EuroCert Sp. z o.o.
Centrum EUROCERT

Kodeks postępowania certyfikacyjnego
kwalifikowanych usług zaufania

Wersja 2.0
Data: 15.11.2017 r.
Status: nieaktualny

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

SPIS TREŚCI

1 Wstęp

Kodeks postępowania certyfikacyjnego kwalifikowanych usług zaufania, zwany dalej „Kodeksem" precyzuje zasady świadczenia usług zaufania przez jednostkę organizacyjną EuroCert Sp. z o.o. – Centrum EuroCert (dalej „EuroCert"), polegających na:

a) wydawaniu kwalifikowanych certyfikatów klucza publicznego,
b) unieważnianiu i zawieszaniu certyfikatów,
c) wystawianiu tokenów znaczników czasu,
d) wystawianiu tokenów statusu certyfikatów.

Powyższe usługi świadczone są zgodnie z:

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

Kodeks odnosi się do urzędu certyfikacji „Centrum Kwalifikowane EuroCert" i związanych z nim punktów rejestracji, urzędu znakowania czasem, urzędu weryfikacji statusu certyfikatu, subskrybentów oraz stron ufających. Postanowienia w nim zawarte (m.in. zasady generowania kluczy i wystawiania certyfikatów, zastosowane mechanizmy zabezpieczeń systemu informatycznego) mają na celu przekonanie użytkowników usług EuroCert, że deklarowana wiarygodność wydawanych certyfikatów jest praktycznym odzwierciedleniem postępowania urzędu certyfikacji.

Obszary zastosowań certyfikatów są opisane w § 1.4, z kolei odpowiedzialność wynikająca ze stosowania ich przez użytkowników końcowych w § 4.5.

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

1.1 Wprowadzenie

EuroCert Sp. z o.o., z siedzibą w Warszawie, przy ulicy Puławskiej 474, którego jednostką organizacyjną jest Centrum EuroCert, świadczące kwalifikowane usługi zaufania, jest kwalifikowanym dostawcą usług zaufania, w myśl Ustawy o usługach zaufania i Rozporządzenia eIDAS, wpisanym do rejestru kwalifikowanych dostawców usług zaufania pod numerem 13.

EuroCert świadczy kwalifikowane usługi zaufania w zakresie:

a) wydawania kwalifikowanych certyfikatów, w ramach których dokonuje następujących czynności:
    - rejestruje subskrybentów,
    - generuje klucze i certyfikaty,
    - dostarcza informacje o statusie certyfikatu w oparciu o listy CRL,
    - unieważnia i zawiesza certyfikaty.

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

b) znakowania czasem,
c) weryfikowania statusu certyfikatów w trybie on-line.

Wydawanie certyfikatów, tokenów przez EuroCert odbywa się w oparciu o pieczęć elektroniczną wydaną przez Narodowe centrum certyfikacji na podstawie art. 10.1 Ustawy o usługach zaufania. Do zasad przedstawionych w tym dokumencie dostosowane powinny być działania tych podmiotów i dostawców usług, którzy korzystają z certyfikatów klucza publicznego.

Certyfikaty wydawane przez EuroCert zawierają identyfikatory polityk certyfikacji, które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Identyfikatory te umieszczane są w rozszerzeniu „certificatePolicies" (patrz § 7.1.2) każdego certyfikatu wydawanego przez EuroCert. Identyfikatory polityk certyfikacji umieszczane są również w tokenach znaczników czasu.

Z Kodeksem związane są inne dodatkowe dokumenty, które regulują funkcjonowanie Eurocert (patrz tab. 1). Dokumenty te ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu EuroCert nie są publicznie udostępniane.

Tab. 1. Ważniejsze dokumenty towarzyszące Kodeksowi postępowania certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Polityka certyfikacji dla kwalifikowanych certyfikatów	jawny	http://www.eurocert.pl/repozytorium/
2.	Informacja o infrastrukturze PKI EuroCert	jawny	http://www.eurocert.pl/repozytorium/
3.	Plan zakończenia działalności	niejawny	n/d
4.	Plan ciągłości działania	niejawny	n/d
5.	Polityka zarządzania ryzykiem	niejawny	n/d

1.2 Identyfikator i nazwa dokumentu

Kodeksowi przypisuje się nazwę własną oraz zarejestrowany identyfikator obiektu (ang. Object Identifier – OID), które przedstawiono w tab.2.

Tab. 2. Karta dokumentu

Nazwa	Kodeks postępowania certyfikacyjnego kwalifikowanych usług zaufania
Właściciel	EuroCert Sp. z o.o.
Wersja	2.0
Status	nieaktualny
Data zatwierdzenia	15.11.2017
Zatwierdzający	Zarząd EuroCert Sp. z o.o.
Obowiązuje od	20.11.2017
Identyfikator obiektu OID	1.2.616.1.113791.1.1
Data wygaśnięcia	01.10.2018 r.

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

Identyfikator Kodeksu nie jest umieszczany w treści wystawianych certyfikatów. W wydawanych przez siebie certyfikatach EuroCert umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru identyfikatorów polityk certyfikacji określonych w § 1.3.1 oraz § 7.1.2.

1.3 Elementy infrastruktury PKI

Infrastruktura klucza publicznego EuroCert składa się z następujących elementów:

a) kwalifikowany urząd certyfikacji: Centrum Kwalifikowane EuroCert,
b) kwalifikowany urząd znacznika czasu: EuroCert QTSA,
c) kwalifikowany urząd weryfikacji statusu certyfikatu,
d) punkty rejestracji, notariusze i inne osoby potwierdzające tożsamość subskrybentów,
e) subskrybenci,
f) strony ufające.

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

1.3.1 Urząd certyfikacji

W skład EuroCert wchodzi jeden urząd certyfikacji – Centrum Kwalifikowane EuroCert, który wystawia certyfikaty dla użytkowników końcowych (subskrybentów) oraz udostępnia informacje niezbędne do weryfikacji ważności wydanych przez siebie certyfikatów. Nadzór nad urzędem sprawuje minister właściwy ds. informatyzacji, który powierzył pełnienie roli nadrzędnego urzędu certyfikacji (tzw. „Root CA") Narodowemu centrum certyfikacji (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 NCcertdo certyfikatu EuroCert wystawionego dla „Centrum Kwalifikowane EuroCert" przez NCcert aż po certyfikat subskrybenta

EuroCert nie wystawia certyfikatów dla żadnych podległych urzędów certyfikacji.

Centrum Kwalifikowane EuroCert wydaje kwalifikowane certyfikaty zgodnie z politykami certyfikacji o identyfikatorach określonych w tab. 3 poniżej i § 7.1.2.

Tab. 3. Identyfikatory polityk certyfikacji umieszczane w certyfikatach wydawanych przez EuroCert

Nazwa certyfikatu	Identyfikator polityki certyfikacji
Certyfikat kwalifikowany (RSA, SHA-1)	1.2.616.1.113791.1.2.1
Certyfikat kwalifikowany (RSA, SHA-2)	1.2.616.1.113791.1.2.2
Certyfikat kwalifikowany (ECDSA, SHA-512)	1.2.616.1.113791.1.2.3

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

1.3.2 Kwalifikowany urząd znacznika czasu

Urząd znacznika czasu wydaje znaczniki czasu zgodnie z zaleceniami „ETSI EN 319 422 Time stamping protocol and time-stamp profiles (marzec 2016)". 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 specjalnie dla usługi znakowania czasem.

1.3.3 Kwalifikowany urząd weryfikacji statusu certyfikatu

EuroCert, oprócz weryfikacji statusu certyfikatu w oparciu o listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu certyfikatu w trybie on-line.
Urząd weryfikacji statusu certyfikatu poświadcza statusy tylko certyfikatów kwalifikowanych i jedynie na moment udzielania odpowiedzi. Poświadczenia te wystawiane są zgodnie z zasadami określonymi w niniejszym Kodeksie.

1.3.4 Punkty Rejestracji

EuroCert, realizując swoje zadania, może działać samodzielnie lub za pośrednictwem punktów rejestracji. Punktami rejestracji mogą osoby fizyczne, prawne i jednostki organizacyjne nieposiadające osobowości prawnej, po podpisaniu stosownej umowy z EuroCert o współpracy w zakresie świadczenia usług zaufania. Podległe EuroCert punkty rejestracji nie mogą akredytować innych punktów rejestracji ani przyjmować wniosków o unieważnienie/zawieszenie certyfikatu.

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

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

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

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

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

1.3.5 Subskrybenci

Subskrybentem może być każda osoba fizyczna, której identyfikator DN zostanie umieszczony w polu podmiot (ang. subject) certyfikatu i która sama dalej nie wydaje certyfikatów innym podmiotom.

Osoby te mogą występować w imieniu własnym lub w imieniu innych podmiotów zwanych zamawiającymi.

EuroCert oferuje certyfikaty różnych typów. Subskrybent powinien zdecydować, jaki certyfikat jest najodpowiedniejszy do jego potrzeb (patrz § 1.4).

1.3.6 Strony ufające

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

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta (patrz § 4.5.2). Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu elektronicznego. Informacje zawarte w kwalifikowanym certyfikacie (m.in. identyfikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.3.7 Pozostali uczestnicy

Nie zdefiniowano.

1.4 Zakres stosowania certyfikatów

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

Certyfikaty wydawane są:

a) osobom prywatnym,
b) osobom fizycznym, będącymi pracownikami dowolnej instytucji lub reprezentującymi tą instytucję.

Tab. 4. Typy certyfikatów

Typ certyfikatu	Opis
osobisty	Kwalifikowane podpisy elektroniczne dokumentów elektronicznych, składane przez osoby prywatne; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię (imiona) subskrybenta, numer seryjny.
firmowy	Kwalifikowany podpisy elektroniczne dokumentów elektronicznych, składane przez osoby fizyczne, będące pracownikami lub reprezentantami firm, organizacji, organów lub innych osób fizycznych; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię (imiona) subskrybenta, nazwę własną reprezentowanego podmiotu i numer seryjny.

Wymienione w tab. 4 certyfikaty wystawiane są subskrybentom (osobom fizycznym), którzy podpiszą umowę z EuroCert Sp. z o.o. na świadczenie usług zaufania i zaakceptują postanowienia niniejszego Kodeksu.

1.4.1 Dozwolone obszary użycia certyfikatów

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

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

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

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

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

1.5 Zarządzanie dokumentem

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

Nowa wersja Kodeksu jest publikowana w repozytorium (patrz rozdz. 2). Subskrybenci oraz pozostałe zainteresowane strony (wymienione w § 1.3) zobowiązani są stosować się wyłącznie do aktualnego Kodeksu.

1.5.1 Odpowiedzialność za zarządzanie dokumentem

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

1.5.2 Dane kontaktowe

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

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

1.5.3 Osoba odpowiedzialna za zgodność dokumentu z Polityką certyfikacji

Za ocenę aktualności i przydatności niniejszego Kodeksu postępowania certyfikacyjnego, Polityki certyfikacji oraz innych dokumentów dotyczących usług zaufania, świadczonych przez EuroCert, a także za zgodność między wymienionymi dokumentami, odpowiada zespół EuroCert.

1.5.4 Procedury zatwierdzania dokumentu

Zatwierdzenia zmian w Kodeksie dokonuje zarząd EuroCert Sp. z o.o. Po zatwierdzeniu dokument otrzymuje status aktualny ze wskazaniem daty początku obowiązywania. Najpóźniej tego dnia jest on publikowany w repozytorium.

1.6 Słownik używanych terminów i akronimów

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

Tab. 5. Terminy i skróty używane w Kodeksie

Termin/akronim	Opis
Urząd certyfikacji	Centrum Kwalifikowane EuroCert
Punkt Rejestracji	jednostka organizacyjna działająca w imieniu EuroCert Sp. z o.o., wykonująca zgodnie z niniejszym Kodeksem niektóre funkcje związane ze świadczeniem usług zaufania
DN	Identyfikator DN – Distinguished Name – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500
OCSP	Online Certificate Status Protocol - protokół i nazwa usługi PKI służącej do informowania o statusie konkretnych certyfikatów, o które pyta usługobiorca (czy certyfikat jest ważny, czy unieważniony)
CRL	Lista unieważnionych certyfikatów (Certificate Revocation List)
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure – infrastruktura klucza publicznego – system obejmujący Centra Certyfikacji Kluczy, Punkty Rejestracji oraz użytkowników końcowych, służący do dystrybucji certyfikatów klucza publicznego oraz zapewnienia możliwości ich wiarygodnej weryfikacji
HSM	Hardware Security Module – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego do generowania podpisów/pieczęci elektronicznych (np. przy wystawianiu certyfikatów, list CRL)
NCCert	Root krajowego systemu PKI, prowadzony przez Narodowy Bank Polski, na podstawie upoważnienia ministra właściwego ds. informatyzacji.
Klucz prywatny	Dane służące do składania podpisu elektronicznego

Klucz publiczny	Dane służące do weryfikacji podpisu elektronicznego, zazwyczaj dystrybuowane w postaci certyfikatu
Ustawa o usługach zaufania	Ustawy o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. poz. 1579)
Rozporządzenie eIDAS	Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r., w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym
QSCD	Qualified Signature Creation Device – urządzenie posiadające certyfikat umożliwiający użycie do wystawiania kwalifikowanego pieczęci/podpisu elektronicznego, na podstawie rozporządzenia eIDAS
Ustawa o ochronie danych osobowych	ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922)
TSL	EU Trust service Status List – listy wydawane przez Komisję Europejską (lista list) oraz kraje członkowskie EU, zawierające informacje o 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 i publikacje

2.1 Repozytorium

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

https://eurocert.pl/repozytorium

2.2 Publikacja informacji w repozytorium

W repozytorium publikowane są następujące informacje:

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

EuroCert nie publikuje certyfikatów subskrybentów.

2.3 Częstotliwość publikowania

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

2.4 Kontrola dostępu do repozytorium

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

3 Identyfikacja i uwierzytelnianie

Niniejszy rozdział przedstawia zasady weryfikacji tożsamości potencjalnych subskrybentów przy wydawaniu, zawieszaniu lub unieważnianiu certyfikatów. Zasady te zawierają środki które należy przedsięwziąć w celu uzyskania pewności, że informacje przekazane przez potencjalnego subskrybenta we wniosku o wydanie certyfikatu są dokładne i wiarygodne w momencie wydania certyfikatu.

3.1 Nazewnictwo używane w certyfikatach

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

3.1.1 Rodzaje nazw

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

3.1.2 Konieczność używania nazw znaczących

Nazwa subskrybenta jest tworzona w oparciu o podzbiór poniższych atrybutów (tab. 6), przy czym powinna zawierać co najmniej nazwę kraju, imię (imiona) i nazwisko oraz numer seryjny (SN).

Tab. 6. Profil nazwy subskrybenta

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

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

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

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

3.1.3 Anonimowość subskrybentów

EuroCert nie wystawia certyfikatów anonimowych. Każdy identyfikator DN zawiera przynajmniej nazwę kraju, imię (imiona), nazwisko oraz numer seryjny (SN).

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 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part: 1,2,5.

3.1.5 Unikalność nazw

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

3.1.6 Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

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

3.2 Identyfikacja i uwierzytelnianie przy wydawaniu pierwszego certyfikatu

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

Potencjalny subskrybent, obok podania danych będących treścią nazwy wyróżniającej certyfikatu (patrz § 3.1.2), jest zobowiązany udzielić dodatkowych informacji pozwalających na jego identyfikację, w tym:

- cechy dokumentu tożsamości,
- datę i miejsce urodzenia,
- dane kontaktowe.

Potwierdzenie tych danych w sytuacji, gdy potencjalny subskrybent nie posiada ważnego certyfikatu kwalifikowanego wydanego przez kwalifikowanego dostawcę usług zaufania następuje przez jego fizyczną obecność w punkcie rejestracji lub osobisty kontakt operatora punktu rejestracji z potencjalnym subskrybentem w innym miejscu.

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

3.2.1 Udowodnienie posiadania klucza prywatnego

Nie dotyczy.

3.2.2 Identyfikacja i uwierzytelnianie osób prawnych

Nie dotyczy.

3.2.3 Identyfikacja i uwierzytelnianie osób fizycznych

EuroCert oraz podległe mu punkty rejestracji potwierdzają tożsamość potencjalnego subskrybenta 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. zaświadczenie o miejscu zatrudnienia.

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

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

EuroCert może również potwierdzić tożsamość osoby ubiegającej się o certyfikat za pośrednictwem notariusza. W takim przypadku wnioskodawca jednostronnie podpisuje umowę z EuroCert w obecności notariusza, która po przekazaniu do EuroCert jest podpisywana przez Inspektora rejestracji i odsyłana na adres wskazany przez wnioskodawcę.

Przed wystawieniem certyfikatu wnioskodawca jest zobowiązany potwierdzić zapoznanie się z Polityką certyfikacji, Kodeksem postępowania certyfikacyjnego, warunkami użycia, zakresem i ograniczeniami stosowania certyfikatu, skutkami prawnymi składania kwalifikowanego podpisu elektronicznego

poprzez złożenie własnoręcznego podpisu pod treścią umowy o świadczenie usług zaufania. Podpisanie umowy oznacza także, że:

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

3.2.4 Dane subskrybenta niepodlegające weryfikacji

Patrz § 3.1.6.

3.2.5 Sprawdzanie praw do otrzymania certyfikatu

Przed przekazaniem certyfikatu subskrybentowi EuroCert sprawdza tożsamość tej osoby na podstawie okazanego przez nią dokumentu tożsamości.

3.2.6 Kryteria interoperacyjności

Nie dotyczy.

3.3 Identyfikacja i uwierzytelnianie przy wydawaniu kolejnego certyfikatu

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

3.3.1 Wydawanie kolejnego certyfikatu w okresie ważności obecnego certyfikatu

W przypadku gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu (oraz pozostałych dokumentów uwierzytelniających), a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone kwalifikowanym podpisem elektronicznym tej osoby, o ile dane te nie różnią się od danych zawartych w certyfikacie związanym z kwalifikowanym podpisem elektronicznym, którego użyto do podpisania tych danych. Wówczas uwierzytelnianie subskrybenta realizowane jest w oparciu o informacje zawarte w bazach danych EuroCert i polega na zweryfikowaniu podpisu elektronicznego złożonego pod wnioskiem o certyfikat oraz potwierdzeniu autentyczności związanego z podpisem certyfikatu (w oparciu o tzw. ścieżkę certyfikacji). Nie oznacza to jednak brak możliwości zastosowania procedury opisanej w § 3.2.

3.3.2 Wydanie kolejnego certyfikatu po wygaśnięciu/unieważnieniu obecnego certyfikatu

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

3.4 Identyfikacja i uwierzytelnianie przy unieważnianiu certyfikatu

Unieważnienie certyfikatu może nastąpić:

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

Unieważnienia certyfikatu można dokonać w następujący sposób:

a) osobiście w EuroCert (adres podano w § 1.5.2), w godzinach pracy tj. od 9.00 do 17.00, po potwierdzeniu tożsamości osoby występującej o unieważnienie przez Inspektora rejestracji na zasadach opisanych w § 3.2,
b) telefonicznie (numer infolinii: 22 490 49 86), w ciągu całej doby, na podstawie hasła do unieważnienia certyfikatu ustalonego przy jego wydawaniu oraz danych osobowych podanych przy wydawaniu certyfikatu,
c) drogą elektroniczną posługując się formularzem on-line na stronie internetowej https://eurocert.pl/uniewaznienia/ lub poprzez wysłanie wniosku o unieważnienie (publikowanym w repozytorium) opatrzonego ważnym kwalifikowanym podpisem elektronicznym na adres uniewaznienia@eurocert.pl.

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

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

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

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

4 Wymagania funkcjonalne

W niniejszym rozdziale przedstawiono sposób realizacji usługi wydawania kwalifikowanych certyfikatów klucza publicznego, ich unieważniania i zawieszania/ odwieszania, wydawania kolejnych certyfikatów, modyfikacji certyfikatu, wystawiania tokenów znaczników czasu oraz tokenów statusu certyfikatów.

4.1 Wniosek o certyfikat

Organizacje pragnące uzyskać dla swoich pracowników certyfikaty, mogą to uczynić poprzez swoich upoważnionych przedstawicieli. Z kolei subskrybent indywidualny występuje o certyfikat, w swoim imieniu.

Niezależnie od tego czy subskrybent występuje o wydanie certyfikatu indywidualnie czy też robi to w jego imieniu upoważniony przedstawiciel (dotyczy to tzw. certyfikatów firmowych), to wydanie certyfikatu musi być poprzedzone zawarciem umowy pomiędzy subskrybentem a EuroCert Sp. z o.o.

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

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

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

4.1.1 Kto składa wniosek o certyfikat

O wydanie certyfikatu mogą się ubiegać wyłącznie osoby prywatne (certyfikat osobisty) oraz osoby fizyczne będące pracownikami lub reprezentantami firm, organizacji, organów lub innych osób fizycznych (certyfikat firmowy).

4.1.2 Rejestracja wniosku

Rejestracja wniosku polega na przyjęciu wniosku oraz wprowadzeniu danych wnioskodawcy do systemu EuroCert. Punkt rejestracji jest odpowiedzialny za wprowadzenie prawidłowych danych, uprzednio zweryfikowanych metodami opisanymi w § 3.2 lub 3.3.

4.2 Przetwarzanie wniosku

Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dołączonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku.

4.2.1 Wykonywanie funkcji identyfikacji i uwierzytelniania

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

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) wnioskodawca nie dostarczył kompletu wymaganych dokumentów,
d) 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

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

EuroCert wydaje certyfikaty za każdym razem generując nową parę kluczy.

4.3.1 Czynności urzędu certyfikacji podczas wydawania certyfikatu

Inspektor rejestracji podpisuje elektronicznie zgłoszenie certyfikacyjne, o którym mowa w § 4.2.1, a następnie przesyła podpisane zgłoszenie certyfikacyjne do systemu generującego certyfikaty uruchamiając procedurę generowania certyfikatu subskrybenta na kwalifikowanym urządzeniu do składania podpisu elektronicznego posiadającego funkcje generowania kluczy przez komponent techniczny, którego konstrukcja:

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

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

4.3.2 Informowanie subskrybenta o wydaniu certyfikatu

O wydaniu certyfikatu subskrybent informowany jest osobiście.

4.4 Akceptacja certyfikatu

Po odebraniu certyfikatu subskrybent jest zobowiązany do niezwłocznego sprawdzenia jego zawartości, nie później niż przed pierwszym użyciem klucza prywatnego związanego z certyfikatem. W przypadku nieprawdziwości danych zawartych w certyfikacie, jest on zobowiązany do niezwłocznego zgłoszenia tego faktu EuroCert, celem unieważnienia certyfikatu zgodnie z obowiązującymi procedurami (patrz § 3.4 i 4.9) i otrzymania nowego, zawierającego poprawne dane certyfikatu.

Posługiwanie się certyfikatem zawierającym nieprawdziwe dane naraża subskrybenta na odpowiedzialność karną określoną w art. 42 ust. 2 Ustawy o usługach zaufania.

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

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 § 4.7) akceptacja certyfikatu przez subskrybenta następuje poprzez pobranie go z systemu EuroCert.

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

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

4.5.1 Zobowiązania subskrybenta

Subskrybent zobowiązuje się do:

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

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

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

4.5.2 Zobowiązania strony ufającej

Strony ufające są zobowiązane do:

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

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

4.6 Odnowienie certyfikatu

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

4.7 Wystawienie kolejnego certyfikatu

Wystawienie kolejnego certyfikatu ma miejsce zawsze wtedy, gdy subskrybent występuje z wnioskiem o dodatkowy certyfikat posiadanego typu dla nowej pary kluczy w okresie ważności obecnego certyfikatu.

Wystawienie kolejnego certyfikatu może być realizowane przez subskrybenta okresowo, w oparciu o parametry wskazanego certyfikatu, będącego już w posiadaniu subskrybenta. W efekcie tworzony jest nowy certyfikat, którego parametry są takie same jak wskazanego we wniosku certyfikatu, poza zawartym w nim nowym kluczem publicznym, numerem seryjnym certyfikatu i innym okresem jego ważności.

Nowy certyfikat będzie zawierał identyfikator DN użytkownika taki sam, jaki znajduje się w certyfikacie subskrybenta, który jest wykorzystywany do weryfikacji podpisu elektronicznego subskrybenta złożonego pod zgłoszeniem certyfikacyjnym.

Proces wydawania kolejnego certyfikatu po unieważnieniu poprzedniego lub wydawania kolejnego certyfikatu w przypadku, gdy upłynął okres ważności posiadanego przez subskrybenta certyfikatu, przebiega analogicznie jak proces wydawania pierwszego certyfikatu.

4.7.1 Warunki wystawienia kolejnego certyfikatu

Subskrybent w każdej chwili może wystąpić z wnioskiem o wystawienie nowego certyfikatu, np. wtedy, gdy obecny certyfikat traci ważność.

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

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

4.7.2 Kto może żądać wydania kolejnego certyfikatu?

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

4.7.3 Przetwarzanie wniosku o wydanie kolejnego certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.7.4 Informowanie podmiotu o wydaniu certyfikatu

Informacja o wygenerowaniu certyfikatu jest przekazywana do subskrybenta elektronicznie.

4.7.5 Akceptacja certyfikatu

Akceptacja certyfikatu przez subskrybenta następuje poprzez pobranie go z systemu.

4.7.6 Publikacja certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.7.7 Powiadomienie innych podmiotów o wydaniu certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8 Modyfikacja certyfikatu

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

4.8.1 Warunki modyfikacji certyfikatu

Modyfikacja certyfikatu:

- odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o wydanie nowego certyfikatu,
- może dotyczyć tylko certyfikatu, którego okres ważności nie minął lub nie został wcześniej unieważniony.

Nowy certyfikat posiada nowy klucz publiczny, nowy numer seryjny i różni się zawartością przynajmniej jednego z pozostałych pól certyfikatu. Modyfikacji nie może ulec identyfikator polityki certyfikacji, według której certyfikat został wystawiony.

4.8.2 Kto może żądać zmiany danych w certyfikacie?

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

4.8.3 Przetwarzanie wniosku o modyfikację certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.4 Informowanie podmiotu o wydaniu zmodyfikowanego certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.5 Akceptacja certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.6 Publikacja certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.8.7 Powiadomienie innych podmiotów o wydaniu certyfikatu

Analogicznie jak przy wydawaniu pierwszego certyfikatu.

4.9 Unieważnienie i zawieszenie certyfikatu

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

4.9.1 Okoliczności unieważnienia certyfikatu

Unieważnienie certyfikatu może wynikać z następujących okoliczności:

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

4.9.2 Kto może żądać unieważnienia certyfikatu

Z żądaniem unieważnienia certyfikatu subskrybenta mogą występować następujące podmioty:

a) subskrybent będący podmiotem unieważnianego certyfikatu,
b) osoba trzecia, której dane występują w certyfikacie,
c) inspektor bezpieczeństwa,
d) upoważniony przedstawiciel reprezentowanego przez subskrybenta podmiotu,
e) organ nadrzędny organizacji, w imieniu której występuje subskrybent,
f) osoba fizyczna udzielająca pełnomocnictwa do reprezentowania jej interesów,
g) minister właściwy ds. informatyzacji,

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

EuroCert zachowuje szczególną ostrożność przy rozpatrywaniu wniosków o unieważnienie certyfikatu, których autorem nie jest subskrybent i honorują tylko te, które obejmują przypadki wymienione w § 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 rejestracji zgodnie z zasadami w § 3.4. W przypadku, gdy istnieją przesłanki do unieważnienia certyfikatu, jednakże Inspektor rejestracji nie jest w stanie w ciągu 1 godziny od momentu otrzymania kompletnego wniosku wyjaśnić wszystkich wątpliwości dotyczących unieważnienia, certyfikat jest zawieszany.

Informacja o unieważnieniu certyfikatu jest umieszczana na liście CRL (patrz § 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 przetwarzanie 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

Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem opublikowanej listy CRL natychmiast po gwarantowanym czasie unieważnienia certyfikatu.

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

4.9.7 Częstotliwość publikacji CRL

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

4.9.8 Maksymalne opóźnienie w publikowaniu list CRL

Listy CRL są publikowane, natychmiast po ich utworzeniu.

4.9.9 Dostępność weryfikacji statusu certyfikatu on-line

Kwalifikowany urząd weryfikacji statusu certyfikatu udostępnia usługę weryfikacji certyfikatów kwalifikowanych w trybie on-line. Usługa tego typu realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 6960 *Internet X.509 Public Key Infrastructure: On-line Certificate Status Protocol – OCSP.*

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:

- poprawny (*ang. good*) – oznacza pozytywną odpowiedź na żądanie, którą należy

jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny,

- unieważniony (*ang. revoked*) – oznacza, że certyfikat został unieważniony,
- 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).

4.9.10 Obowiązek sprawdzenia unieważnień w trybie on-line

Niniejszy Kodeks postępowania certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

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 Centrum Kwalifikowane Eurocert jest jak najszybsze poinformowanie organu nadzoru, subskrybentów i stron ufających o tym fakcie poprzez publikację na stronie internetowej EuroCert oraz jeśli to możliwe w środkach masowego przekazu.

4.9.13 Okoliczności zawieszenia certyfikatu

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

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

a) dane zawarte w elektronicznym lub papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,
b) wniosek o unieważnienie został przekazany telefonicznie i nie można w ciągu 1 godziny, liczonej od chwili otrzymania wniosku potwierdzić tożsamości wnioskodawcy, ale też zanegować słuszności złożonego wniosku,
c) istnieje podejrzenie, że osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,
d) urząd certyfikacji może niezwłocznie zawiesić certyfikat w przypadku uzasadnionego podejrzenia, że certyfikat wydano bez przestrzegania postanowień niniejszego Kodeksu; certyfikat może pozostać zawieszony do czasu aż urząd certyfikacji znajdzie podstawy do unieważnienia certyfikatu, nie dłużej jednak jak 7 dni,
e) 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 z inicjatywy EuroCert w przypadku uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia certyfikatu wskazane w § 4.9.1, w szczególności na wniosek subskrybenta (patrz § 3.4).

4.9.15 Procedura zawieszenia i odwieszenia certyfikatu

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

W przypadku niepotwierdzenia się przesłanek uzasadniających zawieszenie certyfikatu, o których mowa w § 4.9.13 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 Weryfikacja statusu certyfikatu

Weryfikacji statusu certyfikatów wydanych przez EuroCert można dokonać na podstawie list CRL. Listy CRL są generowane nie rzadziej niż co 24 godziny lub w ciągu godziny od zawieszenia/unieważnienia certyfikatu i publikowane automatycznie w repozytorium (patrz rozdz. 2). EuroCert sprawdza co najmniej raz dziennie dostępność list CRL.
Status certyfikatu wydanego przez EuroCert można również zweryfikować korzystając z usługi OCSP, o ile taka informacja jest umieszczona w wydanym certyfikacie. W przypadku gdy w certyfikacie został umieszczony adres usługi OCSP oznacza to, że dla tego certyfikatu jest udostępniania usługa OCSP.

4.11 Rezygnacja z usług

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

4.12 Odzyskiwanie i przechowywanie kluczy prywatnych

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 oraz pomieszczeń EuroCert jest kontrolowany oraz nadzorowanych przez zintegrowany system alarmowy. Ochrona na zewnątrz budynków funkcjonuje 24 godziny na dobę.

Pomieszczenia systemu komputerowego, w tym także pomieszczenia, w którym znajduje się bezpieczny moduł kryptograficzny z pozostającymi w nim kluczami urzędu certyfikacji, wyposażone są w system kontroli dostępu do pomieszczeń oraz system sygnalizacji włamania i napadu. Dostęp do pomieszczeń posiadają tylko osoby upoważnione, tzn. zaufany personel EuroCert. Nadzorowanie praw dostępu realizowane jest w oparciu o posiadane przez nich karty identyfikacyjne.

5.1.3 Zasilanie i klimatyzacja

W przypadku zaniku zasilania podstawowego system przechodzi na zasilanie awaryjne poprzez UPS. Środowisko pracy w pomieszczeniach systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń. Ponadto wszystkie pomieszczenia są klimatyzowane.

5.1.4 Zagrożenie powodziowe

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

5.1.5 Ochrona przeciwpożarowa

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 informacji

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

5.1.7 Niszczenie informacji

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

5.1.8 Kopie bezpieczeństwa i siedziba zapasowa

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

Wszelkie dane i urządzenia 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.

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) 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. 7. Przedstawiony podział ról jest zgodny z wymogami ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

Tab. 7. Zaufane role

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

5.2.2 Liczba osób wymaganych do realizacji zadania

Operacją, która wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich generowaniu powinny być obecne osoby, pełniące role:

- inspektora bezpieczeństwa,
- administratora systemu (operatora modułu kryptograficznego),
- posiadaczy sekretów współdzielonych,
- obserwatorów – (opcjonalnie) np. przedstawiciele audytora.

Szczegółowa procedura generowania kluczy opisana jest w wewnętrznych dokumentach EuroCert.

5.2.3 Identyfikacja oraz uwierzytelnianie ról

Personel EuroCert jest poddawany procedurze identyfikacji oraz uwierzytelniania w następujących przypadkach:

- umieszczania na liście osób posiadających dostęp do pomieszczeń EuroCert,
- umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci EuroCert**,**
- wydawania poświadczenia upoważniającego do wykonywania przypisanej roli,
- przydzielania konta oraz hasła w systemie komputerowym EuroCert.

Każde z powyższych poświadczeń oraz przypisanych kont:

- musi być unikalne i bezpośrednio przypisane konkretnej osobie,
- nie może być współdzielone z innymi osobami,
- musi być ograniczone do funkcji (wynikających z roli pełnionej przez określoną osobę) realizowanych tylko za pośrednictwem dostępnego oprogramowania systemu EuroCert, systemu operacyjnego oraz kontroli proceduralnych.

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

Konta oraz uprawnienia osób, które zakończyły pracę w EuroCert lub utraciły prawo do reprezentowania EuroCert, są natychmiast blokowane.

Inspektorzy bezpieczeństwa EuroCert prowadzą regularne - odbywające się raz na kwartał - przeglądy kont i uprawnień w systemach EuroCert. Wszystkie nieużywane są blokowane.

5.2.4 Role wymagające separacji obowiązków

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

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

5.3 Nadzorowanie Pracowników

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

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 certyfikacyjnych.

5.3.2 Weryfikacja pracowników

Przed powierzeniem pracownikowi którejkolwiek z ról opisanych w § 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,
- zasad Kodeksu postępowania certyfikacyjnego,
- zasad zawartych w dokumentacji, przypisanej 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 § 5.3.3 są powtarzane lub uzupełniane są w zależności od potrzeb oraz zawsze wtedy, gdy nastąpiły istotne zmiany w świadczeniu usług przez EuroCert, funkcjonowaniu EuroCert lub punktów rejestracji, systemie, bądź zostały opublikowane nowe wersje Polityki certyfikacji lub Kodeksu postępowania certyfikacyjnego.

5.3.5 Częstotliwość rotacji stanowisk i jej kolejność

Niniejszy Kodeks postępowania certyfikacyjnego 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 systemu w porozumieniu z Inspektorem bezpieczeństwa może zablokować dostęp do systemu 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 § 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 certyfikacyjnych lub nieprzestrzegające wymagań nałożonych przez przepisy o podpisie elektronicznym (w szczególności wymagań o poufności, wymagań w zakresie wystawiania i unieważniania certyfikatów) podlegają sankcjom karnym określonym w Ustawie o usługach zaufania.

5.3.8 Dokumentacja dla pracowników

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

- Polityki certyfikacji,
- Kodeksu postępowania certyfikacyjnego,
- wzory umów oraz stosowanych formularzy wniosków,
- niezbędne wyciągi 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 z świadczonymi usługami zaufania w celu zapewnienia bezpieczeństwa, nadzoru nad sprawnym działaniem systemu oraz rozliczania użytkowników i personelu z ich działań.

Odpowiedzialnym za prowadzenie rejestru zdarzeń jest Inspektor bezpieczeństwa. Rejestr zdarzeń przechowywany jest w sposób zapewniający integralność.

5.4.1 Typy rejestrowanych zdarzeń

Rejestrowane zdarzenia obejmują:

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

Rejestry zdarzeń zapisywane są w formie elektronicznej. Rekordy zawierają identyfikator zdarzenia, datę i czas wystąpienia, typ zdarzenia, opis szczegółowy. Stary rejestr po zarchiwizowaniu jest usuwany z dysku.

5.4.2 Częstotliwość analizy zapisów zdarzeń

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

5.4.3 Okres przechowywania zapisów rejestrowanych zdarzeń

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

5.4.4 Ochrona zapisów rejestrowanych zdarzeń

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

5.4.5 Tworzenie kopii zapisów rejestrowanych zdarzeń

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

Czynności tworzenia kopii zapasowych wykonywane są przez operatora systemu w obecności Inspektora bezpieczeństwa.

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 ds. bezpieczeństwa. W zależności od poziomu i wagi zagrożenia powiadamiane są osoby odpowiedzialne za działanie komponentów, których dotyczy zdarzenie. Powiadamianie może być wykonane drogą elektroniczną lub telefonicznie.

W przypadku naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe, nie później niż w ciągu 24 godzin od wystąpienia zdarzenia EuroCert zawiadamia organ nadzoru i, w stosowanych przypadkach, inne właściwe podmioty zgodnie z art. 19.2 Rozporządzenia eIDAS (patrz § 5.7.1).

5.4.8 Oszacowanie podatności na zagrożenia

Niniejszy Kodeks postępowania certyfikacyjnego wymaga przeprowadzenia przez EuroCert analizy podatności na zagrożenia wszystkich posiadanych aktywów, w tym w szczególności oprogramowania oraz systemu komputerowego.

Analiza ryzyka dla EuroCert prowadzona jest przynajmniej raz w roku lub przy wprowadzaniu nowych usług, dużych zmian w systemach lub w wyniku incydentu bezpieczeństwa. Za audyt wewnętrzny odpowiedzialny jest inspektor bezpieczeństwa, którego zadanie polega na kontroli zgodności zapisów w rejestrze bezpieczeństwa, poprawności przechowywania jego kopii, działań podejmowanych w sytuacjach zagrożeń oraz przestrzegania postanowień niniejszego dokumentu.

5.5 Archiwizacja danych

5.5.1 Typy archiwizowanych danych

Archiwizacji podlegają następujące dane:

- umowy o świadczenie usług certyfikacyjnych, o których mowa w art. 14 § 1 Ustawy o usługach zaufania,
- otrzymywane wnioski oraz wydawane decyzje, mające postać papierową lub elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane,
- baza danych subskrybentów, w tym wszystkie informacje zebrane w procesie rejestracji subskrybenta,
- baza danych certyfikatów,
- wydane listy CRL,
- historia kluczy urzędu kwalifikowanego, od ich wygenerowania do zniszczenia włącznie,
- politykę świadczenia usług,
- dokumenty wystawiane przez operatora systemu punktu rejestracji, notariusza lub inne osoby potwierdzające tożsamość wnioskodawcy w imieniu EuroCert,
- żądania unieważnienia certyfikatu,
- pozostałe dokumenty papierowe, związane ze świadczeniem usług certyfikacyjnych.

5.5.2 Okres przechowywania archiwów

Dokumenty papierowe oraz dane w postaci elektronicznej, o których mowa w § 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 w postaci elektronicznej przechowywane są w centrum podstawowym w sejfach, z kolei archiwalne dane w postaci papierowej przechowywane są w siedzibie EuroCert Sp. z o.o. w metalowych zamykanych na klucz szafach.

5.5.4 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 oraz sejfów ognioodpornych. 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, co pewien okres testowane oraz porównywane z danymi oryginalnymi. Czynność ta może być przeprowadzona tylko przez inspektora bezpieczeństwa i jest odnotowywana w rejestrze zdarzeń. 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 ośrodków certyfikacji realizowana jest w sposób zapewniający zachowanie ustalonego minimalnego okresu ważności certyfikatów. Odpowiednio wcześniej przed wygaśnięciem certyfikatu danego urzędu certyfikacji tworzona jest nowa, niezależna infrastruktura klucza publicznego w ramach

której generowana jest nowa para kluczy oraz certyfikat nowego urzędu certyfikacji. Do czasu wygaśnięcia certyfikatu starego ośrodka certyfikacji działają dwa ośrodki. Nowy urząd certyfikacji przejmuje rolę wygasającego, świadczy wszystkie czynności związane z obsługą certyfikatów: generowanie, zawieszanie i unieważnianie certyfikatów, generacja list CRL. Wygasający ośrodek certyfikacji obsługuje tylko unieważnienia i zawieszenia certyfikatów wystawionych w ramach swojej infrastruktury oraz generuje listy CRL do czasu zaprzestania swojej działalności operacyjnej (wygaśnięcia certyfikatu).

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

Procedura wymiany pary kluczy przebiega następująco:

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

5.7 Utrata poufności klucza i działanie w przypadku katastrof

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

5.7.1 Procedura obsługi incydentów i reagowania na zagrożenia

Procedury postepowania w przypadku wystąpienia zagrożenia lub naruszenia bezpieczeństwa systemu szczegółowo opisane są w obowiązującej w EuroCert procedurze zarządzania incydentem bezpieczeństwa i planie ciągłości działania. Procedury te są zgodne z wymaganiami art. 19.2 Rozporządzenia eIDAS.

5.7.2 Procedury odzyskiwania zasobów obliczeniowych, oprogramowania i/lub danych

EuroCert dysponuje zestawem procedur operacyjnych 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) procedury operacyjne urzędu certyfikacji.

Procedury odzyskiwania mieszczą się w Planie ciągłości działania i są regularnie testowane. Po testach tworzony jest raport.

5.7.3 Procedury w przypadku kompromitacji klucza urzędu

Eurocert posiada odpowiednie procedury obowiązujące w wypadku utraty poufności klucza prywatnego Eurocert lub uzasadnionego podejrzenie zajścia takiego zdarzenia (patrz § 5.4.7). Procedury te przewidują między innymi:

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

5.7.4 Zapewnienie ciągłości działania po katastrofach

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

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

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

5.8 Zakończenie działalności 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 § 2 Ustawy o usługach zaufania).

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

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

W przeciwnym wypadku konieczne jest unieważnienie certyfikatów subskrybentów, którym przysługuje prawo zwrotu proporcjonalnej do okresu wykorzystania certyfikatu części wynagrodzenia z tytułu jego zakupu.

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

6 Procedury bezpieczeństwa technicznego

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

6.1 Generowanie i instalowanie par kluczy

Urząd certyfikacji Centrum Kwalifikowane EuroCert posiada przynajmniej jedno zaświadczenie certyfikacyjne, które stosowane jest w procesie elektronicznego poświadczania kwalifikowanych 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 w kombinacji z funkcją skrótu SHA-1/SHA-512.

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 certyfikacyjnych (patrz § 5.2.2), w tym Inspektora bezpieczeństwa. Z ceremonii generowania kluczy sporządza się protokół.

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

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

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

6.1.2 Dostarczenie klucza prywatnego subskrybentowi

Para kluczy i certyfikat subskrybenta są wydawane zgodnie z zasadami w § 4.4. Klucze subskrybenta wraz z certyfikatem dostarczane są mu osobiście z informacjami pozwalającymi na aktywację klucza prywatnego, subskrybent ma obowiązek do niezwłocznej zmiany danych pozwalających na aktywację klucza prywatnego. Konieczna jest zmiana PIN-ów przez subskrybenta, przed rozpoczęciem okresu eksploatacji certyfikatu.

Subskrybenci chcący odnowić posiadany na karcie kryptograficznej wydanej przez EuroCert ważny certyfikat kwalifikowany, mogą wygenerować zdalnie kolejną parę kluczy. Wówczas EuroCert udostępnia swoim subskrybentom dedykowaną aplikację, która tworzy klucze bezpośrednio na karcie kryptograficznej subskrybenta.

6.1.3 Dostarczenie klucza publicznego 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 zgodnych z zaleceniem ITU-T X.509 v.3. Klucz publiczny urzędu certyfikacji Centrum Kwalifikowane EuroCert ma postać certyfikatu, wydanego przez Narodowe Centrum Certyfikacji.

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

6.1.5 Rozmiary kluczy

Minimalne parametry algorytmów szyfrowych dopuszczonych do stosowania przez EuroCert oraz odbiorców usług certyfikacyjnych są następujące:

a) dla algorytmu RSA:
   - minimalna długość klucza, rozumianego jako moduł p*q wynosi 2048 bitów,
   - długości liczb pierwszych p i q, składających się na moduł nie mogą się różnić więcej niż o 30 bitów;

b) dla algorytmu ECDSA i ECGDSA:
   - minimalna długość parametru g wynosi 256 bitów,
   - minimalny współczynnik r0 wynosi 10000,
   - minimalna klasa wynosi 200.

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

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

6.1.6 Parametry generowania klucza publicznego i weryfikacja jakości

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

6.1.7 Cel użycia kluczy

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

Klucz prywatny urzędu certyfikacji może być wykorzystywany tylko do podpisywania certyfikatów i list CRL. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów (keyCertSign) i list CRL (cRLSign).

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

6.2 Ochrona klucza prywatnego oraz techniczna kontrola modułu kryptograficznego

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

6.2.1 Standardy dla modułu kryptograficznego

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

6.2.2 Podział klucza prywatnego

Patrz § 6.2.4.

6.2.3 Deponowanie klucza prywatnego

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

6.2.4 Kopie zapasowe klucza prywatnego

Mechanizm zapewnienia kopii zapasowej klucza prywatnego urzędu certyfikacji jest realizowany dzięki podziałowi klucza na części (tzw. sekrety) w liczbie większej niż jest wymagana do odtworzenia klucza. Przyjęta liczba podziałów klucza na sekrety oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w tab. 8.

Tab. 8. Schemat podziału klucza prywatnego

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

Sekrety zapisywane są na kartach kryptograficznych chronionych numerem PIN znanym tylko osobie której został on przekazany podczas ceremonii generowania kluczy. Sekrety, jak też chroniące je numery PIN przechowywane są w różnych, fizycznie chronionych, miejscach. W żadnym z tych miejsc nie jest przechowywany taki zestaw kart oraz numerów PIN, który umożliwia odtworzenie klucza urzędu certyfikacji.

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

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

6.2.5 Archiwizowanie klucza prywatnego

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

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

6.2.6 Wprowadzanie klucza prywatnego do modułu kryptograficznego

Wprowadzanie klucza prywatnego do modułów kryptograficznych realizowane jest w sytuacjach:

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

Załadowanie klucza do modułu odbywa się przy udziale posiadaczy współdzielonych sekretów. Do załadowania klucza konieczna jest obecność liczby sekretów opisana w § 6.2.4. Ładownie odbywa się w ramach zamkniętego środowiska bezpieczeństwa. Klucz prywatny jest składany z elementów. Podawane są kolejno fragmenty klucza tajnego z kart, zaszyfrowane pliki ładowane są do pamięci modułu i następuje ich odszyfrowanie. Klucz prywatny jest gotowy do użycia. Ładownie klucza do modułu odnotowane jest w rejestrze zdarzeń.

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

6.2.7 Przechowywanie klucza prywatnego w module kryptograficznym

Po rozszyfrowaniu i załadowaniu klucza prywatnego do pamięci modułu kryptograficznego jest on chroniony sprzętowo. Nie ma możliwości odczytu wartości klucza prywatnego z modułu, klucz ten nigdy modułu nie opuszcza. Operacje wymagające użycia klucza prywatnego wykonywane są w module kryptograficznym.

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

6.2.8 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 nośniku.

6.2.9 Dezaktywacja klucza prywatnego

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

6.2.10 Metody niszczenia klucza prywatnego

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

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

6.2.11 Standardy modułu kryptograficznego

Parametry modułów kryptograficznych opisuje punkt 6.2.1.

6.3 Inne aspekty zarządzania parą kluczy

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

6.3.1 Archiwizowanie kluczy publicznych

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

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

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

6.3.2 Okres ważności certyfikatów i kluczy prywatnych

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

6.4 Dane aktywujące

6.4.1 Generowanie danych aktywujących i ich instalowanie

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

6.4.2 Ochrona danych aktywujących

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

6.4.3 Inne aspekty związane z danymi aktywującymi

Kopie haseł do zabezpieczania dostępu do karty kryptograficznej nie są przechowywane w EuroCert. EuroCert nie posiada żadnych kodów lub danych umożliwiających odtworzenie kodów PIN i PUK zabezpieczających dostęp do karty nadanych przez subskrybenta.

Uaktywnienie klucza urzędu certyfikacji opisane jest w rozdziałach 6.2.4 i 6.2.8.

6.5 Zabezpieczenia komputerów

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

6.5.1 Wymagania dotyczące zabezpieczeń systemów komputerowych

Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania w punktach rejestracji. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery pracujące w EuroCert wyposażone są w następujące funkcje zabezpieczające:

a) obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),
b) uznaniową kontrolę dostępu,
c) możliwość prowadzenia audytu zabezpieczeń,
d) komputery udostępniane są tylko personelowi, który pełni zaufane role w EuroCert,
e) pracownik, który pełni zaufaną role jest zobowiązany do blokowania swojej stacji roboczej zawsze, jeśli pozostają one poza jego nadzorem,
f) wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
g) wymuszanie wylogowania użytkownika po okresie bezczynności,
h) identyfikację i uwierzytelnienie ról oraz pełniących je osób,
i) kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
j) archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,

k) bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
l) mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
m) mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

6.5.2 Ocena bezpieczeństwa systemów komputerowych

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

6.6 Cykl życia zabezpieczeń technicznych

6.6.1 Kontrola zmian w systemie

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

6.6.2 Kontrola zarządzania bezpieczeństwem

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

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

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

6.6.3 Kontrola cyklu życia zabezpieczeń

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

6.7 Zabezpieczenia sieci komputerowej

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

Nadzór nad bezpieczeństwem sieci komputerowych EuroCert sprawują specjaliści EuroCert.

6.8 Znakowanie czasem

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

7 Profil certyfikatów i list CRL

Profile certyfikatów i list CRL wydawanych zgodnie z Polityką certyfikacji są zgodne z zaleceniami odpowiednio normy ITU-T X.509 v3 oraz ITU-T X.509 v2 a także profilami zawartymi w: ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Parts 1,2,5.

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

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

7.1 Profil 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. 9.

Tab. 9. Profil podstawowych pól certyfikatu

Nazwa pola	Opis		Wartość
Version	certyfikat zgodny z wersją 3 standardu X.509.		V3
SerialNumber	Jednoznaczny w ramach urzędu certyfikacji EuroCert numer certyfikatu.		Jednoznaczny numer seryjny certyfikatu nadany przez EuroCert.
SignatureAlgorithm	identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji pieczęci elektronicznej przez urząd certyfikacji na certyfikacie		SHA1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) lub SHA512WithRSAEncryption (OID: 1.2.840.113549.1.1.13) lub ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Issuer (nazwa wyróżniająca (DN) wystawcy certyfikatu)	Profil nr 1	Common Name	CN = Centrum Kwalifikowane EuroCert
		Organization	O = EuroCert Sp. z o.o.
		Country	C = PL
		Organization identifier	2.5.4.97 = VATPL-9512352379

	Profil nr 2	CN	Centrum Kwalifikowane EuroCert	
		O	EuroCert Sp. z o.o.	
		C	PL	
		SerialNumber	Nr wpisu: 14	
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 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1,2,5.		Identyfikator DN Subskrybenta (patrz § 3.1).	
SubjectPublicKeyInfo	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 5280 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (tzn. o identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego). Wartość klucza publicznego podmiotu wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz;		Public Key Algorithm (algorytm klucza publicznego):	sha1WithRSAEncryption lub SHA512WithRSAEncryption lub ecdsa-with-SHA512
			RSA Public Key (długość klucza)	min. 2048 bit lub ECC 384 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. 10.

Tabela 10. Rozszerzenia certyfikatu

Nazwa rozszerzenia	Krytyczne ?	Opis	Wartość
AuthorityKeyIdentifier	NIE	identyfikator klucza publicznego wystawcy służącego do weryfikacji wydanego certyfikatu	160 bitowy skrót SHA-1/ 512 bitowy skrót SHA-512 z wartości klucza publicznego certyfikatu wystawcy.
SubjectKeyIdentifier	NIE	Identyfikator certyfikatu zawierający skrót klucza publicznego zawartego w certyfikacie	160 bitowy skrót SHA-1/ 512 bitowy skrót SHA-512 z wartości klucza publicznego certyfikatu wystawcy.
KeyUsage	TAK	określa zakres wykorzystania klucza publicznego	nonRepudiation (klucz do realizacji niezaprzeczalności)

		subskrybenta. W przypadku certyfikatów kwalifikowanych ograniczone do niezaprzeczalności.	
CertificatePolicies	NIE	wskazanie na politykę certyfikacji, zgodnie z którą wystawiony jest certyfikat	Identyfikator polityki certyfikacji: 1.2.616.1.113791.1.2.1 lub 1.2.616.1.113791.1.2.2 lub 1.2.616.1.113791.1.2.3
CRLDistributionPoints	NIE	punkt dystrybucji listy CRL (określa adres URL, pod którymi jest publikowana aktualna lista CRL)	http://crl.eurocert.pl/qca03.crl lub http://crl.eurocert.pl/qca02.crl lub http://crl.eurocert.pl/qca04.crl
Authority Info Access	NIE	Dostęp do informacji o urzędzie	http://crl.eurocert.pl/OCSP/
BasicConstraints	TAK	umożliwia sprawdzenie czy podmiot certyfikatu jest użytkownikiem końcowym, czy też podmiotem wydającym certyfikaty	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak
qcCompliance	NIE	Deklaracja wystawcy certyfikatu	Oświadczenie, że certyfikat jest kwalifikowanym certyfikatem w rozumieniu eIDAS; OID: {itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) 1 1}
qcSSCD	NIE	Deklaracja wystawcy certyfikatu	wskazanie, że klucz prywatny jest przechowywany w kwalifikowanym urządzeniu do składania podpisów; OID: {0.4.0.1862.1.4}
qcPDS	NIE	Informacje o usługach EuroCert	Adres URL do dokumentu opisującego podstawowe warunki świadczenia usług zaufania w zakresie wydawania certyfikatów (PDS – PKI Disclosure Statements); OID: {0.4.0.1862.1.5}

7.1.3 Identyfikatory algorytmu

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

- Sha-1WithRSAEncryption: { iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 },
- SHA512WithRSAEncryption (OID: 1.2.840.113549.1.1.13),
- ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4).

7.1.4 Formy nazw

Certyfikaty zawierają wskazanie podmiotu wydawcy certyfikatu (pole issuer) oraz podmiotu certyfikatu (pole subject) sporządzone zgodnie z tab. 9 w § 7.1 oraz z tab. 6 w § 3.1.2.

7.1.5 Ograniczenia nakładane na nazwy

Certyfikaty zawierają wskazanie podmiotu wydawcy certyfikatu oraz podmiotu certyfikatu sporządzone zgodnie z odpowiednio w § 3.1.2 oraz 7.1.4.

7.1.6 Identyfikatory polityk certyfikacji

Patrz § 1.3.1 (tabela 3).

7.1.7 Zastosowanie rozszerzeń niedopuszczalnych w polityce certyfikacji

EuroCert nie przewiduje umieszczania w certyfikatach innych rozszerzeń niż wskazane w § 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 11.

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

Atrybut	Wartość
version	V2
SignatureAlgorithm identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji pieczęci elektronicznej przez urząd certyfikacji na liście CRL)	SHA1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) lub SHA512WithRSAEncryption (OID: 1.2.840.113549.1.1.13) lub ecdsa-with-SHA512 (OID: 1.2.840.10045.4.3.4)
Issuer Identyfikator wystawcy listy CRL, zgodny z identyfikatorem określonym w profilu certyfikatu	Patrz tabela 9 (Issuer)
thisUpdate	data i godzina wydania listy
nextUpdate	data i godzina następnego wydania listy (thisUpdate + nie więcej niż 24 godziny)
SignatureValue	Pieczęć elektroniczna wystawcy listy CRL
revokedCertificates (lista odwołanych certyfikatów) userCertificate revocationDate reasonCode	 numer seryjny unieważnionego certyfikatu data i godzina unieważnienia certyfikatu przyczyna umieszczenia certyfikatu na liście CRL: a) unspecified – nieokreślona, b) keyCompromise – kompromitacja klucza, c) cACompromise - kompromitacja klucza CA, d) affiliationChanged – zmiana danych Subskrybenta, e) superseded – zastąpienie (wymiana) klucza, f) cessationOfOperation – zaprzestanie używania certyfikatu do celu, w jakim został wydany, g) certificateHold – certyfikat został zawieszony.

7.2.1 Wersja listy CRL

Format listy CRL jest zgodny z wersją nr 3 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. 11), zawierające kod przyczyny unieważnienia certyfikatu.

7.3 Profil OCSP

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

8 Audyt zgodności i inne oceny

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

8.1 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 § e) Rozporządzenia eIDAS.

8.2 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.

8.3 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.

8.4 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.

8.5 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 § 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).

8.6 Informowanie o wynikach audytu

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

9 Inne postanowienia (biznesowe, prawne itp.)

9.1 Opłaty

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

9.1.1 Opłaty za wydanie certyfikatu i jego odnowienie

EuroCert pobiera opłaty za wydanie certyfikatu i jego odnowienie.

9.1.2 Opłaty za dostęp do certyfikatów

Eurocert nie pobiera opłat za dostęp do certyfikatów.

9.1.3 Opłaty za unieważnienie lub informacje o statusie certyfikatu

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

9.1.4 Inne opłaty

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

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

9.1.5 Zwrot opłat

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

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 w złotych 250 000 Euro, ale nie więcej niż 1 000 000 Euro w odniesieniu do wszystkich takich zdarzeń.

9.2.2 Inne aktywa

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

9.2.3 Rozszerzony zakres gwarancji

Kodeks 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

Niniejszy Kodeks postępowania certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

9.3.2 Informację nie będące informacjami poufnymi

Niniejszy Kodeks postępowania certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

9.3.3 Ochrona informacji poufnych

Niniejszy Kodeks Postępowania Certyfikacyjnego 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 poufne wszystkie informacje związane ze świadczeniem usług zaufania poza następującymi informacjami:

a) Polityka certyfikacji oraz 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 niebędącymi informacjami poufnymi 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 § 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

Niniejszy Kodeks postępowania certyfikacyjnego 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 przypadku utraty przez subskrybenta prawa do posługiwania się daną nazwą lub innym oznaczeniem zamieszczonym w certyfikacie, jest on zobowiązany do zgłoszenia tego faktu celem unieważnienia certyfikatu z powodu nieaktualności danych zawartych w certyfikacie.

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

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

9.6 Oświadczenia i gwarancje

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 i Polityce certyfikacji, procedurach wewnętrznych oraz w obowiązujących przepisach prawa i zasadach współżycia społecznego ze szczególnym uwzględnieniem dochowania należytej staranności,
b) wydawania koniecznych tokenów zgłoszenia certyfikacyjnego, upoważniających do skorzystania z określonej usługi EuroCert,
c) przesyłania do EuroCert potwierdzonych danych subskrybentów,
d) podporządkowania się w całości zaleceniom EuroCert,
e) ochrony kluczy prywatnych operatorów punktu rejestracji,
f) nie używania kluczy prywatnych operatorów do innych celów niż tych, które określono w niniejszej Polityce Certyfikacji,
g) poddawania się planowym audytom przeprowadzonym lub zleconym przez EuroCert.

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

9.6.3 Zobowiązania i gwarancje subskrybenta

Patrz: § 4.5.1.

9.6.4 Zobowiązania i gwarancje strony ufającej

Patrz: § 4.5.2.

9.6.5 Zobowiązania i gwarancje innych podmiotów

Niniejszy Kodeks postępowania certyfikacyjnego 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 § 4.5.1 oraz 4.5.2.

W szczególnych przypadkach EuroCert nie odpowiada również szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków, jeśli niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności.

9.8 Ograniczenia odpowiedzialności

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

9.9 Przenoszenie roszczeń odszkodowawczych

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

9.10 Przepisy przejściowe i okres obowiązywania polityki certyfikacji

9.10.1 Okres obowiązywania

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

9.10.2 Wygaśnięcie ważności

Kolejna opublikowana wersja Kodeksu wskazuje datę jej obowiązywania, która jest jednocześnie datą zakończenia obowiązywania obecnego Kodeksu. Tym samym poprzedni Kodeks traci status – aktualny.

9.10.3 Skutki wygaśnięcia ważności dokumentu

Subskrybenci przestrzegają tylko aktualnego Kodeksu.

9.11 Określanie trybu i adresów doręczania pism

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

9.12 Wprowadzanie zmian w dokumencie

9.12.1 Procedura wprowadzania zmian

Patrz: § 1.5.4.

9.12.2 Sposób powiadamiania o zmianach

Nie dotyczy.

9.12.3 Okoliczności wymagające zmiany identyfikatora OID

Zmiana identyfikatora (OID) Kodeksu 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 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 Kodeksie postępowania certyfikacyjnego, Polityce Certyfikacji, oraz obowiązujących przepisach prawa. W celu interpretacji terminów zawartych w Kodeksie 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 Kodeksu postępowania certyfikacyjnego.

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 Kodeksu pierwszeństwo stosowania ma Umowa przed Kodeksem.

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 Kodeksu.

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.

Historia dokumentu

Wersja	Data zatwierdzenia	Opis zmian
1.0	14.06.2017	utworzenie dokumentu
2.0	15.11.2017	Uwzględnienie w profilu certyfikatu kluczy RSA (3072 bit) oraz ECDSA. Drobne poprawki redakcyjne.