EuroCert Sp. z o.o.
Centrum EUROCERT

Polityka certyfikacji

dla kwalifikowanych certyfikatów

Wersja 3.0
Data: 15.11.2017
Status: nieaktualna

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

SPIS TREŚCI

1 Wstęp

Polityka certyfikacji dla kwalifikowanych certyfikatów, zwana dalej „Polityką", określa zasady stosowane przez jednostkę organizacyjną EuroCert Sp. z o.o. o nazwie Centrum EuroCert (dalej „EuroCert") podczas świadczenia usług zaufania polegających na wydawaniu kwalifikowanych certyfikatów służących do weryfikacji kwalifikowanych podpisów elektronicznych, unieważnianiu lub zawieszaniu certyfikatów oraz weryfikowaniu statusu certyfikatów w trybie on-line.

EuroCert działa zgodnie z prawem obowiązującym na terytorium Rzeczypospolitej Polskiej, zasadami obowiązującymi kwalifikowanych dostawców usług zaufania, określonymi w Rozporządzeniu eIDAS, Ustawie o usługach zaufania, Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiającej normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 Rozporządzenia eIDAS oraz w zgodzie z niniejszą Polityką.

EuroCert jest kwalifikowanym dostawcą usług zaufania, wpisanym do rejestru kwalifikowanych dostawców usług zaufania pod numerem 13 na podstawie Decyzji Ministerstwa Gospodarki nr 1/10573-13/13 z dnia 23 grudnia 2013 r.

Polityka stosuje się dla urzędu certyfikacji: „Centrum Kwalifikowane EuroCert", po aktualizacji certyfikatu dostawcy usług zaufania z dnia 14.02.2017 r. dokonanego zgodnie z art. 10 ust. 1 § 1 i 2 w zw. z art. 4 ust. 1 § 2 ustawy o usługach zaufania. Poprzedni certyfikat dostawcy usług zaufania będzie stosowane jedynie w celu tworzenia i publikowania list certyfikatów unieważnionych w okresie do dnia 15.01.2019 r.

Z Polityką ściśle związany jest Kodeks postępowania certyfikacyjnego, który definiowany jest jako deklaracja procedur stosowanych przez urząd certyfikacji w procesie wydawania certyfikatów oraz świadczenia dodatkowych usług.

Struktura niniejszego dokumentu została stworzona na podstawie zaleceń RFC 3647 „Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework[1]".

1.1 Wprowadzenie

Polityka opisuje zakres działania EuroCert oraz związanych z nim punktów rejestracji, subskrybentów, jak również stron ufających. Polityka definiuje również strony biorące udział w procesie świadczenia kwalifikowanych usług certyfikacyjnych przez EuroCert, ich obowiązki i odpowiedzialność, typy certyfikatów oraz obszary ich zastosowań oraz procedury weryfikacji tożsamości subskrybentów.

Do zasad przedstawionych w tym dokumencie dostosowane powinny być działania tych podmiotów i dostawców usług, którzy korzystają z certyfikatów wystawionych przez EuroCert.

1.2 Identyfikator i nazwa dokumentu

Polityce przypisuje się nazwę własną oraz zarejestrowany identyfikator obiektu (ang. Object Identifier – OID), które przedstawiono w tab.1.

Tab. 1. Karta dokumentu

Nazwa własna	Polityka certyfikacji dla kwalifikowanych certyfikatów
Właściciel	EuroCert Sp. z o.o.

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

Wersja	3.0
Status	nieaktualna
Data zatwierdzenia	15.11.2017
Zatwierdzający	Zarząd EuroCert Sp. z o.o.
Obowiązuje od	20.11.2017
Identyfikator obiektu OID	1.2.616.1.113791.1.2
Data wygaśnięcia	01.10.2018 r.

Wszystkie wersje Polityki są dostępne w postaci elektronicznej na stronie internetowej https://www.eurocert.pl/repozytorium.

Certyfikaty wydawane przez EuroCert zawierają identyfikatory polityk certyfikacji, które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Deklarowane przeznaczenie certyfikatu można określić na podstawie wpisów umieszczanych w strukturze PolicyInformation rozszerzenia certificatePolicies (patrz § 7.1.2) każdego certyfikatu wydawanego przez EuroCert. Identyfikatory polityki certyfikacji, publikowane w certyfikacie, opisano w § 1.3.1 oraz 7.1.2.

1.3 Elementy infrastruktury PKI

Infrastruktura klucza publicznego EuroCert dla kwalifikowanych certyfikatów składa się z następujących elementów:

a) kwalifikowany urząd certyfikacji: Centrum Kwalifikowane EuroCert,
b) punkty rejestracji, notariusze i inne osoby potwierdzające tożsamość subskrybentów,
c) subskrybenci,
d) strony ufające.

Odbiorcy usług certyfikacyjnych świadczonych przez EuroCert mają obowiązek zapoznania się z niniejszym dokumentem. Subskrybent ma obowiązek zapoznania się z Polityką przed podpisaniem umowy o świadczenie usług zaufania, natomiast strona ufająca przed użyciem jakiegokolwiek certyfikatu wystawionego zgodnie z Polityką.

1.3.1 Urząd certyfikacji

W skład EuroCert wchodzi jeden urząd certyfikacji – Centrum Kwalifikowane EuroCert, który wystawia certyfikaty dla użytkowników końcowych (subskrybentów) oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów. Nadzór nad urzędem sprawuje minister właściwy ds. informatyzacji, który powierzył pełnienie roli nadrzędnego urzędu certyfikacji tzw. „Root CA" Narodowemu Bankowi Polskiemu (dalej jako „NCCert"). NCcert jest punktem zaufania wszystkich subskrybentów i stron ufających dla kwalifikowanych usług EuroCert. Oznacza to, że każda budowana przez nich ścieżka certyfikacji powinna prowadzić od certyfikatu NCCert do certyfikatu wystawionego dla „Centrum Kwalifikowane Eurocert" przez NCCert.

EuroCert nie wystawia certyfikatów dla żadnych podległych urzędów certyfikacji.

Centrum Kwalifikowane EuroCert wydaje kwalifikowane certyfikaty zgodnie z politykami certyfikacji o identyfikatorach określonych w tab. 2 poniżej i § 7.1.2.

Tab. 2. Identyfikatory polityk certyfikacji umieszczane w certyfikatach wydawanych przez EuroCert

Nazwa certyfikatu	Identyfikator polityki certyfikacji
Certyfikat kwalifikowany (RSA, SHA-1)	1.2.616.1.113791.1.2.1
Certyfikat kwalifikowany (RSA, SHA-512)	1.2.616.1.113791.1.2.2
Certyfikat kwalifikowany (ECDSA, SHA-512)	1.2.616.1.113791.1.2.3

Zadania związane z przyjmowaniem wniosków o wydanie oraz z wydawaniem certyfikatów realizują punkty rejestracji.

1.3.2 Punkty Rejestracji

EuroCert, realizując swoje zadania, 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 wniosków o unieważnienie/zawieszenie certyfikatu.

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,
c) podpisywania umów z subskrybentami,
d) tworzenia zgłoszeń certyfikacyjnych,
e) generowania kluczy subskrybentów,
f) przekazywania certyfikatów subskrybentom,
g) udzielania informacji o kwalifikowanym podpisie elektronicznym, w tym o skutkach jakie wywołuje,
h) sprzedaży zestawów do składania podpisu elektronicznego.

Szczegółowy zakres obowiązków punktów rejestracji określany jest przez umowę pomiędzy EuroCert a danym punktem rejestracji.

Kompetencje punktów rejestracji nie mogą obejmować w szczególności posługiwania się kluczem prywatnym służącym do generowania certyfikatów i list CRL.

Lista aktualnych autoryzowanych punktów rejestracji dostępna jest na stronie internetowej https://sklep.eurocert.pl/pl/i/Mapa-Punktow-Partnerskich/14.

1.3.3 Subskrybenci

Subskrybentem certyfikatu wydanego w ramach Polityki może być każda osoba fizyczna, której dane zostaną umieszczone w polu „podmiot” (ang. subject) certyfikatu i która sama dalej nie wydaje certyfikatów innym podmiotom.

1.3.4 Strony ufające

Strona ufająca jest z kolei podmiotem, który posługuje się kwalifikowanym certyfikatem innego podmiotu w celu zweryfikowania jego podpisu elektronicznego.

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta (patrz § 4.5.2). Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do

zweryfikowania podpisu elektronicznego. Informacje zawarte w kwalifikowanym certyfikacie (m.in. identyfikator polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.4 Zakres stosowania certyfikatów

Certyfikaty kluczy weryfikujących podpisy, wydawane przez EuroCert zgodnie z Polityką stanowią certyfikaty kwalifikowane podpisów elektronicznych w rozumieniu Rozporządzenia eIDAS. Zapewniają one bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu.

Klucze prywatne powiązane z certyfikatami powinny być stosowane do składania kwalifikowanych podpisów elektronicznych, zapewniających integralność podpisywanej informacji i nadających jej cechę niezaprzeczalności w środowisku, w którym występuje ryzyko naruszenia informacji oraz skutki tego naruszenia mogą być wysokie.

Kwalifikowane podpisy elektroniczne weryfikowane za pomocą certyfikatów kwalifikowanych wystawianych przez EuroCert mają skutek prawny równoważny podpisowi własnoręcznemu.

Certyfikatów można używać w transakcjach finansowych lub transakcjach o znacznym poziomie ryzyka wystąpienia oszustw, a także w tych przypadkach, w których zwykle stosowany jest podpis własnoręczny.

Klucze prywatne związane z kwalifikowanymi certyfikatami, mogą być przetwarzane wyłącznie w urządzeniach, spełniających wymogi o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiającej normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 Rozporządzenia eIDAS. Lista kwalifikowanych urządzeń do składania podpisu elektronicznego opublikowana jest w repozytorium (patrz § 2).

Certyfikatów wydawanych w ramach Polityki nie wolno używać niezgodnie z przeznaczeniem oraz bez przestrzegania ewentualnych ograniczeń zastosowania danego certyfikatu zapisanych w certyfikacie.

Zakazane jest również używanie certyfikatów przez osoby do tego nieupoważnione.

Certyfikaty nie mogą być stosowane do szyfrowania danych lub kluczy kryptograficznych (ogólnie, w operacjach, których celem jest nadanie informacji cech poufności).

1.5 Zarządzanie Polityką

Każda zmiana Polityki, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymaga nadania nowego numeru wersji oraz zatwierdzenia przez Zarząd EuroCert Sp. z o.o. Obowiązująca w danym czasie wersja ma status aktualny. Każda z wersji jest aktualna do czasu zatwierdzenia i opublikowania kolejnej obowiązującej wersji.

Nowa wersja Polityki jest publikowana w repozytorium (patrz § 2). Subskrybenci oraz pozostałe zainteresowane strony (wymienione w § 1.3) zobowiązani są stosować się do wersji Polityki, zgodnie z którą został wystawiony dany certyfikat.

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

W celu uzyskania dalszych informacji dotyczących usług i działalności EuroCert należy kontaktować się z:

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

1.6 Słownik używanych terminów i akronimów

Określenia wykorzystywane w Polityce, a niezdefiniowane poniżej należy interpretować zgodnie z definicjami zawartymi w Ustawie o usługach zaufania i Rozporządzeniu eIDAS.

Tab. 2. Terminy i skróty używane w Polityce

Termin/akronim	Opis
Urząd certyfikacji	Centrum Kwalifikowane EuroCert
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
OCSP	Online Certificate Status Protocol - protokół i nazwa usługi PKI służącej do informowania o statusie konkretnych certyfikatów, o które pyta usługobiorca (czy certyfikat jest ważny, czy unieważniony)
CRL	Lista unieważnionych certyfikatów (Certificate Revocation List)
PDS	PKI Disclosure Statement, dokument określający warunki stosowania oraz ograniczenia zastosowania kwalifikowanych podpisów elektronicznych
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)
NCCert	Root krajowego systemu PKI, prowadzony przez Narodowy Bank Polski, na podstawie upoważnienia ministra właściwego ds. informatyzacji.
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)

Rozporządzenie 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
QSCD	QSCD - Qualified Signature Creation Device – urządzenie posiadające certyfikat umożliwiający użycie do wystawiania kwalifikowanego podpisu elektronicznego/pieczęci elektronicznej, na podstawie Rozporządzenia eIDAS
Ustawa o ochronie danych osobowych	ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)
TSL	EU Trust service Status List – listy wydawane przez Komisję Europejską (lista list) oraz kraje członkowskie EU, zawierające informacje o dostawcach usług zaufania ich statusie (czy „kwalifikowany") oraz dane umożliwiające weryfikację „tokenów" wystawianych przez dostawców usług zaufania (czyli weryfikację kwalifikowanych certyfikatów, znaczników czasu itd.)

2 Publikowanie i repozytorium

Wszystkie informacje istotne z punktu widzenia subskrybentów, punktów rejestracji, stron ufających publikowane są na stronie internetowej:

https://eurocert.pl/repozytorium

Są to następujące informacje:

a) aktualne certyfikaty dostawcy usług zaufania wydane dla EuroCert, służące do weryfikacji certyfikatów kluczy publicznych wystawionych zgodnie z Polityką,
b) aktualna lista CRL,
c) aktualne oraz poprzednie wersje Kodeksu postępowania certyfikacyjnego i Polityki certyfikacji, z podaniem okresu ich obowiązywania,
d) opisy procedur zawieszania/unieważniania certyfikatów,
e) wykaz rekomendowanych aplikacji i urządzeń do składania i weryfikacji podpisów elektronicznych,
f) dokument określający dokładne warunki użycia certyfikatu (PKI Disclosure Statement), zawierający między innymi:
    - sposoby rozstrzygania skarg i sporów,
    - zakres i ograniczenia stosowania certyfikatów zgodnych z Polityką,
    - skutki prawne składania kwalifikowanych podpisów elektronicznych weryfikowanych przy użyciu certyfikatów zgodnych z Polityką.

EuroCert nie publikuje certyfikatów subskrybentów.

Lista CRL jest generowana i publikowana automatycznie, nie rzadziej niż co 24 godziny lub w ciągu 1 godziny od żądania zawieszenia lub unieważnienia certyfikatu, natomiast pozostałe informacje każdorazowo, gdy zostaną uaktualnione lub zmienione.

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

3 Zasady identyfikacji i uwierzytelnienia

Niniejszy rozdział przedstawia zasady weryfikacji tożsamości potencjalnych subskrybentów przy wydawaniu, zawieszaniu lub unieważnianiu certyfikatów. 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.

3.1 Nazewnictwo używane w certyfikatach

Identyfikacja każdego podmiotu posiadającego certyfikat wydany przez EuroCert realizowana jest w oparciu o nazwę wyróżniającą DN, umieszczaną w polu identyfikatora podmiotu (subject). 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.

Nazwa DN subskrybenta składa się z niektórych lub wszystkich atrybutów zawartych w zbiorze atrybutów przedstawionych w tab. 3, przy czym musi ona zawierać przynajmniej nazwę kraju, imię (imiona), nazwisko oraz numer seryjny (SN).

Tab. 3. Profil identyfikatora DN

Pola	Wartość
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 (Title)	nazwa stanowiska pracy pełnionego przez subskrybenta w danej organizacji
ST	Województwo
L	Miejscowość
A	adres pocztowy

Subskrybent może posiadać dowolną liczbę certyfikatów zawierających ten sam identyfikator DN.

W przypadku subskrybenta identyfikującego się numerem PESEL atrybut Numer seryjny występuje w formacie „PNOPL-XXXXXXXXXX" zgodnie z normą ETSI EN 319 412-2.

Każdy wydany certyfikat posiada unikalny w ramach urzędu certyfikacji numer seryjny. Łącznie z Identyfikatorem DN subskrybenta gwarantuje to jednoznaczną identyfikację certyfikatu.

Dane adresowe (województwo, nazwa miejscowości, adres pocztowy) podmiotu, którego nazwa widnieje w atrybucie 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.

Identyfikator DN powinien zawierać wyłącznie nazwy, do których subskrybent ma prawo. 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. 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

Procedura weryfikacji tożsamości osoby fizycznej przeprowadzana jest przez operatora punktu rejestracji, inspektora rejestracji, notariusza lub inną osobę weryfikującą tożsamość. Polega ona na szczegółowej weryfikacji dokumentów i wniosku okazanych przez subskrybenta oraz opcjonalnie na zweryfikowaniu poprawności nazwy DN.

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.

EuroCert oraz podległe mu punkty rejestracji potwierdzają tożsamość potencjalnego subskrybenta na podstawie ważnego dokumentu tożsamości (m.in. dowodu osobistego lub paszportu) oraz dodatkowo – w przypadku gdy w certyfikacie razem z danymi osoby fizycznej mają być umieszczone dane dotyczące osoby prawnej lub innej jednostki organizacyjnej – na podstawie następujących dokumentów:

a) pełnomocnictwa lub innego dokumentu upoważniającego do występowania w cudzym imieniu, określający precyzyjnie zakres uprawnień do występowania w cudzym imieniu
b) stosownego upoważnienia wystawionego przez daną organizację do umieszczenie danych organizacji w certyfikacie,
c) aktualnego wypisu z Krajowego Rejestru Sądowego lub wypisu z Centralnej Ewidencji i Informacji o Działalności Gospodarczej,
d) innych dokumentów, które są niezbędne do potwierdzenia danych zawartych we wniosku o certyfikat, np. zaświadczenie o miejscu zatrudnienia.

Osoba potwierdzająca tożsamość potencjalnego subskrybenta w imieniu EuroCert, poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości. Następnie podpisuje w imieniu EuroCert umowę z subskrybentem zawierającą następujące dane subskrybenta:

a) imię,
b) nazwisko,
c) datę i miejsce urodzenia,
d) numer PESEL,
e) serię, numer i rodzaj dokumentu tożsamości oraz oznaczenie organu wydającego dowód osobisty lub paszport, na podstawie którego potwierdzono tożsamość wnioskodawcy.

EuroCert może również potwierdzić tożsamość osoby ubiegającej się o certyfikat za pośrednictwem notariusza. W takim przypadku wnioskodawca jednostronnie podpisuje umowę z EuroCert w

obecności notariusza, która po przekazaniu do EuroCert jest podpisywana przez Inspektora rejestracji i odsyłana na adres wskazany przez wnioskodawcę.

Przed wystawieniem certyfikatu wnioskodawca jest zobowiązany potwierdzić zapoznanie się z Polityką certyfikacji, Kodeksem postępowania certyfikacyjnego, warunkami użycia, zakresem i ograniczeniami stosowania certyfikatu, skutkami prawnymi składania kwalifikowanego podpisu elektronicznego poprzez złożenie własnoręcznego podpisu pod treścią umowy o świadczenie usług zaufania. Podpisanie umowy oznacza także, że:

a) subskrybent wyraża zgodę na przetwarzanie przez EuroCert Sp. z o.o. jego danych osobowych dla potrzeb niezbędnych dla procesu certyfikacji,
b) subskrybent oświadcza, że informacje podane przez niego są zgodne z prawdą i zostały podane dobrowolnie,
c) subskrybent potwierdza osobisty odbiór karty kryptograficznej z kluczem prywatnym od osoby weryfikującej jego dane oraz nadanie kodów PIN i PUK zabezpieczających dostęp do karty,
d) subskrybent, występując z wnioskiem o wydanie certyfikatu, jest świadom jaka informacja umieszczana jest w certyfikacie i wyraża zgodę na jej upublicznienie.

3.3 Identyfikacja i uwierzytelnianie przy wydawaniu kolejnego certyfikatu

W przypadku gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada inny ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu (oraz pozostałych dokumentów uwierzytelniających), a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone kwalifikowanym podpisem elektronicznym tej osoby, o ile dane te nie różnią się od danych zawartych w certyfikacie związanym z kwalifikowanym podpisem elektronicznym, którego użyto do podpisania tych danych. Wówczas uwierzytelnianie subskrybenta realizowane jest 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). Nie oznacza to jednak braku możliwości zastosowania procedury opisanej w § 3.2.

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 § 3.2).

3.4 Identyfikacja i uwierzytelnianie przy unieważnianiu certyfikatu

Unieważnienie certyfikatu może nastąpić:

a) na wniosek subskrybenta (osoby fizycznej),
b) na wniosek zamawiającego (organizacji reprezentowanej przez subskrybenta), którego dane zostały zamieszczone w certyfikacie,
c) na żądanie ministra właściwego ds. informatyzacji,
d) z inicjatywy EuroCert.

Unieważnienia certyfikatu można dokonać w następujący sposób:

a) osobiście w EuroCert (adres podano w § 1.5), w godzinach pracy tj. od 9.00 do 17.00, po potwierdzeniu tożsamości osoby występującej o unieważnienie przez Inspektora rejestracji na zasadach opisanych w § 3.2,

b) telefonicznie (numer infolinii: 22 490 49 86), w ciągu całej doby, na podstawie hasła do unieważnienia certyfikatu ustalonego przy jego wydawaniu oraz danych osobowych podanych przy wydawaniu certyfikatu,
c) drogą elektroniczną posługując się formularzem on-line na stronie internetowej https://eurocert.pl/uniewaznienia/ lub poprzez wysłanie wniosku o unieważnienie (opublikowanego w repozytorium) opatrzonego ważnym kwalifikowanym podpisem elektronicznym na adres uniewaznienia@eurocert.pl.

W ostatnim przypadku Inspektor rejestracji dzwoni pod wskazany we wniosku numer telefonu, sprawdza dane z certyfikatu i weryfikuje z danymi we wniosku o unieważnienie.

W przypadku niezgodności weryfikowanych danych certyfikat zostaje zawieszony do czasu wyjaśnienia powstałych niezgodności lub wniosek o unieważnienie zostaje odrzucony.

Identyfikacja i uwierzytelnienie podmiotu trzeciego, którego dane zawarte są w certyfikacie przebiega na zasadach opisanych w § 3.2. Podstawą przyjęcia wniosku w tym przypadku jest pozytywna weryfikacja prawa podmiotu trzeciego do występowania o unieważnienie certyfikatu.

Warunki zawieszenia, uchylenia zawieszenia oraz unieważnienia certyfikatu w szczególności na wniosek zamawiającego lub subskrybenta określone zostały w § 4.9.

4 Wymagania funkcjonalne

W niniejszym rozdziale przedstawiono sposób realizacji usługi wydawania kwalifikowanych certyfikatów klucza publicznego, obejmującej wydawanie certyfikatów, ich modyfikację, unieważnianie i zawieszanie/ odwieszanie oraz wydawanie kolejnych certyfikatów.

4.1 Wniosek o certyfikat

Wniosek o wygenerowanie kluczy i certyfikatu przedkładany jest osobiście w punkcie rejestracji w formie papierowej (własnoręcznie podpisany) lub drogą elektroniczną (podpisany kwalifikowanym podpisem elektronicznym). Wniosek składany jest zawsze przez osobą fizyczną dla której ma zostać wydany certyfikat. Wnioskodawca poświadcza we wniosku, że wszystkie przedstawione przez niego dane niezbędne do wydania certyfikatu są prawdziwe.

Przed przystąpieniem do procedury weryfikacji tożsamości potencjalnego subskrybenta, upoważniony przedstawiciel EuroCert w punkcie rejestracji odbiera od niego pisemne oświadczenie o zapoznaniu się z dokumentem określającym warunki użycia certyfikatu, zawierającym między innymi:

a) sposoby rozstrzygania skarg i sporów,
b) zakres i ograniczenia stosowania certyfikatów zgodnych z Polityką,
c) skutki prawne składania podpisów elektronicznych weryfikowanych przy użyciu certyfikatów zgodnych z Polityką,
d) informację o systemie dobrowolnej rejestracji kwalifikowanych dostawców usług zaufania i ich znaczeniu.

4.2 Przetwarzanie wniosku

Punkt rejestracji weryfikuje tożsamość potencjalnego subskrybenta zgodnie z postanowieniami § 3.2 lub 3.3. Następnie generuje zgłoszenie certyfikacyjne, zawierające wszystkie dane niezbędne do wystawienia certyfikatu, zgodnie z profilem certyfikatu zawartym w § 7.1.

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

4.3 Wydawanie certyfikatu

EuroCert wystawia certyfikat każdorazowo na podstawie zgłoszenia certyfikacyjnego, podpisanego elektronicznie przez uprawnioną osobę pełniącą funkcję Inspektora rejestracji.

EuroCert wydaje certyfikaty za każdym razem generując nową parę kluczy.

Inspektor rejestracji podpisuje elektronicznie zgłoszenie certyfikacyjne, o którym mowa w § 4.2, a następnie przesyła podpisane zgłoszenie certyfikacyjne do systemu generującego certyfikaty uruchamiając procedurę generowania certyfikatu subskrybenta na kwalifikowanym urządzeniu do składania podpisu elektronicznego posiadającego funkcje generowania kluczy przez komponent techniczny, którego konstrukcja:

a) uniemożliwia skopiowanie klucza prywatnego z komponentu technicznego, na którym klucze zostały wygenerowane lub
b) uniemożliwia skopiowanie klucza prywatnego z modułu kluczowego współpracującego z komponentem technicznym, na którym klucze zostały wygenerowane lub
c) umożliwia zapisanie w module kluczowym lub innym komponencie technicznym wygenerowanego klucza prywatnego lub danych służących do odtworzenia klucza i jednocześnie gwarantuje skasowanie klucza prywatnego z nieprzekazywanego Subskrybentowi komponentu technicznego w sposób uniemożliwiający odtworzenie klucza.

Nowy certyfikat będzie zawierał między innymi klucz publiczny oraz dane subskrybenta dostarczone przez niego w zgłoszeniu certyfikacyjnym.

4.4 Akceptacja certyfikatu

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 § 3.4 i 4.9) i otrzymania nowego, zawierającego poprawne dane certyfikatu. Posługiwanie się certyfikatem zawierającym nieprawdziwe dane naraża subskrybenta na odpowiedzialność karną określoną w art. 42 ust. 2 Ustawy o usługach zaufania.

Wstępna akceptacja certyfikatu jest wykonywana przez punkt 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.

Certyfikat jest akceptowany przez subskrybenta poprzez poświadczenie potwierdzenia odbioru certyfikatu z rąk tego samego operatora punktu rejestracji, który dokonał wcześniej weryfikacji jego tożsamości. Potwierdzenie to opatrzone własnoręcznym podpisem subskrybenta jest przechowywane przez EuroCert. Drugi egzemplarz otrzymuje subskrybent.

W przypadku certyfikatów wydawanych online (patrz § 4.7) akceptacja certyfikatu przez subskrybenta następuje poprzez pobranie go z systemu EuroCert.

Certyfikaty nie są publikowane poza siecią wewnętrzną EuroCert.

4.5 Korzystanie z pary kluczy i certyfikatu

W tym podrozdziale przedstawiono zobowiązania subskrybentów i stron ufających związane z korzystaniem z pary kluczy i certyfikatu.

4.5.1 Zobowiązania subskrybenta

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 zgłoszenie certyfikacyjne,
c) dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku,
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 karty kryptograficznej zawierającej 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 powiązany z tym kluczem prywatnym jest przeterminowany (minął jego okres ważności), jest unieważniony lub zawieszony,
k) używania kluczy prywatnych i certyfikatów zgodnie z ich przeznaczeniem określonym w § 1.4 oraz wskazanym w certyfikacie (w polu keyUsage oraz CertificatePolicies, patrz § 7.1.2),
l) niezwłocznego zgłoszenia EuroCert żądania unieważnienia certyfikatu w przypadkach przewidzianych w § 4.9.1.

4.5.2 Zobowiązania strony ufającej

Strony ufające są zobowiązane do:

a) zaufania tylko tym kwalifikowanym 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 certyfikatów zgodnie z ich przeznaczeniem określonym w § 1.4 oraz wskazanym w certyfikacie (w polu keyUsage oraz CertificatePolicies, patrz § 7.1.2).

4.6 Odnowienie certyfikatu

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

4.7 Wystawienie kolejnego certyfikatu

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.

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.

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 zgłoszeniem certyfikacyjnym.

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.

Wydanie kolejnego certyfikatu zawsze następuje z inicjatywy subskrybenta. Subskrybent w każdej chwili może wystąpić z wnioskiem o wystawienie nowego certyfikatu, np. wtedy, gdy obecny certyfikat traci ważność.

Wydanie kolejnego certyfikatu musi być poprzedzone złożeniem niezbędnych dokumentów formalnych w postaci elektronicznej, podpisanych (uwierzytelnionych) przy użyciu ważnego klucza prywatnego, związanego z nie przeterminowanym certyfikatem. Certyfikat ten nie jest unieważniany.

4.8 Modyfikacja certyfikatu

Zmiana treści certyfikatu wymaga wydania nowego certyfikatu. 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.

Modyfikacja certyfikatu może dotyczyć tylko certyfikatu, którego okres ważności nie minął lub nie został wcześniej unieważniony.

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 § 4.5.1).

4.9 Unieważnienie i zawieszenie certyfikatu

EuroCert zapewnia możliwość całodobowego zgłaszania wniosków o unieważnienie/ zawieszenie certyfikatu zgodnie z art. 16 ust. 4 ustawy o usługach zaufania.

Maksymalny dopuszczalny czas na przetworzenie wniosku wynosi 1 godzinę od momentu jego dostarczenia.

4.9.1 Okoliczności unieważnienia certyfikatu

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 kwalifikowanego firmowego – na żądanie upoważnionego przedstawiciela reprezentowanego podmiotu lub innej upoważnionej osoby,
c) na żądanie ministra właściwego ds. informatyzacji,
d) 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),
e) ustąpiły okoliczności uzasadniające zamieszczenie danych organizacji w certyfikacie (np. zwolnienie pracownika, zmiana zakresu obowiązków itd.),

f) przez wystawcę certyfikatu, tzn. przez EuroCert, np. wskutek rażącego naruszenia przez subskrybenta zasad Polityki certyfikacji lub Kodeksu postępowania certyfikacyjnego, w szczególności obowiązków określonych w § 4.5.1,
g) EuroCert zaprzestaje świadczenia usług w zakresie certyfikatów i żaden podmiot nie przejmuje prowadzenia usługi udostępniania informacji o statusie certyfikatu,
h) EuroCert otrzyma dowód, że certyfikat był wykorzystany niezgodnie z przeznaczeniem,
i) Z wyłącznej inicjatywy EuroCert w wyniku uzasadnionego podejrzenia, iż certyfikat wraz z parą kluczy zagraża bezpieczeństwu subskrybenta,
j) certyfikat był wydany niezgodnie z Polityką,
k) klucz prywatny urzędu certyfikacji został skompromitowany lub EuroCert pozyska informację, że mógł zostać skompromitowany.

4.9.2 Kto może żądać unieważnienia certyfikatu

EuroCert przestrzega ogólnej zasady, iż unieważnienia certyfikatu może żądać jedynie osoba występująca w certyfikacie, jego właściciel lub podmiot przez niego reprezentowany. Możliwe są jednak sytuacje, kiedy z wnioskiem o unieważnienie mogą wystąpić inne zainteresowane strony. Lista takich stron oraz sytuacje, w których może to nastąpić przedstawione są Kodeksie postępowania certyfikacyjnego.

4.9.3 Procedura unieważnienia certyfikatu

Certyfikat jest unieważniany po pomyślnej weryfikacji wniosku o unieważnienie przez Inspektora Rejestracji zgodnie z zasadami w § 3.4. W przypadku, gdy istnieją przesłanki do unieważnienia certyfikatu, jednakże Inspektor rejestracji nie jest w stanie w ciągu 1 godziny od momentu otrzymania kompletnego wniosku wyjaśnić wszystkich wątpliwości dotyczących unieważnienia, certyfikat jest zawieszany.

Informacja o unieważnieniu certyfikatu jest umieszczana na liście CRL. Nowa lista CRL jest publikowana w ciągu godziny od przyjęcia wniosku o unieważnienie. EuroCert przekazuje subskrybentowi oraz stronie ubiegającej się o unieważnienie za pośrednictwem poczty elektronicznej potwierdzenie unieważnienia lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy.

4.9.4 Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu następuje niezwłocznie po powzięciu uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu wskazane w § 4.9.1, w szczególności na wniosek złożony przez subskrybenta.

4.9.5 Kto może żądać zawieszenia certyfikatu

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

4.9.6 Procedura zawieszenia i odwieszenia certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu. Po pomyślnej weryfikacji wniosku o zawieszenie przez Inspektora rejestracji przebiegającej jak w § 3.4 zmienia on

status certyfikatu na zawieszony i umieszcza go na liście CRL (z przyczyną unieważnienia *certificateHold*).

W przypadku niepotwierdzenia się przesłanek uzasadniających zawieszenie certyfikatu, o których mowa w § 4.9.4 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.

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

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

4.10 Weryfikacja statusu certyfikatu

Weryfikacji statusu certyfikatów wydanych przez EuroCert można dokonać na podstawie list CRL. Listy CRL są generowane nie rzadziej niż co 24 godziny lub za każdym razem, gdy następuje zawieszenie/ unieważnienie certyfikatu i publikowane automatycznie w repozytorium (patrz § 2). EuroCert sprawdza co najmniej raz dziennie dostępność list CRL.
Status certyfikatu wydanego przez EuroCert można również zweryfikować korzystając z usługi OCSP, o ile taka informacja jest umieszczona w wydanym certyfikacie. 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

Umowa o świadczenie usług zaufania 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

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, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych. Opis rozszerzony tych wymagań zawiera Kodeks postępowania certyfikacyjnego.

5.1 Zabezpieczenia fizyczne

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. Zastosowane środki ochrony fizycznej pomieszczeń obejmują między innymi:

a) system kontroli dostępu do pomieszczeń,
b) system ochrony przeciwpożarowej,
c) system ochrony przeciwzalaniowej,
d) system sygnalizacji włamania i napadu,
e) system chłodzenia,
f) system zasilania awaryjnego.

Fizyczny dostęp do budynków, w których znajdują się te pomieszczenia jest kontrolowany oraz nadzorowanych przez zintegrowany system alarmowy. Ochrona na zewnątrz budynków funkcjonuje 24 godziny na dobę.

Systemy teleinformatyczne wykorzystywane do świadczenia usług zaufania mieszczą się w dwóch niezależnych lokalizacjach (centrum podstawowym i centrum zapasowym) oddalonych od siebie. W przypadku awarii centrum podstawowego, drugie z nich na bieżąco przejmuje pracę związaną z unieważnianiem, zawieszaniem certyfikatów i publikacją list CRL.

5.2 Zabezpieczenia organizacyjne

Osoby sprawujące nadzór nad systemem wykorzystywanym do świadczenia usług zaufania w EuroCert pełnią określone role, jak pokazano w tab. 4. Przedstawiony podział ról jest zgodny z wymogami ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Tab. 4. Zaufane role w EuroCert

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 certyfikacyjnych, zarządzanie uprawnieniami dla operatorów systemu
Operator systemu	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
Inspektor audytu	analizowanie zapisów rejestrów zdarzeń mających miejsce w systemach teleinformatycznych EuroCert

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.

Rozszerzony opis zabezpieczeń organizacyjnych zawiera Kodeks postępowania certyfikacyjnego oraz wewnętrzne dokumenty EuroCert.

5.3 Nadzorowanie Pracowników

EuroCert gwarantuje, że osoby wykonujące swoje obowiązki wynikające z funkcji realizowanych przez urząd certyfikacji:

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 certyfikacyjnych.

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

W takim przypadku 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.

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

5.4 Procedury tworzenia logów audytowych

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

5.4.1 Typy rejestrowanych zdarzeń

Typy rejestrowanych zdarzeń wymieniono w Kodeksie postępowania certyfikacyjnego.

5.4.2 Częstotliwość analizy zapisów zdarzeń

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

5.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń

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

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

5.4.5 Tworzenie kopii zapisów rejestrowanych zdarzeń

Zapisy zdarzeń są kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa systemu. Kopie te przechowywane są w centrum głównym w sejfach.

5.4.6 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenia

Elementy systemu certyfikacji oraz systemów wspomagających podlegają stałemu nadzorowi przez systemy monitorujące oraz personel techniczny. Informacja o wykrytym zagrożeniu lub naruszeniu bezpieczeństwa trafia bezpośrednio do administratora i inspektora bezpieczeństwa. W zależności od poziomu i wagi zagrożenia powiadamiane są osoby odpowiedzialne za działanie komponentów, których dotyczy zdarzenie. Powiadamianie może być wykonane drogą elektroniczną lub telefonicznie.

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 24 godzin od wystąpienia zdarzenia EuroCert zawiadamia organ nadzoru i, w stosowanych przypadkach, inne właściwe podmioty zgodnie z art. 19.2 Rozporządzenia eIDAS.

5.5 Archiwizacja danych

Dokumenty papierowe oraz dane elektroniczne bezpośrednio związane ze świadczonymi usługami zaufania takie jak:

- umowy o świadczenie usług zaufania, o których mowa w art. 14 § 1 Ustawy o usługach zaufania,
- otrzymywane wnioski oraz wydawane decyzje, mające postać papierową lub elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane,
- wszystkie informacje o subskrybentach zebrane w trakcie procesu wydawania certyfikatu,
- baza danych certyfikatów,
- wydane listy CRL,
- historia kluczy urzędu certyfikacji, od ich wygenerowania do zniszczenia włącznie,

- politykę świadczenia usług,
- dokumenty wystawiane przez operatora systemu punktu rejestracji, notariusza lub inne osoby potwierdzające tożsamość wnioskodawcy w imieniu EuroCert,
- żądania unieważnienia certyfikatu,
- pozostałe dokumenty papierowe, związane ze świadczeniem usług zaufania.

są przechowywane i archiwizowane przez 20 lat od ich wytworzenia zgodnie z art. 17 ust. 2 ustawy o usługach zaufania.

Archiwalne dane w postaci elektronicznej przechowywane są w centrum podstawowym w sejfach, z kolei archiwalne dane w postaci papierowej przechowywane są w siedzibie EuroCert Sp. z o.o. w metalowych zamykanych na klucz szafach.

5.6 Wymiana klucza

Procedura wymiany klucza odnosi się do kluczy urzędu certyfikacji używanych do podpisywania certyfikatów i list CRL.

Wymiana kluczy urzędu 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, generacja 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).

Nowy certyfikat urzędu certyfikacji jest publikowany w repozytorium. Informacja o zmianie kluczy może być opublikowana w środkach masowego przekazu.

Procedura wymiany pary kluczy przebiega następująco:

- wystąpieniu do organu nadzoru o wydanie nowego certyfikatu dostawcy usług zaufania,
- wytworzenie nowych kluczy urzędu certyfikacji i zgłoszenie ich ministrowi ds. informatyzacji, w celu wystawienia nowego certyfikatu od NCCert oraz umieszczeniu go na liście TSL,
- otrzymanie certyfikatu od NCCert oraz wydaniu przez NCCert nowej listy TSL.

5.7 Utrata poufności klucza i działanie w przypadku katastrof

Podrozdział ten zawiera opis procedur postępowania, realizowanych przez EuroCert w wypadkach szczególnych (także klęsk żywiołowych) w celu przywrócenia funkcjonalności urzędu certyfikacji. Procedury te realizowane są według opracowanego planu ciągłości działania.

5.7.1 Utrata poufności klucza prywatnego

Eurocert posiada odpowiednie procedury obowiązujące w wypadku utraty poufności klucza prywatnego Eurocert lub uzasadnionego podejrzenie zajścia takiego zdarzenia (patrz § 5.4.6). Procedury te przewidują między innymi:

a) powiadomienie organu nadzoru o wystąpieniu incydentu bezpieczeństwa w "formularzu zgłoszenia incydentu przez dostawcę usług zaufania" zgodnie z wymaganiami art. 19.2 Rozporządzenia eIDAS,
b) poinformowanie Subskrybentów o zaistniałej sytuacji oraz o planie dalszego działania,
c) wystąpienie do organu nadzoru o unieważnienie certyfikatu związanego z ujawnionym kluczem prywatnym oraz wszystkich aktualnie ważnych certyfikatów, podpisanych przy pomocy ujawnionego klucza prywatnego,
d) powiadomienie o unieważnieniu certyfikatu urzędu certyfikacji dostępnymi kanałami informacyjnymi,
e) wytworzenie nowych kluczy urzędu certyfikacji i zgłoszenie ich Ministrowi ds. informatyzacji, w celu wystawienia nowego certyfikatu przez NCCert oraz umieszczeniu na liście TSL,
f) jeśli to będzie w danej sytuacji możliwe (w szczególności bazy danych EuroCert pozostaną wiarygodne) – wystawienie nowych certyfikatów i kluczy subskrybentom, w oparciu o nowe klucze EuroCert, z okresami ważności co najmniej takimi samymi, jakie miały unieważnione certyfikaty, bez obciążania ich kosztami za tą operację.

5.7.2 Katastrofy

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.

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.

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

5.8 Zakończenie działalności EuroCert

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

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

Jeśli żaden kwalifikowany 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.

O ile inny kwalifikowany podmiot nie przejmie działalności EuroCert, dokumenty i zapisy, co do których jest wymagana archiwizacja, są przekazywane po zakończeniu działalności organowi nadzoru lub podmiotowi przez niego wskazanemu.

6 Procedury bezpieczeństwa technicznego

Poniżej zaprezentowano procedury tworzenia oraz zarządzania (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

6.1.1 Generowanie kluczy

Klucze urzędu certyfikacji EuroCert generowane są przez personel EuroCert zgodnie z wewnętrzną procedurą, przy obecności co najmniej dwóch osób pełniących funkcje bezpośrednio związane z realizacją kwalifikowanych usług zaufania (patrz § 5.2), w tym Inspektora bezpieczeństwa. Z ceremonii generowania kluczy sporządza się protokół.

Klucze urzędów świadczących usługi zaufania, funkcjonujących w ramach EuroCert, generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu kryptograficznego, posiadającego certyfikat Common Criteria EAL4+. Generacja kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym.

Klucze Inspektorów rejestracji są generowane samodzielnie przez nich samych, na karcie kryptograficznej pod nadzorem Inspektora bezpieczeństwa. Służą one podpisywaniu żądań subskrybentów o certyfikację kluczy.

Klucze subskrybentów generowane są wyłącznie przez EuroCert w punkcie rejestracji na karcie kryptograficznej spełniającej wymagania SSCD/QSCD w obecności Subskrybenta.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Para kluczy i certyfikat Subskrybenta są wydawane zgodnie z zasadami w § 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.

Subskrybenci chcący odnowić posiadany na karcie kryptograficznej wydanej przez EuroCert ważny certyfikat kwalifikowany, 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 urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu certyfikacji wydającego certyfikaty użytkownikom końcowym rozpowszechniane są tylko w postaci certyfikatów dostawcy usług zaufania zgodnych z zaleceniem ITU-T X.509 v.3. Klucz publiczny urzędu certyfikacji Centrum Kwalifikowane EuroCert ma postać certyfikatu, wydanego przez Narodowe Centrum Certyfikacji.

Klucze publiczne urzędu certyfikacji rozpowszechniane poprzez opublikowanie w ogólnie dostępnym repozytorium (patrz § 2) oraz umieszczenie na liście TSL.

6.1.4 Rozmiary kluczy

Minimalne parametry algorytmów szyfrowych dopuszczonych do stosowania przez EuroCert oraz odbiorców usług certyfikacyjnych w ramach Polityki 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.

Do realizacji pieczęci elektronicznej pod certyfikatem subskrybenta stosowany jest algorytm RSA/ECDSA w kombinacji z funkcją skrótu SHA-1/ SHA-512.

Klucze urzędu certyfikacji mają długość 4096 bitów RSA lub 384 bitów ECC. Klucze subskrybentów mają długość co najmniej 2048 bitów RSA lub 384 bitów ECC.

6.1.5 Cel użycia kluczy

Zastosowanie klucza określone jest w polu KeyUsage (OID: 2.5.29.15), które stanowi jedno z podstawowych rozszerzeń certyfikatów (patrz § 7.1.2). Pole to podlega obligatoryjnej weryfikacji przez strony ufające oraz aplikacje korzystające z certyfikatu.

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).

Certyfikaty subskrybentów mogą być używane wyłącznie do składania kwalifikowanych podpisów elektronicznych i jest przeznaczony do zapewnienia niezaprzeczalności (nonRepudiation).

6.2 Ochrona klucza prywatnego oraz techniczna kontrola modułu kryptograficznego

Każdy subskrybent, a także personel urzędu certyfikacji i operatorzy punktów rejestracji przechowują, użytkują i niszczą swój klucz prywatny tak sposób, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu.

6.2.1 Standardy modułu kryptograficznego

Klucze prywatne Subskrybentów związane z kwalifikowanymi certyfikatami przetwarzane są wyłącznie w kwalifikowanych urządzeniach do składania podpisu elektronicznego, spełniających wymagania określone w załączniku II Rozporządzenia eIDAS. Te urządzenia jak również moduł kryptograficzny (HSM-Hardware Security Module), w którym przechowywany jest klucz prywatny EuroCert posiadają certyfikat zgodności z Common Criteria EAL4+.

6.2.2 Deponowanie klucza prywatnego

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

6.2.3 Kopie zapasowe klucza prywatnego

Mechanizm zapewnienia kopii zapasowej klucza prywatnego EuroCert jest realizowany dzięki podziałowi klucza na części (tzw. sekrety) w liczbie większej niż jest wymagana do odtworzenia klucza. Przyjęta liczba podziałów klucza na sekrety oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w tab. 5.

Tab. 5. Schemat podziału klucza prywatnego

Urząd certyfikacji	Całkowita liczba sekretów [n]	Liczba sekretów koniecznych do użycia klucza [m]
Centrum Kwalifikowane EuroCert	4	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.

W razie konieczności odtworzenia klucza z kopii zapasowych wykonywana jest procedura wprowadzania klucza do modułu opisana w § 6.2.5.

Klucze prywatne subskrybenta związane z certyfikatami służącymi do weryfikacji podpisów elektronicznych nie mogą podlegać procedurom tworzenia kopii zapasowych.

6.2.4 Archiwizowanie klucza prywatnego

Klucze prywatne subskrybenta związane z certyfikatami służącymi do weryfikacji podpisów elektronicznych, klucze prywatne EuroCert służące do realizacji pieczęci elektronicznych oraz klucze prywatne Inspektorów rejestracji służące do podpisywania zgłoszeń certyfikacyjnych nie mogą podlegać procedurom archiwizowania.

Klucze prywatne urzędu certyfikacji służące do realizacji pieczęci elektronicznych nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywania przy ich użyciu operacji podpisywania lub upływie okresu ważności komplementarnego z nimi certyfikatu dostawcy usług zaufania lub jego unieważnieniu.

6.2.5 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Wprowadzanie klucza prywatnego do modułów kryptograficznych realizowane jest w sytuacjach:

a) uruchomienia ośrodka certyfikacji, podczas startu systemu,
b) odtworzenia klucza urzędu certyfikacji w ośrodku zapasowym,
c) wymiany modułu kryptograficznego.

Załadowanie klucza do modułu odbywa się przy udziale posiadaczy współdzielonych sekretów. Do załadowania klucza konieczna jest obecność liczby sekretów opisana w § 6.2.3. Ładowanie 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. Ładowanie klucza do modułu odnotowane jest w rejestrze zdarzeń.

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.

6.2.6 Przechowywanie klucza prywatnego w module kryptograficznym

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.

Klucz urzędu certyfikacji oraz subskrybentów przechowywane są na kartach kryptograficznych chronionych kodami PIN i PUK.

6.2.7 Aktywacja klucza prywatnego

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 pozostają w stanie aktywności aż do momentu jego fizycznego usunięcia z modułu (wyjęcia karty z HSM) lub wyłączenia urządzenia HSM.

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 lub innym nośniku.

6.2.8 Dezaktywacja klucza prywatnego

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 urzędu certyfikacji. Dezaktywowanie klucza polega na wyczyszczeniu pamięci modułu kryptograficznego z załadowanych kluczy. Każda dezaktywacja klucza prywatnego jest odnotowywana w rejestrze zdarzeń.
Dezaktywowanie klucza prywatnego subskrybenta następuje natychmiast po zrealizowaniu podpisu elektronicznego.

6.2.9 Metody niszczenia klucza prywatnego

Niszczenie kluczy prywatnych Subskrybentów wykonywane jest odpowiednio poprzez logiczne usunięcie klucza z nośnika (z karty kryptograficznej, urządzenia HSM, itp.), fizyczne zniszczenie nośnika kluczy (np. z karty kryptograficznej).

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.). 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.

6.3 Inne aspekty zarządzania parą kluczy

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

6.3.1 Archiwizowanie kluczy publicznych

EuroCert prowadzi długoterminową archiwizację swoich kluczy publicznych w postaci certyfikatów, na takich zasadach, jakim podlegają inne archiwowane dane (patrz § 5.5).

Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów elektronicznych po upłynięciu okresu ważności certyfikatu urzędu certyfikacji i zakończeniu jego działalności operacyjnej.

Archiwizacji dokonuje Inspektor bezpieczeństwa. Archiwizacja wykonywana jest poprzez zapisanie plików z certyfikatami na nośniki optyczne. Pliki archiwum opatrzone są podpisem elektronicznym Inspektora bezpieczeństwa. Szczegóły tworzenia archiwum elektronicznego zawiera punkt 5.5. Okres archiwizacji kluczy publicznych urzędu certyfikacji wynosi 20 lat.

6.3.2 Okres ważności certyfikatów i kluczy prywatnych

Okres ważności kluczy prywatnych i certyfikatów Subskrybentów przewidziany przez Politykę wynosi maksymalnie 2 lata i jest określony w polu validity każdego certyfikatu. Data początku ważności certyfikatu pokrywa się z datą jego wydania.

6.4 Dane aktywujące

Subskrybent natychmiast po wygenerowaniu certyfikatu i pary kluczy na karcie kryptograficznej, przy pomocy aplikacji do zarządzania kartą dostarczonej przez EuroCert nadaje kody PIN i PUK zabezpieczające dostęp do karty poświadczając dokonanie tej czynności własnoręcznym podpisem w pisemnym oświadczeniu.

Nadane przez subskrybenta kody PIN PUK znane są 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. 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.

Uaktywnienie klucza urzędu certyfikacji EuroCert opisane jest w § 6.2.7.

6.5 Zabezpieczenia komputerów

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 rozporządzenia eIDAS.

6.6 Cykl życia zabezpieczeń technicznych

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.

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

Dostęp do systemu EuroCert, w ramach którego świadczone są kwalifikowane usługi zaufania, jest zabezpieczony na poziomie określonym dla świadczenia kwalifikowanych usług zaufania polegających na wydawaniu certyfikatów przez kwalifikowanego dostawcę tych usług.

Nadzór nad bezpieczeństwem sieci komputerowych EuroCert sprawują specjaliści EuroCert.

6.8 Znakowanie czasem

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

Profile certyfikatów i list CRL wydawanych zgodnie z Polityką 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.

Zgodnie ze stanowiskiem Ministerstwa Rozwoju Departament Gospodarki Elektronicznej, w okresie przejściowym, który wskazany został w Art. 51, ust. 2 Rozporządzenia eIDAS, EuroCert wykorzystuje w świadczonych przez siebie usługach kwalifikowanych algorytm SHA-1.

Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu, list CRL, stosowanych rozszerzeń.

7.1 Profil certyfikatu

Certyfikaty wydawane przez EuroCert według normy X.509 v3 są sekwencją wartości pól podstawowych oraz rozszerzeń, zdefiniowanych odpowiednio w § 7.1.1 oraz 7.1.2 poniżej.

7.1.1 Pola podstawowe

EuroCert obsługuje pola podstawowe certyfikatu opisane w tab. 7.

Tab. 7. Profil podstawowych pól certyfikatu

<table>
<tr><td>Nazwa pola</td><td colspan="2">Opis</td><td colspan="2">Wartość</td></tr>
<tr><td>Version</td><td colspan="2">certyfikat zgodny z wersją 3 standardu X.509.</td><td colspan="2">V3</td></tr>
<tr><td>SerialNumber</td><td colspan="2">Jednoznaczny w ramach urzędu certyfikacji EuroCert numer certyfikatu.</td><td colspan="2">Jednoznaczny numer seryjny certyfikatu nadany przez EuroCert.</td></tr>
<tr><td>SignatureAlgorithm</td><td colspan="2">identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji pieczęci elektronicznej przez urząd certyfikacji na certyfikacie</td><td colspan="2">SHA1WithRSAEncryption
(OID: 1.2.840.113549.1.1.5) lub
SHA512WithRSAEncryption
(OID: 1.2.840.113549.1.1.13) lub
ecdsa-with-SHA512
(OID: 1.2.840.10045.4.3.4)</td></tr>
<tr><td rowspan="8">Issuer (nazwa wyróżniająca (DN) wystawcy certyfikatu)</td><td rowspan="4">Profil nr 1</td><td>Common Name</td><td colspan="2">CN = Centrum Kwalifikowane EuroCert</td></tr>
<tr><td>Organization</td><td colspan="2">O = EuroCert Sp. z o.o.</td></tr>
<tr><td>Country</td><td colspan="2">C = PL</td></tr>
<tr><td>Organization identifier</td><td colspan="2">2.5.4.97 = VATPL-9512352379</td></tr>
<tr><td rowspan="4">Profil nr 2</td><td>CN</td><td colspan="2">Centrum Kwalifikowane EuroCert</td></tr>
<tr><td>O</td><td colspan="2">EuroCert Sp. z o.o.</td></tr>
<tr><td>C</td><td colspan="2">PL</td></tr>
<tr><td>SerialNumber</td><td colspan="2">Nr wpisu: 14</td></tr>
<tr><td>NotBefore</td><td colspan="2">data wystawienia certyfikatu</td><td colspan="2">data wystawienia certyfikatu</td></tr>
<tr><td>NotAfter</td><td colspan="2">data wygaśnięcia certyfikatu</td><td colspan="2">data wygaśnięcia certyfikatu</td></tr>
<tr><td>Subject</td><td colspan="2">Nazwa subskrybenta zgodna z wymaganiami określonymi w ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1,2,5.</td><td colspan="2">Identyfikator DN Subskrybenta (patrz § 3.1).</td></tr>
<tr><td rowspan="2">SubjectPublicKeyInfo</td><td colspan="2" rowspan="2">Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 5280 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (tzn. o identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego). Wartość klucza publicznego podmiotu wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz;</td><td>Public Key Algorithm (algorytm klucza publicznego):</td><td>sha1WithRSAEncryption lub SHA512WithRSAEncryption lub ecdsa-with-SHA512</td></tr>
<tr><td>RSA Public Key (długość klucza)</td><td>min. 2048 bit lub ECC 384 bit</td></tr>
</table>

SignatureValue	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 (wydawcy).

7.1.2 Rozszerzenia certyfikatu

EuroCert obsługuje pola rozszerzeń opisane w tab. 8.

Tab. 8. 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.	nonRepudiation (klucz do realizacji niezaprzeczalności)
CertificatePolicies	NIE	wskazanie na politykę certyfikacji, zgodnie z którą wystawiony jest certyfikat	Identyfikator polityki certyfikacji: 1.2.616.1.113791.1.2.1 lub 1.2.616.1.113791.1.2.2 lub 1.2.616.1.113791.1.2.3
CRLDistributionPoints	NIE	punkt dystrybucji listy CRL (określa adres URL, pod którymi jest publikowana aktualna lista CRL)	http://crl.eurocert.pl/qca03.crl lub http://crl.eurocert.pl/qca02.crl lub http://crl.eurocert.pl/qca04.crl
Authority Info Access	NIE	Dostęp do informacji o urzędzie	http://crl.eurocert.pl/OCSP/
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
qcCompliance	NIE	Deklaracja wystawcy certyfikatu	Oświadczenie, że certyfikat jest kwalifikowanym certyfikatem w rozumieniu eIDAS; OID: {itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) 1 1}
qcSSCD	NIE	Deklaracja wystawcy certyfikatu	wskazanie, że klucz prywatny jest przechowywany w kwalifikowanym urządzeniu do składania podpisów; OID: {0.4.0.1862.1.4}
qcPDS	NIE	Informacje o usługach EuroCert	Adres URL do dokumentu opisującego podstawowe warunki świadczenia usług zaufania w zakresie wydawania

			certyfikatów (PDS – PKI Disclosure Statements); OID: {0.4.0.1862.1.5}

7.2 Profil listy CRL

Lista unieważnionych i zawieszonych certyfikatów jest zbiorem pól, których znaczenie przedstawiono poniżej w tabeli 9.

Tab. 9. Profil listy CRL w formacie zgodnym ze standardem X.509 V2

Atrybut	Wartość
version	V2
SignatureAlgorithm identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji pieczęci elektronicznej przez urząd certyfikacji na liście CRL)	SHA1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) lub SHA512WithRSAEncryption (OID: 1.2.840.113549.1.1.13) lub 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 7 (Issuer)
thisUpdate	data i godzina wydania listy
nextUpdate	data i godzina następnego wydania listy (thisUpdate + nie więcej niż 24 godziny)
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.

7.3 Profil OCSP

Profil tokena weryfikacji statusu certyfikatów opisany jest w wewnętrznych niejawnych dokumentach EuroCert.

8 Audyt zgodności i inne oceny

Audyty są przeprowadzane w EuroCert w celu sprawdzenia zgodności postępowania EuroCert z wymaganiami nałożonymi na kwalifikowanych dostawców usług zaufania określonych w Rozporządzeniu eIDAS oraz procedurami i procesami opisanymi w dokumentacji EuroCert (w tym Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego).

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 Rozporządzenia eIDAS (audyt zewnętrzny).

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 § e) Rozporządzenia eIDAS.

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

Zagadnienia objęte audytem oraz procedury postępowania w przypadku wykrycia nieprawidłowości funkcjonowania urzędu certyfikacji przedstawiono w Kodeksie Postępowania Certyfikacyjnego.

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.

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.

Usługi związane z zawieszaniem oraz unieważnianiem certyfikatów oraz dostępem do list CRL są nieodpłatne.

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

9.2 Odpowiedzialność finansowa

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.

Odpowiedzialność finansowa EuroCert Sp. z o.o., 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.

9.3 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.

9.4 Ochrona danych osobowych

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.

EuroCert traktuje jako informacje poufne wszystkie informacje związane ze świadczeniem usług zaufania poza następującymi informacjami:

a) Polityka certyfikacji oraz Kodeks postępowania certyfikacyjnego,
b) certyfikaty dostawcy usług zaufania,
c) Listy CRL,
d) Certyfikaty infrastruktury,
e) Informacje bieżące, przeznaczone do publikacji (takie jak cennik usług, oferta handlowa, bieżące komunikaty, dane kontaktowe),
f) Informacje zawarte w treści certyfikatu, na publikację których zgodę wyraził subskrybent.

9.5 Zabezpieczenie własności intelektualnej

Prawa autorskie do niniejszego dokumentu posiada Eurocert Sp. z o.o. Może on być wykorzystywany wyłącznie w celu korzystania z certyfikatów. Wszelkie inne zastosowania, w tym wykorzystanie całości lub fragmentu dokumentu, wymaga pisemnej zgody Eurocert Sp. z o.o., z tym że Eurocert Sp. z o.o. wyraża zgodę na powielanie i publikowanie w całości niniejszego dokumentu.

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.

Certyfikat Centrum Kwalifikowane EuroCert jest własnością EuroCert Sp. z o.o. Udziela licencji na tworzenie kopii tego certyfikatu i umieszczanie jej w oprogramowaniu, w szczególności w magazynach certyfikatów lub sprzęcie wytwórcom oprogramowania lub sprzętu.

Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez EuroCert jest – w przypadku subskrybenta certyfikatu kwalifikowanego osobistego – własnością podmiotu tego certyfikatu, określonego w polu subject certyfikatu (patrz § 7.1.1) lub – w przypadku subskrybenta certyfikatu kwalifikowanego firmowego – własnością podmiotu reprezentowanego przez subskrybenta.

9.6 Oświadczenia i gwarancje

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 rozporządzenia eIDAS,

b) postępuje zgodnie z prawem, a w szczególności nie narusza postanowień Rozporządzenia 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 zaufania, 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.

Punkty rejestracji oraz osoby potwierdzające tożsamość zobowiązują się ponadto do:

a) przestrzegania procedur potwierdzania tożsamości przy wydawaniu certyfikatów zgodnie z zasadami określonymi w niniejszym dokumencie i Polityce certyfikacji, 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 Certyfikacji,
g) poddawania się planowym audytom przeprowadzonym lub zleconym przez EuroCert.

Obowiązki subskrybentów i stron ufających przedstawiono odpowiednio w § 4.5.1 i § 4.5.2

9.7 Wyłączenia odpowiedzialności z tytułu gwarancji

EuroCert nie odpowiada za jakiekolwiek szkody, które powstały lub mogły powstać dla odbiorców usług zaufania 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 § 4.5.1 oraz 4.5.2.

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 § 4.5.1 oraz 4.5.2.

9.9 Przenoszenie roszczeń odszkodowawczych

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

Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią do utraty ważności tych certyfikatów (z powodu zakończenia okresu ważności lub unieważnienia).

9.11 Określanie trybu i adresów doręczania pism

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

9.12 Zmiany w polityce certyfikacji

Zmiana identyfikatora (OID) Polityki może nastąpić jedynie w przypadku zmiany podmiotu zarządzającego urzędem certyfikacji Centrum Kwalifikowane EuroCert oraz w przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników Polityki.

9.13 Rozstrzyganie sporów

Przedmiotem rozstrzygania sporów mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania kwalifikowanego certyfikatu w oparciu o regulacje Kodeksu Postępowania Certyfikacyjnego Kwalifikowanych oraz zawartych umów.

Spory bądź zażalenia powstałe na tle użytkowania certyfikatów, tokenów weryfikacji statusu 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.

Spory związane z kwalifikowanymi usługami zaufania świadczonymi przez EuroCert będą w pierwszej kolejności rozstrzygane na drodze postępowania pojednawczego.

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.

W przypadku wystąpienia innych sporów będących konsekwencją użycia certyfikatu wydanego lub innych kwalifikowanych usług świadczonych przez EuroCert, subskrybent zobowiązuje się pisemnie poinformować EuroCert o przedmiocie powstałego sporu.

9.14 Obowiązujące prawo

Funkcjonowanie EuroCert oparte jest na zasadach zawartych w niniejszej Polityce certyfikacji, Kodeksie postępowania certyfikacyjnego oraz obowiązujących przepisach prawa. W celu interpretacji terminów zawartych w Polityce należy je rozpatrywać zgodnie z Rozporządzeniem eIDAS i Ustawą o usługach zaufania.

9.15 Podstawy prawne

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

Patrz: Kodeks postępowania certyfikacyjnego.

9.17 Inne postanowienia

Nie występują.

Historia dokumentu

Wersja	Data zatwierdzenia	Opis zmian
1.0	01 sierpnia 2013 r.	utworzenie dokumentu
1.1	27 listopada 2013 r.	Powtórne złożenie dokumentu
1.2	15.03.2015 r.	Zmiana adresu w danych kontaktowych
1.3	20.11.2015 r.	Zmiana adresu w danych kontaktowych
2.0	14.06.2017	Dostosowanie do wymogów rozporządzenia eIDAS oraz ustawy o usługach zaufania.
3.0	15.11.2017	Uwzględnienie w profilu certyfikatu kluczy RSA (3072 bit) oraz ECDSA. Drobne poprawki redakcyjne.