Polityka Certyfikacji
i
Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert

Wersja 1

Zatwierdził
Stanowisko: Prezes Zarządu
Imię i nazwisko: Łukasz Konikiewicz

Data zatwierdzenia: 16.07.2018 r.
Data obowiązywania: 02.10.2018 r.

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

Spis treści

1 Wstęp

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert, (dalej „Regulacja") określa zasady świadczenia kwalifikowanych usług zaufania przez jednostkę organizacyjną EuroCert Sp. z o.o. – Centrum EuroCert (dalej „EuroCert"), obejmujących wystawianie:

a) kwalifikowanych certyfikatów do podpisu elektronicznego;
b) kwalifikowanych certyfikatów do pieczęci elektronicznej,
   zwanych dalej „certyfikatami", w tym unieważnianie i zawieszanie certyfikatów oraz informowania o statusie certyfikatu w oparciu o listy CRL oraz usługę OCSP;
c) kwalifikowanych elektronicznych znaczników czasu, zwanych dalej „znacznikami czasu".

Regulacja stanowi politykę certyfikacji dla każdej z wyżej wymienionych usług.

EuroCert jest kwalifikowanym dostawcą usług zaufania, działającym zgodnie z:

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

Struktura regulacji została stworzona na podstawie zaleceń RFC 3647[1].

1.1 Wprowadzenie

EuroCert wydaje certyfikaty i znaczniki czasu odpowiednio za pomocą urzędu certyfikacji Centrum Kwalifikowane EuroCert i urzędu znacznika czasu EuroCert QTSA.

Klucze publiczne do weryfikacji świadczonych usług zaufania:

a) klucz do podpisywania certyfikatów i list CRL,
b) klucz do podpisywania znaczników czasu

są dostępne w postaci certyfikatów dostawców usług zaufania wydanych przez ministra właściwego ds. informatyzacji lub upoważniony przez niego podmiot na podstawie art. 10.1 Ustawy o usługach zaufania.

Certyfikaty wydawane przez EuroCert zawierają w polu *certificate policies* (patrz punkt 7.1.2) identyfikatory polityk certyfikacji, które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Identyfikatory polityk certyfikacji umieszczane są również w znacznikach czasu.

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

1.2 Identyfikator i nazwa dokumentu

Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert jest dostępna w formie elektronicznej pod adresem: https://www.eurocert.pl/repozytorium. Regulacja posiada następujący zarejestrowany identyfikator obiektu (ang. Object Identifier – OID): 1.2.616.1.113791.1.2.

1.3 Elementy infrastruktury PKI

Infrastrukturę klucza publicznego EuroCert służącą do świadczenia kwalifikowanych usług zaufania tworzą:

a) kwalifikowany urząd certyfikacji: Centrum Kwalifikowane EuroCert,
b) kwalifikowany urząd znacznika czasu: EuroCert QTSA,
c) punkty rejestracji,
d) subskrybenci certyfikatów oraz znaczników czasu,
e) strony ufające.

1.3.1 Urzędy certyfikacji

Urząd certyfikacji Centrum Kwalifikowane EuroCert wystawia certyfikaty dla użytkowników końcowych (subskrybentów) oraz udostępnia informacje niezbędne do weryfikacji ważności tych certyfikatów.

Nadzór nad urzędem sprawuje minister właściwy ds. informatyzacji, który powierzył pełnienie roli nadrzędnego urzędu certyfikacji (tzw. „Root CA") Narodowemu Centrum Certyfikacji (dalej „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 – przez certyfikat urzędu certyfikacji Centrum Kwalifikowane EuroCert wystawiony przez NCCert – do certyfikat subskrybenta.

Zadania związane z przyjmowaniem wniosków o wydanie certyfikatów oraz wydawaniem certyfikatów, a także przyjmowaniem wniosków o unieważnienie, zawieszenie lub odwieszenie certyfikatów realizują punkty rejestracji.

Certyfikaty są wydawane przez Centrum Kwalifikowane EuroCert zgodnie z polityką NCP+ określoną w podrozdziale 5.3. normy ETSI EN 319 411-1.

Klucze prywatne subskrybentów certyfikatów mogą znajdować się na karcie elektronicznej. W przypadku karty elektronicznej klucz prywatny znajduje się pod wyłączną kontrolą subskrybenta (lub osoby reprezentującej subskrybenta w przypadku osoby prawnej lub innej jednostki organizacyjnej) i nie podlega operacji deponowania. Z kolei dla HSM, subskrybenci mają wyłączny dostęp do znajdującego się na nim klucza prywatnego po zalogowaniu do indywidualnego konta usługi.

1.3.2 Urząd znacznika czasu

Urząd znacznika czasu wydaje znaczniki czasu zgodnie z zaleceniami ETSI EN 319 422. Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość to 1.2.616.1.113791.1.4) oraz poświadczany jest wyłącznie przy pomocy klucza prywatnego wytworzonego wyłącznie dla usługi znakowania czasem.

Urząd znacznika czasu EuroCert QTSA działa na podstawie wpisu EuroCert na listę kwalifikowanych dostawców usług zaufania i w oparciu o certyfikat wydany mu przez ministra właściwego ds. informatyzacji lub wyznaczony przez niego podmiot (NCCert).

EuroCert QTSA przy świadczeniu usług elektronicznego znakowania czasem stosuje rozwiązania zapewniające synchronizację z międzynarodowym wzorcem czasu (ang. Coordinated Universal Time – UTC), z dokładnością do 1 sekundy.

Polityka EuroCert QTSA działa zgodnie z ETSI EN 319 411-2 oraz wskazuje na kwalifikowany znacznik czasu w rozumieniu Rozporządzenia eIDAS. Klucz tego Urzędu obecny jest na liście TSL i wskazuje na usługę kwalifikowaną.

1.3.3 Punkty rejestracji

Punkty rejestracji zajmują się obsługą subskrybentów. Mogą nimi być osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, po podpisaniu stosownej umowy z EuroCert.

Podległe EuroCert punkty rejestracji nie mogą akredytować innych punktów rejestracji.

Punkty rejestracji reprezentują EuroCert w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez EuroCert uprawnień w zakresie:

a) przyjmowania wniosków o wydanie certyfikatu,
b) potwierdzania tożsamości subskrybentów i ich uprawnień do otrzymania certyfikatów,
c) podpisywania umów z subskrybentami,
d) tworzenia zgłoszeń certyfikacyjnych i przekazywanie ich do urzędu certyfikacji,
e) przekazywania certyfikatów subskrybentom.

Zadania przewidziane dla punktu rejestracji realizują upoważnione osoby, zwane dalej „Operatorami”.

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

Lista aktualnych autoryzowanych punktów rejestracji dostępna jest na stronie internetowej https://sklep.eurocert.pl.

1.3.4 Subskrybenci

Subskrybentem certyfikatu podpisu elektronicznego może być wyłącznie osoba fizyczna.

Subskrybentem certyfikatu pieczęci elektronicznej może być wyłącznie osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej.

Organizacja pragnąca uzyskać certyfikat do pieczęci elektronicznej może to uczynić poprzez swoich upoważnionych przedstawicieli.

Subskrybentem znacznika czasu może być każda osoba fizyczna, osoba prawna w rozumieniu prawa krajowego, jak też inna jednostka o podobnym charakterze (jednostka organizacyjna nieposiadająca osobowości prawnej, spółka cywilna itd.).

1.3.5 Strony ufające

Strona ufająca jest podmiotem, który posługuje się certyfikatem innego podmiotu w celu zweryfikowania jego podpisu elektronicznego lub pieczęci elektronicznej.

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta (patrz punkt 4.5.2). Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego lub pieczęci elektronicznej. Informacje zawarte w

certyfikacie (m.in. identyfikator polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.3.6 Pozostali uczestnicy

Nie zdefiniowano.

1.4 Zakres stosowania certyfikatów

Certyfikaty podpisu elektronicznego służą do weryfikacji kwalifikowanych podpisów elektronicznych i są przeznaczone do zapewnienia niezaprzeczalności (ang. *non-repudiation*).

Kwalifikowany podpis elektroniczny weryfikowany za pomocą certyfikatu ma skutek prawny równoważny podpisowi własnoręcznemu.

Kwalifikowana pieczęć elektroniczna korzysta z domniemania integralności danych i autentyczności pochodzenia danych, z którymi kwalifikowana pieczęć jest powiązana.

Tab. 1. Rodzaje certyfikatów

Rodzaj certyfikatu		Zastosowanie
Kwalifikowany certyfikat podpisu elektronicznego	osobisty	weryfikacja kwalifikowanych podpisów elektronicznych składanych przez osoby fizyczne; certyfikat zawiera wyłącznie dane osoby fizycznej (przynajmniej: nazwę kraju, nazwisko i imię subskrybenta, numer seryjny).
	profesjonalny	weryfikacja kwalifikowanych podpisów elektronicznych, składanych przez osoby fizyczne; certyfikat zawiera oprócz danych osoby fizycznej także dane osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej reprezentowanej przez subskrybenta; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię subskrybenta, numer seryjny, nazwę własną reprezentowanego podmiotu.
Kwalifikowany certyfikat pieczęci elektronicznej		weryfikacja kwalifikowanych pieczęci elektronicznych; certyfikaty pieczęci elektronicznej zapewniają wysoki poziom wiarygodności tożsamości podmiotu certyfikatu pieczęci elektronicznej; są one wydawane jedynie dla osób prawnych i jednostek organizacyjnych nie posiadających osobowości prawnej; powinny być stosowane do składania kwalifikowanych pieczęci elektronicznych zapewniając integralność i autentyczność podpisywanej informacji.

1.4.1 Dozwolone obszary użycia certyfikatów

Klucze prywatne powiązane z certyfikatami powinny być stosowane do składania kwalifikowanych podpisów (pieczęci) 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.

Certyfikatów podpisu elektronicznego 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 (pieczęci) opublikowana jest w repozytorium (patrz rozdz. 2).

1.4.2 Zakazane obszary użycia certyfikatów

Certyfikatów nie wolno używać niezgodnie z przeznaczeniem oraz bez przestrzegania ewentualnych ograniczeń zastosowania danego certyfikatu zapisanymi 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).

Kwalifikowane certyfikaty pieczęci elektronicznej nie służą do wyrażania woli podmiotu, który się nim posługuje.

1.5 Zarządzanie dokumentem

Każda zmiana Regulacji, 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 jest wyraźnie oznaczona jako aktualna.

Aktualna wersja Regulacji jest publikowana w repozytorium (patrz rozdz. 2). Subskrybenci, strony ufające i punkty rejestracji zobowiązani są stosować się wyłącznie do aktualnej wersji Regulacji.

1.5.1 Odpowiedzialność za zarządzanie dokumentem

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

1.5.2 Dane kontaktowe

Wszelką korespondencję dotyczącą kwalifikowanych usług zaufania należy kierować na adres siedziby EuroCert:

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

1.5.3 Procedury zatwierdzania dokumentu

Zatwierdzenia zmian w Regulacji dokonuje zarząd EuroCert Sp. z o.o. Po zatwierdzeniu dokument otrzymuje status zatwierdzony ze wskazaniem daty początku obowiązywania.

1.6 Słownik używanych terminów i akronimów

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

Tab. 2. Terminy i skróty używane w Regulacji

Termin/ skrót	Opis
DN – Distinguished Names	Nazwa wyróżniająca podmiotu certyfikatu 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 – Certificate Revocation List	lista zawieszonych i unieważnionych certyfikatów.
PDS – PKI Disclosure Statement	Informacje o infrastrukturze klucza publicznego.
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
QSCD – Qualified Signature Creation Device	urządzenie posiadające certyfikat umożliwiający użycie do wystawiania kwalifikowanego podpisu elektronicznego (pieczęci elektronicznej), na podstawie Rozporządzenia eIDAS.
TSL – Trust Service Status List	listy wydawane przez Komisję Europejską oraz kraje członkowskie UE, zawierające informacje o podmiotach świadczących usługi zaufania, ich statusie (czy kwalifikowany) oraz dane umożliwiające weryfikację tokenów wystawianych przez podmioty świadczące usługi zaufania (czyli weryfikację kwalifikowanych certyfikatów, znaczników czasu itd.)

2 Repozytorium urzędu certyfikacji

2.1 Repozytorium

Repozytorium jest publicznym zbiorem dokumentów dotyczących subskrybentów, stron ufających, punktów rejestracji dostępnym 24/7 na stronie internetowej: https://eurocert.pl/repozytorium.

2.2 Publikacja informacji w repozytorium

W repozytorium publikowane są:

a) Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert,
b) certyfikaty dostawców usług zaufania,
c) Regulamin Kwalifikowanych Usług Zaufania EuroCert,
d) listy CRL,
e) wykaz kwalifikowanych urządzeń do składania podpisów (pieczęci) elektronicznych,
f) wzory umów, wniosków o wydanie certyfikatu, formularzy zamówień.

Informacje dotyczące kwalifikowanych usług zaufania świadczonych przez EuroCert są publikowane w repozytorium automatycznie (np. listy CRL) lub po zatwierdzeniu przez upoważnione osoby (np. certyfikaty dostawcy usług zaufania, Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert oraz pozostałe dokumenty).

2.3 Częstotliwość publikacji

Listy CRL są generowane i publikowane automatycznie, nie rzadziej niż co 24 godziny oraz w ciągu 1 godziny od żądania zawieszenia (unieważnienia) certyfikatu, natomiast pozostałe informacje każdorazowo, gdy zostaną uaktualnione lub zmienione.

2.4 Kontrola dostępu do repozytorium

Informacje umieszczone w repozytorium są zabezpieczone przed nieautoryzowanym zmienianiem, dodawaniem i usuwaniem oraz są przechowywane z zachowaniem kopii zapasowych.

3 Identyfikacja i uwierzytelnianie

Niniejszy rozdział przedstawia ogólne zasady weryfikacji tożsamości subskrybentów jakimi kieruje się EuroCert przy wydawaniu, zawieszaniu i unieważnianiu certyfikatów, które mają na celu uzyskanie pewności, że informacje przekazane we wniosku o wydanie certyfikatu są prawidłowe i odnoszą się do istniejącej osoby fizycznej oraz że wnioskodawca jest rzeczywiście tą osobą fizyczną, która została wymieniona we wniosku.

3.1 Nazewnictwo używane w certyfikatach

Certyfikaty wydawane przez Eurocert są zgodne ze standardem X.509. Nazwy subskrybentów oraz wystawcy certyfikatów umieszczane w certyfikatach są zgodne z nazwami wyróżniającymi (DN), budowanymi zgodnie z zaleceniami ITU z serii X.500 oraz ETSI EN 319 412.

3.1.1 Rodzaje nazw

Na podstawie danych zawartych we wniosku o wydanie certyfikatu tworzona jest nazwa wyróżniająca DN subskrybenta w oparciu o podzbiór poniższych atrybutów (tab. 3 i tab. 4).

Tab. 3. Nazwa subskrybenta dla certyfikatu do podpisu elektronicznego

Pola	Wartość
C*	Międzynarodowy dwuliterowy skrót nazwy kraju (dla Polski – PL).
G*	Imię (imiona) subskrybenta.
S*	Nazwisko subskrybenta plus ewentualnie nazwisko rodowe.
CN	Nazwa powszechna subskrybenta.
SERIALNUMBER*	numer paszportu, numer dowodu osobistego, numer PESEL, numer identyfikacji podatkowej subskrybenta lub lokalny identyfikator subskrybenta specyficzny dla danego kraju notyfikowany i rozpoznawalny na poziomie Unii Europejskiej zg. z pkt 5.1.3 ETSI EN 319 412-1. W przypadku subskrybenta identyfikującego się numerem PESEL atrybut *serialNumber* występuje zgodnie z normą ETSI EN 319 412-1 (punkt 5): „PNOPL-XXXXXXXXXXX”.
O	Nazwa organizacji zatrudniającej lub reprezentowanej przez subskrybenta.
OU	Nazwa jednostki organizacyjnej.
T	Nazwa stanowiska pracy pełnionego przez subskrybenta w organizacji.
ST	Województwo.
L	Miejscowość.
A	Adres pocztowy.

*- pole obowiązkowe

Tab. 4. Nazwa subskrybenta dla certyfikatu do pieczęci elektronicznej

Pola	Wartość
C*	Międzynarodowy dwuliterowy skrót nazwy kraju (dla Polski – PL).
CN	Nazwa powszechna subskrybenta.
ORGANIZATIONIDENTIFIER*	Identyfikator organizacji: numer identyfikacji podatkowej, numer rejestrowy w krajowym rejestrze gospodarczym lub identyfikator regionalny specyficzny dla danego kraju notyfikowany i rozpoznawalny na poziomie Unii Europejskiej zg. z pkt 5.1.4 ETSI EN 319 412-1.
O*	Oficjalna nazwa subskrybenta.
OU	Nazwa jednostki organizacyjnej subskrybenta.
ST	Województwo.
L	Miejscowość.
A	Adres pocztowy.

*- pole obowiązkowe

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

Subskrybent może posiadać dowolną liczbę certyfikatów zawierających tę samą nazwę wyróżniającą.

3.1.2 Konieczność używania nazw znaczących

Obowiązkowe dane w certyfikacie umożliwiające jednoznaczną identyfikację subskrybenta zostały zaznaczone w punkcie 3.1.1.

3.1.3 Anonimowość subskrybentów

EuroCert nie wystawia certyfikatów anonimowych, tzn. zawierających niedostateczne dane do jednoznacznej identyfikacji subskrybenta. Każdy identyfikator subskrybenta zawiera przynajmniej informacje zaznaczone jako obowiązkowe w punkcie 3.1.1.

3.1.4 Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez EuroCert w wydawanych przez siebie certyfikatach jest zgodna z profilem certyfikatów opisanym w ETSI EN 319 412 (części: 1,2,3,5). Przy konstrukcji i interpretacji nazw wyróżniających stosuje się zalecenia przedstawione w punkcie 3.1.1.

3.1.5 Unikalność nazw

EuroCert gwarantuje unikalność nazwy wyróżniającej subskrybenta w domenie kwalifikowanych usług zaufania EuroCert. Każdy wydany certyfikat posiada unikalny w ramach danego urzędu certyfikacji numer seryjny. Łącznie z nazwą wyróżniającą subskrybenta gwarantuje jednoznaczną identyfikację subskrybenta certyfikatu.

3.1.6 Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

Nazwa wyróżniająca subskrybenta powinna 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 subskrybenta polega na potwierdzeniu danych identyfikujących jego tożsamość oraz weryfikacji uprawnień subskrybenta do otrzymania certyfikatu przez operatora punktu rejestracji lub inspektora ds. rejestracji.

EuroCert oraz podległe mu punkty rejestracji potwierdzają tożsamość i wszelkie specjalne atrybuty osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej ubiegającej się o wydanie kwalifikowanego certyfikatu na podstawie ważnego dowodu osobistego, paszportu lub aktualnego wpisu do rejestru działalności gospodarczej właściwego dla rodzaju prowadzonej działalności, z zastrzeżeniem Art. 24 (c) Rozporządzenia eIDAS.

W szczególnym przypadku, gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego ani paszportu (oraz pozostałych dokumentów uwierzytelniających), a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone kwalifikowanym podpisem lub pieczęcią elektroniczną tej osoby – zgodnie z art. 24 (c) Rozporządzenia eIDAS.

3.2.1 Udowodnienie posiadania klucza prywatnego

Certyfikaty są wystawiane tylko dla pary kluczy wygenerowanej przez EuroCert.

3.2.2 Identyfikacja i uwierzytelnianie osób prawnych

Inspektor ds. rejestracji lub operator punktu rejestracji są zobowiązani zweryfikować posiadane przez subskrybenta pełnomocnictwo bądź upoważnienie zawsze wtedy, gdy subskrybent wnioskuje o:

a) wydanie certyfikatu kwalifikowanego podpisu elektronicznego (profesjonalnego), zawierającego wskazanie czy działa w imieniu innego podmiotu, którego dane znajdują się we wniosku,
b) wydanie pieczęci elektronicznej.

Uwierzytelnienie pełnomocnictw bądź uprawnień jest częścią procesu przetwarzania przez punkt rejestracji i urząd certyfikacji wniosku o wydanie kwalifikowanego certyfikatu podpisu elektronicznego osobie fizycznej, reprezentującej interesy innej osoby (fizycznej lub prawnej) lub pieczęci elektronicznej. Wydany certyfikat jest w tym przypadku zaświadczeniem, że osoba fizyczna może posługiwać się kluczem prywatnym działając w imieniu innej osoby.

Proces uwierzytelniania pełnomocnictw stosowany w EuroCert oprócz weryfikacji samych pełnomocnictw obejmuje także uwierzytelnienie osoby fizycznej, która otrzymała pełnomocnictwo bądź upoważnienie.

Proces potwierdzania pełnomocnictw polega na weryfikacji dostarczonego pełnomocnictwa na podstawie:

a) przedłożonych dokumentów upoważniających (np. notarialnie potwierdzonego dokumentu udzielenia pełnomocnictwa przez osobę fizyczną),
b) sprawdzeniu czy dokument taki został podpisany przez osobę upoważnioną do reprezentacji,
c) na sprawdzeniu zgodności danych podmiotu prawnego umieszczonych we wniosku z dostarczonymi dokumentami.

3.2.3 Weryfikacja tożsamości osób fizycznych

Weryfikacja tożsamości osób fizycznych dokonywana jest przez upoważnioną przez EuroCert osobę w punkcie rejestracji na podstawie ważnego 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 wypis z Centralnej Ewidencji i Informacji o Działalności Gospodarczej,
d) innych dokumentów, które są niezbędne do potwierdzenia danych zawartych we wniosku o certyfikat, np. zaświadczenia o miejscu zatrudnienia, potwierdzenia prawa do wykonywania określonego zawodu.

Osoba potwierdzająca tożsamość osoby fizycznej w imieniu EuroCert, poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem pod 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 lub NIP,
e) serię, numer i rodzaj dokumentu tożsamości oraz oznaczenie organu wydającego ten dokument,
f) adres poczty elektronicznej e-mail oraz nr telefonu.

W przypadku potwierdzania tożsamości przez notariusza wnioskodawca jednostronnie podpisuje umowę z EuroCert w obecności notariusza, która po przekazaniu do EuroCert jest podpisywana przez inspektora ds. rejestracji i odsyłana na adres wskazany przez wnioskodawcę.

Przed wystawieniem certyfikatu wnioskodawca jest zobowiązany potwierdzić zapoznanie się z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert, Regulaminem Kwalifikowanych Usług Zaufania (zawierającym m.in. informacje o warunkach użycia certyfikatów, zakresie i ograniczeniach stosowania certyfikatów, skutkach prawnych 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.

3.2.4 Dane subskrybenta niepodlegające weryfikacji

EuroCert weryfikuje wszystkie dane, które mają być umieszczone w certyfikacie (patrz punkt 3.1.1).

3.2.5 Sprawdzanie praw do otrzymania certyfikatu

Przed przekazaniem certyfikatu podpisu elektronicznego (pieczęci elektronicznej) EuroCert sprawdza tożsamość subskrybenta (osoby reprezentującej subskrybenta) na podstawie okazanego przez niego (nią) dokumentu tożsamości.

3.2.6 Kryteria interoperacyjności

Nie dotyczy.

3.3 Identyfikacja i uwierzytelnianie przy odnawianiu certyfikatu

Odnowienie certyfikatu oznacza wydanie dotychczasowemu subskrybentowi nowego certyfikatu tego samego typu i nowej pary kluczy. Odnowienie certyfikatu wymaga ponownej weryfikacji tożsamości subskrybenta zgodnie z opisem w podrozdz. 3.2 lub metodą uproszczoną przedstawioną w punkcie 3.3.1 poniżej, zgodną z art. 24 ust. 1 lit. c) Rozporządzenia eIDAS.

3.3.1 Odnowienie certyfikatu w okresie ważności obecnego certyfikatu

Potwierdzenie tożsamości subskrybenta posiadającego ważny certyfikat kwalifikowany nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu (oraz pozostałych dokumentów uwierzytelniających), a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone kwalifikowanym podpisem elektronicznym (kwalifikowaną pieczęcią elektroniczną) tej osoby, o ile dane te nie różnią się od danych zawartych w certyfikacie związanym z kwalifikowanym podpisem elektronicznym (kwalifikowaną pieczęcią elektroniczną), 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 (pieczęci elektronicznej) złożonego pod wnioskiem o certyfikat oraz potwierdzeniu autentyczności związanego z podpisem (pieczęcią) certyfikatu (w oparciu o tzw. ścieżkę certyfikacji). Nie oznacza to jednak brak możliwości zastosowania procedury opisanej w podrozdz. 3.2.

3.3.2 Odnowienie po wygaśnięciu lub unieważnieniu certyfikatu

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

3.4 Identyfikacja i uwierzytelnianie przy unieważnianiu lub zawieszaniu certyfikatu

O unieważnienie lub zawieszenie certyfikatu może wystąpić:

a) subskrybent (w przypadku certyfikatu do pieczęci elektronicznej – osoba fizyczna reprezentująca subskrybenta),
b) organizacja reprezentowana przez subskrybenta (osobę fizyczną), której dane zostały zawarte w certyfikacie,
c) minister właściwy ds. informatyzacji,
d) EuroCert,
e) inna osoba, jeżeli wynika to z umowy o świadczenie usług zaufania lub innych zobowiązań EuroCert.

Certyfikat można unieważnić lub zawiesić:

a) osobiście w EuroCert pod adresem podanym w punkcie 1.5.2, w godzinach 8.00-16.00,
b) telefonicznie na numer infolinii: 22 490 49 86, przez całą dobę, m.in. na podstawie hasła do unieważnienia certyfikatu przyznanego razem z certyfikatem,
c) wysyłając drogą elektroniczną na adres uniewaznienia@eurocert.pl wypełnionego i podpisanego kwalifikowanym podpisem elektronicznym (kwalifikowaną pieczęcią elektroniczną) wniosku o unieważnienie/zawieszenie certyfikatu dostępnego na stronie internetowej https://eurocert.pl/index.php/dokumenty/zawieszenie-lub-uniewaznienie-certyfikatu,
d) wypełniając formularz na stronie internetowej https://eurocert.pl/uniewaznienia/.

Podstawą przyjęcia wniosku o unieważnienie/zawieszenie certyfikatu jest pomyślna weryfikacja przez inspektora ds. rejestracji:

a) tożsamości wnioskodawcy i prawa tej osoby do wnioskowania o unieważnienie/zawieszenie certyfikatu,
b) danych zawartych we wniosku o unieważnienie/zawieszenie certyfikatu.

W przypadku braku możliwości kompletnego uwierzytelnienia wniosku o unieważnienie przez inspektora ds. rejestracji certyfikat zostaje zawieszony do czasu wyjaśnienia powstałych niezgodności lub wniosek o unieważnienie zostaje odrzucony.

4 Wymagania funkcjonalne

Procedura uzyskiwania certyfikatu rozpoczyna się od złożenia stosownego wniosku w punkcie rejestracji, skierowanego do urzędu certyfikacji lub urzędu elektronicznego znacznika czasu. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania subskrybenta.

4.1 Składanie wniosków

Wniosek o wygenerowanie kluczy i certyfikatu przedkładany jest osobiście w formie papierowej (własnoręcznie podpisany) lub drogą elektroniczną (podpisany kwalifikowanym podpisem elektronicznym lub kwalifikowaną pieczęcią elektroniczną) w punkcie rejestracji. Wniosek jest podpisywany zawsze przez subskrybenta dla którego ma zostać wydany certyfikat. Organizacje pragnące uzyskać pieczęć elektroniczną, mogą to uczynić poprzez swoich upoważnionych przedstawicieli w ten sam sposób co osoby fizyczne działające we własnym imieniu.

4.1.1 Kto składa wniosek o certyfikat

O wydanie certyfikatu mogą się ubiegać osoby fizyczne (we własnym imieniu) oraz osoby prawne i organizacje nieposiadające osobowości prawnej poprzez uprawnionych przedstawicieli.

4.1.2 Rejestracja wniosku

Wniosek o wydanie certyfikatu po raz pierwszy składany jest przez wnioskodawcę w punkcie rejestracji osobiście lub poprzez elektroniczny formularz (w tym przypadku konieczne jest potwierdzenie tożsamości za pośrednictwem notariusza lub operatora punktu rejestracji). Wniosek o odnowienie certyfikatu, którego termin ważności nie upłynął składany jest wyłącznie poprzez elektroniczny formularz.

4.2 Przetwarzanie wniosku

Wniosek o wydanie certyfikatu podlega obowiązkowemu uwierzytelnieniu przez operatora punktu rejestracji zgodnie z postanowieniami podrozdz. 3.2 lub 3.3.

4.2.1 Wykonywanie funkcji identyfikacji i uwierzytelniania

Funkcje identyfikacji i uwierzytelniania wszystkich wymaganych danych subskrybenta są realizowane przez punkty rejestracji zgodnie z warunkami określonymi w rozdz. 3.

4.2.2 Przyjęcie/odrzucenie wniosku

EuroCert może odrzucić wniosek o wydania certyfikatu, gdy:

a) identyfikator subskrybenta (DN) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,
b) istnieje uzasadnione podejrzenie, że subskrybent sfałszował lub podał nieprawdziwe dane we wniosku,
c) subskrybent nie dostarczył kompletu wymaganych dokumentów,
d) został on podpisany przez osobę nieuprawnioną do reprezentacji subskrybenta (dotyczy certyfikatów pieczęci elektronicznych),
e) z innych ważnych nie wymienionych powyżej przyczyn, po uprzednim uzgodnieniu odmowy z inspektorem bezpieczeństwa.

EuroCert może odmówić wydania certyfikatu dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą wskutek poniesionych przez wnioskodawcę (w wyniku odmowy) strat lub kosztów. EuroCert zwraca w takim przypadku wnioskodawcy wniesioną przez niego opłatę za wydanie certyfikatu (jeśli dokonał stosownej

przedpłaty), chyba że wnioskodawca we wniosku o wydanie certyfikatu umieścił sfałszowane lub nieprawdziwe dane.

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

4.2.3 Okres oczekiwania na przetworzenie wniosku

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

Po pomyślnym uwierzytelnieniu wnioskodawcy operator punktu rejestracji przygotowuje token zgłoszenia certyfikacyjnego i przesyła go do urzędu certyfikacji, w celu wygenerowania certyfikatu przez inspektora ds. rejestracji. EuroCert, generując certyfikat, poświadcza elektronicznie klucz publiczny wraz z danymi o subskrybencie.

4.3.1 Czynności urzędu certyfikacji podczas wydawania certyfikatu

Inspektor ds. rejestracji podpisuje elektronicznie token zgłoszenia certyfikacyjnego, a następnie przesyła go do systemu generującego certyfikaty uruchamiając procedurę generowania certyfikatu na kwalifikowanym urządzeniu do składania podpisu elektronicznego (pieczęci elektronicznej).

Operator punktu rejestracji personalizuje kartę oraz zabezpiecza ją poprzez nadanie kodów PIN i PUK do karty zapisanych w bezpiecznej kopercie. Certyfikaty wydawane są bezpośrednio subskrybentowi albo za pośrednictwem osoby uprawnionej w przypadku kwalifikowanych certyfikatów pieczęci elektronicznej.

4.3.2 Informowanie subskrybenta o wydaniu certyfikatu

O wydaniu certyfikatu subskrybent informowany jest osobiście przez osobę weryfikującą jego dane osobowe, gdyż para kluczy i certyfikat generowane są w obecności subskrybenta, natychmiast po pomyślnym przeprowadzeniu etapu weryfikacji tożsamości. Jeśli w certyfikacie zawarto dane osoby trzeciej (np. dane podmiotu reprezentowanego przez subskrybenta), osoba ta jest również informowana o wydaniu certyfikatu.

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

Wstępna akceptacja certyfikatu jest wykonywana przez inspektora ds. rejestracji niezwłocznie po wystawieniu certyfikatu przez urząd certyfikacji, a przed nagraniem go na jakikolwiek nośnik. Inspektor ds. rejestracji sprawdza, czy dane zawarte w certyfikacie są prawidłowe. Jeśli zawiera on jakiekolwiek wady, to powinien zostać niezwłocznie unieważniony, a na jego miejsce wydany nowy pozbawiony

błędów bez obciążania subskrybenta kosztami za tę operacje. W takiej sytuacji nie wymaga się podpisania umowy i/lub dostarczenia dodatkowych dokumentów.

4.4.1 Potwierdzenie akceptacji certyfikatu

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 przechowywany przez EuroCert. Drugi egzemplarz otrzymuje subskrybent.

W przypadku certyfikatów wydawanych online (patrz podrozdz. 4.7) akceptacja certyfikatu przez subskrybenta następuje poprzez pobranie go z systemu EuroCert i zainstalowanie na bezpiecznym urządzeniu.

4.4.2 Publikacja certyfikatu

Certyfikaty nie są publikowane poza siecią wewnętrzną EuroCert.

4.4.3 Poinformowanie innych podmiotów o wydaniu certyfikatu

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

4.5 Korzystanie z pary kluczy i certyfikatu

Certyfikaty mogą być wykorzystywane wyłącznie do weryfikowania podpisów lub pieczęci elektronicznych, zgodnie z niniejszą Regulacją, z uwzględnieniem ewentualnych ograniczeń zapisanych w certyfikacie.

Klucz prywatny związany z certyfikatem może służyć wyłącznie do celów wynikających z zastosowań zapisanych w powiązanym z nim certyfikacie.

Klucz prywatny do podpisu elektronicznego powinien pozostawać w wyłącznej dyspozycji subskrybenta – osoby fizycznej, której dane są umieszczone w certyfikacie. Nie jest dopuszczalne, aby kluczem tym posługiwała się inna osoba.

Klucz prywatny do pieczęci elektronicznej powinien pozostawać w wyłącznej dyspozycji osoby lub osób upoważnionych przez daną organizację.

4.5.1 Zobowiązania subskrybenta

Subskrybent zobowiązuje się do:

a) informowania EuroCert o wszelkich zmianach informacji zawartych w jego certyfikacie, w celu unieważnienia certyfikatu i ewentualnie wystawienia nowego, zawierającego poprawne dane,
b) sprawdzenia poprawności danych zawartych w certyfikacie niezwłocznie po jego otrzymaniu i w przypadku wystąpienia jakichkolwiek nieprawidłowości, w szczególności nieprawidłowych danych określających tożsamość subskrybenta niezwłocznego zgłoszenia tego faktu EuroCert celem unieważnienia certyfikatu i wygenerowania nowego certyfikatu z prawidłowymi danymi,
c) niezwłocznego złożenia wniosku o unieważnienie certyfikatu w przypadku powzięcia uzasadnionego podejrzenia, że dostęp do klucza prywatnego ma osoba nieupoważniona (np. utraty klucza prywatnego, ujawnienia haseł dostępu) oraz zaistnienia okoliczności wymienionych w punkcie 4.9.1,

d) 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,
e) używania kluczy prywatnych i certyfikatów tylko w okresie ich ważności oraz zgodnie z ich przeznaczeniem określonym w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert oraz wskazanym w treści certyfikatu (w polu keyUsage),
f) nieużywania klucza prywatnego w okresie zawieszenia certyfikatu.

4.5.2 Zobowiązania strony ufającej

Strony ufające są zobowiązane do:

a) używania kluczy prywatnych i certyfikatów tylko w okresie ich ważności oraz zgodnie z ich przeznaczeniem określonym w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert oraz wskazanym w certyfikacie (w polu keyUsage),
b) zaufania tylko tym certyfikatom, które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca,
c) używania kluczy publicznych i certyfikatów tylko po zweryfikowaniu ich statusu oraz ważności pieczęci elektronicznej urzędu certyfikacji, który wystawił certyfikat,
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 certyfikacji 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.

4.6 Odnawianie certyfikatu dla starej pary kluczy

Nie ma możliwości zastąpienie używanego (aktualnie ważnego) certyfikatu nowym certyfikatem bez zmiany klucza publicznego lub jakiejkolwiek innej informacji (poza nowym okresem ważności, numerem seryjnym i podpisem urzędu certyfikacji) zawartej w zastępowanym certyfikacie (patrz podrozdz. 4.7).

4.7 Odnawianie certyfikatu dla nowej pary kluczy

Odnowienie certyfikatu, o którym mowa w podrozdz. 3.3 jest nierozerwalnie związane z wygenerowaniem nowej pary kluczy.

Odnowienie 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 (pieczęci elektronicznej subskrybenta złożonego pod zgłoszeniem certyfikacyjnym.

4.7.1 Warunki odnawiania certyfikatu

Subskrybent w każdej chwili może wystąpić z wnioskiem o odnowienie certyfikatu, lecz nie później niż po upływie okresu ważności certyfikatu.

Odnowienie 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.

Weryfikacja tożsamości subskrybenta w tym przypadku realizowana jest na podstawie podpisu elektronicznego (pieczęci elektronicznej), złożonego pod wnioskiem o wydanie certyfikatu.

4.7.2 Kto może żądać wydania kolejnego certyfikatu?

Odnowienie certyfikatu następuje z inicjatywy subskrybenta posiadającego ważny certyfikat wydany przez kwalifikowanego dostawcę usług zaufania.

4.7.3 Przetwarzanie wniosku o wydanie kolejnego certyfikatu

Procedura przetwarzania wniosku o odnowienie certyfikatu jest zgodna z procedurą opisaną w punkcie 3.3.1.

4.7.4 Informowanie podmiotu o wydaniu certyfikatu

Informacja o wygenerowaniu certyfikatu jest przekazywana subskrybentowi elektronicznie.

4.7.5 Akceptacja certyfikatu

Patrz punkt 4.4.1.

4.7.6 Publikacja certyfikatu

Patrz punkt 4.4.2.

4.7.7 Powiadomienie innych podmiotów o wydaniu certyfikatu

Patrz punkt 4.4.3.

4.8 Modyfikacja certyfikatu

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

4.8.1 Warunki modyfikacji certyfikatu

Konieczność zmiany danych w certyfikacie oznacza wygenerowanie nowego certyfikatu. Nowy certyfikat posiada nowy klucz publiczny, nowy numer seryjny i różni się zawartością przynajmniej jednego z pozostałych pól certyfikatu.

4.8.2 Kto może żądać zmiany danych w certyfikacie?

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 punkt 4.5.1).

4.8.3 Przetwarzanie wniosku o modyfikację certyfikatu

Procedura przetwarzania wniosku o modyfikację danych w certyfikacie jest taka sama jak w przypadku wydawania nowego certyfikatu i wymaga zweryfikowania wszystkich informacji zgodnie z podrozdz. 3.2.

4.8.4 .Informowanie podmiotu o wydaniu zmodyfikowanego certyfikatu

Patrz punkt 4.3.2.

4.8.5 Akceptacja certyfikatu

Patrz punkt 4.4.1.

4.8.6 Publikacja certyfikatu

Patrz punkt 4.4.2.

4.8.7 Powiadomienie innych podmiotów o wydaniu certyfikatu

Patrz punkt 4.4.3.

4.9 Unieważnienie i zawieszenie certyfikatu

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

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) nastąpiło naruszenie bezpieczeństwa kryptograficznego klucza prywatnego subskrybenta powiązanego z kluczem publicznym w certyfikacie, lub istnieje uzasadnione podejrzenie, iż fakt taki mógł mieć miejsce, (np. w wyniku utraty klucza prywatnego, nieuprawnionego dostępu do klucza prywatnego, zagubienia klucza prywatnego, kradzieży klucza prywatnego, przypadkowego zniszczenie klucza prywatnego),
c) ustąpiły okoliczności uzasadniające zamieszczenie danych organizacji w certyfikacie (np. zwolnienie pracownika, zmiana zakresu obowiązków itd.),
d) EuroCert zaprzestaje świadczenia usług zaufania w zakresie certyfikatów i nie kontynuuje usługi udostępniania informacji o statusie certyfikatu,
e) istnieje dowód, że certyfikat był wykorzystany niezgodnie z przeznaczeniem,
f) certyfikat był wydany niezgodnie z niniejszą Regulacją,
g) nastąpiło naruszenie bezpieczeństwa klucza prywatnego urzędu certyfikacji lub zachodzi uzasadnione podejrzenie, że takie naruszenie mogło mieć miejsce.

4.9.2 Kto może żądać unieważnienia certyfikatu

Z żądaniem unieważnienia certyfikatu mogą występować następujące podmioty:

a) subskrybent będący podmiotem unieważnianego certyfikatu,
b) upoważniony przedstawiciel reprezentowanego przez subskrybenta podmiotu, którego dane występują w certyfikacie,
c) osoba reprezentująca subskrybenta, niebędącego osobą fizyczną (dotyczy certyfikatów pieczęci elektronicznych),
d) wystawca certyfikatu, (tj. EuroCert), np. wskutek rażącego naruszenia przez subskrybenta zasad Regulacji, umowy, regulaminu usług zaufania, a w szczególności obowiązków określonych w punkcie 4.5.1,
e) minister właściwy ds. informatyzacji,
f) operator punktu rejestracji, inspektor ds. rejestracji, którzy mogą wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli są w posiadaniu informacji uzasadniającej unieważnienie certyfikatu.

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

Jeśli wnioskujący o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu (subskrybentem), to urząd certyfikacji:

- sprawdza, czy dany wnioskodawca może żądać unieważnienia certyfikatu,
- wysyła powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

4.9.3 Procedura unieważniania certyfikatu

Certyfikat jest unieważniany po pomyślnej weryfikacji wniosku o unieważnienie przez inspektora ds. rejestracji zgodnie z zasadami w podrozdz. 3.4. W przypadku, gdy istnieją przesłanki do unieważnienia certyfikatu, jednakże inspektor ds. 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 (patrz punkt 4.9.7 oraz 7.2). EuroCert przekazuje subskrybentowi certyfikatu oraz stronie ubiegającej się o unieważnienie za pośrednictwem poczty elektronicznej potwierdzenie unieważnienia lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy.

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

4.9.4 Dopuszczalny okres zwłoki w unieważnieniu certyfikatu

EuroCert gwarantuje unieważnienie certyfikatu w ciągu 1 godziny od otrzymania kompletnego wniosku.

4.9.5 Maksymalny czas przetwarzania wniosku o unieważnienie

Maksymalny dopuszczalny czas na przetworzenie wniosku o unieważnienie certyfikatu wynosi 1 godzinę od momentu wpłynięcia kompletnego wniosku.

4.9.6 Obowiązek sprawdzania unieważnień przez stronę ufającą

Strona ufająca danym umieszczonym w certyfikacie jest zobowiązana do każdorazowego sprawdzania, czy certyfikat nie został umieszczony na liście CRL przed jego wykorzystaniem do weryfikacji podpisu elektronicznego (pieczęci elektronicznej).

4.9.7 Częstotliwość publikacji CRL

Listy CRL dla certyfikatów wystawionych przez Centrum Kwalifikowane EuroCert są automatycznie publikowane w repozytorium nie rzadziej niż co 24 godziny. W przypadku unieważnienia lub zawieszenia certyfikatu, nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie (patrz punkt 4.9.5).

4.9.8 Maksymalne opóźnienie w publikowaniu list CRL

Listy CRL są publikowane, natychmiast po ich utworzeniu.

4.9.9 Weryfikacja statusu certyfikatu on-line

Kwalifikowany urząd weryfikacji statusu certyfikatu udostępnia usługę weryfikacji certyfikatów w trybie on-line. Usługa tego typu realizowana jest w oparciu o protokół OCSP przedstawiony w RFC 6960. Usługa OCSP daje możliwość częstszego pozyskania bardziej aktualnych informacji o statusie certyfikatu w porównaniu do listy CRL.

Protokół OCSP działa w oparciu o model żądanie – odpowiedź. W odpowiedzi na każde żądanie, urząd kwalifikowany zwraca następujące standardowe, poświadczone przez niego informacje o statusie certyfikatu:

a) poprawny (ang. good) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny,
b) unieważniony (ang. revoked) – oznacza, że certyfikat został unieważniony,
c) nieznany (ang. unknown) – oznacza, że weryfikowany certyfikat nie został wydany przez kwalifikowany urząd certyfikacji.

Status certyfikatu podawany jest w czasie rzeczywistym (tzn. natychmiast po unieważnieniu certyfikatu).

Informacja o statusie certyfikatu dostępna jest publicznie. Adres usługi zawarty jest w wydanym certyfikacie (patrz punkt 7.1.2).

Status certyfikatu pobierany jest z serwera urzędu certyfikacji i jest dostępny nie później niż 60 sekund po unieważnieniu danego certyfikatu.

Listy CRL emitowane przez EuroCert oraz odpowiedzi urzędu EuroCert QOCSP są podpisywane elektronicznie przez wydające je urzędy dzięki czemu EuroCert gwarantuje ich integralność oraz autentyczność.

4.9.10 Obowiązek sprawdzenia unieważnień w trybie on-line

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie on-line, realizowanej w oparciu o usługę przedstawioną w punkcie 4.9.9. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy ryzyko zaakceptowania nieważnego lub sfałszowanego podpisu (pieczęci) jest wysokie.

4.9.11 Inne formy ogłaszania unieważnień certyfikatów

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

4.9.12 Specjalne obowiązki w przypadku kompromitacji klucza

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

4.9.13 Okoliczności zawieszenia certyfikatu

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

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

a) dane zawarte w elektronicznym lub papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,
b) wniosek o unieważnienie został przekazany telefonicznie lub elektronicznie i nie można w ciągu 1 godziny, liczonej od chwili otrzymania wniosku potwierdzić tożsamości wnioskodawcy, ale też zanegować słuszności złożonego wniosku,
c) urząd certyfikacji może niezwłocznie zawiesić certyfikat w przypadku uzasadnionego podejrzenia, że certyfikat wydano bez przestrzegania postanowień niniejszego dokumentu; certyfikat może pozostać zawieszony do czasu aż urząd certyfikacji znajdzie podstawy do unieważnienia certyfikatu, nie dłużej jednak niż 7 dni,
d) innych okoliczności wymagających wyjaśnień ze strony subskrybenta lub wnioskodawcy.

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

4.9.14 Kto może żądać zawieszenia certyfikatu

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

4.9.15 Procedura zawieszenia i odwieszenia certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu. Po pomyślnej weryfikacji wniosku o zawieszenie przez inspektora ds. rejestracji przebiegającej jak w podrozdz. 3.4 zmienia on status certyfikatu na zawieszony i umieszcza go na liście CRL (z przyczyną unieważnienia *certificate hold*).

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

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.

4.9.16 Ograniczenie czasowe zawieszenia

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

4.10 Usługa znakowania czasem

Podstawowym celem usługi znakowania czasem, świadczonej przez urząd elektronicznego znacznika czasu EuroCert QTSA jest kryptograficzne związanie z dowolnymi danymi (mającymi postać dokumentów, wiadomości, podpisu elektronicznego, itd.) wiarygodnych elektronicznych znaczników czasu. Wiązanie elektronicznego znacznika czasu z danymi (token elektronicznego znacznika czasu) umożliwia udowodnienie, że dane zostały utworzone przed określonym momentem czasu. Dzięki temu:

a) urząd elektronicznego znacznika czasu potwierdza istnienie danych,
b) urząd elektronicznego znacznika czasu stwarza możliwość zweryfikowania, że podpis elektroniczny został złożony pod danymi jeszcze przed unieważnieniem klucza użytego do podpisu.

Urząd elektronicznego znacznika czasu EuroCert QTSA nie jest stroną w trakcie realizowania transakcji, które uzależnione są od czasu i oznaczane znacznikiem czasu.

Proces uzyskania elektronicznego znacznika czasu, wystawianego przez urząd elektronicznego znacznika czasu przebiega w pięciu następujących etapach:

a) wnioskodawca wysyła żądanie, zawierające wartość skrótu (powiązana z dokumentem, wiadomością, itd.), identyfikator funkcji skrótu oraz identyfikator sesji (ang. nonce), żądanie powinno zawierać OID, wg którego ma być wydany token elektronicznego znacznika czasu, w przypadku braku identyfikator token zostanie wydany zgodnie z domyślnym formatem,
b) urząd elektronicznego znacznika czasu weryfikuje poprawność formatu wniosku oraz jego kompletność,
c) urząd elektronicznego znacznika czasu tworzy znacznik czasu (token elektronicznego znacznika czasu), który zawiera m.in. numer seryjny, identyfikator protokołu, przy pomocy którego został utworzony znacznik czasu, zależny od czasu parametr (czas), pobrany z zaufanego źródła, dane (m.in. skrót), dostarczone w żądaniu, dane utworzone przez urząd elektronicznego znacznika czasu, które kryptograficznie wiążą wartość czasu z wartością skrótu, identyfikatorem funkcji skrótu oraz identyfikatorem sesji,
d) urząd elektronicznego znacznika czasu odsyła token elektronicznego znacznika czasu podmiotowi żądającemu,
e) podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena elektronicznego znacznika czasu, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Proces świadczenia usługi elektronicznego znacznika czasu przez EuroCert QTSA spełnia następujące wymagania bezpieczeństwa:

a) zaufane źródło czasu EuroCert QTSA jest synchronizowane z międzynarodowym wzorcem czasu z dokładnością do 1 sekundy,
b) numer seryjny umieszczony w tokenie elektronicznego znacznika czasu jest unikalny w domenie Eurocert QTSA; cecha ta jest zachowana także w przypadku wznowienia usługi po awarii,
c) klucz prywatny urzędu elektronicznego znacznika czasu jest generowany i przechowywany w sprzętowym module kryptograficznym spełniającym wymagania FIPS 140 Level 3,
d) urząd elektronicznego znacznika czasu EuroCert QTSA posiada własny klucz prywatny stosowany jedynie do poświadczania tokenów elektronicznego znacznika czasu.

4.11 Rezygnacja z usług

Umowa o świadczenie usług zaufania pomiędzy EuroCert a subskrybentem, kończy się wraz z upłynięciem terminu ważności certyfikatu wydanego na jej podstawie. 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 i certyfikatów, uwierzytelniania podmiotów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych.

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.

5.1.1 Lokalizacja i budynki

Systemy teleinformatyczne wykorzystywane do świadczenia usług zaufania mieszczą się w dwóch niezależnych lokalizacjach (centrum podstawowym i centrum zapasowym) oddalonych od siebie.

5.1.2 Dostęp fizyczny

Fizyczny dostęp do budynku jest monitorowany przez 24 godziny na dobę. Dostęp do pomieszczeń EuroCert jest kontrolowany przez System Kontroli Dostępu oraz nadzorowany przez system alarmowy.

Pomieszczenia systemu komputerowego w których znajduje się HSM z pozostającymi w nim kluczami urzędu certyfikacji, znajdują się w Strefie Ograniczonego Dostępu. Dostęp do tych pomieszczeń podlega ograniczeniom, jest strzeżony przez System Kontroli Dostępu do pomieszczeń oraz systemy sygnalizacji włamania i napadu. Dostęp do tych pomieszczeń jest ograniczony do wąskiej grupy upoważnionych osób zaufanego personelu EuroCert. Egzekwowanie praw dostępu realizowane jest w oparciu o posiadane przez personel karty dostępu do pomieszczeń.

5.1.3 Zasilanie i klimatyzacja

W przypadku zaniku zasilania podstawowego systemy komputerowe przechodzą na zasilanie awaryjne zapewniane przez UPS.

Środowisko pomieszczeń systemów komputerowych jest kontrolowane w sposób ciągły. Wszystkie pomieszczenia są klimatyzowane.

5.1.4 Zagrożenie zalaniem

Czujniki zalania są zainstalowane w pomieszczeniach serwerowni. Alarmy o zalaniu automatycznie przekazywane są do ochrony i administratora budynku, którzy podejmują właściwe działania, zawiadamiają odpowiednie służby miejskie, Inspektora bezpieczeństwa oraz Administratora systemu.

5.1.5 Ochrona przeciwpożarowa

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

5.1.6 Nośniki danych

Nośniki, na których przechowywane są dane archiwalne oraz kopie zapasowe danych składowane są w sejfach ognioodpornych zlokalizowanych w centrum podstawowym. Dostęp do sejfów mają upoważnieni pracownicy w trybie określonym wewnętrznymi regulacjami.

5.1.7 Niszczenie danych i nośników danych

EuroCert realizuje politykę bezpieczeństwa mającą na celu ochronę poufności danych.

Regulacje wewnętrzne wprowadzają klasyfikację danych pod względem ich poufności i określają wymogi bezpieczeństwa oraz sposoby postępowania z danymi w celu zapobieżenia naruszeniu bezpieczeństwa danych.

Wycofywane z eksploatacji nośniki na których przechowywane były dane mające znaczenie dla bezpieczeństwa EuroCert niszczone są w sposób uniemożliwiający odzyskanie danych lub czyniący odzyskanie danych ekonomicznie nieopłacalnym. Na przykład w przypadku nośników na których przechowywano klucze kryptograficzne lub numery PIN, nośniki na których informacje takie były przechowywane są niszczone w urządzeniach zapewniających co najmniej poziom klasy DIN-3 lub w inny sposób zapewniający co najmniej analogiczny poziom bezpieczeństwa.

5.1.8 Kopie bezpieczeństwa

Wszelkie dane istotne dla bezpieczeństwa EuroCert i usług przez nią świadczonych (w szczególności kopie haseł, numerów PIN oraz kluczy kryptograficznych stosowanych w systemie EuroCert, archiwa, kopie danych bieżących, pełna wersja instalacyjna oprogramowania) są przechowywane w centrum podstawowym w sejfach lub szafach metalowych w zależności od klasy ochrony danych.

5.1.9 Serwerownia zapasowa

Na wypadek awarii centrum podstawowego, uniemożliwiającej świadczenie usług zaufania, prace systemu przejmuje zapasowy system zlokalizowany w serwerowni zapasowej. W przypadku awarii, zapasowy system na bieżąco przejmuje pracę związaną z unieważnianiem, zawieszaniem certyfikatów i publikacją list CRL.

Poziom bezpieczeństwa serwerowni zapasowej odpowiada poziomowi bezpieczeństwa serwerowni zlokalizowanej w siedzibie EuroCert.

5.2 Zabezpieczenia organizacyjne

EuroCert zapewnia realizację zabezpieczeń organizacyjnych poprzez określenie, między innymi:

a) zaufanych ról, które mogą być pełnione przez jedną lub więcej osób w urzędzie certyfikacji,
b) zakazu łączenia określonych ról,
c) zakresu obowiązków i odpowiedzialności osób pełniących określone role,
d) liczby osób koniecznych do realizacji poszczególnych zadań,
e) identyfikacji oraz uwierzytelniania personelu.

5.2.1 Kadra

Osoby sprawujące nadzór nad systemem wykorzystywanym do świadczenia usług zaufania w EuroCert pełnią określone role, jak pokazano w tab. 5. Przedstawiony podział ról jest zgodny z wymogami ETSI EN 319 401.

Tab. 5. Zaufane role

Rola	Zakres obowiązków
Inspektor bezpieczeństwa	Opracowywanie i udział w opracowywaniu, wdrażaniu i stosowaniu regulacji w obszarze bezpieczeństwa w rozumieniu ogólnym i bezpieczeństwa eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług zaufania. Wdrażanie postanowień zawartych w obowiązujących regulacjach. Sprawowanie nadzoru nad działaniami administratorów systemu według obowiązujących uregulowań. Inicjowanie i nadzór nad procesem generowania kluczy oraz sekretów współdzielonych zgodnie z obowiązującymi regulacjami. Udział w procesie kontroli wewnętrznej zgodnie z obowiązującymi regulacjami. Kontrola przebiegu i realizacji procesów bezpieczeństwa.
Administrator systemu	Instalowanie, konfigurowanie i zarządzanie systemami oraz sieciami teleinformatycznymi wykorzystywanymi na potrzeby świadczenia usług zaufania. Zarządzanie uprawnieniami operatorów systemu.
Operator system	Obsługa systemu teleinformatycznego, w tym wykonywanie kopii zapasowych, zarządzanie uprawnieniami inspektorów ds. rejestracji.
Inspektor ds. rejestracji	Podpisywanie zgłoszeń certyfikacyjnych oraz przyjmowanie wniosków o zawieszenie, unieważnienie i odwieszenie certyfikatów, tworzenie nowych list CRL.
Inspektor audytu	Prowadzenie audytów planowych i doraźnych audytów zgodnie z obowiązującymi regulacjami.

5.2.2 Minimalny skład osobowy EuroCert

EuroCert przestrzega zasad określonych w regulacjach wewnętrznych dotyczących minimalnego składu osobowego. Przestrzeganie tych zasad zapewnia utrzymanie ciągłości działania biznesowego w sytuacji kryzysowej nawet w wypadku dostępności 50% personelu.

5.2.3 Uprawnienia i konta użytkowników systemów

Personel EuroCert podlega procedurom:

- umieszczania na liście osób posiadających dostęp do pomieszczeń EuroCert,
- umieszczania na liście osób posiadających logiczny dostęp do systemu lub sieci EuroCert**,**
- przydzielania dostępów oraz haseł w systemach komputerowych EuroCert.

Realizacja wymienionych procedur prowadzi do nadania osobom stającym się użytkownikami systemów indywidualnych identyfikatorów pozwalających jednoznacznie zidentyfikować użytkowników.

Każdy z powyższych identyfikatorów:

- musi być unikalny w obszarze systemu i bezpośrednio przypisany konkretnej osobie,
- nie może być współdzielony z innymi osobami,
- musi być powiązany z zakresem uprawnień (wynikających z roli pełnionej przez określoną osobę) i ewentualnie kontem użytkownika w systemie.

Przy zarządzaniu uprawnieniami użytkowników obowiązuje zasada nadawania minimalnych uprawnień niezbędnych do realizacji zadań pracownika w zakresie jego obowiązków przypisanych do jego stanowiska.

Operacje wykonywane w EuroCert, które wymagają dostępu poprzez sieć współdzieloną są zabezpieczone dzięki wprowadzonym mechanizmom uwierzytelniania oraz szyfrowania przesyłanej informacji.

Uprawnienia osób, które zakończyły pracę w EuroCert lub utraciły prawo do reprezentowania EuroCert, są natychmiast blokowane. Konta zablokowanego użytkownika mogą zostać usunięte dopiero po upływie ustawowego czasu archiwizacji danych.

Inspektor bezpieczeństwa EuroCert prowadzi regularne planowe kontrole wewnętrzne dostępów i kont użytkowników systemów jak również jest upoważniony do prowadzenia kontroli doraźnych w trybie obowiązujących regulacji.

5.2.4 Separacja obowiązków

Rola:

a) Prezesa Zarządu,
b) Inspektora Bezpieczeństwa,,
c) Inspektora Audytu

nie może być łączona z żadnymi innymi rolami w EuroCert.

Wyodrębnione w EuroCert stanowiska i role oraz zasady separacji stanowisk zapobiegają nadużyciom przy korzystaniu z systemów EuroCert. Każdej osobie odpowiedzialnej za eksploatację systemów EuroCert wykorzystywanych do świadczenia usług zaufania przydzielono tylko takie prawa, które wynikają z pełnionej przez niego roli i ponoszonej z tego tytułu odpowiedzialności.

5.3 Odpowiedzialności

Cały personel EuroCert, w tym szczególnie osoby piastujące tzw. zaufane role, zobowiązane są postępować zgodnie z przepisami Rozporządzenia eIDAS, ustawy o usługach zaufania, przepisów o ochronie danych osobowych i zgodnie z postanowieniami obowiązujących regulacji wewnętrznych.

5.3.1 Kwalifikacje, doświadczenie, upoważnienia

Osoby zajmujące się świadczeniem usług zaufania posiadają odpowiednie kwalifikacje przewidziane dla kwalifikowanych dostawców usług zaufania, w szczególności wiedzę i umiejętności z zakresu infrastruktury klucza publicznego oraz przetwarzania danych osobowych, a ponadto:

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

5.3.2 Weryfikacja pracowników

Przed powierzeniem pracownikowi którejkolwiek z ról opisanych w punkcie 5.2.1 przeprowadzana jest weryfikacja:

a) świadectwa pracy z poprzedniego miejsca zatrudnienia (w przypadku nowego pracownika),
b) dyplomu i świadectwa potwierdzające wykształcenie pracownika,
c) kwalifikacji i doświadczenia zawodowego,
d) oświadczenia pracownika o niekaralności.

5.3.3 Szkolenia

Personel zaufany EuroCert oraz operatorzy punktów rejestracji przed uzyskaniem uprawnień do pełnienia swojej roli muszą przejść cykl szkoleń dotyczących:

- zasad Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert,
- zasad zawartych w dokumentacji i obwiązujących regulacjach, przypisanego stanowiska lub roli, którą dana osoba pełni,
- ochrony danych osobowych i ochrony informacji,
- infrastruktury klucza publicznego,
- weryfikacji tożsamości na podstawie dokumentów potwierdzających tożsamość,
- zasad i mechanizmów zabezpieczeń stosowanych w urzędzie certyfikacji oraz punktach rejestracji,
- oprogramowania systemu komputerowego urzędu certyfikacji,
- zakresu obowiązków, które będą wykonywały,
- procedur realizowanych po awariach lub katastrofach systemu urzędu certyfikacji.

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

5.3.4 Powtarzanie szkoleń

Szkolenia o których mowa w punkcie 5.3.3 są powtarzane lub uzupełniane w zależności od potrzeb oraz zawsze wtedy, gdy nastąpiły istotne zmiany w świadczeniu usług przez EuroCert, funkcjonowaniu EuroCert lub punktów rejestracji, systemie, niniejszej Regulacji lub innych istotnych regulacjach wewnętrznych.

5.3.5 Częstotliwość rotacji stanowisk i jej kolejność

Niniejsza Regulacja nie określa żadnych wymagań w tym zakresie.

5.3.6 Sankcje z tytułu nieuprawnionych działań

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

5.3.7 Pracownicy kontraktowi

EuroCert dopuszcza wykonywanie czynności związanych z pełnieniem roli, spośród wymienionych w punkcie 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 podpisie elektronicznym (w szczególności wymagań o poufności, wymagań w zakresie wystawiania i unieważniania certyfikatów) podlegają sankcjom karnym określonym w Ustawie o usługach zaufania.

5.3.8 Dokumentacja dla pracowników

EuroCert umożliwia swojemu personelowi jak również operatorom punktów rejestracji dostęp do następujących dokumentów:

- Polityki certyfikacji i kodeksu postępowania certyfikacyjnego kwalifikowanych usług zaufania Eurocert,
- wzorów umów oraz stosowanych formularzy wniosków,
- niezbędnych wyciągów z dokumentacji (właściwej dla pełnionej roli), w tym procedur awaryjnych,
- zakresu obowiązków i uprawnień wynikających z pełnionej roli.

5.4 Procedury tworzenia logów audytowych

EuroCert prowadzi rejestr wszelkich istotnych z punktu widzenia bezpieczeństwa EuroCert zdarzeń związanych ze świadczonymi usługami zaufania w celu zapewnienia bezpieczeństwa, nadzoru nad sprawnym działaniem systemów 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

Rejestrowane zdarzenia obejmują:

a) zdarzenia bezpośrednio związane ze świadczeniem usług zaufania, a w szczególności: generowanie kluczy urzędu certyfikacji, przyjęcie wniosku o wydanie certyfikatu, generowanie kluczy i certyfikatów dla subskrybentów, unieważnianie/zawieszanie certyfikatów, generowanie list CRL, przyjęcie żądania wydania znacznika czasu,
b) czynności związane z obsługą klientów i subskrybentów: przyjmowanie i podpisywanie umów, wniosków, wydawanie certyfikatów, dostarczanie certyfikatów, fakturowanie itp.,
c) logi systemowe z serwerów i stacji roboczych wchodzących w skład systemu generującego certyfikaty,
d) zdarzenia związane z obsługą techniczną systemu: błędy i alarmy, rejestr wprowadzanych zmian w systemie, obsługa użytkowników.

Rejestry zdarzeń zapisywane są w formie elektronicznej. Rekordy zawierają identyfikator zdarzenia, datę i czas wystąpienia, typ zdarzenia, opis szczegółowy. Rejestr zdarzeń podlega archiwizacji.

5.4.2 Kontrola zapisów zdarzeń

Zapisy rejestrowanych zdarzeń podlegają kontroli bieżącej przez Administratora systemów oraz kontroli planowej przez Inspektora bezpieczeństwa.

Każdorazowo po wystąpieniu alarmu systemu monitorującego kluczowe elementy systemu urzędu certyfikacji analizy zdarzenia dokonuje Administrator Systemów we współpracy z Inspektorem

Bezpieczeństwa, w celu wykrycia ewentualnych nieuprawnionych działań lub innych nieprawidłowości wskazujących na zagrożenia 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 mają Inspektor audytu i Inspektor bezpieczeństwa. Logi są zabezpieczone przed modyfikacją, podlegają procedurom tworzenia kopii zapasowych oraz są archiwizowane. Archiwa rejestru zdarzeń są przechowywane w zasobach archiwalnych, do których dostęp mają Inspektorzy audytu, Inspektorzy Bezpieczeństwa 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 podstawowym w sejfach lub w zabezpieczonych zasobach sieciowych w wewnętrznej zabezpieczonej sieci logicznej EuroCert.

Czynności tworzenia kopii zapasowych wykonywane są automatycznie lub ręcznie w zależności od rodzaju i przeznaczenia kopii.

Ręczne sporządzanie kopii zapasowych jest wykonywane przez Administratora Systemów pod nadzorem Inspektora Bezpieczeństwa.

Automatyczne sporządzanie kopii zapasowych poddane jest kontroli bieżącej Administratora Systemów oraz kontroli planowej Inspektora Bezpieczeństwa. W wypadku stwierdzenia nieprawidłowości realizowana jest kontrola w trybie doraźnym.

5.4.6 System gromadzenia danych na potrzeby audytu

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

5.4.7 Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenia

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

W przypadku naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania, przetwarzanie w jej ramach, czy też na bezpieczeństwo danych osobowych, nie później niż w ciągu 24 godzin od wystąpienia zdarzenia EuroCert zawiadamia organ nadzoru i w stosowanych wypadkach, inne właściwe podmioty zgodnie z art. 19.2 Rozporządzenia eIDAS (patrz punkt 5.7.1).

5.4.8 Oszacowanie podatności na zagrożenia

Wymagane jest przeprowadzanie przez EuroCert analizy podatności na zagrożenia wszystkich posiadanych aktywów, w tym w szczególności oprogramowania oraz systemów komputerowych.

Analiza ryzyka jest prowadzona jest przynajmniej raz w roku lub przy wprowadzaniu nowych usług, istotnych zmian w systemach lub w wyniku incydentu bezpieczeństwa. Za audyt wewnętrzny odpowiada jest inspektor audytu, którego zadanie polega na kontroli zgodności zapisów w rejestrze bezpieczeństwa, poprawności przechowywania jego kopii, kontroli działań podejmowanych w sytuacjach zagrożeń oraz przestrzegania postanowień niniejszej Regulacji.

5.5 Archiwizacja danych

Archiwizacja danych jest realizowana zgodnie z postanowieniami niniejszej Regulacji.

5.5.1 Typy archiwizowanych danych

Archiwizacji podlegają:

- umowy o świadczenie usług zaufania, o których mowa w art. 14 Ustawy o usługach zaufania,
- otrzymywane wnioski oraz wydawane decyzje, mające postać papierową lub elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane,
- baza danych subskrybentów, w tym wszystkie informacje zebrane w procesie rejestracji subskrybenta,
- baza danych certyfikatów,
- wydane listy CRL,
- certyfikaty dostawcy usług zaufania,
- historia kluczy urzędów certyfikacji, od ich wygenerowania do zniszczenia włącznie,
- polityka 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

oraz inne dokumenty podlegające archiwizacji wymienione z osobna w pozostałych rozdziałach i pod-rozdziałach niniejszej Regulacji.

5.5.2 Okres przechowywania archiwów

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

5.5.3 Ochrona archiwów

Archiwalne dane na zewnętrznych nośnikach elektronicznych przechowywane są w centrum podstawowym w sejfach, elektroniczne dane w postaci plików są przechowywane w dedykowanym zabezpieczonym zasobie przeznaczonym dla elektronicznych materiałów archiwalnych, archiwalne dokumenty papierowe są przechowywane w siedzibie EuroCert Sp. z o.o. w metalowych zamykanych na klucz szafach.

5.5.4 Procedury tworzenia kopii zapasowych

Kopie zapasowe tworzone są w celu ochrony danych oraz odtworzenia systemu po awarii. W tym celu kopiowaniu podlegają:

- dyski instalacyjne z oprogramowaniem systemowym, m.in. systemami operacyjnymi,

- dyski instalacyjne z aplikacjami urzędu certyfikacji i punktów rejestracji,
- historie kluczy urzędu, certyfikatów i list CRL,
- dane z repozytorium urzędu certyfikacji,
- dane o subskrybentach oraz personelu EuroCert,
- rejestry zdarzeń.

Szczegółowe procedury wykonywania kopii zapasowych regulują procedury wewnętrzne EuroCert.

5.5.5 Wymaganie znakowania czasem archiwizowanych danych

Nie stosuje się znakowania czasem archiwizowanych danych.

5.5.6 System archiwizacji danych

EuroCert archiwizuje dane we własnym zakresie, korzystając z metalowych szaf zamykanych na klucz, sejfów ognioodpornych oraz dedykowanego zabezpieczonego zasobu sieciowego. Archiwalne kopie danych elektronicznych przechowywane są w centrum podstawowym. Szczegółowe procedury wykonywania archiwów regulują procedury wewnętrzne EuroCert.

5.5.7 Procedura weryfikacji i dostępu do zarchiwizowanych danych

W celu sprawdzenia integralności zarchiwizowane dane są, tam gdzie jest to zasadne, co pewien okres testowane oraz porównywane z danymi oryginalnymi. Czynność ta jest realizowana w trybie wewnętrznej kontroli planowej. W przypadku wykrycia uszkodzeń lub zniszczeń w danych oryginalnych lub w danych zarchiwizowanych, zauważone uszkodzenia są usuwane tak szybko jak to możliwe.

5.6 Wymiana klucza

Procedura wymiany klucza odnosi się do kluczy urzędu certyfikacji używanych do podpisywania certyfikatów, list CRL, znaczników czasu oraz zweryfikowanych statusów certyfikatów.

Wymiana kluczy urzędów kwalifikowanych realizowana jest w sposób zapewniający zachowanie ustalonego minimalnego okresu ważności certyfikatów. Odpowiednio wcześniej przed wygaśnięciem certyfikatu danego urzędu tworzona jest nowa, niezależna infrastruktura klucza publicznego w ramach której generowana jest nowa para kluczy oraz certyfikat nowego urzędu. Do czasu wygaśnięcia certyfikatu starego urzędu działają dwa urzędy. Nowy urząd przejmuje rolę wygasającego, świadczy wszystkie czynności związane z obsługą certyfikatów: generowanie, zawieszanie i unieważnianie certyfikatów, generowanie list CRL. Wygasający urząd obsługuje tylko unieważnienia i zawieszenia certyfikatów wystawionych w ramach swojej infrastruktury oraz generuje listy CRL do czasu zaprzestania swojej działalności operacyjnej (wygaśnięcia certyfikatu).

Certyfikat nowego urzędu 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 kwalifikowanego i zgłoszenie ich ministrowi ds. informatyzacji, w celu wystawienia nowego certyfikatu oraz umieszczenia go na liście TSL,
- otrzymanie certyfikatu oraz wydanie nowej listy TSL.

5.7 Utrata poufności klucza i działanie w przypadku katastrof

EuroCert posiada odpowiednie plany postępowania na wypadek sytuacji kryzysowych (np. klęsk żywiołowych) umożliwiające przywrócenie funkcjonowania procesów biznesowych co najmniej na minimalnym wymaganym przez biznes poziomie usług.

Plan ciągłości działania BCP (ang. Business Continuity Plan) podlega corocznemu przeglądowi i w razie potrzeby podlega aktualizacji. Przegląd BCP następuje również w wypadku zmian organizacyjnych lub technicznych. BCP służy przygotowaniu EuroCert na wypadek sytuacji kryzysowych.

W wypadku wystąpienia sytuacji kryzysowej wdrażany jest plan odtworzenia działalności (ang. Disaster Recovery Plan – DRP). DRP jest elementem składowym BCP i zawiera scenariusze działania w sytuacjach kryzysowych. Podlega przeglądowi w ramach przeglądów BCP.

BCP i DRP podlegają co najmniej raz w roku testom technologicznym i biznesowym. Testy technologiczne obejmują odtworzenie systemów w sytuacji kryzysowej. Testy biznesowe pozwalają sprawdzić realizację procesów biznesowych w takiej sytuacji. Realizowane są również testy „call tree" powiadamiania o zdarzeniu członków zespołów awaryjnych.

5.7.1 Procedura obsługi incydentów i reagowania na zagrożenia

Tryb postępowania w przypadku wystąpienia zagrożenia lub naruszenia bezpieczeństwa systemu jest opisany w obowiązującej w EuroCert procedurze zarządzania incydentem bezpieczeństwa i planie ciągłości działania BCP. Procedura i BCP są zgodne z wymaganiami art. 19.2 Rozporządzenia eIDAS.

5.7.2 Procedury odzyskiwania zasobów obliczeniowych, oprogramowania i/lub danych

EuroCert dysponuje regulacjami na wypadek konieczności odtwarzania zasobów. W każdej lokalizacji znajdują się zasoby pozwalające na odtworzenie podstawowej funkcjonalności urzędu certyfikacji. W szczególności są to:

a) backu-up danych,
b) back-up kluczy ośrodków certyfikacji,
c) kopie kart kryptograficznych z dzielonymi sekretami oraz operatorskie,
d) nośniki z oprogramowaniem systemu certyfikacji kluczy,
e) regulacje urzędu certyfikacji.

Plan odtwarzania działalności biznesowej w sytuacji kryzysowej DRP mieści się w Planie ciągłości działania BCP jest regularnie testowany. Po testach tworzony jest raport.

5.7.3 Procedury w przypadku naruszenia bezpieczeństwa kryptograficznego klucza urzędu

Eurocert posiada odpowiednie plany postępowania obowiązujące w wypadku utraty poufności klucza prywatnego urzędu kwalifikowanego Eurocert lub w wypadku uzasadnionego podejrzenia że takie zdarzenie nastąpiło (patrz punkt 5.4.7). Plany 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 dostawcy usług zaufania związanego z ujawnionym kluczem prywatnym oraz wszystkich aktualnie ważnych certyfikatów, pod-pisanych przy pomocy ujawnionego klucza prywatnego,

d) powiadomienie o unieważnieniu certyfikatu urzędu kwalifikowanego dostępnymi kanałami informacyjnymi,
e) wytworzenie nowych kluczy urzędu kwalifikowanego i zgłoszenie ich ministrowi ds. informatyzacji, w celu wystawienia nowego certyfikatu dostawcy usług zaufania i umieszczeniu go na liście TSL,
f) jeśli to będzie w danej sytuacji możliwe (w szczególności bazy danych EuroCert pozostaną wiarygodne) – wystawienie nowych certyfikatów dla subskrybentów, w oparciu o nowe klucze urzędu, z okresami ważności co najmniej takimi samymi, jakie miały unieważnione certyfikaty, bez obciążania subskrybentów kosztami za tą operację.

5.7.4 Zapewnienie ciągłości działania po katastrofach

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

Infrastruktura techniczna EuroCert posiada zabezpieczenia umożliwiające kontynuację pracy w wypadku awarii, natomiast sytuacji kryzysowej: w wypadku katastrofy, awarii sprzętu lub infrastruktury przekraczającej możliwości wynikające z tych zabezpieczeń urząd kwalifikowany 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 kwalifikowanego w zakresie unieważniania, zawieszania certyfikatów oraz publikacji list CRL.

5.8 Zakończenie działalności urzędu

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 Ustawy o usługach zaufania).

Na wymienioną okoliczność sporządzony jest przez EuroCert plan zakończenia działalności jako kwalifikowanego dostawcy usług zaufania zgodny z postanowieniami art. 24 ust. 2 lit. i Rozporządzenia eIDAS oraz art. 19 ust. 3. Ustawy o usługach zaufania.

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. Po wystawieniu ostatniej listy CRL klucz prywatny urzędu kwalifikowanego jest niszczony. Dokumenty i zapisy, co do których jest wymagana archiwizacja, są przekazywane po zakończeniu działalności organowi nadzoru lub podmiotowi przez niego wskazanemu.

6 Bezpieczeństwo techniczne

W niniejszym rozdziale zaprezentowano zasady tworzenia oraz zarządzania (m.in. przechowywania i używania) parami kluczy kryptograficznych będących pod kontrolą ich właścicieli (urzędu kwalifikowanego lub subskrybentów), wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1 Generowanie i instalowanie par kluczy

Urząd certyfikacji Centrum Kwalifikowane EuroCert posiada przynajmniej jeden certyfikat dostawcy usług zaufania, który stosowany jest w procesie elektronicznego poświadczania certyfikatów i list CRL. Klucze prywatne Centrum Kwalifikowane EuroCert stosowane są do podpisywania certyfikatów oraz list CRL. Do realizacji podpisu elektronicznego stosowany jest algorytm RSA (4096 bit) w kombinacji z funkcją skrótu SHA-1 lub SHA-2.

6.1.1 Generowanie par kluczy

Klucze urzędu certyfikacji 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 punkt 5.2.2), 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, posiadający certyfikat Common Criteria dla poziomu EAL4+ albo bezpieczniejszego oraz FIPS PUB 140-2 dla poziomu 3 albo bezpieczniejszego. Generowanie kluczy i operacje związane z wykorzystaniem klucza prywatnego odbywają się wyłącznie w module kryptograficznym.

Klucze inspektorów ds. 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 a następnie bezpośrednio przekazywana temu subskrybentowi.

6.1.2 Dostarczenie klucza prywatnego subskrybentowi

Klucze subskrybenta generowane są przez urząd certyfikacji na karcie kryptograficznej. Mogą one być mu dostarczane osobiście z informacjami pozwalającymi na aktywację klucza prywatnego, pocztą kurierską lub udostępnione zdalnie. Subskrybent ma obowiązek do niezwłocznej zmiany danych pozwalających na aktywację klucza prywatnego. Konieczna jest zmiana PIN-ów przez subskrybenta, przed rozpoczęciem okresu eksploatacji certyfikatu.

Dane do aktywowania karty (m.in. PUK/PIN) udostępniane są subskrybentom niezależnie od wydawanych certyfikatów.

EuroCert umożliwia subskrybentom korzystanie z kluczy wyłącznie w certyfikowanych urządzeniach wpisanych na listę certyfikowanych urządzeń do składania kwalifikowanych podpisów i kwalifikowanych pieczęci notyfikowanych zgodnie z artykułem 30(2), 39(2) oraz 39(3) Rozporządzenia eIDAS.

Subskrybenci chcący odnowić ważny certyfikat kwalifikowany na karcie kryptograficznej wydanej przez EuroCert, mogą wygenerować zdalnie nową parę kluczy. EuroCert udostępnia swoim

subskrybentom w tym celu dedykowaną aplikację, która tworzy klucze bezpośrednio na karcie kryptograficznej subskrybenta.

EuroCert gwarantuje, że procedury stosowane w urzędzie w żadnym momencie po wygenerowaniu na żądanie subskrybenta klucza prywatnego nie pozwalają na użycie go do realizacji podpisu elektronicznego lub pieczęci elektronicznej ani też nie stwarzają warunków, które umożliwią zrealizowanie takiego podpisu lub pieczęci innemu podmiotowi, poza właścicielem tego klucza.

6.1.3 Dostarczenie klucza publicznego urzędowi certyfikacji

Nie dotyczy.

6.1.4 Dostarczenie klucza publicznego urzędu 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, które są wydawane przez Narodowe Centrum Certyfikacji.

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

6.1.5 Rozmiary kluczy

Wszystkie urzędy działające w domenie kwalifikowanych usług zaufania EuroCert używają kluczy o długości 2048 lub 4096 bitów, z funkcją skrótu SHA-2.

Wszystkie certyfikaty wydawane użytkownikom końcowym w ramach kwalifikowanego urzędu certyfikacji posiadają długość klucza 2048 bitów lub 3072 bitów i funkcję skrótu SHA-2.

6.1.6 Parametry generowania klucza publicznego i weryfikacja jakości

Parametry generowania klucza publicznego spełniają wymagania określone w normach ETSI EN 319 401 i 319 411-2.

6.1.7 Cel użycia kluczy

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

Kwalifikowane certyfikaty wydawane subskrybentom mogą być używane do podpisywania. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie dla zapewnienia usługi niezaprzeczalności (ustawiony bit nonRepudiation).

Urząd certyfikacji Centrum Kwalifikowane EuroCert posiada klucze do elektronicznego poświadczania certyfikatów i list CRL (ustawione bity keyCertSign oraz cRLSign). Odpowiadający mu klucz publiczny służy wyłączenie do weryfikowania certyfikatów i list CRL.

Urząd elektronicznego znacznika czasu EuroCert QTSA posiada klucze stosowane do elektronicznego poświadczania tokenów (ustawiony bit digitalSignature oraz bit nonRepudiation).

6.2 Ochrona klucza prywatnego oraz techniczna kontrola modułu kryptograficznego

Każdy subskrybent, a także operatorzy urzędów kwalifikowanych przechowują swój klucz prywatny, wykorzystując w tym celu wiarygodny system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu. Urząd certyfikacji, który generuje parę kluczy w imieniu subskrybenta,

musi przekazać go w sposób bezpieczny oraz pouczyć subskrybenta o zasadach ochrony klucza prywatnego (patrz punkt 6.1.2).

6.2.1 Standardy dla modułu kryptograficznego

Klucze prywatne subskrybentów związane z certyfikatami przetwarzane są wyłącznie w kwalifikowanych urządzeniach do składania podpisu elektronicznego (pieczęci elektronicznej), spełniających wymagania normy FIPS 140 oraz Common Criteria EAL 4+.

6.2.2 Podział klucza prywatnego

Klucze prywatne wszystkich urzędów certyfikacji EuroCert podlegają ochronie za pomocą podziału 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. 6.

Tab. 6. Schemat podziału klucza prywatnego

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

Sekrety zapisywane są na kartach kryptograficznych chronionych numerem PIN znanym tylko osobie której został on przekazany w trybie określonym w regulacjach wewnętrznych. Sekrety, jak też chroniące je numery PIN przechowywane są w sposób uniemożliwiający ich nieuprawnione wykorzystanie.

W razie konieczności odtworzenia klucza z kopii zapasowych wykonywana jest procedura wprowadzania klucza do modułu opisana w punkcie 6.2.6.

6.2.3 Deponowanie klucza prywatnego

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

6.2.4 Kopie zapasowe klucza prywatnego

Klucze prywatne subskrybentów powiązane z certyfikatami służącymi do weryfikacji podpisów elektronicznych (pieczęci elektronicznych) nie mogą podlegać procedurom tworzenia kopii zapasowych.

Mechanizm zapewnienia kopii zapasowej klucza prywatnego urzędu certyfikacji jest realizowany dzięki podziałowi klucza na części (patrz punkt 6.2.2).

6.2.5 Archiwizowanie klucza prywatnego

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

Klucze prywatne subskrybenta związane z certyfikatami służącymi do weryfikacji podpisów (pieczęci) elektronicznych, klucze prywatne inspektorów ds. rejestracji służące do podpisywania zgłoszeń certyfikacyjnych nie mogą podlegać procedurom archiwizowania.

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Wprowadzanie klucza prywatnego do HSM realizowane jest w sytuacjach:

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

Załadowanie klucza do modułu odbywa się przy udziale posiadaczy współdzielonych sekretów. Do załadowania klucza konieczna jest obecność liczby sekretów opisana w punkcie 6.2.2. Ładownie odbywa się w ramach zamkniętego środowiska bezpieczeństwa. Klucz prywatny jest składany z elementów. Podawane są kolejno fragmenty klucza tajnego z kart, zaszyfrowane pliki ładowane są do pamięci modułu i następuje ich odszyfrowanie. Klucz prywatny jest gotowy do użycia. Ładownie klucza do modułu odnotowane jest w rejestrze zdarzeń.

Wprowadzanie klucza prywatnego do HSM jest operacją krytyczną. Z tego względu w trakcie jej realizacji stosowane są takie środki i procedury, które zapobiegają ujawnieniu klucza, jego modyfikacji lub podstawienia.

6.2.7 Przechowywanie klucza prywatnego w HSM

Po załadowaniu klucza prywatnego do pamięci HSM jest on chroniony sprzętowo. Nie ma możliwości odczytu wartości klucza prywatnego z HSM, klucz ten nigdy nie opuszcza HSM w postaci jawnej. Operacje wymagające użycia klucza prywatnego wykonywane są w HSM.

6.2.8 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 kwalifikowanym urządzeniu do składania podpisu elektronicznego (pieczęci elektronicznej).

6.2.9 Dezaktywacja klucza prywatnego

Dezaktywowanie kluczy urzędu certyfikacji EuroCert jest wykonywane komisyjnie w obecności Inspektora bezpieczeństwa wyłącznie w wypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego. Dezaktywowanie klucza polega na wyczyszczeniu pamięci modułu kryptograficznego z załadowanych kluczy. Każda dezaktywacja klucza prywatnego jest odnotowywane w protokole sporządzanym przez komisję.

Dezaktywowanie klucza prywatnego subskrybenta następuje natychmiast po zrealizowaniu podpisu elektronicznego lub pieczęci elektronicznej.

6.2.10 Metody niszczenia klucza prywatnego

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

Niszczenie kluczy prywatnych urzędów certyfikacji oznacza fizyczne zniszczenie kart kryptograficznych, na których są przechowywane sekrety współdzielone lub ich bezpieczne wymazanie z nośnika (z karty kryptograficznej lub HSM, itp.). Niszczenie kluczy prywatnych urzędów certyfikacji wykonywane jest komisyjnie przez personel EuroCert zgodnie z udokumentowaną procedurą. Wymagana jest obecność co najmniej dwóch osób, w tym Inspektora bezpieczeństwa. Wymagana jest identyfikacja kart przed zniszczeniem. Z procedury niszczenia sporządza się protokół.

6.2.11 Standardy modułu kryptograficznego

Patrz punkt 6.2.1.

6.3 Inne aspekty zarządzania parą kluczy

Niniejszy rozdział dotyczy okresów ważności i archiwizowania certyfikatów i kluczy prywatnych subskrybentów oraz urzędów certyfikacji.

6.3.1 Archiwizowanie kluczy publicznych

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

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

Urząd certyfikacji przechowuje klucze publiczne tych subskrybentów, którym wydał je w postaci certyfikatów.

6.3.2 Okres ważności certyfikatów i kluczy prywatnych

Okres ważności certyfikatów subskrybentów a tym samym kluczy prywatnych wynosi maksymalnie 2 lata i jest określony w polu validity każdego certyfikatu. Data początku ważności certyfikatu nie może być wcześniejsza niż data jego wydania.

6.4 Dane aktywujące

Dane aktywujące stosowane są do uaktywniania kluczy prywatnych stosowanych przez urzędy certyfikacji oraz subskrybentów. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

6.4.1 Generowanie danych aktywujących i ich instalowanie

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

Sekrety współdzielone używane do ochrony kluczy prywatnych wszystkich urzędów certyfikacji świadczących usługi zaufania są generowane zgodnie z wymaganiami określonymi w punkcie 6.2.2.

6.4.2 Ochrona danych aktywujących

Nadane przez subskrybenta kody dostępu do klucza prywatnego powinny być znane tylko jemu. 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.

Kilkakrotne nieudane próby dostępu do klucza prywatnego prowadzą do zablokowania karty kryptograficznej. Zapisywane dane aktywujące nie są nigdy przechowywane razem z kartą kryptograficzną.

6.4.3 Inne aspekty związane z danymi aktywującymi

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.

6.5 Zabezpieczenia komputerów

Nie jest wymagane używanie przez urząd certyfikacji serwerów posiadających certyfikaty bezpieczeństwa na sprzęt lub oprogramowanie systemu operacyjnego.

Urząd certyfikacji przeprowadza regularne testy podatności oraz testy penetracyjne używanego systemu informatycznego, nie rzadziej niż co 6 miesięcy. Wyniki testów nie są publikowane.
Wszystkie operacje przewidziane do wykonania na komputerach i serwerach urzędu certyfikacji można wykonać po uprzednim uwierzytelnieniu się i kontroli uprawnień. Wykonywane operacje są zapisywane w dziennikach zdarzeń.

6.6 Cykl życia zabezpieczeń technicznych

6.6.1 Kontrola zmian w systemie

Nadzór i kontrolę nad wprowadzaniem modyfikacji lub zmian w systemie EuroCert sprawuje Inspektor bezpieczeństwa. Akceptuje on konfigurację systemu oraz wszelkie zmiany oprogramowania i sprzętu. Modyfikacje dokonywanych zmian zatwierdza Zarząd.

Testy nowych wersji oprogramowania i/lub wykorzystanie do tego celu istniejących baz danych odbywa się w środowisku testowym separowanym logicznie od środowiska produkcyjnego. Zasady obowiązujące w EuroCert podczas przeprowadzania testów gwarantują nieprzerwaną pracę systemów EuroCert, integralność zasobów oraz zachowanie poufności danych.

Wymiana sprzętu w systemach jest rejestrowana i monitorowana. W szczególności:

a) sprzęt jest dostarczany w sposób, który umożliwia prześledzenie całej drogi przebytej przez sprzęt od dostawcy do miejsca zainstalowania,
b) dostawa sprzętu do wymiany jest realizowana w taki sam sposób jak dostawa sprzętu oryginalnego; sama wymiana jest dokonywana przez zaufany i przeszkolony personel.

Odnośnie modułów kryptograficznych obowiązują wymagania określone w punkcie 6.2.1.

Sprzętowe moduły kryptograficzne, dostarczane do EuroCert, są każdorazowo sprawdzane czy nie nastąpiło naruszenie przesyłki oraz czy moduł zachowuje integralność fizyczną oraz logiczną. Weryfikację, z której sporządzany jest raport, przeprowadza wyłącznie zaufany personel EuroCert. Sprzętowe moduły kryptograficzne, nie będące w użyciu, zabezpieczone są opakowaniem uniemożliwiającym jego otwarcie bez pozostawienia śladów. Tak przygotowane moduły przechowywane są w sejfach zlokalizowanych w specjalnie strzeżonych pomieszczeniach, do których dostęp posiada wyłącznie wskazana grupa osób piastująca tzw. zaufane role w EuroCert.

6.6.2 Kontrola zarządzania bezpieczeństwem

Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania systemów oraz procesów bezpieczeństwa EuroCert, które daje pewność i widome dowody, że systemy są obsługiwane i pracują prawidłowo, a ich funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.

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

Aktualna konfiguracja systemu EuroCert, jak również dowolne modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w systemie EuroCert mechanizmy pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, uwierzytelnianie, weryfikowanie źródła pochodzenia.

6.6.3 Kontrola cyklu życia zabezpieczeń

Niniejszy dokument nie narzuca cyklu życia stosowanych zabezpieczeń. Zabezpieczenia podlegają zmianom w wypadku zaistnienia potrzeby zastosowania innych niż obecnie używane z powodu zmian w regulacjach prawnych, normach, standardach lub dobrych praktykach, lub są technologicznie przestarzałe czy też wyeksploatowane.

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.

Szczegółowy opis konfiguracji sieci EuroCert oraz jej zabezpieczeń zawarty jest w dokumentacji infrastruktury technicznej systemu EuroCert. Dokument udostępniany jest tylko inspektorowi bezpieczeństwa, administratorom systemów, Zarządowi i audytorom.

6.8 Znakowanie czasem

Elektroniczne znaczniki czasu są zgodne z ETSI EN 319 422 (patrz punkt 1.3.2 oraz podrozdz. 4.10).

7 Profil certyfikatów i list CRL

Profile certyfikatów i list CRL wydawane są zgodnie z zaleceniami normy ITU-T X.509 v3 oraz ETSI EN 319 412 (części: 1,2,3,5). Profil tokena znacznika czasu jest zgodny z ETSI EN 319 422.

7.1 Profil certyfikatów

Certyfikaty wydawane przez EuroCert według normy X.509 v3 są sekwencją wartości pól podstawowych oraz rozszerzeń. EuroCert obsługuje pola podstawowe certyfikatu opisane w tab. 7.

Tab. 7. Profil podstawowych pól certyfikatu

Nazwa pola	Opis	Wartość	
Version	Certyfikat zgodny z wersją 3 standardu X.509.	V3	
SerialNumber	Jednoznaczny w ramach urzędu certyfikacji numer certyfikatu.	numer seryjny certyfikatu	
SignatureAlgorithm	Identyfikator algorytmu kryptograficznego stosowanego do realizacji pieczęci elektronicznej przez urząd certyfikacji na certyfikacie.	sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)	
Issuer (nazwa wyróżniająca wystawcy certyfikatu)	Common Name	CN = Centrum Kwalifikowane EuroCert	
	Organization	O = EuroCert Sp. z o.o.	
	Country	C = PL	
	Organization identifier	2.5.4.97 = VATPL-9512352379	
NotBefore	Data wystawienia certyfikatu	data wystawienia certyfikatu	
NotAfter	Data wygaśnięcia certyfikatu	data wygaśnięcia certyfikatu	
Subject	Nazwa subskrybenta zgodna z wymaganiami określonymi w ETSI EN 319 412 (części: 1,2,3,5).	Identyfikator DN Subskrybenta (patrz podrozdz. 3.1.1).	
SubjectPublicKeyInfo	identyfikator algorytmu klucza publicznego podmiotu, długość klucza w bitach oraz wartość klucza publicznego.	Public Key Algorithm (algorytm klucza publicznego):	SHA256WithRSAEncryption
		RSA Public Key (długość klucza)	2048/3072 bit
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).	

7.1.1 Wersja certyfikatu

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

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.	
SubjectKeyIdentifier	NIE	Identyfikator certyfikatu zawierający skrót klucza publicznego zawartego w certyfikacie.	
KeyUsage	TAK	Określa zakres wykorzystania klucza publicznego subskrybenta. W wypadku 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 zgodny z pkt 7.1.6.
CRLDistributionPoints	NIE	Punkt dystrybucji listy CRL (określa adres URL, pod którymi jest publikowana aktualna lista CRL).	http://crl.eurocert.pl/qca03.crl
AuthorityInformationAccess	NIE	Dostęp do informacji o urzędzie.	http://crl.eurocert.pl/OCSP/
BasicConstraints	TAK	Umożliwia sprawdzenie czy podmiot certyfikatu jest użytkownikiem koń-cowym, czy też podmiotem wydają-cym 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 kwalifikowa-nym urządzeniu do składania podpisów; OID: {0.4.0.1862.1.4}

Nazwa rozszerzenia	Krytyczne ?	Opis	Wartość
qcType	NIE	Wskazanie rodzaju certyfikatu.	Wskazanie jednego z dwóch rodzajów certyfikatu: - certyfikat do podpisu elektronicz-nego (OID: 0.4.0.1862.1.6.1), - certyfikat do pieczęci elektronicz-nej (0.4.0.1862.1.6.2).
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}

7.1.3 Identyfikatory algorytmu

EuroCert pieczętuje certyfikaty algorytmem RSA (4096 bitów) i funkcją skrótu SHA-256. Certyfikaty subskrybentów wydawane są dla kluczy RSA o długości 2048/3072 bitów i funkcji skrótu SHA-256.

7.1.4 Formy nazw

Patrz: punkt 3.1.1 oraz tabela 7 w podrozdz. 7.1.

7.1.5 Ograniczenia nakładane na nazwy

Patrz punkt 7.1.4.

7.1.6 Identyfikatory polityk certyfikacji

Identyfikator polityki dla kwalifikowanych certyfikatów podpisów elektronicznych wygląda następująco: 1.2.616.1.113791.1.2.2.

Identyfikator polityki dla kwalifikowanych certyfikatów pieczęci elektronicznych wygląda następująco: 1.2.616.1.113791.1.2.3.

7.1.7 Zastosowanie rozszerzeń niedopuszczalnych

EuroCert nie przewiduje umieszczania w certyfikatach innych rozszerzeń niż wskazane w punkt 7.1.2.

7.1.8 Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

EuroCert nie określa wymagań w tym zakresie.

7.2 Profil listy CRL

Lista unieważnionych i zawieszonych certyfikatów jest zbiorem pól, których znaczenie przedstawiono poniżej w tabeli 8.

Tab. 8. 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 sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)
Issuer Identyfikator wystawcy listy CRL, zgodny z identyfikatorem określonym w profilu certyfikatu.	Patrz tabela 7 w podrozdz. 7.1.
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.

7.2.1 Wersja listy CRL

Format listy CRL jest zgodny z wersją nr 2 standardu X.509.

7.2.2 Obsługiwane rozszerzenia dostępu do listy CRL

EuroCert obsługuje niekrytyczne rozszerzenie dostępu do listy CRL o nazwie reasonCode (patrz tab. 8), zawierające kod przyczyny unieważnienia certyfikatu.

7.3 Profil OCSP

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

8 Audyt i kontrola

8.1 Audyt zgodności

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.

8.1.1 Częstotliwość i okoliczności oceny

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 lit. e) Rozporządzenia eIDAS.

8.1.2 Tożsamość i kwalifikacje audytora

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

8.1.3 Związek audytora z audytowaną jednostką

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

8.1.4 Zagadnienia objęte audytem wewnętrznym

Do zagadnień objętych audytem należą:

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

8.1.5 Działania podejmowane celem usunięcia usterek wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są osobom zarządzającym EuroCert, które powołują zespół składający się z pracowników wymienionych w punkt 5.2.1 w celu przygotowania w terminie określonym w raporcie pisemne stanowiska EuroCert wobec wszelkich

uchybień wskazanych w raportach. Odpowiedź musi określić także sposoby i terminy usunięcia usterek. Informacja o usunięciu usterek przekazywana jest instytucji audytującej.

W przypadku audytu zleconego przez ministra właściwego do spraw informatyzacji minister po zapoznaniu się z protokołem i zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez EuroCert powiadamia ten podmiot o wynikach kontroli i w razie stwierdzenia nieprawidłowości wyznacza termin ich usunięcia, nie krótszy niż 14 dni (Art. 34 Ustawy o usługach zaufania).

8.1.6 Informowanie o wynikach audytu

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

8.2 Kontrola wewnętrzna

EuroCert w celu utrzymania należytego poziomu usług oraz bezpieczeństwa ustanowił procesy kontroli wewnętrznej regulowane przez wewnętrzne regulacje polityki kontroli wewnętrznej i audytu oraz metodyki kontroli wewnętrznej i audytu.

8.2.1 Rodzaje kontroli

W EuroCert występują trzy rodzaje kontroli:

1) kontrole bieżące realizowane przez pracowników na bieżąco w ramach bieżącej realizacji czynności służbowych,
2) kontrole doraźne, realizowane w wypadku zaobserwowania nieprawidłowości lub w wypadku uzasadnionej potrzeby dokonania rozpoznania sposobu lub stanu realizacji określonego procesu biznesowego, procesu bezpieczeństwa obszaru IT itp.,
3) kontrole planowe, planowane i rozliczane w cyklach półrocznych, których celem jest dokonanie weryfikacji przestrzegania postanowień zapisanych w regulacjach.

8.2.2 Podstawy kontroli

Podstawą realizacji kontroli bieżących są zapisy regulacji upoważniające lub nakazujące pracownikom prowadzenie tego rodzaju kontroli w ramach realizowanych przez nich obowiązków służbowych.

Kontrole doraźne są realizowane na podstawie pisemnego polecenia służbowego przeprowadzenia kontroli wydawanego pracownikowi w okolicznościach o których mowa w p. 8.2.1.

Kontrole planowe są realizowane na podstawie planów kontroli wewnętrznych sporządzanych raz na pół roku i zatwierdzanych przez Zarząd.

8.2.3 Rozliczanie kontroli

Realizacja kontroli bieżących jest poddawana kontrolom planowym w trybie określonym w obowiązujących regulacjach wewnętrznych.

Z kontroli doraźnych i z kontroli planowych pracownicy wyznaczeni do przeprowadzenia kontroli sporządzają raporty. Raporty te są przedstawiane Inspektorowi bezpieczeństwa do akceptacji a następnie zatwierdzane przez Zarząd. Zatwierdzenie raportów jest równoznaczne z zatwierdzeniem realizacji zaleceń pokontrolnych, o ile takie zostały w raportach zawarte.

Inspektor bezpieczeństwa prowadzi rejestr kontroli zawierający wyniki przeprowadzonych kontroli, w tym informacje o czynnościach kontrolnych, podjętych działaniach, zrealizowanych działaniach, zaleceniach pokontrolnych.

Inspektor Bezpieczeństwa przedstawia Zarządowi w cyklach półrocznych raport z przeprowadzonych kontroli.

8.2.4 Realizacja zaleceń

Inspektor Bezpieczeństwa nadzoruje proces realizacji zaleceń pokontrolnych. W sytuacji wystąpienia trudności realizacyjnych dokonuje eskalacji w trybie określonym w obowiązujących regulacjach.

9 Inne postanowienia (biznesowe, prawne itp.)

9.1 Opłaty

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

9.1.1 Opłaty za wydanie certyfikatu i jego odnowienie

EuroCert pobiera opłaty za wydanie certyfikatu i jego odnowienie.

9.1.2 Opłaty za dostęp do certyfikatów

Eurocert nie pobiera opłat za dostęp do certyfikatów.

9.1.3 Opłaty za unieważnienie lub informacje o statusie certyfikatu

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

9.1.4 Inne opłaty

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

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

9.1.5 Zwrot opłat

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

9.2 Odpowiedzialność finansowa

9.2.1 Polisa ubezpieczeniowa

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, w stosunku do jednego zdarzenia wynosi równowartość 250 000 Euro wyrażoną w PLN, ale nie więcej niż 1 000 000 Euro w odniesieniu do wszystkich takich zdarzeń.

9.2.2 Inne aktywa

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

9.2.3 Rozszerzony zakres gwarancji

EuroCert nie określa żadnych wymagań w tym zakresie.

9.3 Poufność informacji biznesowej

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

9.3.1 Zakres informacji poufnych
EuroCert nie określa żadnych wymagań w tym zakresie.

9.3.2 Informację nie będące informacjami poufnymi
EuroCert nie określa żadnych wymagań w tym zakresie.

9.3.3 Ochrona informacji poufnych
EuroCert nie określa żadnych wymagań w tym zakresie.

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.

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

9.4.2 Informacje traktowane jako prywatne
EuroCert traktuje jako informacje klasy ochrony „do użytku służbowego" lub wyższej wszystkie informacje związane ze świadczeniem usług zaufania poza następującymi informacjami:

a) Polityka certyfikacji i kodeks postępowania certyfikacyjnego,
b) Zaświadczenia certyfikacyjne,
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.

Stronom trzecim udostępniane są tylko te informacje, które są publicznie dostępne w certyfikacie i na których opublikowanie zgodę wyraził subskrybent.

9.4.3 Informacje nie traktowane jako prywatne
Informacjami jawnymi są wszystkie informacje nieoznaczone jako poufne przez subskrybentów, osoby ufające lub EuroCert. Za informacje nie objęte poufnością uznaje się dane wpisane do certyfikatu.

Wszystkie informacje, które niezbędne są w procesie prawidłowego funkcjonowania usług certyfikacyjnych uważane są za informacje jawne. W szczególności za informacje jawne uważa się te informacje, które umieszczane są w certyfikacie przez organy wydające certyfikaty zgodnie z opisem przedstawionym w rozdz. 7. Subskrybent występując z wnioskiem o wydanie certyfikatu wyraża zgodę na upublicznienie informacji zawartej w certyfikacie.

Część informacji wpływających i przekazywanych od/do użytkowników może być udostępniana innym podmiotom wyłącznie za zgodą użytkownika.

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

9.4.5 Zastrzeżenia i zezwolenie na użycie informacji prywatnej

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

9.4.6 Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

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

9.4.7 Inne okoliczności ujawniania informacji

Niniejsza Regulacja nie określa żadnych wymagań w tym zakresie.

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 wypadku 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 punkt 7.1) lub – w przypadku subskrybenta certyfikatu kwalifikowanego firmowego – własnością podmiotu reprezentowanego przez subskrybenta.

9.6 Oświadczenia i gwarancje

9.6.1 Zobowiązania i gwarancje EuroCert

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 certyfikacyjnymi, w tym w szczególności obejmujących dziedziny:
    - automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
    - mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
    - kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego,
    - sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.

9.6.2 Zobowiązania i gwarancje punktu rejestracji

Punkty rejestracji oraz osoby potwierdzające tożsamość zobowiązują do:

a) przestrzegania procedur potwierdzania tożsamości przy wydawaniu certyfikatów zgodnie z zasadami określonymi w niniejszym dokumencie, procedurach wewnętrznych oraz w obowiązujących przepisach prawa i zasadach współżycia społecznego ze szczególnym uwzględnieniem dochowania należytej staranności,
b) wydawania koniecznych tokenów zgłoszenia certyfikacyjnego, upoważniających do skorzystania z określonej usługi EuroCert,
c) przesyłania do EuroCert potwierdzonych danych subskrybentów,
d) podporządkowania się w całości zaleceniom EuroCert,
e) ochrony kluczy prywatnych operatorów punktów rejestracji,
f) nie używania kluczy prywatnych operatorów do innych celów niż tych, które określono w niniejszej Regulacji,
g) poddawania się planowym audytom przeprowadzonym lub zleconym przez EuroCert.

9.6.3 Zobowiązania i gwarancje subskrybenta

Patrz: punkt 4.5.1.

9.6.4 Zobowiązania i gwarancje strony ufającej

Patrz: punkt 4.5.2.

9.6.5 Zobowiązania i gwarancje innych podmiotów

EuroCert nie określa żadnych wymagań w tym zakresie.

9.7 Wyłączenia odpowiedzialności z tytułu gwarancji

EuroCert nie odpowiada za jakiekolwiek szkody, które powstały lub mogły powstać dla odbiorców usług certyfikacyjnych lub osób trzecich, wynikające z przyczyn innych niż niewykonanie lub nienależyte wykonanie obowiązków przez EuroCert lub podmioty działające w jego imieniu. W szczególności EuroCert nie odpowiada za skutki naruszenia obowiązków nałożonych na subskrybenta i strony ufające, wymienionych odpowiednio w punkcie 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 punkcie 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

9.10.1 Okres obowiązywania

Niniejszy dokument obowiązuje od kolejnego dnia następującego po dniu wydania przez ministra właściwego ds. informatyzacji decyzji administracyjnej dotyczącej pieczęci elektronicznej do momentu wejścia w życie kolejnej wersji Regulacji.

9.10.2 Wygaśnięcie ważności

Kolejna wersja Regulacji wskazuje datę jej obowiązywania, która jest jednocześnie datą zakończenia obowiązywania obecnej Regulacji. Tym samym poprzednia Regulacja traci status – aktualna.

9.10.3 Skutki wygaśnięcia ważności dokumentu

Subskrybenci przestrzegają tylko aktualnej Regulacji.

9.11 Określanie trybu i adresów doręczania pism

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

9.12 Wprowadzanie zmian w dokumencie

9.12.1 Procedura wprowadzania zmian

Patrz: punkt 1.5.4.

9.12.2 Sposób powiadamiania o zmianach

Nie dotyczy.

9.12.3 Okoliczności wymagające zmiany identyfikatora OID

Zmiana identyfikatora (OID) Regulacji 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 subskrybentów.

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 Polityki certyfikacji i kodeksu postępowania certyfikacyjnego oraz zawartych umów.

Spory bądź zażalenia powstałe na tle użytkowania certyfikatów, tokenów weryfikacji statusu certyfikatów, tokenów znaczników czasu 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 certyfikacyjnymi 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 Regulacji oraz obowiązujących przepisach prawa. W celu interpretacji terminów zawartych w Regulacji należy je rozpatrywać zgodnie z rozporządzeniem eIDAS i Ustawą o usługach zaufania.

9.15 Zgodność z obowiązującym prawem

Zasady działania EuroCert są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

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

9.16 Przepisy różne

9.16.1 Kompletność warunków umowy

Strony obowiązują postanowienia Umowy i Regulacji.

9.16.2 Cesja praw

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

9.16.3 Rozłączność postanowień

W razie wątpliwości lub nie dającej się usunąć sprzeczności pomiędzy postanowieniami Umowy i Regulacji pierwszeństwo stosowania ma Umowa przed Regulacją.

W razie niezgodności z prawem postanowień któregokolwiek z powyższych dokumentów skutkujących ich nieważnością, pozostają w mocy niewadliwe postanowienia zawarte w pozostałych dokumentach.

9.16.4 Klauzula wykonalności

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

9.16.5 Siła wyższa

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

9.17 Inne postanowienia

Nie występują.

10 Postanowienia przejściowe

Z dniem obowiązywania niniejszej Regulacji uchylone zostają dotychczas obowiązujące:

1) Kodeks postępowania certyfikacyjnego kwalifikowanych usług zaufania,
2) Polityka certyfikacji dla kwalifikowanych certyfikatów,
3) Polityka certyfikacji dla kwalifikowanych znaczników czasu.

Historia dokumentu

Historia zmian			
Data zatwierdzenia	Data obowiązywania	Wersja	Dokonane zmiany
16.07.2018 r.	02.10.2018 r.	1	Wersja inicjalna powstała z połączenia dotychczasowych: 1. Kodeksu postępowania certyfikacyjnego kwalifikowanych usług zaufania, 2. Polityki certyfikacji dla kwalifikowanych certyfikatów, 3. Polityki certyfikacji dla kwalifikowanych znaczników czasu.