teleinformatycznych EuroCert.

5.2.2 Liczba osób wymaganych do realizacji zadania

1. Operacją, która wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich generowaniu powinny być obecne osoby, pełniące role:
   - inspektora bezpieczeństwa,
   - administratora systemu (operatora modułu kryptograficznego),
   - posiadaczy sekretów współdzielonych,
   - obserwatorów – (opcjonalnie) np. przedstawiciele audytora.
2. Szczegółowa procedura generowania kluczy opisana jest w wewnętrznych dokumentach EuroCert.

5.2.3 Identyfikacja oraz uwierzytelnianie ról

1. Personel EuroCert jest poddawany procedurze identyfikacji oraz uwierzytelniania w następujących przypadkach:
   a) umieszczania na liście osób posiadających dostęp do pomieszczeń EuroCert,
   b) umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci EuroCert**,**
   c) wydawania poświadczenia upoważniającego do wykonywania przypisanej roli,
   d) przydzielania konta oraz hasła w systemie komputerowym EuroCert.
2. Każde z powyższych poświadczeń oraz przypisanych kont:
   a) musi być unikalne i bezpośrednio przypisane konkretnej osobie,
   b) nie może być współdzielone z innymi osobami,
   c) musi być ograniczone do funkcji (wynikających z roli pełnionej przez określoną osobę) realizowanych tylko za pośrednictwem dostępnego oprogramowania systemu EuroCert, systemu operacyjnego oraz kontroli proceduralnych.
3. Operacje wykonywane w EuroCert, które wymagają dostępu poprzez sieć współdzieloną są zabezpieczone dzięki wprowadzonym mechanizmom silnego uwierzytelniania oraz szyfrowaniu przesyłanej informacji.
4. Konta oraz uprawnienia osób, które zakończyły pracę w EuroCert lub utraciły prawo do reprezentowania EuroCert, są natychmiast blokowane.
5. Inspektorzy bezpieczeństwa EuroCert prowadzą regularne - odbywające się raz na kwartał - przeglądy kont i uprawnień w systemach EuroCert. Wszystkie nieużywane konta są blokowane.

5.2.4 Role wymagające separacji obowiązków

1. Wyodrębnione w EuroCert role zapobiegają nadużyciom przy korzystaniu z systemu EuroCert. Każdej osobie odpowiedzialnej za eksploatację systemu EuroCert wykorzystywanego do świadczenia usług zaufania przydzielono tylko takie prawa, które wynikają z pełnionej przez niego roli i ponoszonej z tego tytułu odpowiedzialności.

2. Rola Inspektora bezpieczeństwa nie może być łączona z rolą Administratora systemu ani z rolą Operatora systemu. Rola Inspektora audytu nie może być łączona z żadną z pozostałych wymienionych ról.

5.3 Nadzorowanie Pracowników

1. Personel EuroCert, zwłaszcza osoby piastujące tzw. zaufane role, zobowiązane są postępować zgodnie z przepisami EIDAS i ustawy o usługach zaufania.

5.3.1 Kwalifikacje, doświadczenie, upoważnienia

1. Osoby zajmujące się świadczeniem usług zaufania posiadają odpowiednie kwalifikacje przewidziane dla kwalifikowanych dostawców usług zaufania, w szczególności wiedzę i umiejętności z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych, a ponadto:
   a) posiadają pełną zdolność do czynności prawnych,
   b) nie były skazane prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami wartościowymi, przestępstwo skarbowe, przestępstwa określone w rozdziale VI ustawy o usługach zaufania,
   c) posiadają minimum wykształcenie średnie,
   d) podpisały klauzule o nieujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa urzędu certyfikacji lub poufności danych subskrybenta,
   e) nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem certyfikacji a działającymi w jego imieniu punktami rejestracji,
   f) zapoznały się z wewnętrznymi procedurami EuroCert,
   g) zostały poinformowane o odpowiedzialności karnej w zakresie związanym z świadczeniem usług zaufania.

5.3.2 Weryfikacja pracowników

1. Przed powierzeniem pracownikowi którejkolwiek z ról opisanych w pkt 5.2.1 przeprowadzana jest weryfikacja:
   a) świadectwa pracy z poprzedniego miejsca zatrudnienia (w przypadku nowego pracownika),
   b) dyplomu i świadectwa potwierdzające wykształcenie pracownika,
   c) kwalifikacji i doświadczenia zawodowego,
   d) oświadczenia pracownika o niekaralności.

5.3.3 Szkolenia

1. Personel zaufany EuroCert oraz operatorzy punktów rejestracji przed uzyskaniem uprawnień do pełnienia swojej roli muszą przejść cykl szkoleń dotyczących:
   a) zasad niniejszej Polityki,
   b) zasad zawartych w dokumentacji, przypisanej roli, którą dana osoba pełni,
   c) ochrony danych osobowych i ochrony informacji,
   d) infrastruktury klucza publicznego,
   e) weryfikacji tożsamości na podstawie dokumentów potwierdzających tożsamość,

f) zasad i mechanizmów zabezpieczeń stosowanych w urzędzie certyfikacji oraz punktach rejestracji,
g) oprogramowania systemu komputerowego urzędu certyfikacji,
h) zakresu obowiązków, które będą wykonywały
i) procedur realizowanych po awariach lub katastrofach systemu urzędu certyfikacji,

2. Po zakończeniu szkolenia jego uczestnicy podpisują dokument potwierdzający zapoznanie się z przedstawioną dokumentacją oraz akceptację wynikających z nich ograniczeń.

5.3.4 Powtarzanie szkoleń

1. Szkolenia o których mowa w pkt 5.3.3 są powtarzane lub uzupełniane są w zależności od potrzeb oraz zawsze wtedy, gdy nastąpiły istotne zmiany w świadczeniu usług przez EuroCert, funkcjonowaniu EuroCert lub punktów rejestracji, systemie, bądź zostały opublikowane nowe wersje Polityki.

5.3.5 Częstotliwość rotacji stanowisk i jej kolejność

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

5.3.6 Sankcje z tytułu nieuprawnionych działań

1. W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie Administrator systemu w porozumieniu z Inspektorem bezpieczeństwa może zablokować dostęp do systemu EuroCert sprawcy takiego zdarzenia. Dalsze postępowanie przeprowadzane jest w porozumieniu z kierownictwem EuroCert.

5.3.7 Pracownicy kontraktowi

1. EuroCert dopuszcza wykonywanie czynności związanych z pełnieniem roli, spośród wymienionych w pkt 5.2.1 przez osoby niezatrudnione na podstawie umowy o pracę (pracowników kontraktowych).

2. W przypadku pracowników kontraktowych EuroCert zawiera w umowie z tą osobą lub z firmą, w której jest ona zatrudniona, możliwość dochodzenia przez EuroCert wszelkich strat, które ewentualnie może ponieść w wyniku nienależytego wykonywania przez daną osobę obowiązków wynikających z realizowanej przez nią roli lub w wyniku nieprzestrzegania obowiązujących przepisów prawa, jak też zasad i regulaminów obowiązujących w EuroCert.

3. Niezależnie od ewentualnej odpowiedzialności finansowej, osoby wykonujące nierzetelnie swoje obowiązki związane ze świadczeniem usług certyfikacyjnych lub nieprzestrzegające wymagań nałożonych przez przepisy o podpisie elektronicznym (w szczególności wymagań o poufności, wymagań w zakresie wystawiania i unieważniania certyfikatów) podlegają sankcjom karnym określonym w Ustawie o usługach zaufania.

5.3.8 Dokumentacja dla pracowników

1. EuroCert umożliwia swojemu personelowi jak również operatorom punktów rejestracji dostęp do następujących dokumentów:
   a) Polityk i innych regulacji wewnętrznych,
   b) wzorów umów oraz stosowanych formularzy wniosków,

c) niezbędnych wyciągów z dokumentacji (właściwych dla pełnionej roli), w tym procedur awaryjnych,
d) zakresu obowiązków i uprawnień wynikających z pełnionej roli.

5.4 Procedury tworzenia logów audytowych

1. EuroCert prowadzi rejestr wszelkich istotnych z punktu widzenia bezpieczeństwa zdarzeń związanych ze świadczonymi usługami zaufania w celu zapewnienia bezpieczeństwa, nadzoru nad sprawnym działaniem systemu oraz rozliczania użytkowników i personelu z ich działań.
2. Rejestr zdarzeń przechowywany jest w sposób zapewniający integralność i niezaprzeczalność.

5.4.1 Typy rejestrowanych zdarzeń

1. Rejestrowane zdarzenia obejmują:
   a) zdarzenia bezpośrednio związane ze świadczeniem usług zaufania, a w szczególności: generowanie kluczy urzędów certyfikacji, przyjęcie wniosku o wydanie certyfikatu, generowanie kluczy i certyfikatów subskrybentom, unieważnianie certyfikatów, generowanie list CRL itp.;
   b) czynności związane z obsługą klientów i subskrybentów: przyjmowanie i podpisywanie umów, wniosków, wydawanie certyfikatów, dostarczanie certyfikatów, fakturowanie itp.;
   c) logi systemowe z serwerów i stacji roboczych wchodzących w skład systemu generującego certyfikaty;
   d) zdarzenia związane z obsługą techniczną systemu: błędy i alarmy, rejestr wprowadzanych zmian w systemie, obsługa użytkowników.
2. Rejestry zdarzeń zapisywane są w formie elektronicznej.
3. Rekordy rejestrów zdarzeń zawierają identyfikatory zdarzeń, daty i czasy wystąpienia, typy zdarzeń, opis szczegółowy zdarzeń.
4. Rejestry zdarzeń podlegają procesom:
   a) sporządzania kopii zapasowych,
   b) archiwizacji.

5.4.2 Częstotliwość analizy zapisów zdarzeń

1. Zapisy rejestrowanych zdarzeń analizowane są przez Inspektorów bezpieczeństwa, audytu oraz przez Administratora systemu każdorazowo po wystąpieniu alarmu systemu monitorującego kluczowe elementy systemu urzędu certyfikacji, w celu rozpoznania ewentualnych nieuprawnionych działań lub innych zdarzeń zagrażających bezpieczeństwu EuroCert.

5.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń

1. Po zarchiwizowaniu zapisy rejestrowanych zdarzeń przechowywane są przez okres min. 20 lat tak jak pozostałe dane i dokumenty związane ze świadczeniem usług zaufania, zgodnie z art. 17.2 Ustawy o usługach zaufania.

5.4.4 Ochrona zapisów rejestrowanych zdarzeń

1. Dostęp do rejestrów zdarzeń mają Administrator Systemów oraz Inspektorzy bezpieczeństwa i audytu.

2. Logi są zabezpieczone przed modyfikacją, podlegają procedurom tworzenia kopii zapasowych oraz są archiwizowane.
3. Archiwa rejestru zdarzeń są przechowywane w sejfie, do którego dostęp mają tylko Inspektorzy audytu oraz Zarząd.

5.4.5 Tworzenie kopii zapisów rejestrowanych zdarzeń

1. Zapisy zdarzeń są kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa systemu. Kopie te przechowywane są w lokalizacji podstawowej w sejfach.
2. Czynności tworzenia kopii zapasowych wykonywane są przez Administratora lub Operatora systemu.

5.4.6 System gromadzenia danych na potrzeby audytu

1. Moduły programowe systemu certyfikacji kluczy oraz serwery tworzą automatycznie zapisy w rejestrach zdarzeń. Inne zdarzenia rejestrowane są ręcznie w odpowiednich bazach.
2. Na potrzeby audytu wewnętrznego dane są udostępniane on-line bądź z zapisów archiwalnych składowanych w sejfach.

5.4.7 Powiadamianie o zaistniałych zdarzeniach

1. Elementy systemu certyfikacji oraz systemów wspomagających podlegają stałemu nadzorowi przez systemy monitorujące oraz zaufany personel techniczny.
2. Informacja o wykrytym zagrożeniu lub naruszeniu bezpieczeństwa trafia bezpośrednio do administratora systemu i inspektora bezpieczeństwa. W zależności od poziomu i wagi zagrożenia powiadamiane są osoby odpowiedzialne za działanie komponentów, których dotyczy zdarzenie.
3. Powiadamianie może być wykonane drogą elektroniczną lub telefonicznie.
4. W przypadku naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe, nie później niż w ciągu jednego dnia roboczego od wystąpienia zdarzenia EuroCert zawiadamia organ nadzoru i, w stosownych przypadkach, inne właściwe podmioty zgodnie z art. 19.2 EIDAS (patrz pkt 5.7.1).

5.4.8 Oszacowanie podatności na zagrożenia

1. Niniejszy dokument wymaga przeprowadzenia przez EuroCert analizy podatności na zagrożenia wszystkich posiadanych aktywów, w tym w szczególności oprogramowania oraz systemu komputerowego.
2. Analiza ryzyka dla EuroCert prowadzona jest przynajmniej raz w roku lub przy wprowadzaniu nowych usług, dużych zmian w systemach lub w wyniku incydentu bezpieczeństwa.
3. Za audyt wewnętrzny odpowiedzialny jest inspektor Audytu, którego zadanie polega na kontroli zgodności zapisów w rejestrze bezpieczeństwa, poprawności przechowywania jego kopii, działań podejmowanych w sytuacjach zagrożeń oraz przestrzegania postanowień niniejszego dokumentu.

5.5 Archiwizacja danych

5.5.1 Typy archiwizowanych danych

1. Archiwizacji podlegają następujące dane:
   a) umowy o świadczenie usług zaufania, o których mowa w art. 14 pkt 1 Ustawy o usługach zaufania,
   b) otrzymywane wnioski oraz wydawane decyzje, mające postać papierową lub elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane,
   c) baza danych subskrybentów, w tym wszystkie informacje zebrane w procesie rejestracji subskrybenta,
   d) baza danych certyfikatów,
   e) wydane listy CRL,
   f) historia kluczy urzędów certyfikacji, od ich wygenerowania do zniszczenia włącznie,
   g) polityka świadczenia usług,
   h) dokumenty wystawiane przez operatora systemu punktu rejestracji, notariusza lub inne osoby potwierdzające tożsamość wnioskodawcy w imieniu EuroCert,
   i) żądania unieważnienia certyfikatu,
   j) pozostałe dokumenty papierowe, związane ze świadczeniem usług zaufania.

5.5.2 Okres przechowywania archiwów

1. Dokumenty papierowe oraz dane w postaci elektronicznej, o których mowa w pkt 5.5.1, bezpośrednio związane z wykonywanymi usługami zaufania, są przechowywane przez okres 20 lat od ich wytworzenia (zgodnie z ustawą o usługach zaufania art. 17 ust. 2).

5.5.3 Ochrona archiwów

1. Archiwalne dane są przechowywane w siedzibie EuroCert:
   a) w postaci elektronicznej – w sejfach,
   b) archiwalne dane w postaci papierowej – w metalowych zamykanych na klucz szafach.

5.5.4 Procedury tworzenia kopii zapasowych

1. Kopie zapasowe tworzone są w celu ochrony danych oraz odtworzenia systemu po awarii.
2. Kopiowaniu podlegają:
   a) dyski instalacyjne z oprogramowaniem systemowym, m.in. systemami operacyjnymi,
   b) dyski instalacyjne z aplikacjami urzędu certyfikacji i punktów rejestracji,
   c) historie kluczy urzędów certyfikacji, certyfikatów i list CRL,
   d) dane z repozytorium urzędu certyfikacji,
   e) dane o subskrybentach oraz personelu EuroCert,
   f) rejestry zdarzeń.

5.5.5 Wymaganie znakowania czasem archiwizowanych danych

Nie stosuje się znakowania czasem archiwizowanych danych.

5.5.6 System archiwizacji danych

1. EuroCert archiwizuje dane we własnym zakresie, korzystając z metalowych szaf zamykanych na klucz oraz sejfów ognioodpornych.

2. Archiwalne kopie danych elektronicznych przechowywane są w siedzibie EuroCert.

5.5.7 Procedura weryfikacji i dostępu do zarchiwizowanych danych

1. W celu sprawdzenia integralności dane archiwalne poddawane są okresowym przeglądom i sprawdzaniu poprawności odtwarzania. W zależności od właściwego dla danego nośnika danych okresu archiwizacji dane są przepisywane na nowe nośniki. Proces nadzoruje Inspektor Bezpieczeństwa, wykonują Administrator i Operator systemów.

5.6 Wymiana klucza

1. Procedura wymiany kluczy odnosi się do kluczy urzędu certyfikacji używanych do podpisywania certyfikatów, list CRL, znaczników czasu oraz zweryfikowanych statusów certyfikatów.
2. Wymiana kluczy urzędów certyfikacji realizowana jest w sposób zapewniający zachowanie ustalonego minimalnego okresu ważności certyfikatów. Odpowiednio wcześniej przed wygaśnięciem certyfikatu danego urzędu certyfikacji tworzona jest nowa, niezależna infrastruktura klucza publicznego w ramach której generowana jest nowa para kluczy oraz certyfikat nowego urzędu certyfikacji. Do czasu wygaśnięcia certyfikatu starego urzędu certyfikacji działają dwa ośrodki. Nowy urząd certyfikacji przejmuje rolę wygasającego, świadczy wszystkie czynności związane z obsługą certyfikatów: generowanie, zawieszanie i unieważnianie certyfikatów, generowanie list CRL. Wygasający ośrodek certyfikacji obsługuje tylko unieważnienia i zawieszenia certyfikatów wystawionych w ramach swojej infrastruktury oraz generuje listy CRL do czasu zaprzestania swojej działalności operacyjnej (wygaśnięcia certyfikatu).
3. Nowy certyfikat urzędu certyfikacji jest publikowany w repozytorium. Informacja o zmianie kluczy może być opublikowana w środkach masowego przekazu.

5.7 Utrata poufności klucza i działanie w przypadku katastrof

Podrozdział ten zawiera opis postępowania przez EuroCert w wypadkach szczególnych (także klęsk żywiołowych) w celu przywrócenia funkcjonalności urzędu certyfikacji. Postępowanie jest realizowane według opracowanego planu ciągłości działania.

5.7.1 Procedura obsługi incydentów i reagowania na zagrożenia

Procedury postepowania w przypadku wystąpienia zagrożenia lub naruszenia bezpieczeństwa systemu szczegółowo opisane są w obowiązującej w EuroCert procedurze zarządzania incydentem bezpieczeństwa oraz planie ciągłości działania. Postępowanie jest zgodne z wymaganiami art. 19.2 EIDAS.

5.7.2 Odzyskiwanie zasobów obliczeniowych, oprogramowania i/lub danych

1. EuroCert dysponuje zestawem procedur operacyjnych na wypadek konieczności odtwarzania zasobów. W każdej lokalizacji (podstawowej i zapasowej) znajdują się zasoby pozwalające na odtworzenie podstawowej funkcjonalności urzędu certyfikacji:
   a) kopie danych,
   b) kopie kluczy urzędów certyfikacji,
   c) kopie kart kryptograficznych z dzielonymi sekretami oraz administratorskich,

d) nośniki z oprogramowaniem systemu certyfikacji kluczy,
e) procedury operacyjne urzędu certyfikacji.

2. Plan ciągłości działania (BCM – Business Continuity Plan) opisuje sposób utrzymania gotowości na wypadek wdrożenia Planu Odtworzenia Systemów (DRP – Disaster Recovery Plan). Wymienione plany są regularnie testowane.

5.7.3 Procedury w przypadku kompromitacji klucza urzędu

1. EuroCert posiada odpowiednie procedury obowiązujące w wypadku utraty poufności klucza prywatnego lub uzasadnionego podejrzenie zajścia takiego zdarzenia (patrz pkt 5.4.7). Procedury te przewidują między innymi:
   a) poinformowanie subskrybentów o zaistniałej sytuacji oraz o planie dalszego działania,
   b) unieważnienie certyfikatu związanego z ujawnionym kluczem prywatnym oraz wszystkich aktualnie ważnych certyfikatów, podpisanych przy pomocy ujawnionego klucza prywatnego,
   c) powiadomienie o unieważnieniu certyfikatu urzędu certyfikacji dostępnymi kanałami informacyjnymi,
   d) wytworzenie nowych kluczy urzędu certyfikacji,
   e) jeśli to będzie w danej sytuacji możliwe (w szczególności bazy danych EuroCert pozostaną wiarygodne) – wystawienie nowych certyfikatów i kluczy dla subskrybentów , w oparciu o nowe klucze EuroCert, z okresami ważności co najmniej takimi samymi, jakie miały unieważnione certyfikaty, bez obciążania ich kosztami za tę operację.

5.7.4 Zapewnienie ciągłości działania po katastrofach

1. EuroCert posiada wdrożone procedury, zapewniające bezpieczeństwo i ciągłość świadczenia krytycznych usług urzędu certyfikacji w przypadku fizycznego uszkodzenia systemu komputerowego, awarii oprogramowania oraz sieci telekomunikacyjnej i zasilania, katastrof i innych nieprzewidzianych okoliczności.

2. Infrastruktura techniczna urzędu certyfikacji posiada zabezpieczenia umożliwiające kontynuację pracy w przypadku jakiejkolwiek awarii, natomiast w przypadku katastrofy, awarii sprzętu lub infrastruktury przekraczającej możliwości wynikające z tych zabezpieczeń urząd certyfikacji zostanie uruchomiony w centrum zapasowym w ciągu 1 godziny od momentu stwierdzenia awarii zgodnie z procedurą przełączania ośrodków obowiązującą w EuroCert.

3. Centrum zapasowe zapewnia ciągłość pracy urzędu certyfikacji w zakresie unieważniania lub zawieszania certyfikatów oraz publikacji list CRL.

5.8 Zakończenie działalności urzędu

1. EuroCert jest obowiązany informować z co najmniej 90-dniowym wyprzedzeniem wszystkich subskrybentów z ważnym certyfikatem o zamiarze zakończeniu działalności w zakresie świadczenia usług zaufania (patrz art. 7 pkt 2 Ustawy o usługach zaufania).

2. Szczegółowy sposób postępowania w takim przypadku zawiera plan zakończenia działalności kwalifikowanego dostawcy usług zaufania, o którym mowa w art. 24 ust. 2 lit. i EIDAS oraz w art. 19 ust. 3. Ustawy o usługach zaufania, będący w posiadaniu EuroCert.

3. Jeśli żaden inny dostawca usług zaufania nie przejmie działalności EuroCert w zakresie udostępniania informacji o statusie certyfikatu konieczne jest unieważnienie certyfikatów subskrybentów, którym przysługuje prawo zwrotu proporcjonalnej do okresu wykorzystania certyfikatu części wynagrodzenia z tytułu jego zakupu.

6 Bezpieczeństwo techniczne

Poniżej omówiono tworzenie oraz zarządzanie (m.in. przechowywania i używania) parami kluczy kryptograficznych będących pod kontrolą ich właścicieli (urzędu certyfikacji lub subskrybentów), wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1 Generowanie i instalowanie par kluczy

1. Urząd certyfikacji EuroCert COMMERCIAL stosowany jest w procesie elektronicznego poświadczania certyfikatów i list CRL.
2. Klucz prywatny EuroCert COMMERCIAL stosowany jest do podpisywania certyfikatów oraz list CRL.
3. Do realizacji podpisu elektronicznego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-512/SHA-256.

6.1.1 Generowanie par kluczy

1. Klucze urzędu certyfikacji generowane są przez personel EuroCert zgodnie z wewnętrzną procedurą, przy obecności co najmniej dwóch osób pełniących funkcje bezpośrednio związane z realizacją usług zaufania (patrz pkt 5.2.2), w tym Inspektora bezpieczeństwa.
2. Z ceremonii generowania kluczy sporządza się protokół.

6.1.2 Dostarczenie klucza prywatnego subskrybentowi

1. Para kluczy i certyfikat subskrybenta są wydawane zgodnie z zasadami w pkt 4.4. Klucze subskrybenta wraz z certyfikatem dostarczane są mu osobiście z informacjami pozwalającymi na aktywację klucza prywatnego, subskrybent ma obowiązek do niezwłocznej zmiany danych pozwalających na aktywację klucza prywatnego. Konieczna jest zmiana PIN-ów przez subskrybenta, przed rozpoczęciem okresu eksploatacji certyfikatu.
2. Subskrybenci chcący odnowić posiadany na karcie kryptograficznej wydanej przez EuroCert ważny certyfikat, mogą wygenerować zdalnie kolejną parę kluczy. Wówczas EuroCert udostępnia swoim subskrybentom dedykowaną aplikację, która tworzy klucze bezpośrednio na karcie kryptograficznej subskrybenta.

6.1.3 Dostarczenie klucza publicznego urzędowi certyfikacji

Nie dotyczy.

6.1.4 Dostarczenie klucza publicznego urzędu stronom ufającym

1. Klucze publiczne urzędu certyfikacji wydającego certyfikaty użytkownikom końcowym rozpowszechniane są tylko w postaci certyfikatów zgodnych z zaleceniem ITU-T X.509 v.3.

2. Klucz publiczny urzędu certyfikacji EuroCert COMMERCIAL ma postać certyfikatu, wydanego przez samego siebie.
3. Klucze publiczne urzędu certyfikacji rozpowszechniane są poprzez opublikowanie w ogólnie dostępnym repozytorium (patrz rozdział nr 2).

6.1.5 Rozmiary kluczy

1. Minimalne parametry algorytmów szyfrowych dopuszczonych do stosowania przez EuroCert oraz odbiorców usług certyfikacyjnych są następujące:
   a) dla algorytmu RSA:
      - minimalna długość klucza, rozumianego jako moduł p*q wynosi 2048 bitów,
      - długości liczb pierwszych p i q, składających się na moduł nie mogą się różnić więcej niż o 30 bitów;
   b) dla algorytmu ECDSA i ECGDSA:
      - minimalna długość parametru g wynosi 256 bitów,
      - minimalny współczynnik r0 wynosi 10000,
      - minimalna klasa wynosi 200.
2. Do realizacji pieczęci elektronicznej pod certyfikatem subskrybenta stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-256.
3. Klucze urzędu certyfikacji mają długość minimum 2048 bitów RSA. Klucze subskrybentów mają długość co najmniej 2048 bitów RSA.

6.1.6 Parametry generowania klucza publicznego i weryfikacja jakości

Parametry generowania klucza publicznego spełniają wymagania określone w eIDAS oraz ustawy o usługach zaufania.

6.1.7 Cel użycia kluczy

1. Zastosowanie klucza określone jest w polu KeyUsage (OID: 2.5.29.15), które stanowi jedno z podstawowych rozszerzeń certyfikatów (patrz pkt 7.1.2). Pole to podlega obligatoryjnej weryfikacji przez strony ufające oraz aplikacje korzystające z certyfikatu.
2. Klucz prywatny urzędu certyfikacji może być wykorzystywany tylko do podpisywania certyfikatów i list CRL. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów (keyCertSign) i list CRL (cRLSign).

6.2 Ochrona klucza prywatnego oraz techniczna kontrola modułu kryptograficznego

1. Każdy subskrybent, a także personel urzędu certyfikacji i operatorzy punktów rejestracji przechowują, użytkują i niszczą swój klucz prywatny w taki sposób, aby zapobiec jego:
   a) utracie,
   b) ujawnieniu,
   c) modyfikacji,
   d) nieautoryzowanemu użyciu.

6.2.1 Standardy dla modułu kryptograficznego

Polityka nie określa wymagań w tym zakresie.

6.2.2 Podział klucza prywatnego

Patrz pkt 6.2.4.

6.2.3 Deponowanie klucza prywatnego

1. Klucz prywatny urzędu certyfikacji EuroCert nie jest przekazywany (w tym powierzany) innym podmiotom.
2. EuroCert nie świadczy usług deponowania i przechowywania kluczy prywatnych subskrybentów.

6.2.4 Kopie zapasowe klucza prywatnego

1. Mechanizm zapewnienia kopii zapasowej klucza prywatnego urzędu certyfikacji jest realizowany dzięki podziałowi klucza na części (tzw. sekrety) w liczbie większej niż jest wymagana do odtworzenia klucza.
2. Przyjęta liczba podziałów klucza na sekrety oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w tab. 6.

Tab. 6. Schemat podziału klucza prywatnego

Urząd certyfikacji	Całkowita liczba sekretów [n]	Liczba sekretów koniecznych do użycia klucza [m]
EuroCert COMMERCIAL	4	3

3. Sekrety zapisywane są na kartach kryptograficznych chronionych numerem PIN znanym tylko osobie której został on przekazany podczas ceremonii generowania kluczy. Sekrety, jak też chroniące je numery PIN przechowywane są w różnych, fizycznie chronionych, miejscach. W żadnym z tych miejsc nie jest przechowywany taki zestaw kart oraz numerów PIN, który umożliwia odtworzenie klucza urzędu certyfikacji.
4. W razie konieczności odtworzenia klucza z kopii zapasowych wykonywana jest procedura wprowadzania klucza do modułu opisana w pkt 6.2.6.
5. Klucze prywatne subskrybenta związane z certyfikatami służącymi do weryfikacji podpisów elektronicznych nie mogą podlegać procedurom tworzenia kopii zapasowych.

6.2.5 Archiwizowanie klucza prywatnego

1. Klucze prywatne subskrybenta związane z certyfikatami służącymi do weryfikacji podpisów elektronicznych, klucze prywatne EuroCert służące do realizacji elektronicznych poświadczeń oraz klucze prywatne Inspektorów rejestracji służące do podpisywania zgłoszeń certyfikacyjnych nie mogą podlegać procedurom archiwizowania.
2. Klucze prywatne urzędu certyfikacji służące do realizacji elektronicznych poświadczeń nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywania przy ich użyciu operacji podpisywania lub upływie okresu ważności komplementarnego z nimi zaświadczenia certyfikacyjnego lub jego unieważnieniu.

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

1. Wprowadzanie klucza prywatnego do modułów kryptograficznych realizowane jest w sytuacjach:
   a) Uruchomienia urzędu certyfikacji, podczas startu systemu,
   b) odtworzenia klucza urzędu certyfikacji w centrum zapasowym,
   c) wymiany modułu kryptograficznego.
2. Załadowanie klucza do modułu odbywa się przy udziale posiadaczy współdzielonych sekretów. Do załadowania klucza konieczna jest obecność liczby sekretów opisana w pkt 6.2.4. Ładownie odbywa się w ramach zamkniętego środowiska bezpieczeństwa. Klucz prywatny jest składany z elementów. Podawane są kolejno fragmenty klucza tajnego z kart, zaszyfrowane pliki ładowane są do pamięci modułu i następuje ich odszyfrowanie. Klucz prywatny jest gotowy do użycia. Ładownie klucza do modułu odnotowane jest w rejestrze zdarzeń.
3. Wprowadzanie klucza prywatnego do modułu kryptograficznego jest operacją krytyczną. Z tego względu w trakcie jej realizacji stosowane są takie środki i procedury, które zapobiegają ujawnieniu klucza, jego modyfikacji lub podstawienia.

6.2.7 Przechowywanie klucza prywatnego w module kryptograficznym

1. Po rozszyfrowaniu i załadowaniu klucza prywatnego do pamięci modułu kryptograficznego jest on chroniony sprzętowo. Nie ma możliwości odczytu wartości klucza prywatnego z modułu, klucz ten nigdy modułu nie opuszcza. Operacje wymagające użycia klucza prywatnego wykonywane są w module kryptograficznym.
2. Klucz urzędu certyfikacji oraz subskrybentów przechowywane są na kartach kryptograficznych chronionych kodami PIN i PUK lub w formie plików.

6.2.8 Aktywacja klucza prywatnego

1. Klucz prywatny urzędu certyfikacji załadowany do urządzenia HSM po jego wygenerowaniu, przeniesieniu w postaci zaszyfrowanej z innego modułu lub odtworzeniu z części współdzielonych przez zaufane osoby pozostaje w stanie aktywności aż do momentu jego fizycznego usunięcia z modułu (wyjęcia karty z HSM) lub wyłączenia urządzenia HSM.
2. Klucze prywatne subskrybentów są uaktywniane dopiero po uwierzytelnieniu (podaniu numeru PIN) i tylko na czas wykonania pojedynczej operacji kryptograficznej z użyciem tego klucza. Po zakończeniu wykonywania operacji klucz prywatny jest automatycznie dezaktywowany i musi być ponownie uaktywniony przed wykonaniem kolejnej operacji niezależnie od tego czy klucze przechowywane są na karcie elektronicznej czy też na innym nośniku.

6.2.9 Dezaktywacja klucza prywatnego

1. Dezaktywowanie kluczy urzędu certyfikacji EuroCert jest wykonywane przez Inspektora bezpieczeństwa tylko w przypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego. Dezaktywowanie klucza polega na wyczyszczeniu pamięci modułu kryptograficznego z załadowanych kluczy. Każda dezaktywacja klucza prywatnego jest odnotowywana w rejestrze zdarzeń.

2. Dezaktywowanie klucza prywatnego subskrybenta następuje natychmiast po zrealizowaniu podpisu elektronicznego.

6.2.10 Metody niszczenia klucza prywatnego

1. Niszczenie kluczy prywatnych Subskrybentów wykonywane jest odpowiednio poprzez logiczne usunięcie klucza z nośnika (z karty kryptograficznej, urządzenia HSM, itp.), fizyczne zniszczenie nośnika kluczy (np. karty kryptograficznej).
2. Niszczenie klucza prywatnego urzędu certyfikacji oznacza fizyczne zniszczenie kart kryptograficznych, na których są przechowywane sekrety współdzielone lub ich bezpieczne wymazanie z nośnika (z karty kryptograficznej, sprzętowego modułu kryptograficznego, itp.).
3. Niszczenie kluczy prywatnych urzędu certyfikacji wykonywane jest komisyjnie przez personel EuroCert zgodnie z udokumentowaną procedurą. Wymagana jest obecność co najmniej dwóch osób, w tym Inspektora bezpieczeństwa oraz świadka. Wymagana jest identyfikacja kart przed zniszczeniem. Z procedury niszczenia sporządza się protokół.

6.2.11 Standardy modułu kryptograficznego

Parametry modułów kryptograficznych opisuje punkt 6.2.1.

6.3 Inne aspekty zarządzania parą kluczy

Poniższe punkty opisują aspekty związane z okresem ważności certyfikatów oraz archiwizacją kluczy.

6.3.1 Archiwizowanie kluczy publicznych

1. EuroCert prowadzi długoterminową archiwizację swoich kluczy publicznych w postaci certyfikatów, na takich zasadach, jakim podlegają inne archiwowane dane (patrz pkt 5.5).
2. Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów elektronicznych po upłynięciu okresu ważności certyfikatu urzędu certyfikacji i zakończeniu jego działalności operacyjnej.
3. Archiwizacji dokonuje Inspektor bezpieczeństwa. Archiwizacja wykonywana jest poprzez zapisanie plików z certyfikatami na zewnętrzne nośniki wymienne. Pliki archiwum opatrzone są podpisem elektronicznym Inspektora bezpieczeństwa. Szczegóły tworzenia archiwum elektronicznego zawiera pkt 5.5. Okres archiwizacji kluczy publicznych urzędu certyfikacji wynosi 20 lat.

6.3.2 Okres ważności certyfikatów i kluczy prywatnych

1. Okres ważności klucza publicznego określony w polu *validity* (patrz pkt 7.1) każdego certyfikatu. Okres ważności klucza prywatnego może być krótszy niż okres życia certyfikatu. Okres ważności certyfikatu i tym samym klucza prywatnego mogą ulec skróceniu w wyniku unieważnienia certyfikatu.

Tab. 7. Maksymalne okresy ważności certyfikatów urzędów certyfikacji

Urząd certyfikacji	Rodzaj klucza	Zastosowanie klucza	
		Certyfikaty i listy CRL	Tokeny
	Klucz prywatny	15 lat	-

Urząd certyfikacji	Rodzaj klucza	Zastosowanie klucza	
		Certyfikaty i listy CRL	Tokeny
EUROCERT COMMERCIAL	Klucz publiczny	15 lat	-

Tab. 8. Maksymalne okresy ważności certyfikatów subskrybentów

	Zastosowanie klucza	
	RSA do podpisywania wiadomości	RSA do wymiany kluczy
Certyfikat subskrybenta	5 lat	5 lat

6.4 Dane aktywujące

6.4.1 Generowanie danych aktywujących i ich instalowanie

1. Nadanie przez subskrybenta kodów PIN i PUK do zabezpieczania karty z parą kluczy oraz certyfikatem powinno być przeprowadzone z wykorzystaniem aplikacji do zarządzania kartą dostarczonej przez EuroCert wraz z kartą.

6.4.2 Ochrona danych aktywujących

1. Nadany przez subskrybenta kod PIN oraz PUK powinny być znane tylko subskrybentowi. Za ochronę kodów PIN i PUK do karty o odpowiada subskrybent. Ujawnienie kodów PIN i PUK powinno być przesłanką do żądania zawieszenia lub unieważnienia certyfikatu.

6.4.3 Inne aspekty związane z danymi aktywującymi

1. Kopie haseł do zabezpieczania dostępu do karty kryptograficznej nie są przechowywane w EuroCert. EuroCert nie posiada żadnych kodów lub danych umożliwiających odtworzenie kodów PIN i PUK zabezpieczających dostęp do karty nadanych przez subskrybenta.
2. Uaktywnienie klucza urzędu certyfikacji opisane jest w rozdziałach 6.2.4 i 6.2.8.

6.5 Zabezpieczenia komputerów

1. Ocena bezpieczeństwa pojedynczego komputera oraz zainstalowanego na nim oprogramowania prowadzona jest w oparciu o wymagania norm, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016r. ustanawiającej normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 eIDAS.

6.5.1 Wymagania dotyczące zabezpieczeń systemów komputerowych

1. Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania w punktach rejestracji. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.
2. Komputery pracujące w EuroCert wyposażone są w następujące funkcje zabezpieczające:
   a) obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),

b) uznaniową kontrolę dostępu,
c) możliwość prowadzenia audytu zabezpieczeń,
d) komputery udostępniane są tylko personelowi, który pełni zaufane role w EuroCert,
e) pracownik, który pełni zaufaną role jest zobowiązany do blokowania swojej stacji roboczej zawsze, jeśli pozostają one poza jego nadzorem,
f) wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
g) wymuszanie wylogowania użytkownika po okresie bezczynności,
h) identyfikację i uwierzytelnienie ról oraz pełniących je osób,
i) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
j) archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
k) bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
l) mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
m) mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

6.5.2 Ocena bezpieczeństwa systemów komputerowych

Ocena bezpieczeństwa systemów komputerowych prowadzona jest w oparciu o wymagania eIDAS.

6.6 Cykl życia zabezpieczeń technicznych

6.6.1 Kontrola zmian w systemie

1. Nadzór nad wprowadzaniem modyfikacji lub zmian w systemie EuroCert sprawuje Inspektor bezpieczeństwa. Zatwierdza on konfigurację systemu oraz wszelkie zmiany oprogramowania i sprzętu. Testy nowych wersji oprogramowania i/lub wykorzystanie do tego celu istniejących baz danych odbywa się w środowisku testowym. Zasady stosowane przez EuroCert podczas przeprowadzania tych testów gwarantują nieprzerwaną pracę systemu EuroCert, integralność jego zasobów oraz zachowanie poufności danych.

6.6.2 Kontrola zarządzania bezpieczeństwem

1. Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania systemu EuroCert, które daje pewność, że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.

2. Mimo, że prace administracyjne oraz zmiany w systemach EuroCert są rejestrowane, to każda z nich wymaga dodatkowo zweryfikowania i akceptacji przez przynajmniej dwóch administratorów EuroCert. System kontroli zmiany informuje uprawnionych pracowników o wystąpieniu modyfikacji w systemie EuroCert i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.

3. Aktualna konfiguracja systemu EuroCert, jak również dowolne modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w systemie EuroCert mechanizmy

pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia.

6.6.3 Kontrola cyklu życia zabezpieczeń

1. Polityka nie narzuca cyklu życia stosowanych zabezpieczeń. Zabezpieczenia są wymieniane w przypadku zaistnienia potrzeby zastosowania innych niż obecnie używane, zmian w regulacjach prawnych lub jeśli są technologicznie przestarzałe i nie odpowiadają bieżącym normom i standardom.

6.7 Zabezpieczenia sieci komputerowej

1. Dostęp do systemu EuroCert, w ramach którego świadczone są usługi zaufania, jest zabezpieczony na poziomie określonym dla świadczenia kwalifikowanych usług zaufania polegających na wydawaniu certyfikatów przez kwalifikowanego dostawce tych usług.
2. Nadzór nad bezpieczeństwem sieci komputerowych EuroCert sprawują specjaliści EuroCert.

6.8 Znakowanie czasem

1. Wszystkie zegary funkcjonujące w ramach systemu EuroCert i wykorzystywane w trakcie świadczenia usług certyfikacyjnych są synchronizowane z międzynarodowym wzorcem czasu (Coordinated Universal Time), z dokładnością do 1 sekundy. Zsynchronizowane są za pomocą protokołu NTP z serwerem czasu. Wzorcowy czas pobierany jest za pośrednictwem satelitarnych systemów nawigacyjnych GPS.

7 Profil certyfikatów i list CRL

1. Profile certyfikatów i list CRL są zgodne z zaleceniami odpowiednio normy ITU-T X.509 v3 oraz ITU-T X.509 v2 a także profilami zawartymi w: ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Parts 1,2,5.
2. Przedstawione w niniejszym rozdziale informacje przedstawiają znaczenie poszczególnych pól certyfikatów oraz list CRL.

7.1 Profil certyfikatów

1. Zgodnie z normą X.509 v3 certyfikat jest sekwencją wartości pól podstawowych przedstawionych w tabeli 9 oraz rozszerzeń o których mowa w pkt 7.1.2.

Tab. 9. Podstawowe pola certyfikatu

Nazwa pola	Opis	Wartość
Version	certyfikat zgodny z wersją 3 standardu X.509.	V3
Serial Number	Jednoznaczny w ramach urzędu certyfikacji EuroCert numer certyfikatu.	numer certyfikatu zapisany w formie ciągu liczb
Signature Algorithm	identyfikator algorytmu kryptograficznego,stosowanego do realizacji pieczęci elektronicznej przez urząd certyfikacji na certyfikacie subskrybenta	Jeden z pośród poniższych: sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13); ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4);

Nazwa pola	Opis	Wartość	
Issuer (nazwa wyróżniająca – DN) wystawcy certyfikatu)	Common Name	CN = nazwa urzędu certyfikacji	
	Organization	O = EuroCert Sp. z o.o.	
	Country	C = PL	
	Organization Identifier	2.5.4.97 = VATPL-9512352379	
Not Before	Początek okresu ważności	data wystawienia certyfikatu	
Not After	Koniec okresu ważności	data wygaśnięcia certyfikatu	
Subject	Nazwa subskrybenta zgodna z wymaganiami określonymi w ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1,2,5.	Identyfikator DN Subskrybenta (patrz pkt 3.1). Wszystkie atrybuty tego pola są opcjonalne, z wyjątkiem pola mailAddress	
Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 5280 i może zawierać informacje o kluczach publicznych RSA lub ECDSA (tzn. o identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego).	Public Key Algorithm (algorytm klucza publicznego)	Jeden spośród poniższych: sha512WithRSAEncryption; ecdsa-with-SHA512
		RSA Public Key (długość klucza)	min. 2048 bit
Signature Value	Pieczęć elektroniczna składana na certyfikacie przez urząd certyfikacji.	Wartość pola signatureValue jest wynikiem zastosowania algorytmu funkcji skrótu do wszystkich pól certyfikatu, określonych przez pola jego treści (tbsCertificate) i następnie zaszyfrowania wyniku przy pomocy klucza prywatnego urzędu certyfikacji (wystawcy).	

7.1.1 Wersja certyfikatu

Certyfikaty wystawiane są zgodnie z wersją nr 3 standardu X.509.

7.1.2 Rozszerzenia certyfikatu

1. Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być krytyczne lub niekrytyczne. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać. Z kolei każde niekrytyczne rozszerzenie może być ignorowane. Stosowane przez EuroCert pola rozszerzeń zostały opisane w tab. 10.

Tabela 10. Rozszerzenia certyfikatu

Nazwa rozszerzenia	Krytyczne ?	Opis	Wartość
AuthorityKeyIdentifier	NIE	identyfikator klucza publicznego wystawcy służącego do weryfikacji wydanego certyfikatu	160 bitowy skrót SHA-1/ 512 bitowy skrót SHA-512 z wartości klucza publicznego certyfikatu wystawcy.
SubjectKeyIdentifier	NIE	Identyfikator certyfikatu zawierający skrót klucza publicznego zawartego w certyfikacie	160 bitowy skrót SHA-1/ 512 bitowy skrót SHA-512 z wartości klucza publicznego certyfikatu wystawcy.
KeyUsage	TAK	określa zakres wykorzystania klucza publicznego subskrybenta. W przypadku certyfikatów kwalifikowanych ograniczone do niezaprzeczalności.	digitalSignature, contentCommitment, keyEncipherment, dataEncipherment, keyAgreement

Nazwa rozszerzenia	Krytyczne ?	Opis	Wartość
CertificatePolicies	NIE	wskazanie na politykę certyfikacji, zgodnie z którą wystawiony jest certyfikat	Identyfikator polityki certyfikacji: 1.2.616.1.113791.2.1.
CRLDistributionPoints	NIE	punkt dystrybucji listy CRL (określa adres URL, pod którymi jest publikowana aktualna lista CRL)	http://nqcrl.eurocert.pl/nqca01.crl
Authority Info Access	NIE	Dostęp do informacji o urzędzie	Adres URL certyfikatu głównego EUROCERT COMMERCIAL
BasicConstraints	TAK	umożliwia sprawdzenie czy podmiot certyfikatu jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak

7.1.3 Identyfikatory algorytmu

1. Identyfikatory algorytmów kryptograficznych stosowanych do realizacji pieczęci elektronicznej składanej przez urząd certyfikacji na certyfikacie:
   a) sha512WithRSAEncryption OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 },
   b) ecdsa-with-sha512 OBJECT IDENTIFIER::= {iso(1) member-body(2) us(840) ansi-x962(10045) signatures(4) ecdsa-with-SHA2(3) ecdsa-with-SHA512(4)}.

7.1.4 Formy nazw

Nazwy wystawcy certyfikatu oraz subskrybenta certyfikatu zawarte odpowiednio w polu issuer oraz w polu subject są zgodne z zasadami opisanymi w pkt 3.1.2.

7.1.5 Ograniczenia nakładane na nazwy

Polityka nie określa wymagań w tym zakresie.

7.1.6 Identyfikatory polityk certyfikacji

Certyfikat zawiera informację typu Policy Information (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez dany organ wydający certyfikaty – rozszerzenie nie jest krytyczne.

7.1.7 Zastosowanie rozszerzeń niedopuszczalnych w polityce certyfikacji

Polityka nie określa wymagań w tym zakresie.

7.1.8 Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

Polityka nie określa wymagań w tym zakresie.

7.2 Profil listy CRL

1. Lista unieważnionych i zawieszonych certyfikatów jest zbiorem pól, których znaczenie przedstawiono poniżej w tabeli 11.

Tabela 11. Profil listy CRL w formacie zgodnym ze standardem X.509 V2

Atrybut	Wartość
Version	V2
Signature Algorithm identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji pieczęci elektronicznej przez urząd certyfikacji na liście CRL)	Jeden z pośród poniższych: sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13); ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4);
Issuer Identyfikator wystawcy listy CRL, zgodny z identyfikatorem określonym w profilu certyfikatu	Patrz tabela 9 (Issuer)
thisUpdate	data i godzina wydania listy
nextUpdate	data i godzina następnego wydania listy
SignatureValue	Pieczęć elektroniczna wystawcy listy CRL
revokedCertificates (lista odwołanych certyfikatów) userCertificate revocationDate reasonCode	 numer seryjny unieważnionego certyfikatu data i godzina unieważnienia certyfikatu przyczyna umieszczenia certyfikatu na liście CRL: a) unspecified – nieokreślona, b) keyCompromise – kompromitacja klucza, c) caCompromise - kompromitacja klucza CA, d) affiliationChanged – zmiana danych Subskrybenta, e) superseded – zastąpienie (wymiana) klucza, f) cessationOfOperation – zaprzestanie używania certyfikatu do celu, w jakim został wydany, g) certificateHold – certyfikat został zawieszony.
Extensions	Zbiór rozszerzeń określających dodatkowe informacje związane z wykorzystaniem certyfikatu. Pełen zbiór dopuszczalnych rozszerzeń znajduje się w pkt 7.2.2.

7.2.1 Wersja listy CRL

Listy CRL są zgodne z wersją nr 2 standardu X.509.

7.2.2 Obsługiwane rozszerzenia dostępu do listy CRL

1. Spośród wielu rozszerzeń CRL najbardziej istotne są dwa, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL (pole authorityKeyIdentifier)), zaś drugie (pole cRLNumber) zawiera monotonicznie zwiększany numer listy CRL, wydawanej przez urząd certyfikacji (dzięki temu rozszerzeniu użytkownik listy jest w stanie określić, kiedy jakiś CRL zastąpił inny CRL). Funkcje oraz sens rozszerzeń są takie same jak w przypadku rozszerzeń certyfikatu (patrz pkt 7.1.2).

7.3 Profil OCSP

Polityka nie określa wymagań w tym zakresie.

8 Audyt zgodności i inne oceny

1. Audyty są przeprowadzane w EuroCert w celu sprawdzenia zgodności postępowania EuroCert z wymaganiami nałożonymi na dostawców usług zaufania określonych w eIDAS oraz procedurami i procesami opisanymi w niniejszej Polityce oraz wewnętrznej dokumentacji EuroCert.

8.1 Częstotliwość i okoliczności oceny

1. Audyt przeprowadzany jest samodzielnie przez EuroCert (audyt wewnętrzny) zgodnie z wewnętrzną polityką audytu lub raz na 2 lata przez zewnętrzną jednostkę oceniającą zgodność na podstawie art. 20 ust. 1 EIDAS (audyt zewnętrzny).
2. Audyt zewnętrzny może być dokonany również w każdym momencie na wniosek Organu Nadzoru w trybie art. 31 Ustawy o usługach zaufania w związku z art. 20.2 i 17.4 pkt e) EIDAS.

8.2 Tożsamość i kwalifikacje audytora

1. Audyt zewnętrzny wykonywany jest przez upoważnioną do tego rodzaju działalności i niezależną od EuroCert instytucję krajową lub europejską posiadającą akredytację do przeprowadzania audytów zgodności dostawców usług zaufania spełniającą wymogi określone w normie ETSI EN 319 403.

8.3 Związek audytora z audytowaną jednostką

1. Audytorzy nie mogą prowadzić działalności gospodarczej w zakresie świadczenia usług zaufania, świadczyć usług zaufania, być wspólnikami albo akcjonariuszami dostawcy usług zaufania ani wykonywać obowiązków osoby reprezentującej lub członka rady nadzorczej albo komisji rewizyjnej tego dostawcy, a także pozostawać z tym dostawcą w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze.

8.4 Zagadnienia objęte audytem wewnętrznym

1. Do zagadnień objętych audytem należą:
   a) sprawdzenie wymagań organizacyjno-prawnych wynikających z EIDAS i wydanymi decyzjami wykonawczymi do niego,
   b) monitorowanie i zapewnianie zgodności działalności z procedurami,
   c) procedury weryfikacji tożsamości subskrybentów,
   d) zabezpieczenia fizyczne EuroCert,
   e) zarządzanie bezpieczeństwem informacji,
   f) bezpieczeństwo personelu,
   g) usługi certyfikacyjne i procedury ich świadczenia,
   h) zabezpieczenia oprogramowania i dostępu do sieci,
   i) rejestry zdarzeń i procedury monitorowania systemu,
   j) procedury sporządzania kopii zapasowych oraz ich odtwarzania,
   k) realizacja procedur archiwizacji,
   l) dokumentowanie zmian parametrów konfiguracyjnych EuroCert,
   m) dokumentowanie przeglądów i serwisu sprzętu oraz oprogramowania.

8.5 Działania podejmowane celem realizacji zaleceń poaudytowych

1. Raporty audytów wewnętrznych i zewnętrznych przekazywane są osobom zarządzającym EuroCert, które powołują zespół składający się z pracowników wymienionych w pkt 5.2.1 w celu przygotowania w terminie określonym w raporcie pisemnego stanowiska EuroCert wobec wszelkich uchybień wskazanych w raportach oraz zaleceń zawartych w raportach. Odpowiedź musi określić także sposoby i terminy usunięcia usterek i realizacji zaleceń. Informacja o usunięciu usterek i realizacji zaleceń przekazywana jest instytucji audytującej.
2. W przypadku audytu zleconego przez ministra właściwego do spraw informatyzacji minister po zapoznaniu się z protokołem i zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez EuroCert powiadamia ten podmiot o wynikach kontroli i w razie stwierdzenia nieprawidłowości wyznacza termin ich usunięcia, nie krótszy niż 14 dni (Art. 34 Ustawy o usługach zaufania).

8.6 Informowanie o wynikach audytu

Informacje o wynikach audytu w postaci raportu z jego przeprowadzenia lub podsumowania z takiego raportu są udostępniane wyłącznie wewnętrznie.

9 Inne postanowienia (biznesowe, prawne itp.)

9.1 Opłaty

Z tytułu świadczonych usług zaufania EuroCert pobiera opłaty według cennika publikowanego na stronie internetowej https://sklep.eurocert.pl.

9.1.1 Opłaty za wydanie certyfikatu i jego odnowienie

EuroCert pobiera opłaty za wydanie certyfikatu i jego odnowienie.

9.1.2 Opłaty za dostęp do certyfikatów

Eurocert nie pobiera opłat za dostęp do certyfikatów.

9.1.3 Opłaty za unieważnienie lub informacje o statusie certyfikatu

EuroCert nie pobiera opłat za unieważnianie certyfikatów oraz udostępnianie list CRL.

9.1.4 Inne opłaty

EuroCert może pobierać także inne opłaty, o ile zostaną one wprowadzone do cennika. Mogą to być opłaty m.in. za:

a) szkolenia i konsultacje,
b) karty,
c) czytniki,
d) licencje na oprogramowanie,
e) realizację prac projektowych, wdrożeniowych i instalacyjnych.

9.1.5 Zwrot opłat

Zwrot opłat jest dopuszczalny na podstawie przepisów polskiego prawa, w przypadku niewywiązywania się EuroCert z umowy lub wykonanie usługi niezgodnie z postanowieniami Polityki.

9.2 Odpowiedzialność finansowa

9.2.1 Polisa ubezpieczeniowa

1. EuroCert sp. o.o. posiada ubezpieczenie odpowiedzialności cywilnej zgodne z wymaganiami Rozporządzenia Ministra Rozwoju i Finansów z dnia 19 grudnia 2016 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego dostawcy usług zaufania.
2. Odpowiedzialność finansowa EuroCert, w stosunku do jednego zdarzenia wynosi równowartość w złotych 250 000 Euro, ale nie więcej niż 1 000 000 Euro w odniesieniu do wszystkich takich zdarzeń.

9.2.2 Inne aktywa

EuroCert posiada wystarczające środki finansowe niezbędne do prowadzenia działalności oraz wywiązywania się ze swoich obowiązków.

9.2.3 Rozszerzony zakres gwarancji

Polityka nie określa żadnych wymagań w tym zakresie.

9.3 Poufność informacji biznesowej

EuroCert i osoby w niej zatrudnione, bądź podmioty działające w jej imieniu są obowiązane do zachowania w tajemnicy wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich wykonywania.

9.3.1 Zakres informacji poufnych

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

9.3.2 Informację nie będące informacjami poufnymi

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

9.3.3 Ochrona informacji poufnych

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

9.4 Ochrona danych osobowych

1. Dane osobowe przekazywane EuroCert przez subskrybentów usług certyfikacyjnych oraz zamawiających certyfikaty objęte są ochroną określoną przez Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

9.4.1 Zasady prywatności

1. Wszelkie dane osobowe (w szczególności dane subskrybentów) będące w posiadaniu EuroCert są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującymi w tym zakresie przepisami prawa, a w szczególności Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

9.4.2 Informacje traktowane jako prywatne

1. EuroCert klasyfikuje informacje na cztery klasy ochrony (od 0 – jawnych , poprzez 1 – do użytku służbowego i 2 – chronione do 3 – poufne firmowe). Informacje klas ochrony od 1 do 3 nazywamy dla potrzeb niniejszej polityki poufnymi.
2. Klasa ochrony danych określa tryb i sposób ich ochrony oraz sposób postępowania z danymi.
3. Do danych jawnych (publicznie dostępnych) zaliczane są:
   a) Polityka,
   b) Certyfikaty urzędu certyfikacji,
   c) Listy CRL,
   d) Informacje bieżące, przeznaczone do publikacji (takie jak cennik usług, oferta handlowa, bieżące komunikaty, dane kontaktowe),
   e) Informacje zawarte w treści certyfikatu, na publikację których zgodę wyraził subskrybent.
4. Stronom trzecim udostępniane są tylko te informacje, które są publicznie dostępne w certyfikacie i na których opublikowanie zgodę wyraził subskrybent.

9.4.3 Informacje nie traktowane jako prywatne

1. Informacjami jawnymi są wszystkie informacje nieoznaczone jako poufne przez subskrybentów, osoby ufające lub EuroCert. Za informacje jawne, nie objęte poufnością, uznaje się dane wpisane do certyfikatu.
2. Wszystkie informacje, które są niezbędne w procesie prawidłowego funkcjonowania usług certyfikacyjnych uważane są za informacje jawne. W szczególności za informacje jawne uważa się te informacje, które umieszczane są w certyfikacie przez organy wydające certyfikaty zgodnie z opisem przedstawionym w rozdz. 7. Subskrybent występując z wnioskiem o wydanie certyfikatu wyraża zgodę na upublicznienie informacji zawartej w certyfikacie.
3. Część informacji wpływających i przekazywanych od/do użytkowników może być udostępniana innym podmiotom wyłącznie za zgodą użytkownika.

9.4.4 Odpowiedzialność za ochronę informacji prywatnej

1. EuroCert Sp. z o.o., ul. Puławska 474, 02-884 Warszawa jest administratorem danych osobowych subskrybenta, w rozumieniu art. 7 pkt 4 ustawy o ochronie danych osobowych, i ponosi odpowiedzialność za ochronę danych osobowych oraz innych powierzonych mu informacji poufnych.

9.4.5 Zastrzeżenia i zezwolenie na użycie informacji prywatnej

1. EuroCert może, zgodnie z wymogami ustawy o ochronie danych osobowych, powierzyć do przetwarzania danych osobowych podmiotowi trzeciemu.

9.4.6 Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

1. EuroCert jest zobowiązany, zgodnie z wymogami prawa o ochronie danych osobowych, do udostępniania danych osobowych podmiotom, które mogą przedstawić takie żądanie na podstawie bezwzględnie obowiązujących przepisów prawa.

9.4.7 Inne okoliczności ujawniania informacji

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

9.5 Zabezpieczenie własności intelektualnej

1. Prawa autorskie do niniejszej Polityki posiada EuroCert Sp. z o.o. Polityka może być wykorzystywana wyłącznie w celu korzystania z certyfikatów. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga pisemnej zgody EuroCert Sp. z o.o., przy czym EuroCert Sp. z o.o. wyraża zgodę na powielanie i publikowanie w całości niniejszego dokumentu pod warunkiem nie wprowadzania jakichkolwiek zmian.
2. Subskrybent ponosi pełną odpowiedzialność za podane przez niego dane zawarte w certyfikacie. EuroCert nie weryfikuje prawa do posługiwania się zastrzeżonymi znakami towarowymi, nie odpowiada za nieuprawnione wykorzystywanie znaków towarowych i nie jest stroną w przypadku tego typu sporów. W przypadku utraty przez subskrybenta prawa do posługiwania się daną nazwą lub innym oznaczeniem zamieszczonym w certyfikacie, jest on zobowiązany do zgłoszenia tego faktu celem unieważnienia certyfikatu z powodu nieaktualności danych zawartych w certyfikacie.
3. Certyfikat EUROCERT COMMERCIAL jest własnością EuroCert Sp. z o.o. EuroCert udziela licencji na tworzenie kopii tego certyfikatu i umieszczanie jej w oprogramowaniu, w szczególności w magazynach certyfikatów lub sprzęcie wytwórcom oprogramowania lub sprzętu.
4. Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez EuroCert jest – w przypadku subskrybenta certyfikatu osobistego – własnością podmiotu tego certyfikatu, określonego w polu subject certyfikatu (patrz pkt 7.1.1) lub – w przypadku subskrybenta certyfikatu firmowego – własnością podmiotu reprezentowanego przez subskrybenta.

9.6 Oświadczenia i gwarancje

9.6.1 Zobowiązania i gwarancje EuroCert

1. EuroCert gwarantuje, że:
   a) do generowania kluczy subskrybenta wykorzystuje wiarygodny sprzęt zgodnie z normami, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r., ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 eIDAS,
   b) postępuje zgodnie z prawem, a w szczególności nie narusza postanowień EIDAS, Ustawy o usługach zaufania wraz z przepisami wykonawczymi oraz nie narusza praw autorskich i licencyjnych stron trzecich,

c) świadczone usługi są zgodne z powszechnie akceptowanymi normami i standardami, m.in.:
   - ITU-T X.509 (odpowiada jej norma ISO/IEC 9594-8),
   - ISO/IEC 15945 (protokół CMP),
   - *de facto* PKCS#10, PKCS#7, PKCS#12,
   - ETSI EN 319 401,
   - ETSI EN 319 411-1,
   - ETSI EN 319 411-2,
   - ETSI EN 319 412-1,
   - ETSI EN 319 412-2,
   - ETSI EN 319 412-5;
d) przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym dokumencie,
e) wystawiane certyfikaty zawierają dane zgodne z prawdą oraz że dane te były aktualne w momencie ich potwierdzania,
f) wystawiane certyfikaty nie zawierają żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty,
g) nazwy wyróżnione (DN) subskrybentów umieszczane w certyfikatach są unikalne,
h) zapewnia ochronę danych osobowych subskrybenta zgodnie z Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późn. zm. oraz dokumentami wykonawczymi do tej ustawy,
i) nie kopiuje, ani nie przechowuje kluczy prywatnych swoich klientów, służących do składania podpisów elektronicznych,
j) zatrudnia pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługami certyfikacyjnymi, w tym w szczególności obejmujących dziedziny:
   - automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
   - mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
   - kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego,
   - sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.

9.6.2 Zobowiązania i gwarancje punktu rejestracji

1. Punkty rejestracji oraz osoby potwierdzające tożsamość zobowiązują do:
   a) przestrzegania procedur potwierdzania tożsamości przy wydawaniu certyfikatów zgodnie z zasadami określonymi w niniejszym dokumencie, procedurach wewnętrznych oraz w obowiązujących przepisach prawa i zasadach współżycia społecznego ze szczególnym uwzględnieniem dochowania należytej staranności,
   b) wydawania koniecznych tokenów zgłoszenia certyfikacyjnego, upoważniających do skorzystania z określonej usługi EuroCert,
   c) przesyłania do EuroCert potwierdzonych danych subskrybentów,
   d) podporządkowania się w całości zaleceniom EuroCert,
   e) ochrony kluczy prywatnych operatorów punktu rejestracji,
   f) nie używania kluczy prywatnych operatorów do innych celów niż tych, które określono w niniejszej Polityce,

g) poddawania się planowym audytom przeprowadzonym lub zleconym przez EuroCert.

2. Obowiązki subskrybentów i stron ufających przedstawiono odpowiednio w pkt 4.5.1 i pkt 4.5.2

9.6.3 Zobowiązania i gwarancje subskrybenta

Patrz: pkt 4.5.1.

9.6.4 Zobowiązania i gwarancje strony ufającej

Patrz: pkt 4.5.2.

9.6.5 Zobowiązania i gwarancje innych podmiotów

Niniejsza Polityka nie określa żadnych wymagań w tym zakresie.

9.7 Wyłączenia odpowiedzialności z tytułu gwarancji

1. EuroCert nie odpowiada za jakiekolwiek szkody, które powstały lub mogły powstać dla odbiorców usług certyfikacyjnych lub osób trzecich, wynikające z przyczyn innych niż niewykonanie lub nienależyte wykonanie obowiązków przez EuroCert lub podmioty działające w jego imieniu. W szczególności EuroCert nie odpowiada za skutki naruszenia obowiązków nałożonych na subskrybenta i strony ufające, wymienionych odpowiednio w pkt 4.5.1 oraz 4.5.2.
2. W szczególnych przypadkach EuroCert nie odpowiada również szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków, jeśli niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności.

9.8 Ograniczenia odpowiedzialności

EuroCert nie odpowiada za szkody wynikające z nieprzestrzegania obowiązków nałożonych na odbiorców jego usług, wymienionych odpowiednio w pkt 4.5.1 oraz 4.5.2.

9.9 Przenoszenie roszczeń odszkodowawczych

1. EuroCert może domagać się zadośćuczynienie od subskrybenta za poniesione przez EuroCert szkody w wyniku podania przez subskrybenta fałszywych danych, które – mimo zachowania przez EuroCert należytej staranności – umieszczone zostały w wydanym certyfikacie klucza publicznego.

9.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji

9.10.1 Okres obowiązywania

Niniejszy dokument obowiązuje od momentu nadania mu statusu obowiązujący i opublikowania w repozytorium EuroCert, do momentu opublikowania kolejnej obowiązującej wersji.

9.10.2 Wygaśnięcie ważności

Kolejna opublikowana wersja Polityki wskazuje datę jej obowiązywania, która jest jednocześnie datą zakończenia obowiązywania obecnej Polityki. Tym samym poprzednia Polityka traci status – obowiązująca.

9.10.3 Skutki wygaśnięcia ważności dokumentu

Subskrybenci przestrzegają tylko aktualnej Polityki.

9.11 Określanie trybu i adresów doręczania pism

Wszelkie pisma związane z działalnością EuroCert powinny być dostarczane pod adres podany w pkt 1.5.

9.12 Wprowadzanie zmian w dokumencie

9.12.1 Procedura wprowadzania zmian

Patrz: pkt 1.5.4.

9.12.2 Sposób powiadamiania o zmianach

Nie dotyczy.

9.12.3 Okoliczności wymagające zmiany identyfikatora OID

1. Zmiana identyfikatora (OID) Polityki może nastąpić jedynie w przypadku zmiany podmiotu zarządzającego urzędem certyfikacji EUROCERT COMMERCIAL oraz w przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę subskrybentów.

9.13 Rozstrzyganie sporów

1. Przedmiotem rozstrzygania sporów mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania certyfikatu w oparciu o regulacje Polityki oraz zawartych umów.
2. Spory bądź zażalenia powstałe na tle użytkowania certyfikatów wystawianych przez EuroCert, będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Postępowanie ze skargami jest zastrzeżone do wyłącznego działania Prezesa Zarządu. Podlegają one pisemnemu rozpatrzeniu w terminie do 10 dni.
3. Spory związane z usługami zaufania świadczonymi przez EuroCert będą w pierwszej kolejności rozstrzygane na drodze postępowania pojednawczego.
4. W przypadku braku rozstrzygnięcia sporu w terminie 30 dni od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sądem właściwym do rozpoznania sprawy będzie Sąd Powszechny właściwy dla pozwanego.
5. W przypadku wystąpienia innych sporów będących konsekwencją użycia certyfikatu wydanego lub innych usług świadczonych przez EuroCert, subskrybent zobowiązuje się pisemnie poinformować EuroCert o przedmiocie powstałego sporu.

9.14 Obowiązujące prawo

1. Funkcjonowanie EuroCert oparte jest na zasadach zawartych w Polityce oraz obowiązujących przepisach prawa. W celu interpretacji terminów zawartych w Polityce należy je rozpatrywać zgodnie z eIDAS i Ustawą o usługach zaufania.

9.15 Zgodność z obowiązującym prawem

1. Zasady działania EuroCert są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:
   a) Rozporządzeniu Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. oraz wydanymi na podstawie tego rozporządzenia decyzjami wykonawczymi Komisji (UE),
   b) Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej,
   c) Ustawie z dnia 29 sierpnia 1997 o ochronie danych osobowych,
   d) Ustawie z dnia 6 czerwca 1997 Kodeks karny,
   e) Ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych,
   f) Ustawie z dnia 13 lipca 2006 r. o dokumentach paszportowych,
   g) Ustawie z dnia 12 grudnia 2013 r. o cudzoziemcach,
   h) Ustawie z dnia 4 lutego 1994 Prawo autorskie.

9.16 Przepisy różne

9.16.1 Kompletność warunków umowy

Strony obowiązują postanowienia Umowy i Polityki.

9.16.2 Cesja praw

1. Żaden podmiot trzeci nie może wstąpić w prawa i obowiązki strony Umowy bez zgody drugiej strony. W przypadku zakończenia działalności w zakresie świadczenia usług objętych niniejszą dokumentem EuroCert może przenieść uprawnienia do korzystania z klucza prywatnego i wydawania oraz publikowania listy CRL na inny podmiot bez zgody zamawiającego, subskrybenta czy strony ufającej.

9.16.3 Rozłączność postanowień

1. W razie wątpliwości lub nie dającej się usunąć sprzeczności pomiędzy postanowieniami Umowy i Polityki pierwszeństwo stosowania ma Umowa przed Polityką.
2. W razie niezgodności z prawem postanowień któregokolwiek z powyższych dokumentów skutkujących ich nieważnością, pozostają w mocy niewadliwe postanowienia zawarte w pozostałych dokumentach.

9.16.4 Klauzula wykonalności

1. Czasowe niewykonywanie uprawnień EuroCert, jak również niekorzystanie z nich w stosunku do jednego lub wielu subskrybentów, nie może być interpretowane jako zrzeczenie się, czy trwałe odstąpienie od korzystania z nich i pozostaje bez wpływu na treść i interpretację Polityki.

9.16.5 Siła wyższa

1. Okoliczności siły wyższej rozumiane są jako wszelkie nadzwyczajne zdarzenia o charakterze zewnętrznym, niemożliwe do przewidzenia, takie jak katastrofy, pożary, powodzie, wybuchy, niepokoje społeczne, działania wojenne, akty władzy państwowej, awaria zasilania energią elektryczną lub łącza telekomunikacyjnego, które w części lub w całości uniemożliwiają wykonanie zobowiązań zawartych w Umowie lub Polityce albo utrudniają wykonanie tych zobowiązań na warunkach w nich określonych. Eurocert nie będzie odpowiedzialny za jakiekolwiek naruszenie swoich obowiązków, jeśli będzie to wynikiem działań siły wyższej.

9.17 Inne postanowienia

Nie występują.

10 Metryczka dokumentu

Informacje ogólne		
Sygnatura		0-PT-013-02
Klasa ochrony		0 – Jawne
Status		obowiązująca
Historia zmian		
Data zatwierdzenia	Wersja	Dokonane zmiany
01.12.2017	1	Powstanie dokumentu
02.06.2020	2	Zmian częstotliwości publikacji listy CRL oraz wprowadzenie metody weryfikacji tożsamości poprzez wideo-weryfikację.