Zasady i warunki świadczenia usług zaufania przez EuroCert

Wersja 1

Zatwierdził
Prezes Zarządu /-/
Łukasz Konikiewicz .....

Data zatwierdzenia 08.11.2018 r.

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

Spis treści

1 Przedmiot regulacji

Niniejszy dokument, zwany dalej „Zasadami" został opracowany zgodnie z wymaganiami załącznika A normy ETSI EN 319 411-1 w celu wspieranie zastosowania Polityki certyfikacji.

Postanowienia Zasad dotyczą świadczenia przez EuroCert kwalifikowanych usług zaufania w rozumieniu eIDAS oraz Ustawy o usługach zaufania.

Dokument ten określa w szczególności: zakres i ograniczenia stosowania certyfikatów, zasady weryfikacji tożsamości stosowane przy ich wydawaniu, zakres i ograniczenia świadczenia usługi kwalifikowanego znacznika czasu, obowiązki Subskrybentów i Stron ufających, ograniczenia odpowiedzialności EuroCert, sposoby rozstrzygania skarg i sporów, zasady unieważniania certyfikatów.

2 Odbiorcy dokumentu

Postanowienia niniejszego dokumentu są wiążące dla EuroCert, Subskrybentów, Stron ufających oraz innych podmiotów (w tym dostawców usług), którzy korzystają z certyfikatów lub znaczników czasu wystawionych przez EuroCert.

Subskrybent ma obowiązek zapoznania się z niniejszym dokumentem i zaakceptowania jego postanowień przed złożeniem wniosku o certyfikat i podpisaniem Umowy, natomiast Strona ufająca przed użyciem jakiegokolwiek certyfikatu lub znacznika czasu wystawionych zgodnie z Polityką certyfikacji.

3 Regulacje i dokumenty powiązane

3.1 Regulacje zewnętrzne

EuroCert świadczy usługi zaufania zgodnie z zasadami przedstawionymi w Polityce certyfikacji oraz obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

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 (łącznie z przepisami wykonawczymi), zwanym dalej „eIDAS";
2) Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. poz. 1579) (łącznie z przepisami wykonawczymi), 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, (łącznie z przepisami wykonawczymi), 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), (łącznie z przepisami wykonawczymi), zwaną dalej „Ustawą o chronię danych osobowych".

3.2 Regulacje wewnętrzne

Z Polityką certyfikacji związane są inne dodatkowe dokumenty, które EuroCert jest obowiązane stosować w swoim działaniu. Dokumenty te mają różny status (jawny, niejawny). Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane (niejawne):

1) Polityka Bezpieczeństwa Informacji (niejawna);
2) Instrukcja Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w EuroCert Sp. z o.o. (niejawna);

3) Instrukcja Bezpieczeństwa Informacji i Systemów Informatycznych (niejawna);
4) Regulamin Świadczenia Usług Drogą Elektroniczną (jawny);
5) Polityka Prywatności (jawna);
6) Plan Zakończenia Świadczenia Kwalifikowanych Usług Zaufania EuroCert (niejawny);
7) Regulamin Organizacyjny EuroCert sp. z o.o (niejawny);
8) Procedury Zarządzania Uprawnieniami i Dostępami (niejawny);
9) Procedura Korzystania z Komputerów Przenośnych (niejawny);
10) Procedura Tworzenia Kopii Zapasowych (niejawny);
11) Polityka Zarządzania Ciągłością Działania (niejawny);
12) Polityka Zarządzania Podatnościami (niejawny);
13) Polityka Zarządzania Ryzykiem (niejawny);
14) Polityka Zarządzania Ryzykiem Zasobowym (niejawny);
15) Procedura Zarządzania Kartami Kryptograficznymi (niejawny);
16) Procedura Obsługi Incydentu Bezpieczeństwa (niejawny);
17) Polityka Kontroli Wewnętrznej i Audytu (niejawny);
18) Ogólna Architektura Rozwiązania (niejawny);
19) Instrukcja Zarządzania Aktywami IT (niejawny).

4 Dane teleadresowe

W sprawach związanych z wykonaniem Umowy oraz zgłoszeniem reklamacji Subskrybent powinien kontaktować się z EuroCert pod adresem:
EuroCert Sp. z o.o.
ul. Puławska 474
02-884 Warszawa
tel. +48 22 490 36 45
e-mail: biuro@eurocert.pl

W sprawach zawieszania, uchylenia zawieszenia oraz unieważniania certyfikatu, Subskrybent powinien kontaktować się pod adresem poczty elektronicznej uniewaznienia@eurocert.pl lub pod numerem telefonu +48 22 490 49 86. Powinien przed tym zapoznać się z instrukcjami przedstawionymi na stronie https://eurocert.pl/index.php/dokumenty/zawieszenie-lub-uniewaznienie-certyfikatu.

Ze wsparciem technicznym można się skontaktować pod adresem poczty elektronicznej wsparcie@eurocert.pl lub pod numerem telefonu +48 22 490 49 86.

W celu zakupu usługi lub produktu z oferty EuroCert należy skorzystać z następujących adresów:
1) lista Punktów rejestracji: http://eurocert.pl/PunktyPartnerskie;
2) strona internetowa: https://eurocert.pl;
3) sklep internetowy: https://sklep.eurocert.pl.

5 Słownik pojęć, skrótów i skrótowców

1) EuroCert – jednostka organizacyjna EuroCert sp. z o.o. tj. „Centrum EuroCert", świadcząca kwalifikowane usługi zaufania.
2) Polityka certyfikacji – aktualna (obowiązująca) w chwili akceptacji postanowień niniejszego dokumentu polityka świadczenia usług zaufania przez EuroCert opublikowana na stronie internetowej https://eurocert.pl/repozytorium.
3) Subskrybent – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, której wystawiono kwalifikowany certyfikat lub dla której EuroCert świadczy usługę wystawiania znaczników czasu na podstawie Polityki certyfikacji.

4) Strona ufająca – osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która podejmuje działania lub jakąkolwiek decyzję w zaufaniu do danych podpisanych elektronicznie lub opatrzonych pieczęcią elektroniczną z wykorzystaniem klucza publicznego zawartego w certyfikacie wydanym przez EuroCert lub wydanego przez EuroCert znacznika czasu.
5) Usługi Zaufania – usługi zaufania świadczone przez EuroCert:
   - usługa kwalifikowanego podpisu elektronicznego,
   - usługa kwalifikowanej pieczęci elektronicznej,
   - usługa kwalifikowanego znacznika czasu.
6) Niezaprzeczalność – brak możliwości wyparcia się swego uczestnictwa w całości lub w części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie.
7) Umowa – umowa dotycząca świadczenia usług zaufania przez EuroCert.
8) CRL - listy zawieszonych i unieważnionych kwalifikowanych certyfikatów.
9) OCSP – protokół serwera weryfikacji statusu certyfikatów w trybie on-line (ang. On-line Certificate Status Protocol).

6 Rodzaje usług zaufania EuroCert i ich zastosowanie

Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim Unii Europejskiej jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich Unii Europejskiej. Analogiczna zasada obowiązuje w przypadku kwalifikowanej pieczęci elektronicznej oraz kwalifikowanego znacznika czasu.

Kwalifikowane certyfikaty są wydawane przez urząd certyfikacji Centrum Kwalifikowane EuroCert zgodnie z polityką NCP+ (ang. Normalized Certificates Policy requiring a secure cryptographic device) określoną w punkcie 5.3 normy ETSI EN 319 411-1, która jest fundamentem Polityki certyfikacji EuroCert.

Kwalifikowany urząd znacznika czasu EuroCert QTSA wystawia znaczniki czasu zgodnie z wymaganiami normy ETSI EN 319 421.

Nadzór nad urzędami Centrum Kwalifikowane EuroCert oraz EuroCert QTSA sprawuje minister właściwy ds. informatyzacji oraz wskazany przez niego podmiot (Narodowe centrum certyfikacji).

Certyfikaty wydawane przez EuroCert zawierają w polu „certificate policies” identyfikatory polityk certyfikacji, które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Kwalifikowanym certyfikatom podpisu elektronicznego został przypisany identyfikator: 1.2.616.1.113791.1.2.2, natomiast kwalifikowanym certyfikatom pieczęci elektronicznej identyfikator: 1.2.616.1.113791.1.2.3.

Identyfikator polityki certyfikacji umieszczony jest również w znacznikach czasu: 1.2.616.1.113791.1.4.

Kwalifikowane certyfikaty podpisu elektronicznego są wydawane osobom fizycznym występującym w imieniu własnym (certyfikat osobisty) lub w imieniu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej (certyfikat profesjonalny), kwalifikowane certyfikaty pieczęci elektronicznych są wydawane osobom prawnym oraz jednostkom organizacyjnym nieposiadającym osobowości prawnej (patrz tab. 1).

Tab. 1. Rodzaje usług zaufania EuroCert

Rodzaj usługi zaufania		Opis
Kwalifikowany certyfikat podpisu elektronicznego	Osobisty	-wykorzystywany do składania i weryfikacji kwalifikowanego podpisu elektronicznego, który ma skutek prawny równoważny podpisowi własnoręcznemu, - kwalifikowany podpis elektroniczny zapewnia integralność (i autentyczność) podpisywanej informacji i nadaje jej cechę niezaprzeczalności, - zawiera przynajmniej następujące dane osoby fizycznej: nazwę kraju, nazwisko i imię, numer seryjny (np.: PESEL, NIP, nr paszportu).
	profesjonalny	- wykorzystywany do składania i weryfikacji kwalifikowanego podpisu elektronicznego, który ma skutek prawny równoważny podpisowi własnoręcznemu, - kwalifikowany podpis elektroniczny zapewnia integralność (i autentyczność) podpisywanej informacji i nadaje jej cechę niezaprzeczalności, - oprócz danych osoby fizycznej przedstawionych powyżej zawiera ponadto dane osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej reprezentowanej przez subskrybenta: nazwę reprezentowanego podmiotu, NIP lub KRS, adres.
Kwalifikowany certyfikat pieczęci elektronicznej		- wykorzystywany do składania i weryfikacji kwalifikowanej pieczęci elektronicznej, która gwarantuje autentyczność pochodzenia podpisywanych danych oraz integralność powiązanych z nią danych, - zawiera dane osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości: nazwę reprezentowanego podmiotu, NIP lub KRS, adres.
Kwalifikowany elektroniczny znacznik czasu		- służy do poświadczania daty i czasu oraz integralności danych, z którymi data i czas są powiązane, - znakowanie czasem wywołuje w szczególności skutki prawne daty pewnej w rozumieniu przepisów Kodeksu cywilnego (art. 81 §2 pkt 3), - służy do oznaczanie czasem kwalifikowanych podpisów (pieczęci) elektronicznych w przypadku ich długookresowej ważności, - usługa znakowania czasem świadczona jest w odpowiedzi na żądanie zawierające podpis zaawansowany Subskrybenta uprawnionego do otrzymania znacznika lub po uwierzytelnieniu się Subskrybenta przy pomocy loginu i hasła, - Subskrybent powinien wystąpić o wydanie kolejnego elektronicznego znacznika czasu przed końcem okresu ważności certyfikatu wydanego dla EuroCert QTSA.

7 Zasady weryfikacji tożsamości

Weryfikacja tożsamości osób fizycznych ubiegających się o wydanie certyfikatu dokonywana jest przez upoważnioną przez EuroCert osobę w punkcie rejestracji na podstawie ważnego dowodu osobistego lub paszportu oraz dodatkowo – w przypadku certyfikatu profesjonalnego lub pieczęci elektronicznej – na podstawie następujących dokumentów:

1) pełnomocnictwa lub innego dokumentu upoważniającego do występowania w imieniu organizacji, określającego precyzyjnie zakres umocowania;
2) stosownego upoważnienia wystawionego przez daną organizację do umieszczenia danych organizacji w certyfikacie;
3) aktualnego wypisu z Krajowego Rejestru Sądowego lub wypis z Centralnej Ewidencji i Informacji o Działalności Gospodarczej;
4) innych dokumentów, które są niezbędne do potwierdzenia danych zawartych we wniosku o certyfikat, np. zaświadczenia o miejscu zatrudnienia, potwierdzenia prawa do wykonywania określonego zawodu.

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

Weryfikacja odbiorców usług świadczonych przez urząd elektronicznego znacznika czasu odbywa się na podstawie podpisu elektronicznego lub przydzielonego loginu i hasła.

8 Okres przechowywania danych

Wszystkie dokumenty i dane związane ze świadczeniem kwalifikowanych Usług Zaufania w tym wszystkie zaakceptowane przez subskrybentów warunki świadczenia Usług Zaufania (zawarte w niniejszym dokumencie i Polityce certyfikacji), Umowy, certyfikaty Subskrybentów, certyfikaty dostawcy usług zaufania, żądania unieważnienia i zawieszenia kwalifikowanego certyfikatu, listy CRL są przechowywane przez okres 20 lat od dnia ich wytworzenia zgodnie z Ustawą o usługach zaufania (art. 17 ust. 1).

Klucz prywatny powiązany z certyfikatem może służyć wyłącznie do składania kwalifikowanych podpisów (pieczęci) elektronicznych a certyfikat do weryfikowania podpisów (pieczęci) elektronicznych, zgodnie z Polityką certyfikacji, z uwzględnieniem ewentualnych ograniczeń zapisanych w certyfikacie.

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

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

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).

Zabrania się używania certyfikatów niezgodnie z przeznaczeniem wynikającym z typu certyfikatu, określonym w Polityce certyfikacji oraz w urządzeniach, które nie spełniają wymagań dla kwalifikowanych urządzeń do składania podpisu elektronicznego lub kwalifikowanych urządzeń do składania pieczęci elektronicznej określonych normami, 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 eIDAS. Zakazane jest również używanie certyfikatów przez osoby do tego nieupoważnione.

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

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

9 Obowiązki subskrybentów

Subskrybent zobowiązany jest do:

1) zapoznania się z niniejszym dokumentem oraz Polityką certyfikacji i zaakceptowania postanowień w nich zawartych przed złożeniem wniosku o certyfikat i podpisaniem Umowy;
2) wykorzystywania kwalifikowanego certyfikatu i odpowiadającego mu klucza prywatnego tylko zgodnie z ich przeznaczeniem, określonym w Polityce certyfikacji i wskazanym w danym certyfikacie (w polach keyUsage i extendedKeyUsage);
3) wykorzystywania kluczy prywatnych związanych z kwalifikowanymi certyfikatami wydanymi zgodnie z Polityką certyfikacji jedynie w urządzeniach do składania podpisów (pieczęci) elektronicznych, które spełniają wymagania dla kwalifikowanych urządzeń do składania podpisu elektronicznego lub pieczęci elektronicznej określone normami, 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 eIDAS;
4) podania w Umowie i wniosku certyfikacyjnym prawdziwych i kompletnych danych w zakresie wymaganym odpowiednio przez Umowę i wniosek certyfikacyjny;
5) dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku certyfikacyjnym w celu wypełnienia wymagań procesu rejestracji, unieważnienia i odnowienia certyfikatu;
6) sprawdzenia poprawności danych umieszczonych w certyfikacie niezwłocznie po jego otrzymaniu a przed jego użyciem (w szczególności przed wykonaniem pierwszego podpisu elektronicznego lub pieczęci elektronicznej) i niezwłocznego poinformowania EuroCert o jakichkolwiek błędach w jego certyfikacie lub o zmianach informacji w nim zawartych w celu unieważnienia certyfikatu i wygenerowania nowego prawidłowego certyfikatu;
7) ochrony swojego klucza prywatnego, tj.:
   a) nie przechowywania urządzenia zawierającego klucz prywatny razem z hasłem dostępu (PIN) do niego,
   b) nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim,
   c) kontroli i zabezpieczenia dostępu do urządzenia zawierającego jego klucz prywatny,
   d) zabezpieczenia i ochrony dostępu do nośników, na których przechowywane są hasła dostępu do klucza prywatnego;
8) niezwłocznego poinformowanie EuroCert o wszelkich okolicznościach (np. utracie klucza prywatnego, utracie lub ujawnieniu kodu PIN i/lub SO PIN), 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;
9) zaprzestania posługiwania się unieważnionym, zawieszonym lub przeterminowanym certyfikatem;
10) potwierdzenia odbioru urządzenia zawierającego jego klucz prywatny;

11) Wpisywania kodu PIN i/lub SO PIN do urządzenia zawierającego klucze służące do składania podpisów lub pieczęci elektronicznych jedynie w bezpiecznym środowisku – to jest na komputerze, do którego dostęp mają jedynie osoby zaufane przez Subskrybenta, zabezpieczonym przed wszelkiego rodzaju niebezpiecznym oprogramowaniem, przy użyciu w szczególności odpowiednich programów antywirusowych oraz zapory firewall.

10 Obowiązki stron ufających

Jedynym sposobem potwierdzenia ważności certyfikatu Subskrybenta pod kątem ewentualnego unieważnienia bądź zawieszenia, jest sprawdzenie statusu certyfikatu na odpowiedniej liście CRL albo za pomocą usługi OCSP. Usługa OCSP realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 6960.

Informacja o statusie certyfikatu dostępna jest publicznie. Adresy usług CRL i OCSP zawarte są w wydanym certyfikacie odpowiednio w polach CrlDistributionPoints oraz AuthorityInformationAccess. Listy CRL oraz certyfikaty dostawcy usług zaufania EuroCert 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
2) pobrać listę CRL wydaną po momencie, na który badamy ważność certyfikatu i sprawdzić status certyfikatu na CRL.

Ważność podpisów pod tokenem OCSP oraz listą CRL należy sprawdzać w oparciu o bieżącą listę TSL.

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

Strona ufająca zobowiązana jest do:
1) zapoznania się z niniejszym dokumentem oraz Polityką certyfikacji i zaakceptowania postanowień w nich zawartych przed zaakceptowaniem podpisu elektronicznego, pieczęci elektronicznej lub znacznika czasu;
2) wykorzystywania kwalifikowanego certyfikatu zgodnie z jego przeznaczeniem, określonym w Polityce certyfikacji i wskazanym w danym certyfikacie (w polach keyUsage i extendedKeyUsage);
3) zweryfikowania podpisu elektronicznego lub pieczęci elektronicznej z wykorzystaniem listy CRL, usługi OCSP i właściwej ścieżki certyfikacji;
4) zweryfikowania pieczęci elektronicznej urzędu EuroCert QTSA lub Centrum Kwalifikowane EuroCert oraz sprawdzenia listy CRL, pod kątem unieważnienia certyfikatu urzędu;
5) sprawdzenia czy certyfikat podpisu elektronicznego lub pieczęci elektronicznej, znacznik czasu, zostały użyte zgodnie z ich przeznaczeniem określonym w Polityce certyfikacji oraz czy są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca (np. w formie polityki podpisu); strona ufająca powinna zwrócić w tym przypadku uwagę na rodzaj certyfikatu, znacznika czasu i politykę certyfikacji, według której zostały one wydane;
6) zgłoszenia do EuroCert wątpliwości, czy dany certyfikat lub znacznik czasu został wydany poprawnie oraz czy jest używany przez upoważniony do tego podmiot; zgłoszenie może być dokonane telefonicznie pod numerem infolinii w godzinach jej pracy lub całodobowo pod adresem poczty elektronicznej wsparcie@eurocert.pl;
7) zweryfikowania, czy podpis elektroniczny lub pieczęć elektroniczna zostały zrealizowane za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie kwalifikowanym subskrybenta;

8) zweryfikowania, czy podpisana wiadomość (dokument) lub certyfikat nie zostały zmodyfikowane po złożeniu na nim podpisu;
9) uznania podpisu cyfrowego (certyfikatu podpisu elektronicznego lub pieczęci) za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis cyfrowy (podpis elektroniczny lub certyfikat) jest ważny lub uzyskany wynik weryfikacji jest negatywny.

11 Ograniczenie odpowiedzialności EuroCert

EuroCert podlega obowiązkowemu ubezpieczeniu odpowiedzialności cywilnej za szkody wyrządzone odbiorcom Usług Zaufania powstałe w okresie świadczenia Usług Zaufania.

Suma gwarancyjna ubezpieczenia OC, w odniesieniu do jednego zdarzenia, którego skutki są objęte umową ubezpieczenia OC, wynosi równowartość w złotych 250000 euro, ale nie więcej niż 1000000 euro w odniesieniu do wszystkich zdarzeń. Odpowiedzialność odszkodowawcza EuroCert nie obejmuje utraconych korzyści i ogranicza się do szkody rzeczywistej.

EuroCert odpowiada wobec Subskrybenta za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swoich obowiązków w zakresie Usług Zaufania świadczonych zgodnie z Umową, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności za które EuroCert nie ponosi odpowiedzialności, i którym nie mogła zapobiec mimo dołożenia należytej staranności. Odpowiedzialność odszkodowawcza EuroCert w takim przypadku jest ograniczona do wysokości sum gwarancyjnych, określonych powyżej.

EuroCert nie odpowiada wobec Subskrybenta za jakiekolwiek szkody wynikające z przyczyn innych niż niewykonanie lub nienależyte wykonanie obowiązków przez EuroCert lub upoważnione podmioty działające w jej imieniu, w szczególności EuroCert nie odpowiada za:
1) środowisko sprzętowe i oprogramowanie systemowe zainstalowane na komputerze Subskrybenta;
2) skutki nieprawidłowego użycia klucza prywatnego przez Subskrybenta;
3) skutki użycia klucza prywatnego Subskrybenta przez nieuprawnioną osobę;
4) skutki utraty bezpieczeństwa stosowanych przez EuroCert algorytmów kryptograficznych, chyba że użycie tych algorytmów przez EuroCert nie jest zgodne z Polityką certyfikacji lub obowiązującymi przepisami prawa;
5) skutki ujawnienia przez Subskrybenta osobom trzecim informacji takich jak: kod PIN, SO PIN;
6) skutki oświadczenia woli złożonego przez Subskrybenta przy użyciu certyfikatu zawierającego błędy lub braki powstałe z przyczyn leżących po stronie Subskrybenta;
7) za szkody wynikające z użycia certyfikatów poza zakresem określonym w Polityce certyfikacji, która została wskazana w certyfikacie;
8) za szkody wynikłe z nieprawdziwości danych zawartych w certyfikacie, których weryfikacja oparta była na ich oświadczeniach lub wpisanych zgodnie z przedstawionymi dokumentami, które zostały sfałszowane lub przedstawiały nieprawdziwe lub nieaktualne dane;
9) za szkody wynikłe z nieaktualności danych wpisanych do certyfikatu, jeżeli w chwili wydawania certyfikatu były one prawdziwe;
10) za szkody powstałe na skutek działania siły wyższej lub innych, za których wystąpienie nie ponosi odpowiedzialności, tj.: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka;
11) za szkody powstałe na skutek instalacji, użytkowania oraz zarządzania aplikacjami innymi niż dostarczone przez EuroCert;
12) za szkody powstałe na skutek używania certyfikatu przeterminowanego, unieważnionego lub zawieszonego;
13) za szkody wynikające z nieprzestrzegania przez odbiorcę Usług Zaufania zasad określonych w Polityce certyfikacji;

14) skutki przechowywania lub używania przez odbiorców Usług Zaufania kluczy prywatnych do składania podpisu elektronicznego, pieczęci elektronicznej w sposób niezapewniający ich ochrony przed nieuprawnionym wykorzystaniem;
15) za niedostępność usługi OCSP, o ile w okresie niedostępności działają poprawnie usługi informowania o statusie certyfikatów na podstawie listy CRL;
16) utratę dostępu Subskrybenta do klucza prywatnego służącego do realizacji podpisów lub pieczęci, spowodowaną blokadą karty elektronicznej z powodu błędnie wprowadzonego kodu PIN i/lub SO PIN, przy przekroczeniu ustalonego limitu błędnych prób, o którym Subskrybent został poinformowany;
17) za niedostępność usługi znakowania czasem, o ile okres niedostępności nie narusza deklaracji dostępności usługi określonej w rozdziale 6.8 Polityki certyfikacji;
18) szkody wynikłe z podjęcia działań przez odbiorców Usług Zaufania, mimo negatywnie lub niekompletnie zweryfikowanego albo nieważnego certyfikatu lub znacznika czasu, jak również w przypadku, gdy zaniechają weryfikacji statusu lub kompletności certyfikatu lub znacznika czasu;
19) ryzyko związane z tym, że podpis elektroniczny, ważny w chwili weryfikacji, może w dowolnej chwili stracić możliwość weryfikacji ważności (a więc stracić moc dowodową) w przypadku nie dysponowania przez Stronę ufającą ważnym znacznikiem czasu.

W przypadku skrócenia okresu ważności certyfikatów z winy EuroCert, odpowiedzialność EuroCert ogranicza się do zwrotu kosztów wystawienia certyfikatów, proporcjonalnie do skrócenia okresu ważności lub wydania nowego certyfikatu, którego ważność pokrywa się z ważnością certyfikatu poprzedniego.

12 Polityka prywatności

Dane osobowe przekazywane do EuroCert przez Subskrybentów są objęte ochroną określoną przez RODO oraz Ustawę o ochronie danych osobowych.

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

Administratorem danych osobowych Subskrybentów jest Eurocert Sp. z o. o. z siedzibą w Warszawie (02-884) przy ul. Puławskiej 474, wpisana do Rejestru Przedsiębiorców prowadzonego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS 0000408592, zwana dalej Administratorem. Administrator prowadzi operacje przetwarzania danych osobowych Subskrybentów.

Kontakt z Administratorem we wszelkich sprawach związanych z przetwarzaniem danych osobowych jest możliwy pod adresem biuro@eurocert.pl.

Administrator przetwarza dane osobowe w celu:
1) realizacji Usługi Zaufania tj. na podstawie art. 6 ust. 1 lit. b RODO zgodnie z którym przetwarzanie jest niezbędne do wykonania Umowy której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem Umowy. Dane osobowe będą przetwarzane przez okres realizacji Usługi Zaufania oraz następnie przez 20 lat od początku okresu ważności certyfikatu kwalifikowanego zgodnie z Ustawą o usługach zaufania;
2) wypełnienia procesu reklamacyjnego na podstawie art. 6 ust. 1 lit. c RODO, zgodnie z którym przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze. Dane osobowe będą przetwarzane przez okres wypełnienia obowiązku prawnego i ewentualny dalszy okres korzystania z Usług Zaufania oferowanych przez Administratora;
3) dochodzenia roszczeń na podstawie art. 6 ust. 1 lit. f RODO tj. prawnie uzasadnionego interesu Administratora, którym jest dochodzenie jego roszczeń i obrona jego praw, a także art. 9 ust.

2 lit. f RODO tj. przetwarzanie jest niezbędne do dochodzenia roszczeń. Dane osobowe będą przetwarzane przez okres dochodzenia roszczeń;

4) wypełnienia obowiązków podatkowych na podstawie art. 6 ust. 1 lit. c RODO (przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Administratorze) w zw. z art. 74 ust. 2 Ustawy z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2018 r. poz. 395 z późn. zm.). Dane osobowe będą przetwarzane przez okres konieczny do wypełnienia obowiązku podatkowego. Wszelkie dane przetwarzane na potrzeby rachunkowości oraz ze względów podatkowych przetwarzamy przez 5 lat liczonych od końca roku kalendarzowego, w którym powstał obowiązek podatkowy;
5) marketingowym na podstawie art. 6 ust. 1 lit. a RODO (osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów). Dane będą przetwarzane przez czas trwania akcji marketingowej lub do momentu cofnięcia zgody na ich przetwarzanie.

Ponadto Administrator gromadzi dane osobowe – za zgodą Subskrybentów – w celach marketingowych polegających na kierowaniu do Subskrybentów (na adres e-mail) powiadomień o ofertach Administratora lub treści, która może zawierać informacje handlowe, przesyłaniu informacji drogą elektroniczną oraz poprzez podejmowanie działań telemarketingowych. Przy realizowaniu celów marketingowych Administrator w niektórych przypadkach korzysta z profilowania tj. automatycznego przetwarzania danych osobowych, które polega na wykorzystaniu tych danych do oceny niektórych czynników osobowych Subskrybentów, w szczególności do analizy lub prognozy aspektów dotyczących ich preferencji i zainteresowań.

Dane osobowe mogą być udostępniane innym podmiotom w zakresie niezbędnym do realizacji Umowy, tj.:

1) Platforma Shoper (DreamCommerce S.A.), Kraków (31-280), ul. Władysława Łokietka 79, NIP: 9452156998;
2) DPD Polska Sp. z o.o., Warszawa (02-274), ul. Mineralna 15, NIP: 5260204110;
3) PayPro S.A., Poznań (60-327), ul. Kanclerska 15;
4) IFirma S.A., Wrocław (53-234), ul. Grabiszyńska 241 B, NIP: 898-16-47-572;
5) Biuro rachunkowe Aspekt Consulting, Lesznowola, ul. Leśna 87, NIP: 1230213295;
6) Odpowiednim autoryzowanym punktom rejestracji EuroCert wyszczególnionym na stronie http://eurocert.pl/PunktyPartnerskie.

Ponadto dane osobowe mogą zostać przekazane organom państwowym lub podmiotom wykonującym zadania publiczne w związku z prowadzonym przez te organy postępowaniem i na podstawie przepisów prawa.

Subskrybenci posiadają prawo do żądania od Administratora:

1) dostępu do swoich danych osobowych;
2) sprostowania swoich danych osobowych;
3) usunięcia swoich danych osobowych;
4) ograniczenia przetwarzania danych osobowych;
5) wniesienia skargi do organu nadzorczego;
6) przenoszenia danych;
7) cofnięcia zgody na przetwarzanie danych osobowych w dowolnym momencie. Cofnięcie zgody nie wpłynie na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jednakże uniemożliwi świadczenie przez Administratora usług od których zgoda jest uzależniona;
8) wniesienia sprzeciwu wobec przetwarzania danych osobowych – w przypadku, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi oraz, gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią, w tym w przypadku profilowania.

Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

W celu wykonania powyższych uprawnień należy skontaktować się z nami za pośrednictwem poczty elektronicznej – biuro@eurocert.pl.

Dane osobowe chronione są zgodnie z zasadami zawartymi w Polityce Bezpieczeństwa Informacji.

Polityka Prywatności dostępna jest pod adresem: https://sklep.eurocert.pl/pl/i/Polityka-prywatnosci/11.

Wszystkie informacje udostępniane publicznie w certyfikacie nie są uważane za informacje prywatne, o ile reguła ta nie narusza wymagań wynikających z RODO.

13 Warunki rozstrzygania sporów, reklamacje

Subskrybent może żądać zwrotu wniesionej opłaty, jeżeli Usługa Zaufania była wykonana niezgodnie z umową, Polityką certyfikacji, warunkami przedstawionymi w niniejszym dokumencie. Żądania o zwrot opłat należy kierować pod adres podany w rozdz. 4.

W przypadku unieważnienia certyfikatu z przyczyn leżących po stronie EuroCert, wystawia ona nowy certyfikat ważny do końca okresu ważności certyfikatu poprzedniego lub zwraca Subskrybentowi opłatę za świadczenie Usług Zaufania, w części proporcjonalnej do niewykorzystanego okresu ważności certyfikatu. Te same zasady obowiązują w przypadku ograniczenia funkcjonalności certyfikatu na skutek zmiany polityki certyfikacji mającej zastosowanie do tego certyfikatu, z przyczyn leżących po stronie EuroCert.

Przedmiotem rozstrzygania sporów, w tym reklamacji, mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania kwalifikowanego certyfikatu w oparciu o regulacje Polityki certyfikacji oraz zawartych umów.

Spory, reklamacje, skargi bądź zażalenia powstałe na tle użytkowania certyfikatów, znaczników czasu, tokenów weryfikacji statusu certyfikatów 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 rozdz. 4.

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

14 Audyty

Kwalifikowane usługi zaufania świadczone przez EuroCert podlegają corocznemu badaniu zgodności z eIDAS na podstawie art. 20 ust. 1 i 21 ust. 1.

Audyt zewnętrzny może być przeprowadzony również na wniosek ministra właściwego ds. informatyzacji w trybie art. 31 Ustawy o usługach zaufania w związku z art. 20 ust. 2 i art. 17 ust. 4 lit. e) eIDAS.

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.

Podmiotem zewnętrznym oceniającym zgodność z eIDAS jest TAYLLORCOX PCEB.

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).

15 Okres obowiązywania

Zasady obowiązują od dnia zatwierdzenia.

16 Status i historia dokumentu

Status		obowiązująca
Historia zmian		
Data zatwierdzenia	Wersja	Dokonane zmiany
08.11.2018 r.	1	Opracowanie dokumentu