

Regulamin usług zaufania EuroCert

Wersja 2

Zatwierdził
Prezes Zarządu /-/
Łukasz Konikiewicz

Data zatwierdzenia 24.02.2021

1	PRZEDMIOT REGULACJI	3
2	ODBIORCY DOKUMENTU.....	4
3	REGULACJE I DOKUMENTY POWIĄZANE	5
3.1	REGULACJE ZEWNĘTRZNE.....	5
3.2	REGULACJE WEWNĘTRZNE.....	5
4	SŁOWNIK POJĘĆ, SKRÓTÓW I SKRÓTOWCÓW	5
5	DANE TELEADRESOWE	6
6	WARUNKI ZAWARCIA I ROZWIĄZANIA UMOWY	7
7	ZAKRES I OGRANICZENIA KORZYSTANIA Z USŁUG	7
8	REJESTRACJA SUBSKRYBENTA.....	8
9	OKRES PRZECHOWYWANIA DANYCH	9
10	OBOWIAZKI SUBSKRYBENTÓW.....	10
11	OBOWIAZKI STRON UFAJĄCYCH	11
12	UNIEWAŻNIENIE	11
13	ZAWIESZENIE CERTYFIKATU	12
14	OGRANICZENIE ODPOWIEDZIALNOŚCI EUROCERT	13
15	POLITYKA PRYWATNOŚCI.....	13
16	WARUNKI ROZSTRZYGANIA SPORÓW, REKLAMACJE.....	13
17	AUDYTY.....	14
18	OKRES OBOWIĄZYWANIA.....	14
19	METRYCZKA DOKUMENTU	15

1 Przedmiot regulacji

Niniejszy dokument, zwany dalej „Regulaminem” został opracowany w celu wspieranie zastosowania dokumentu: „Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert”, zwanego dalej Polityką Certyfikacji.

W ramach Polityki Certyfikacji, EuroCert świadczy kwalifikowane usługi zaufania w rozumieniu rozporządzenia eIDAS. Informacje na temat zakresu usług znajdują się na stronach internetowych podanych w rozdziale 5 oraz na stronie organu nadzoru (<https://www.nccert.pl/>) lub liście TSL (<https://webgate.ec.europa.eu/tl-browser/#/>).

Usługi zaufania są świadczone wyłącznie po akceptacji niniejszego Regulaminu i Polityki Certyfikacji.

2 Odbiorcy dokumentu

Niniejszy Regulamin stanowi dodatkowy dokument w stosunku do Polityki Certyfikacji, służący do informowania o warunkach korzystania z usług zaufania Subskrybentów przed wydaniem Certyfikatu lub Znacznika Czasu, natomiast Stron Ufających przed użyciem Certyfikatu lub Znacznika Czasu wydanych przez EuroCert.

Stanowi on odpowiedź na potrzeby tych Subskrybentów i Stron Ufających, którzy uznają Politykę Certyfikacji za zbyt trudną do zrozumienia i pomaga im podjąć świadomą decyzję.

Stanowi również kompromis w sprawie tych elementów Polityki Certyfikacji, które wymagają podkreślenia i szczególnej uwagi.

Regulamin nie zastępuje Polityki Certyfikacji.

Subskrybent ma obowiązek zapoznania się z niniejszym dokumentem i zaakceptowania jego postanowień przed złożeniem Wniosku o Certyfikat lub uzyskaniem dostępu do usługi znacznika czasu, natomiast Strona Ufająca przed użyciem Certyfikatu lub Znacznika Czasu wystawionych przez EuroCert.

Akceptacja postanowień niniejszego Regulaminu oznacza, że Subskrybent:

- 1) zapoznał się z treścią niniejszego Regulaminu i Polityki Certyfikacji, opublikowanych na stronie <https://eurocert.pl/repozytorium>;
- 2) oświadcza, że informacje podane przez niego we Wniosku o Certyfikat i podczas weryfikacji tożsamości są zgodne z prawdą i zostały podane dobrowolnie;
- 3) wyraża zgodę na obowiązki, wymienione w rozdziale 10 Regulaminu;
- 4) jest świadomy, że w przypadku podpisu zdalnego w usłudze ECSigner, środowisko, w ramach którego odbywają się operacje kryptograficzne z wykorzystaniem jego klucza prywatnego, zarządzane jest przez kwalifikowanego dostawcę usług zaufania, jakim jest EuroCert;
- 5) wyraża zgodę na przetwarzanie przez EuroCert jego danych osobowych wyłącznie w celu wydania Certyfikatu (patrz rozdział 15), oraz przyjmuje do wiadomości, iż ma prawo dostępu do treści danych osobowych, o których mowa wyżej oraz ich zmiany;
- 6) wyraża zgodę na umieszczenie przez EuroCert w Certyfikacie jego danych osobowych zgodnie z Wnioskiem o Certyfikat oraz na stosowanie tych danych do weryfikacji jego podpisu elektronicznego lub pieczęci elektronicznej;
- 7) jest świadomy, że Certyfikat, a tym samym zawarte w nim dane identyfikujące Subskrybenta, co do zasady, są dostępne publicznie;
- 8) wyraża zgodę na przechowywanie przez EuroCert informacji związanych z wydanymi Certyfikatami przez wymagany prawem okres 20 lat (patrz rozdział 9);
- 9) wyraża zgodę na przekazanie swoich danych osobowych do innego kwalifikowanego dostawcy usług zaufania w przypadku zakończenia działalności przez EuroCert, w celu zachowania ciągłości świadczenia usług;
- 10) zapoznał się z klauzulą informacyjną o ochronie danych osobowych, zgodnie z RODO, umieszczoną na stronie <https://eurocert.pl/repozytorium>;
- 11) wyraża zgodę na rejestrację wideokonferencji z operatorem weryfikującym jego tożsamość oraz wykonanie przez tego operatora zdjęć Subskrybentowi a także zdjęć jego dokumentu tożsamości;
- 12) jest świadomy, iż w celu przeprowadzenia wideo weryfikacji wymagane jest posiadanie urządzenia z dostępem do Internetu i kamerą; Subskrybent jest odpowiedzialny za zapewnienie tego, że jego urządzenie spełnia wymogi w zakresie niezbędnym do przeprowadzenia wideo weryfikacji;
- 13) zgadza się na używanie kwalifikowanego urządzenia do składania podpisu elektronicznego lub pieczęci elektronicznej;
- 14) wyraża zgodę na otrzymywanie informacji o zbliżającym się terminie wygaśnięcia certyfikatu, informacji o zmianach Polityki Certyfikacji, Regulaminu na swój adres e-mail i numer telefonu.

3 Regulacje i dokumenty powiązane

3.1 Regulacje zewnętrzne

EuroCert świadczy Usługi Zaufania zgodnie z następującymi przepisami prawnymi:

- 1) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, zwanym dalej „rozporządzeniem eIDAS”;
- 2) Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. poz. 1579), zwaną dalej „Ustawą o usługach zaufania”;
- 3) Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwanym dalej „RODO”;
- 4) Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z dn. 24 maja 2018 r., poz. 1000), zwaną dalej „Ustawą o ochronie danych osobowych”.

3.2 Regulacje wewnętrzne

EuroCert świadczy Usługi Zaufania zgodnie z zasadami przedstawionymi w dokumencie „Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert”. Dokument dostępny jest na stronie internetowej pod adresem: <https://eurocert.pl/repozytorium>.

Certyfikaty wydawane zgodnie z ww. dokumentem są kwalifikowanymi certyfikatami w rozumieniu rozporządzenia eIDAS.

4 Słownik pojęć, skrótów i skrótowców

- 1) EuroCert – kwalifikowany dostawca usług zaufania EuroCert sp. z o.o., świadczący kwalifikowane usługi zaufania, w rozumieniu rozporządzenia eIDAS.
- 2) Urząd Certyfikacji – komponent techniczny EuroCert odpowiedzialny za generowanie Certyfikatów, zidentyfikowany w każdym Certyfikacie jako wystawca Certyfikatu i który podpisuje Certyfikaty przy użyciu swojego klucza prywatnego.
- 3) Punkt Rejestracji – podmiot podległy EuroCert wykonujący czynności w zakresie rejestracji Subskrybentów oraz potwierdzania ich tożsamości.
- 4) Polityka Certyfikacji – polityka świadczenia usług zaufania przez EuroCert pod nazwą „Polityka Certyfikacji i Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Zaufania EuroCert”, opublikowana na stronie internetowej <https://eurocert.pl/repozytorium>, pełniąca również rolę kodeksu postępowania certyfikacyjnego.
- 5) Usługa ESigner – usługa podpisu lub pieczęci elektronicznej, w przypadku których klucz prywatny Subskrybenta jest przechowywany przez EuroCert.
- 6) Certyfikat – poświadczenie elektroniczne, za pomocą którego dane służące do weryfikacji podpisu elektronicznego lub pieczęci elektronicznej są przyporządkowane do podmiotu składającego podpis elektroniczny lub pieczęć elektroniczną i które umożliwiają identyfikację tego podmiotu; ilekroć w niniejszym Regulaminie mowa o certyfikacie, należy przez to rozumieć kwalifikowany certyfikat podpisu elektronicznego, kwalifikowany certyfikat pieczęci elektronicznej i kwalifikowany certyfikat uwierzytelniania witryn internetowych, w rozumieniu rozporządzenia eIDAS.
- 7) Znacznik czasu – dane w postaci elektronicznej, które wiążą inne dane w postaci elektronicznej z określonym czasem, stanowiąc dowód na to, że te inne dane istniały w danym czasie. ilekroć w niniejszym Regulaminie mowa o Znaczniku Czasu, należy przez to rozumieć kwalifikowany Znacznik Czasu.

- 8) Żądanie Certyfikacji – żądanie wydania Certyfikatu w formacie akceptowanym przez system informatyczny odpowiedzialny za generowanie Certyfikatów w EuroCert, wystosowane przez Punkt Rejestracji w imieniu Subskrybenta.
- 9) Lista TSL (Trust Service Status List) – listy wydawane przez Komisję Europejską oraz kraje członkowskie UE, zawierające informacje o podmiotach świadczących usługi zaufania, ich statusie (czy kwalifikowany?) oraz dane umożliwiające weryfikację tokenów wystawianych przez podmioty świadczące usługi zaufania (czyli weryfikację kwalifikowanych certyfikatów, znaczników czasu itd.).
- 10) Subskrybent – podmiot wnioskujący o Certyfikat lub Znacznik Czasu lub dla którego Certyfikat lub Znacznik Czasu został wydany.
- 11) Wniosek o certyfikat – zestaw danych niezbędnych do wydania Certyfikatu.
- 12) Strona ufająca – dowolny podmiot, który podejmuje decyzję o akceptacji Certyfikatu lub Znacznika Czasu wydanych przez EuroCert.
- 13) Usługi Zaufania – kwalifikowane usługi zaufania w rozumieniu rozporządzenia eIDAS świadczone przez EuroCert w ramach Polityki Certyfikacji.
- 14) CRL – listy zawieszonych i unieważnionych Certyfikatów.
- 15) Usługa OCSP – usługa weryfikacji statusu certyfikatów w trybie on-line (ang. On-line Certificate Status Protocol).

5 Dane teleadresowe

Adres korespondencyjny:

EuroCert Sp. z o.o.
ul. Puławska 472
02-884 Warszawa
<https://eurocert.pl>
tel. +48 22 390 59 95
e-mail: biuro@eurocert.pl

Dział Handlowy:

tel. +48 22 490 36 45
WWW: <https://sklep.eurocert.pl>
<http://eurocert.pl/PunktyPartnerskie>

Unieważnienie Certyfikatu:

uniewaznienia@eurocert.pl
+48 22 490 49 86 wewnętrzny 201
WWW: [link](#)

Wsparcie techniczne:

wsparcie@eurocert.pl
+48 22 490 49 86

Reklamacje:

biuro@eurocert.pl
+48 22 390 59 95

Inspektor ochrony danych:

iod@eurocert.pl

6 Warunki zawarcia i rozwiązania umowy

Umowa o świadczenie kwalifikowanych usług zaufania zawarta zostaje poprzez złożenie Wniosku o Certyfikat oraz akceptację Regulaminu oraz Polityki Certyfikacji przez Subskrybenta i potwierdzenie jego tożsamości.

Rezygnacja z Usług Zaufania możliwa jest tylko w przypadku unieważnienia Certyfikatu, dokonana na warunkach określonych w rozdziale 12 Regulaminu oraz w Polityce Certyfikacji (rozdziały 3.4 i 4.9).

7 Zakres i ograniczenia korzystania z usług

Klucz prywatny do składania podpisu elektronicznego lub pieczęci elektronicznej komplementarny do Certyfikatu służącego do weryfikacji tego podpisu lub pieczęci, generowany przez EuroCert, może znajdować się:

- 1) na karcie kryptograficznej, której Subskrybent jest jedynym użytkownikiem i wyłącznie on zna kod PIN i PUK umożliwiające jej użycie w celu złożenia podpisu elektronicznego (pieczęci elektronicznej),
- 2) w zdalnym komponencie usługi ECSigner, nad którym jedynie Subskrybent ma kontrolę poprzez dysponowanie unikatowym środkiem identyfikacji, za którego pomocą Subskrybent będzie identyfikowany i logowany w usłudze ECSigner oraz jednorazowym hasłem, który bezpośrednio pozwala na użycie klucza prywatnego znajdujących się w komponencie ECSigner do składania podpisu lub pieczęci.

W przypadku usługi ECSigner EuroCert zarządza kluczem prywatnym w imieniu Subskrybenta i zapewnia, że Subskrybent ma nad nim wyłączną kontrolę.

Certyfikat zawiera datę ważności zgodnie ze złożonym wnioskiem, przy czym okres ważności nie może być dłuższy niż 3 lata w przypadku Certyfikatów do podpisu lub pieczęci oraz 825 dni w przypadku Certyfikatów uwierzytelniania witryn internetowych.

Certyfikat do podpisu elektronicznego służy tylko do weryfikacji kwalifikowanego podpisu elektronicznego, który wywołuje skutek prawny równoważny podpisowi własnoręcznemu Subskrybenta i jako taki uznawany jest na terenie wszystkich państw członkowskich Unii Europejskiej.

Certyfikat do pieczęci elektronicznej służy tylko do weryfikowania kwalifikowanej pieczęci elektronicznej, która zapewnia autentyczność pochodzenia oraz integralność powiązanych z nią danych (np. dokumentu elektronicznego).

Kwalifikowana pieczęć elektroniczna nie służy do wyrażania woli podmiotu, który się nią posługuje.

Znacznik Czasu służy do poświadczania daty i czasu oraz integralności danych, z którymi data i czas są powiązane. Znacznik Czasu wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego (art. 81 §2 pkt 3).

Zabrania się używania kluczy prywatnych związanych z Certyfikatami do podpisu lub pieczęci w urządzeniach, które nie spełniają wymagań dla kwalifikowanych urządzeń do składania podpisu elektronicznego lub pieczęci elektronicznej.

Kwalifikowane Certyfikaty uwierzytelniania witryn internetowych służą do potwierdzania wiarygodności serwerów i potwierdzania ich autentyczności. Pozwalają zestawiać szyfrowane połączenie TLS pomiędzy serwerami posiadającymi takie Certyfikaty, a także udostępniać bezpieczne logowanie klientom. Certyfikaty tego typu mogą być wydawane wyłącznie dla serwerów działających w sieciach publicznych i posiadać pełną, jednoznaczną nazwę domenową (ang. Fully Qualified Domain Name), określającą położenie danego węzła w systemie DNS.

Zakazane jest używanie Certyfikatów i kluczy prywatnych przez osoby do tego nieupoważnione. Klucze prywatne związane z Certyfikatami powinny pozostawać w wyłącznej dyspozycji osoby/podmiotu, której dane są umieszczone w Certyfikacie. Nie jest dopuszczalne, aby kluczem tym posługiwała się inna osoba/podmiot.

Kto składa kwalifikowany podpis elektroniczny lub zaawansowany podpis elektroniczny z wykorzystaniem danych do składania podpisu elektronicznego przyporządkowanych do innej osoby, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3. Tej samej karze podlega, kto składa kwalifikowaną pieczęć elektroniczną lub zaawansowaną pieczęć elektroniczną, nie będąc do tego uprawnionym (art. 40 Ustawy o usługach zaufania).

8 Rejestracja Subskrybenta

Rejestracja, czyli proces przyjęcia i weryfikacji Wniosku o Certyfikat jest przeprowadzana przez EuroCert albo bezpośrednio albo przez podległy Punkt Rejestracji, prowadzony na podstawie odpowiedniej umowy.

EuroCert potwierdza tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych we Wniosku o Certyfikat.

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

- a) przez fizyczną obecność osoby fizycznej lub upoważnionego przedstawiciela osoby prawnej; lub
- b) zdalnie, przy użyciu wideo weryfikacji; lub
- c) za pomocą Certyfikatu kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej wydanych zgodnie z lit. a) powyżej.

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

EuroCert informuje Subskrybentów o dostępnych metodach weryfikacji tożsamości.

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

W przypadku użycia systemu wideo weryfikacji (lit. b) powyżej), Subskrybent składa Wniosek o Certyfikat wyłącznie poprzez elektroniczny formularz. Przed inicjacją sesji wideo z operatorem weryfikującym tożsamość Subskrybent jest zobowiązany zapoznać się z postanowieniami niniejszego Regulaminu i zaakceptować je.

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

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

Operator przeprowadza wideo weryfikację na podstawie okazanego elektronicznie dokumentu tożsamości.

Operator weryfikuje ważność i autentyczność dokumentu tożsamości Subskrybenta oraz sprawdza czy dane na dokumencie odpowiadają tym wprowadzonym w elektronicznym Wniosku o Certyfikat.

Powyższy proces weryfikacji przeprowadzany jest ponownie przez drugiego operatora.

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

Podwójna kontrola zapewnia, że Żądanie Certyfikacyjne może być przesłane do EuroCert, tylko wówczas, gdy weryfikacja tożsamości i rejestracja zakończy się powodzeniem.

Żądania Certyfikacyjne przekazywane są do EuroCert w postaci elektronicznej. Poufność transmisji Żądań Certyfikacyjnych jest zapewniona poprzez zestawienie szyfrowanego kanału w protokole TLS.

EuroCert weryfikuje, czy Żądanie Certyfikacyjne pochodzi z zaufanego Punktu Rejestracji.

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

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

EuroCert generuje klucze Subskrybenta i Certyfikat w komponencie ECSigner.

Po pozytywnym zakończeniu weryfikacji tożsamości, Punkt Rejestracji przekazuje wszystkie dane, zawierające potwierdzenie tożsamości Subskrybenta do EuroCert w ciągu 7 dni.

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

9 Okres przechowywania danych

EuroCert archiwizuje poniższe dokumenty i dane związane ze świadczeniem kwalifikowanych Usług Zaufania:

- 1) Dane Subskrybenta, w tym dane dokumentu tożsamości (rodzaj, numery, data ważności, organ wydający) oraz wszelkie inne dokumenty lub dane potwierdzające tożsamość Subskrybenta;
- 2) Wnioski o wydanie, odnowienie Certyfikatu;
- 3) Żądania unieważnienia, zawieszenia, uchylecia zawieszenia Certyfikatu;
- 4) Zaakceptowane przez Subskrybentów warunki korzystania z Usług Zaufania, zawarte w niniejszym Regulaminie oraz Polityce Certyfikacji, w tym zgoda na przetwarzanie danych osobowych;
- 5) Pisemne oraz elektroniczne oświadczenia o potwierdzeniu tożsamości od Punktów Rejestracji i notariuszy;
- 6) nagrania obrazu i dźwięku z wideo weryfikacji, zdjęcia dokumentu tożsamości;
- 7) Wszystkie wydane Certyfikaty;
- 8) Listy CRL;
- 9) certyfikaty dostawcy usług zaufania dla Urzędów Certyfikacji;
- 10) Politykę certyfikacji;
- 11) Kodeks postępowania certyfikacyjnego;
- 12) Regulamin usług zaufania;
- 13) Regulacje wewnętrzne;
- 14) Rejestry zdarzeń, logi systemowe, zdarzenia związane z bezpieczeństwem m.in. zmiany dotyczące polityki bezpieczeństwa, włączenie i wyłączenie systemu, awarie systemu i uszkodzenia sprzętu, aktywność firewall i router, próby uzyskania dostępu do systemu;
- 15) Zdarzenia związane z cyklem życia kluczy Urzędów Certyfikacji;
- 16) Zdarzenia związane z cyklem Certyfikatów Subskrybentów;
- 17) Zdarzenia związane z cyklem życia kluczy zarządzanych przez EuroCert, w tym wszystkich kluczy Subskrybentów wygenerowanych przez EuroCert;

- 18) Inne dokumenty lub dane, o ile Polityka Certyfikacji wymagała ich utworzenia i przechowywania,
- w sposób umożliwiający odczytanie oraz zapewniający bezpieczeństwo przechowywania dokumentów i danych,
 - przez okres 20 lat od dnia ich wytworzenia zgodnie z Ustawą o usługach zaufania (art. 17),
 - zgodnie z Polityką sporządzania kopii zapasowych i archiwizacji, zarządzania dziennikami zdarzeń systemów i dokumentacją usług zaufania EuroCert,
 - w szczególności do celów przedstawienia dowodów w postępowaniach sądowych i do celów zapewnienia ciągłości usług.

10 Obowiązki subskrybentów

Subskrybent jest zobowiązany do:

- 1) zapoznania się z niniejszym Regulaminem i zaakceptowania jego postanowień przed złożeniem Wniosku o Certyfikat;
- 2) bezpiecznego przechowywania klucza prywatnego oraz kodów dostępu do tego klucza (np. PIN, PUK);
- 3) przekazywania do EuroCert wyłącznie prawdziwych i kompletnych danych;
- 4) dostarczenia dokumentów potwierdzających prawdziwość dostarczonych danych;
- 5) używania kluczy prywatnych i Certyfikatów tylko w okresie ich ważności oraz zgodnie z ich przeznaczeniem określonym w rozdziale 7 Regulaminu, rozdziale 1.4 Polityki Certyfikacji oraz wskazanym w Certyfikacie (użycie klucza, rozszerzone użycie klucza, zasady certyfikatu);
- 6) sprawdzenia poprawności danych zawartych w Certyfikacie niezwłocznie po jego otrzymaniu, nie później niż przed jego pierwszym użyciem; w przypadku stwierdzenia nieprawidłowości danych tożsamości jest on zobowiązany do niezwłocznego zgłoszenia tego faktu EuroCert w celu unieważnienia Certyfikatu i wygenerowania nowego;
- 7) nieprzekazywania swojego klucza prywatnego osobom nieupoważnionym, nieujawnianie kodów PIN i PUK, sprawowania wyłącznej kontroli na kluczem prywatnym (lub kontroli w przypadku osób prawnych);
- 8) generowania kluczy przy użyciu algorytmów i długości klucza określonych w rozdziale 6.1.5 Polityki Certyfikacji;
- 9) zachowania klucza prywatnego pod swoją wyłączną kontrolą (lub kontrolą w przypadku osób prawnych) przy generowaniu kluczy;
- 10) użycia do generowania kluczy wyłącznie kwalifikowanego urządzenia do składania podpisu lub pieczęci elektronicznej;
- 11) wykonywanie operacji związanych z wykorzystaniem klucza prywatnego wyłącznie przy użyciu kwalifikowanego urządzenia do składania podpisu lub pieczęci elektronicznej;
- 12) niezwłocznego poinformowania EuroCert o wystąpieniu następujących okoliczności w trakcie ważności certyfikatu:
 - a) klucz prywatny został zgubiony, skradziony,
 - b) klucz prywatny został skompromitowany,
 - c) utrata kontroli nad kluczem prywatnym, z powodu ujawnienia danych aktywujących (np. PIN) innej osobie lub innych powodów,
 - d) nieprawidłowości lub zmiany danych zawartych w certyfikacie;
- 13) niezwłocznego i trwałego zaprzestania używania klucza prywatnego w przypadku ujawnienia klucza prywatnego;
- 14) zaprzestanie używania klucza prywatnego w przypadku unieważnienia, zawieszenia bądź wygaśnięcia Certyfikatu lub skompromitowania klucza Urzędu Certyfikacji (wystawcy);
- 15) nieujawniania żadnych danych otrzymanych od EuroCert lub Punktu Rejestracji, sprawowania wyłącznej kontroli nad tymi danymi oraz ochrony tych danych przed dostępem osób trzecich;

- 16) weryfikowania Znacznika Czasu przy pomocy pieczęci elektronicznej wystawcy tego znacznika i sprawdzenia ważności certyfikatu tego wystawcy przy użyciu listy TSL.

11 Obowiązki stron ufających

Strony ufające są zobowiązane do:

- 1) zapoznania się z niniejszym Regulaminem i zaakceptowania jego postanowień przed użyciem Certyfikatu lub Znacznika Czasu wystawionych przez EuroCert,
- 2) weryfikowania ważności Certyfikatu pod kątem ewentualnego, unieważnienia lub zawieszenia z wykorzystaniem listy CRL lub usługi OCSP, przed jego użyciem do zweryfikowania podpisu elektronicznego, pieczęci elektronicznej, witryny internetowej,
- 3) sprawdzenia czy Certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem (rodzaj certyfikatu, polityka certyfikacji, dozwolone użycie zapisane w Certyfikacie: keyUsage, extKeyUsage),
- 4) weryfikowania Znacznika Czasu przy pomocy pieczęci elektronicznej wystawcy tego znacznika i sprawdzenia ważności certyfikatu tego wystawcy przy użyciu listy TSL.

Informacja o statusie Certyfikatu dostępna jest publicznie. Weryfikacja statusu Certyfikatów wydawanych przez EuroCert odbywa się na podstawie publikowanych list CRL lub usługi OCSP. Adresy usług CRL i OCSP zawarte są w wydany Certyfikacie odpowiednio w polach: punkty dystrybucji listy CRL oraz dostęp do informacji o urzędzie. Listy CRL oraz certyfikaty dostawcy usług zaufania znajdują się na stronie <https://eurocert.pl/index.php/dokumenty/certyfikaty-i-listy-crl>. W celu zbadania statusu Certyfikatu należy:

- 1) pobrać token OCSP dla tego Certyfikatu i sprawdzić status Certyfikatu zapisany w tym tokenie, albo/i
- 2) pobrać listę CRL wydaną po momencie, na który badamy ważność Certyfikatu i sprawdzić status Certyfikatu na liście CRL.

Ważność pieczęci pod tokenem OCSP oraz listą CRL należy sprawdzać w oparciu o bieżącą listę TSL na stronie <https://webgate.ec.europa.eu/tl-browser/#/>.

Z faktu nieukazania się w określonym czasie nowej listy CRL nie można wnioskować o braku unieważnień Certyfikatów.

12 Unieważnienie

EuroCert unieważnia Certyfikat na podstawie:

- 1) żądania unieważnienia zgłoszonego przez Subskrybenta,
- 2) żądania uprawnionego podmiotu, którego dane zawarte są w Certyfikacie,
- 3) stwierdzenia zagrożenia interesu prawnego lub faktycznego Subskrybenta lub osób trzecich wynikającego z wykorzystywania Certyfikatu, o czym niezwłocznie informuje Subskrybenta, tzn. EuroCert unieważnia każdy niewygasły Certyfikat:
 - a) który nie spełnia już wymogów polityki certyfikacji według której został wystawiony,
 - b) w stosunku do którego EuroCert posiada informacji uzasadniającej unieważnienie Certyfikatu (np. dane w Certyfikacie są nieprawdziwe, nieprawidłowe lub nieaktualne),
 - c) dla którego użyte metody kryptograficzne nie zapewniają pewności ważności powiązania pomiędzy tożsamością Subskrybenta a należącym do niego kluczem publicznym, potwierdzonym Certyfikatem,
 - d) który uległ skompromitowaniu lub którego wystawca (Urząd Certyfikacji) uległ skompromitowaniu (tzn. ich klucze prywatne),
 - e) jeśli EuroCert zakończył działalność, łącznie z obsługą unieważnień i publikacją informacji o statusie Certyfikatu,

- f) w przypadku, gdy EuroCert lub podległy mu Punkt Rejestracji posiada informacje, że klucz prywatny Subskrybenta został przekazany do osoby nieupoważnionej lub organizacji z którą Subskrybent nie jest powiązany; EuroCert unieważnia w tym przypadku wszystkie Certyfikaty zawierające klucz publiczny odpowiadający niewłaściwie przekazanemu kluczowi prywatnemu.

Wniosek o unieważnienie lub zawieszenie Certyfikatu może być złożony w Punkcie Rejestracji pod adresem w rozdziale 5 (w godzinach pracy), przekazany drogą elektroniczną lub telefonicznie zgodnie z rozdziałem 5.

Prawidłowy wniosek o unieważnienie lub zawieszenie musi zawierać imię (imiona), nazwisko, numer telefonu, adres email, hasło do unieważnienia, powód, dane Subskrybenta zawarte w Certyfikacie.

Żądanie unieważnienia lub zawieszenia wymaga potwierdzenia przez Subskrybenta, jeżeli zostało zgłoszone przez osobę trzecią.

EuroCert unieważnia lub zawiesza Certyfikat i publikuje na liście CRL jego status odpowiednio jako „unieważniony” lub „zawieszony” w ciągu 24 godzin od skutecznego zgłoszenia żądania unieważnienia, jednak nie później niż 60 minut od potwierdzeniu żądania unieważnienia lub zawieszenia.

Jeśli żądanie unieważnienia lub zawieszenia nie może zostać potwierdzone w przeciągu 24 godzin, status Certyfikatu nie zostaje zmieniony.

Nie można przywrócić ważności unieważnionemu Certyfikatowi.

W przypadku unieważnienia, zawieszenia lub uchylecia zawieszenia Certyfikatu, Subskrybent lub inna upoważniona osoba otrzyma potwierdzenie na adres swojej poczty elektronicznej.

13 Zawieszenie certyfikatu

Certyfikat może być zawieszony jeśli istnieją przesłanki do unieważnienia Certyfikatu (rozdział 12), jednakże Inspektor ds. rejestracji EuroCert nie jest w stanie w ciągu 24 godzin od skutecznego złożenia żądania unieważnienia wyjaśnić wszystkich wątpliwości dotyczących unieważnienia.

Zawieszenie Certyfikatu jest czasowe, zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia. Certyfikat może zostać odwieszony w ciągu 7 dni od daty zawieszenia. W przeciwnym wypadku Certyfikat zostaje unieważniony.

Zawieszenie Certyfikatu może zostać uchylone w wyniku niepotwierdzenia się przesłanek uzasadniających zawieszenie Certyfikatu, w szczególności po potwierdzeniu tego faktu przez Subskrybenta. W przeciwnym wypadku Certyfikat zostaje unieważniony.

Weryfikacja wniosków o uchylenie zawieszenia odbywa się zgodnie z rozdziałem 8.

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. To oznacza, że podpis elektroniczny złożony w okresie zawieszenia nie wywołuje skutku prawnego.

Po uchyleniu zawieszenia Certyfikatu, skutek prawny podpisu elektronicznego weryfikowanego tym Certyfikatem, złożonego w trakcie zawieszenia, następuje z chwilą uchylenia tego zawieszenia.

14 Ograniczenie odpowiedzialności EuroCert

Zgodnie z art. 21 ustawy o usługach zaufania EuroCert nie odpowiada za szkody wynikające z nieprzestrzegania przez Subskrybenta zasad określonych w Polityce Certyfikacji.

Odpowiedzialność finansowa EuroCert za szkody wyrządzone odbiorcom usług zaufania w okresie świadczenia usług zaufania wynosi 250 000 euro (równowartość w złotych) w stosunku do jednego zdarzenia, ale nie więcej niż 1000 000 euro (równowartość w złotych) w stosunku do wszystkich zdarzeń.

Subskrybent jest zobowiązany do pisemnego poinformowania o wszelkich szkodach przewidzianych w niniejszym Regulaminie bez zbędnej zwłoki tak, aby można było ograniczyć szkody w najwyższym możliwym stopniu.

15 Polityka prywatności

Dane osobowe subskrybentów są gromadzone i przetwarzane w EuroCert wyłącznie w celu i zakresie koniecznym do świadczenia Usług Zaufania.

Informacje gromadzone podczas weryfikacji tożsamości Subskrybenta zawierają:

- 1) Pełną nazwę: imię (imiona) i nazwisko
- 2) Datę i miejsce urodzenia,
- 3) Dane dokumentu tożsamości: rodzaj, okres ważności, organ wydający, numer,
- 4) Adres,
- 5) Kraj,
- 6) Numer telefonu,
- 7) Adres e-mail,
- 8) zdjęcia dokumentu tożsamości,
- 9) Nagrania obrazu i dźwięku z wideo weryfikacji, zdjęcia.

EuroCert zbiera tylko te dane które są niezbędne do wydania danego typu Certyfikatu o określonym przeznaczeniu.

Więcej informacji znajduje się w klauzuli informacyjnej o ochronie danych osobowych (Klauzula informacyjna RODO) umieszczonej na stronie <https://eurocert.pl/repozytorium>.

Dane zawarte w Certyfikacie składają się z pełnej nazwy, tzn. imienia (imion) i nazwiska zgodnej z dokumentem tożsamości oraz poniższych informacji:

- 1) numer dokumentu tożsamości,
- 2) narodowość.

Administratorem danych osobowych Subskrybentów jest Eurocert Sp. z o. o., którego dane znajdują się w rozdziale 5.

Dane osobowe mogą być udostępniane innym podmiotom w zakresie niezbędnym do realizacji Umowy, w szczególności podmiotom pełniącym funkcje Punktów Rejestracji.

16 Warunki rozstrzygania sporów, reklamacje

Przedmiotem rozstrzygania sporów, w tym reklamacji, mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania Certyfikatu w oparciu o Regulamin i Politykę Certyfikacji.

Spory, reklamacje, skargi bądź zażalenia powstałe na tle użytkowania Certyfikatów, Znaczników Czasu wystawianych przez EuroCert, będą rozstrzygane w pierwszej kolejności na podstawie pisemnych informacji w drodze mediacji. Skargi i reklamacje należy kierować w formie pisemnej na adres podany w rozdziale 5.

Skargi podlegają pisemnemu rozpatrzeniu w terminie 21 dni roboczych od dnia ich doręczenia. W przypadku braku rozstrzygnięcia sporu w terminie 45 dni roboczych od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sędem właściwym do rozpoznania sprawy będzie Sąd Powszechny miejscowo właściwy dla pozwanego.

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

17 Audyty

Kwalifikowane Usługi Zaufania świadczone przez EuroCert podlegają corocznemu badaniu zgodności z rozporządzeniem eIDAS.

Podmiotem zewnętrznym oceniającym zgodność jest TAYLLORCOX PCEB.

Audyty wewnętrzne przeprowadzane są zgodnie z Polityką kontroli wewnętrznej i audytu, będącą własnością EuroCert. Audyt wewnętrzny jest prowadzony celem sprawdzenia zgodności rzeczywistych działań i czynności podejmowanych przez EuroCert z procedurami i procesami opisanymi w dokumentacji EuroCert.

Lista zawierająca informacje dotyczące kwalifikowanych dostawców usług zaufania, wraz z informacjami dotyczącymi świadczonych usług zaufania dostępna jest w serwisie internetowym Narodowego Centrum Certyfikacji pod adresem www.nccert.pl (Lista TSL).

18 Okres obowiązywania

Regulamin obowiązuje od dnia zatwierdzenia.

19 Metryczka dokumentu

Informacje ogólne		
Sygnatura		0-RG-028-02
Status		Zatwierdzona
Numer Inwentarzowy		
Poufność, Integralność, Dostępność, Archiwizacja (PIDA)		
Klasa Poufności		0 - Jawne
Klasa Integralności		1 - Zabezpieczona
Dostępność	Klasa Uprawnień Dostępu	1 - Powszechnie Dostępne Zarządzane
	Klasa Krytyczności Czasu Dostępu	2 - Istotna
Wymóg archiwizacji		B20 - dwudziestoletni okres archiwizacji
Historia zmian		
Data zatwierdzenia	Wersja	Dokonane zmiany
08.11.2018	1	Opracowanie dokumentu.
24.02.2021	2	Zmiana nazwy z Zasady i warunki świadczenia usług zaufania przez EuroCert na Regulamin usług zaufania EuroCert, rozszerzenie metod weryfikacji tożsamości o wideo weryfikację, dodanie informacji o podpisie zdalnym, zmiana terminów ważności certyfikatów.