EuroCERT sp. z o.o.
Centrum EUROCERT

Polityka Certyfikacji
dla kwalifikowanych certyfikatów

Wersja 1.3

Spis treści

1 WPROWADZENIE 3

1.1 ODBIORCY USŁUG CERTYFIKACYJNYCH 3
1.2 WAŻNE INFORMACJE DLA ODBIORCÓW USŁUG CERTYFIKACYJNYCH 3
1.3 IDENTYFIKATOR POLITYKI 3
1.4 HISTORIA ZMIAN 3
1.5 DANE KONTAKTOWE 4

2 ZARYS POLITYKI 4

3 POSTANOWIENIA POLITYKI 4

3.1 ODBIORCY USŁUG CERTYFIKACYJNYCH ORAZ ZASTOSOWANIE CERTYFIKATÓW 4
3.2 PRAWA I OBOWIĄZKI STRON 4
3.3 OPŁATY 6
3.4 ODPOWIEDZIALNOŚĆ CENTRUM EUROCERT 6
3.5 UMOCOWANIA PRAWNE I INTERPRETACJE 8
3.6 OCHRONA I ARCHIWIZACJA INFORMACJI 8

4 WERYFIKACJA TOŻSAMOŚCI I UWIERZYTELNIENIE 9

4.1 REJESTRACJA OSOBISTA 9
4.2 REJESTRACJA W PRZYPADKU POSIADANIA WAŻNEGO KWALIFIKOWANEGO CERTYFIKATU 10
4.3 ZARZĄDZANIE CERTYFIKATEM 10

5 WYMAGANIA OPERACYJNE 10

5.1 WYDANIE KWALIFIKOWANEGO CERTYFIKATU PRZEZ CENTRUM EUROCERT 10
5.2 PUBLIKOWANIE INFORMACJI O UNIEWAŻNIONYCH I WYDANYCH KWALIFIKOWANYCH CERTYFIKATACH 11
5.3 UNIEWAŻNIANIE, ZAWIESZANIE ORAZ UCHYLANIE ZAWIESZENIA KWALIFIKOWANYCH CERTYFIKATÓW 11
5.4 TECHNICZNE ŚRODKI ZAPEWNIENIA BEZPIECZEŃSTWA 12
5.5 PROFILE CERTYFIKATU I LISTY CERTYFIKATÓW UNIEWAŻNIONYCH (CRL) 15

6 ADMINISTROWANIE POLITYKĄ 18

1 Wprowadzenie

Niniejsza Polityka Certyfikacji, dalej zwana Polityką, określa szczegółowe rozwiązania (techniczne i organizacyjne) wskazujące sposób, zakres oraz warunki ochrony, tworzenia i stosowania kwalifikowanych certyfikatów.

Certyfikaty wydawane zgodnie z Polityką są kwalifikowanymi certyfikatami w rozumieniu ustawy z dnia 18 września 2001 o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450 z późn. zm.).

Usługi certyfikacyjne opisywane w Polityce są świadczone przez EuroCERT sp. z o.o. nazywaną dalej w Polityce Certyfikacji „Centrum EUROCERT" (EUROCERT).

1.1 Odbiorcy usług certyfikacyjnych

W ramach Polityki wyróżnia się następujących odbiorców usług certyfikacyjnych

- **Zamawiający** – osoba fizyczna, która zawarła umowę o świadczenie usług certyfikacyjnych z Centrum EUROCERT.
- **Subskrybent** – osoba fizyczna, której tożsamość została zweryfikowana podczas procesu rejestracji i której dane zostały umieszczone w wydanym kwalifikowanym certyfikacie.
- **Strona ufająca** – osoba fizyczna, osoba prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która weryfikuje podpis elektroniczny lub w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat.

1.2 Ważne informacje dla odbiorców usług certyfikacyjnych

Każdy odbiorca usług certyfikacyjnych zamierzający wykorzystać lub zaufać certyfikatowi wydanemu na podstawie Polityki ma obowiązek zapoznać się z tym dokumentem i zrozumieć występujące w nim zapisy.

1.3 Identyfikator polityki

Nazwa polityki	Polityka Certyfikacji dla Kwalifikowanych Certyfikatów Centrum Certyfikacji EUROCERT
Wersja	1.0
Status wersji	nieaktualna
Numer referencyjny	EuroCERT.polityka.1.0
Data wydania	1 sierpnia 2013 roku
Data ważności	Do odwołania

1.4 Historia zmian

Wersja	Data	Opis zmian
1.0	01 sierpnia 2013 roku	utworzenie dokumentu
1.1	27 listopada 2013 roku	Powtórne złożenie dokumentu

1.2	15.03.2015	Zmiana adresu w danych kontaktowych
1.3	20.11.2015	Zmiana adresu w danych kontaktowych

1.5 Dane kontaktowe

W celu uzyskania dalszych informacji dotyczących usług Centrum EUROCERT prosimy o kontakt:

Centrum EUROCERT
Ul. Puławska 474
02-884 Warszawa
+48 22 490 36 45
biuro@eurocert.pl

2 Zarys polityki

Certyfikaty wydawane zgodnie z Polityką są przeznaczone dla osób fizycznych i są wydawane na podstawie umowy o świadczenie usług certyfikacyjnych (Umowa).

W ramach niniejszej Polityki wydawane są tylko kwalifikowane certyfikaty.

Przed wystawieniem certyfikatu pomiędzy Zamawiającym a Centrum EUROCERT zostaje zawarta umowa o świadczenie usług certyfikacyjnych. Umowa musi być podpisana własnoręcznie przez Zamawiającego oraz osobę reprezentującą Centrum EUROCERT.

Zamawiający jest zobowiązany do złożenia pisemnego oświadczenia o zapoznaniu się z informacjami dotyczącymi warunków i skutków prawnych użycia certyfikatów, zakresu i ograniczeń ich stosowania oraz o systemie dobrowolnej rejestracji podmiotów kwalifikowanych i jej znaczeniu, przed zawarciem Umowy.

3 Postanowienia polityki

3.1 Odbiorcy usług certyfikacyjnych oraz zastosowanie certyfikatów

W ramach Polityki Centrum EUROCERT wydaje kwalifikowane certyfikaty do weryfikowania bezpiecznego podpisu elektronicznego. Okres ważności wydawanych certyfikatów nie może przekraczać 2 lat od daty ich wydania.

Na wniosek osoby ubiegającej się o wydanie certyfikatu, w kwalifikowanym certyfikacie mogą zostać umieszczone inne informacje, w szczególności - wskazanie czy osoba ta działa:

1. we własnym imieniu, albo
2. jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo
3. w charakterze członka organu albo organu osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej, albo
4. jako organ władzy publicznej.

3.2 Prawa i obowiązki stron

3.2.1 Obowiązki Subskrybentów

1. Przed złożeniem wniosku o wydanie kwalifikowanego certyfikatu wnioskodawca zobowiązany jest do zapoznania się z treścią Polityki.
2. Jeżeli wnioskodawca nie jest Zamawiającym, to jest on zobowiązany do złożenia pisemnego oświadczenia o zapoznaniu się z informacjami dotyczącymi warunków i skutków prawnych użycia certyfikatów, zakresu i ograniczeń ich stosowania oraz o systemie dobrowolnej rejestracji podmiotów kwalifikowanych i jej znaczeniu oraz o zapoznaniu się z treścią Umowy, przed złożeniem wniosku o wydanie kwalifikowanego certyfikatu.
3. Subskrybent zobowiązuje się do bezpiecznego przechowywania danych służących do składania podpisów elektronicznych oraz informacji związanych z uwierzytelnieniem wobec komponentu technicznego.
4. Subskrybent zobowiązuje się do ochrony przed ujawnieniem hasła do zarządzania tym certyfikatem.
5. W przypadku ujawnienia danych służących do składania podpisu elektronicznego, komplementarnych do danych służących do weryfikacji podpisu elektronicznego zawartych w kwalifikowanym certyfikacie lub też w przypadku uzasadnionego podejrzenia, iż fakt taki mógł mieć miejsce, Subskrybent zobowiązuje się niezwłocznie powiadomić o tym Centrum EUROCERT poprzez złożenie żądania unieważnienia tego certyfikatu.
6. Subskrybent jest odpowiedzialny za prawdziwość danych przekazywanych we wniosku o wydanie certyfikatu.
7. Subskrybent zobowiązuje się do informowania Centrum EUROCERT o wszelkich zmianach informacji zawartych w jego certyfikacie lub podanych we wniosku o wydanie tego certyfikatu.
8. Po upływie okresu ważności, bądź po unieważnieniu kwalifikowanego certyfikatu Subskrybent zobowiązuje się do zaprzestania stosowania danych, służących do składania podpisu elektronicznego, komplementarnych do danych służących do weryfikacji podpisu elektronicznego zawartych w tym certyfikacie.

3.2.2 Obowiązki weryfikującego bezpieczny podpis elektroniczny (strony ufającej)

1. Strona ufająca jest zobowiązana do bezpiecznego pobrania certyfikatu głównego urzędu certyfikacji w hierarchicznej strukturze zaufania Centrum EUROCERT (zaświadczenia certyfikacyjnego, o którym mowa w art. 23 ust. 2 Ustawy z dn. 18.09.2001 o podpisie elektronicznym), w tym weryfikacji odcisku palca publicznego klucza głównego urzędu certyfikacji.
2. Podczas każdej weryfikacji bezpiecznego podpisu elektronicznego, weryfikowanego kwalifikowanym certyfikatem wydanym zgodnie z Polityką, wymaga się sprawdzenia ważności ścieżki certyfikacji. Ścieżką certyfikacji jest uporządkowany ciąg zaświadczeń certyfikacyjnych i kwalifikowanego certyfikatu użytego do weryfikacji podpisu, utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i

kwalifikowanego certyfikatu, poświadczenie elektroniczne zawarte w następnym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego komplementarnych do danych do weryfikacji podpisu elektronicznego, zawartych w poprzednim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego punktem zaufania. Ścieżka certyfikacji musi zawierać zaświadczenie certyfikacyjne, określone w art. 23 ust. 2 Ustawy z dn. 18.09.2001 o podpisie elektronicznym.

3. Wymaga się również sprawdzenia, czy identyfikatory polityk certyfikacji, umieszczone w kwalifikowanych certyfikatach i zaświadczeniach zawartych w ścieżce znajdują się w określonym przez weryfikującego zbiorze identyfikatorów dopuszczalnych.

3.3 Opłaty

Usługi związane z wydawaniem kwalifikowanych certyfikatów, których dotyczy Polityka, są płatne zgodnie z aktualnie obowiązującym Cennikiem, dostępnym http://www.EuroCERT.pl

Usługi związane z zawieszaniem oraz unieważnianiem kwalifikowanych certyfikatów oraz dostępem do list CRL i list unieważnionych zaświadczeń certyfikacyjnych dla odbiorców usług certyfikacyjnych są nieodpłatne.

3.4 Odpowiedzialność Centrum EUROCERT

Centrum EUROCERT zobowiązuje się do postępowania zgodnie z zapisami Polityki, a w szczególności do przeprowadzania procedur rejestracji, wydawania i unieważniania kwalifikowanych certyfikatów zgodnie z zasadami opisanymi w Polityce oraz w Umowie.

Centrum EUROCERT odpowiada za zgodność informacji zawartych w kwalifikowanym certyfikacie z informacjami zawartymi we wniosku o wydanie tego certyfikatu. w szczególności Centrum EUROCERT odpowiada za zgodność danych osobowych umieszczonych w kwalifikowanym certyfikacie z informacjami zawartymi w dokumencie tożsamości wnioskodawcy okazanym w czasie rejestracji.

Centrum EUROCERT odpowiada za przedsięwzięcie odpowiednich kroków mających na celu weryfikację informacji identyfikującej tożsamość subskrybenta wniosków składanych przez strony.

Centrum EUROCERT nie odpowiada wobec odbiorców usług certyfikacyjnych za szkody wynikłe z nieprawdziwości wszelkich danych zawartych w kwalifikowanym certyfikacie, które zostały wpisane na wniosek Subskrybenta.

Zakres i sposób weryfikacji danych podanych w zgłoszeniu certyfikacyjnym jest opisany w rozdziale 4 Polityki.

Centrum EUROCERT, wydając kwalifikowane certyfikaty, jest obowiązane stosować takie procedury ich wydawania, aby uzyskać od Subskrybenta pisemną zgodę na stosowanie danych służących do weryfikacji jej podpisu elektronicznego, które są zawarte w wydanym certyfikacie.

Centrum EUROCERT odpowiada za przestrzeganie przyjętych procedur postępowania, obowiązujących przy czynnościach związanych ze świadczeniem usług certyfikacyjnych w ramach Polityki. W szczególności, Centrum EUROCERT odpowiada za publikowanie

aktualnych informacji o unieważnieniach kwalifikowanych certyfikatów w Repozytorium Centrum EUROCERT, zgodnie z Polityką.

Kwalifikowane certyfikaty wydawane przez Centrum EUROCERT w ramach Polityki zawierają informacje wskazujące, że przy ich tworzeniu korzystano z następujących algorytmów:

- algorytm szyfrowy: RSA – zarejestrowany pod identyfikatorem obiektu {joint-iso-ccitt(2) ds(5) module(1) algorithm(8) encryptionAlgorithm(1) 1};
- funkcja skrótu: SHA-1 – zarejestrowana pod identyfikatorem obiektu {iso(1) identifiedOrganization(3) oIW(14) oIWSecSig(3) oIWSecAlgorithm(2) 26}.

W certyfikatach tych jest również zawarta informacja, z jakim algorytmem stowarzyszone są dane do weryfikacji podpisu elektronicznego, zawarte w certyfikacie.

Szczegółowy opis pól kwalifikowanego certyfikatu wskazujących na stosowane algorytmy, bądź algorytmy dopuszczone do tworzenia podpisów elektronicznych jest zawarty w rozdziale 5.5 Polityki.

Zgłoszenia certyfikacyjne są opatrzone podpisem elektronicznym Inspektora do spraw Rejestracji, który je zatwierdził.

Przy świadczeniu usług wykorzystujących oznaczanie czasu (w szczególności przy określaniu początku okresu ważności kwalifikowanego certyfikatu) Centrum EUROCERT stosuje rozwiązania zapewniające synchronizację z Międzynarodowym Wzorcem Czasu (Coordinated Universal Time) z dokładnością nie mniejszą niż do 1 sekundy.

Centrum EUROCERT zapewnia, że dane których ujawnienie spowodowałoby brak skuteczności mechanizmów zabezpieczających, w szczególności dane służące do składania bezpiecznego podpisu elektronicznego są dostarczane użytkownikom w modułach kluczowych lub komponentach technicznych przekazywanych bezpiecznymi kanałami.

Centrum EUROCERT zapewnia, że dane służące do weryfikacji bezpiecznego podpisu lub poświadczenia elektronicznego i publiczne klucze infrastruktury są wysyłane do odbiorców usług certyfikacyjnych w sposób zapewniający ich integralność i autentyczność.

Centrum EUROCERT zapewnia możliwość unieważniania kwalifikowanych certyfikatów oraz tworzenia i publikowania list CRL oraz publikowania list unieważnionych zaświadczeń certyfikacyjnych przez całą dobę, zgodnie z przyjętymi okresami publikacji. W celu zapewnienia odpowiedniego poziomu dostępności tych usług Centrum EUROCERT posiada zapasowy ośrodek przetwarzania danych.

Centrum EUROCERT zawiadamia Subskrybenta o unieważnieniu lub zawieszeniu tego certyfikatu w sposób ustalony w Umowie.

Klucze chroniące dane służące do składania poświadczeń elektronicznych w ramach Polityki, przechowywane są w modułach kryptograficznych. Klucze są podzielone na części według schematu progowego stopnia (m, n), gdzie wartość „m” wynosi co najmniej 2, natomiast n > m + 1. Każdą z części przechowuje się w modułach kluczowych. Klucze te pojawiają się w pełnej formie jedynie w komponencie technicznym.

Komponenty techniczne posiadają certyfikat zgodności z normą ITSEC v. 1.2 poziom 3 lub bezpieczniejszy, FIPS 140 poziom 3 lub bezpieczniejszy, albo ISO/IEC 1540 poziom EAL4 lub bezpieczniejszy.

Komponenty techniczne stosowane przez Centrum EUROCERT do świadczenia usług w ramach Polityki nie są stosowane do żadnego innego celu, w tym do świadczenia usług w ramach innej polityki certyfikacji ani do świadczenia usługi znakowania czasem.

3.5 Umocowania prawne i interpretacje

Centrum EUROCERT funkcjonuje zgodnie z przepisami prawa obowiązującego na terenie Rzeczypospolitej Polskiej, w szczególności z Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450) i powiązanymi przepisami wykonawczymi.

Podpis elektroniczny złożony z użyciem klucza prywatnego, w połączeniu z certyfikatem wydanym przez Centrum EUROCERT zgodnie z Polityką będzie traktowany równoprawnie z podpisem odręcznym osoby, która ten podpis złożyła.

3.6 Ochrona i archiwizacja informacji

Informacje gromadzone i przetwarzane w ramach realizacji Polityki podlegają ochronie, w zakresie i trybie przewidzianym obowiązującymi przepisami prawa. Tajemnicą objęte są informacje, których nieuprawnione ujawnienie mogłoby narazić na szkodę odbiorcę usług certyfikacyjnych lub Centrum EUROCERT .

Centrum EUROCERT udostępnia stronom trzecim wyłącznie informacje zawarte w kwalifikowanych certyfikatach zgodnie z upoważnieniem złożonym przez Zamawiającego. Zobowiązanie to nie dotyczy przypadku skierowania żądania o udostępnienie informacji przez:

1. sąd lub prokuratora – w związku z toczącym się postępowaniem;
2. ministra odpowiedzialnego za nadzór nad kwalifikowanymi podmiotami świadczącymi usługi certyfikacyjne;
3. organów państwowych upoważnionych do tego na mocy odpowiednich ustaw, w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne, lub w związku ze sprawowaniem przez nie nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne.

Centrum EUROCERT przechowuje, przez co najmniej 20 lat:

1. wszystkie kwalifikowane certyfikaty i zaświadczenia certyfikacyjne wydane w ramach Polityki;
2. wszystkie listy CRL i listy unieważnionych zaświadczeń certyfikacyjnych wydane w ramach Polityki;
3. umowy o świadczenie usług certyfikacyjnych;
4. pisemne oraz elektroniczne oświadczenia potwierdzające tożsamość;
5. wnioski o unieważnienie i uchylenie zawieszenia kwalifikowanego certyfikatu.

Centrum EUROCERT przechowuje, przez co najmniej 3 lata wszystkie stworzone przez siebie rejestry zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie. Stosowany system teleinformatyczny zawiera mechanizmy zapewniające zachowanie integralność rejestrów zdarzeń w stopniu uniemożliwiającym ich modyfikacje po przeniesieniu do archiwum.

Umowa oraz wszelkie pisemne dokumenty związane z wydaniem kwalifikowanego certyfikatu są przechowywane w punkcie rejestracji albo w Centrum EUROCERT . W

przypadku przekazywania dokumentów z punktu rejestracji do Centrum EUROCERT zapewniony jest odpowiedni poziom ochrony tych danych.

4 Weryfikacja tożsamości i uwierzytelnienie

4.1 Rejestracja osobista

Rejestracja, czyli proces przyjęcia i weryfikacji zgłoszenia certyfikacyjnego wnioskodawcy jest przeprowadzana przez Centrum EUROCERT bądź podległy punkt rejestracji, prowadzony na podstawie odpowiedniej umowy.

Osoba, która w imieniu Centrum EUROCERT przeprowadza proces rejestracji ma obowiązek uwierzytelnienia się wobec wnioskodawcy. Uwierzytelnienie polega na:

1. okazaniu upoważnienia do działania w imieniu Centrum EUROCERT w zakresie weryfikowania i przyjmowania zgłoszeń certyfikacyjnych podpisanego przez osobę uprawnioną do reprezentowania Centrum EUROCERT,
2. okazaniu ważnego wypisu Centrum EUROCERT z rejestru KRS;
3. okazaniu kopii zaświadczenia o wpisaniu Centrum EUROCERT na listę kwalifikowanych podmiotów certyfikacyjnych.

Centrum EUROCERT potwierdza tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym.

W przypadku żądania wnioskodawcy umieszczenia w kwalifikowanym certyfikacie informacji, że będzie on działał w imieniu innego podmiotu Centrum EUROCERT sprawdza czy wnioskodawca posiada odpowiednie upoważnienia.

Jeśli jest to konieczne, to tworząc zgłoszenie certyfikacyjne Centrum EUROCERT potwierdza, że dane służące do składania bezpiecznego podpisu elektronicznego komplementarne z danymi służącymi do weryfikacji bezpiecznego podpisu elektronicznego umieszczonymi w zgłoszeniu certyfikacyjnym, znajdują się w posiadaniu osoby ubiegającej się o kwalifikowany certyfikat.

Potwierdzenie tożsamości wnioskodawcy odbywa się na podstawie ważnego dowodu osobistego lub paszportu.

Osoba potwierdzająca w imieniu Centrum EUROCERT tożsamość wnioskodawcy, poświadcza dokonanie tego potwierdzenia własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości wnioskodawcy, z zastrzeżeniem do rozdziału 4.2.

W procesie potwierdzania tożsamości, Centrum EUROCERT może korzystać z notarialnego potwierdzania tożsamości odbiorców usług certyfikacyjnych.

W trakcie rejestracji wnioskodawca podpisuje własnoręcznie wniosek o wydanie kwalifikowanego certyfikatu.

Wniosek o wydanie kwalifikowanego certyfikatu zawiera co najmniej następujące dane wnioskodawcy:

1. imię i nazwisko;
2. datę i miejsce urodzenia;
3. numer PESEL;

4. serię, numer i rodzaj dokumentu tożsamości oraz oznaczenie organu wydającego dowód tożsamości lub paszport, na podstawie którego potwierdzono tożsamość wnioskodawcy.

Jeżeli w kwalifikowanym certyfikacie zostały zawarte informacje, że Subskrybent działa nie we własnym imieniu, to Centrum EUROCERT powiadamia podmiot, w imieniu którego będzie działał Subskrybent, o treści tego certyfikatu oraz poucza go o możliwości unieważnienia tego certyfikatu na jego wniosek.

W przypadku, o którym mowa w rozdziale 4.2, Centrum EUROCERT sprawdza prawdziwość danych podanych przez wnioskodawcę przez porównanie ich z danymi zawartymi w umowie dotyczącej kwalifikowanego certyfikatu uwierzytelniającego bezpieczny podpis elektroniczny, którego użyto do podpisania Umowy.

4.2 Rejestracja w przypadku posiadania ważnego kwalifikowanego certyfikatu

W przypadku, gdy wnioskodawca posiada ważny kwalifikowany certyfikat, potwierdzenie jego tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu, a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone bezpiecznym podpisem elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat, służący do weryfikacji tego podpisu został wydany przez Centrum EUROCERT w ramach danej Polityki.

Dane podane przez użytkownika są sprawdzane na zgodność z danymi zawartymi w umowie o wydanie certyfikatu osoby składającej bezpieczny podpis elektroniczny.

4.3 Zarządzanie certyfikatem

Zgodnie z niniejszą polityką zarządzanie certyfikatem obejmuje czynności unieważnienia lub zawieszenie certyfikatu z inicjatywy Subskrybenta oraz odnowienia certyfikatu na te same klucze kryptograficzne.

Odnowienie certyfikatu oraz wymiana kluczy są realizowane tylko poprzez złożenie wniosku o wydanie nowego certyfikatu.

Procedura unieważnienia certyfikatu wymaga uwierzytelnienia osoby wnioskującej o unieważnienie certyfikatu zgodnie z informacjami przekazanymi Subskrybentowi, najpóźniej w momencie wydania certyfikatu.

Procedura odnowienia ważności certyfikatu na te same klucze kryptograficzne z inicjatywy Subskrybenta możliwa jest tylko i wyłącznie w czasie ważności kwalifikowanego certyfikatu.

5 Wymagania operacyjne

5.1 Wydanie kwalifikowanego certyfikatu przez Centrum EUROCERT

Po otrzymaniu zgłoszenia certyfikacyjnego, opatrzonego podpisem elektronicznym Inspektora do spraw Rejestracji Centrum EUROCERT niezwłocznie wydaje kwalifikowany certyfikat, w którym są zawarte dane przekazane w zgłoszeniu.

Czas ważności certyfikatu jest wskazywany przez czas synchronizowany ze wzorcem czasu z dokładnością do jednej sekukndy. Czas początku ważności certyfikatu nie może być wcześniejszy od czasu wydania certyfikatu.

5.2 Publikowanie informacji o unieważnionych i wydanych kwalifikowanych certyfikatach

Centrum EUROCERT publikuje wydane przez siebie listy certyfikatów unieważnionych i zawieszonych w ogólnie dostępnym Repozytorium informacji. Szczegóły organizacji Repozytorium i opis metod dostępu do tych informacji znajdują się http://www.EuroCERT.pl

Jeśli Centrum EUROCERT będzie publikować kwalifikowane certyfikaty wystawione w ramach Polityki w ogólnodostępnym Repozytorium, to przed wystawieniem certyfikatu ma obowiązek uzyskać pisemną zgodę Subskrybenta. Certyfikaty Subskrybentów, którzy nie wyrazili zgody, nie są publikowane. Publikacja następuje niezwłocznie po wydaniu certyfikatu.

Informacja o unieważnieniu, zawieszeniu kwalifikowanego certyfikatu publikowana jest niezwłocznie po utworzeniu nowej listy certyfikatów unieważnionych. Nowa lista certyfikatów unieważnionych dla kwalifikowanych certyfikatów wydawanych zgodnie z Polityką jest tworzona niezwłocznie po każdej operacji unieważnienia, zawieszenia lub uchylenia zawieszenia kwalifikowanego certyfikatu, jednak nie później niż 1 godzina od odebrania uprawnionego żądania unieważnienia kwalifikowanego certyfikatu, bądź unieważnienia lub zawieszenia kwalifikowanego certyfikatu z innej przyczyny, jednak nie rzadziej, niż co 24 godziny.

5.3 Unieważnianie, zawieszanie oraz uchylanie zawieszenia kwalifikowanych certyfikatów

Kwalifikowany certyfikat wydany w ramach Polityki może zostać unieważniony przed upływem okresu jego ważności. Centrum EUROCERT unieważnia kwalifikowany certyfikat w przypadku:

- otrzymania żądania unieważnienia kwalifikowanego certyfikatu od Subskrybenta, Zamawiającego lub osoby trzeciej wskazanej w tym certyfikacie;
- wydania kwalifikowanego certyfikatu na podstawie nieprawdziwych lub nieaktualnych danych dotyczących tożsamości Subskrybenta oraz wskazania w czyim imieniu on działa;
- niedopełnienia przez Centrum EUROCERT obowiązków wynikających z obowiązujących aktów prawnych;
- popełnienia błędów przy wprowadzaniu danych lub innych błędów przetwarzania;
- otrzymania żądania unieważnienia kwalifikowanego certyfikatu od ministra właściwego do spraw gospodarki;
- utraty przez Subskrybenta pełnej zdolności do czynności prawnych;
- dezaktualizacji informacji zawartych w kwalifikowanym certyfikacie.

Centrum EUROCERT niezwłocznie powiadamia Subskrybenta o unieważnieniu kwalifikowanego certyfikatu.

W przypadku istnienia uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, Centrum EUROCERT niezwłocznie zawiesza ważność tego certyfikatu, podejmuje działania niezbędne do wyjaśnienia tych wątpliwości i informuje o tym Subskrybenta.

Centrum EUROCERT uchyla zawieszenie certyfikatu w przypadku wyjaśnienia wątpliwości, będących powodem zawieszenia kwalifikowanego certyfikatu. Jeżeli w ciągu 168 godzin (7 dni) od zawieszenia kwalifikowanego certyfikatu nie zostanie ono uchylone, lub w przypadku potwierdzenia podejrzeń, na podstawie których dokonano zawieszenia, Centrum EUROCERT unieważnia ten certyfikat.

Centrum EUROCERT zapewnia możliwość zgłoszenia żądania unieważnienia kwalifikowanego certyfikatu przez całą dobę. W przypadku wystąpienia z żądaniem unieważnienia kwalifikowanego certyfikatu, Subskrybent zobowiązany jest podać hasło do unieważnienia, które otrzymał najpóźniej w chwili wydania certyfikatu.

Procedury zgłoszenia żądania unieważnienia są przedstawiane osobie ubiegającej się o wydanie takiego certyfikatu, najpóźniej w momencie jego wydania.

Centrum EUROCERT informuje Subskrybenta o konieczności niezwłocznego unieważnienia tego certyfikatu w przypadku utraty lub ujawnienia danych Subskrybenta, służących do składania bezpiecznego podpisu elektronicznego innej osobie lub podejrzenia zajścia takiego zdarzenia.

Listy CRL wydawane w ramach Polityki zapewniają możliwość określenia momentu unieważnienia lub zawieszenia kwalifikowanego certyfikatu z dokładnością do 1 sekundy.

Oprogramowanie stosowane do unieważniania lub zawieszania kwalifikowanych certyfikatów oraz unieważniania zaświadczeń certyfikacyjnych dokonuje automatycznie zapisu czasu unieważnienia lub zawieszenia i umieszcza go odpowiednio na liście CRL lub liście unieważnionych zaświadczeń certyfikacyjnych, korzystając z rozwiązań zapewniających synchronizację z międzynarodowym wzorcem czasu z dokładnością nie mniejszą niż 1 sekunda.

5.4 Techniczne środki zapewnienia bezpieczeństwa

5.4.1 Generowanie i przechowywanie danych do składania bezpiecznego podpisu elektronicznego i do składania poświadczenia elektronicznego.

Centrum EUROCERT wymaga, żeby dane służące do składania bezpiecznego podpisu elektronicznego były wygenerowane i przechowywane w komponencie technicznym, wymienionym na liście bezpiecznych urządzeń do składania podpisu elektronicznego. Lista bezpiecznych urządzeń do składania podpisu, które mogą być stosowane do wykonywania działań przy użyciu danych do składania podpisu elektronicznego komplementarnych do danych do weryfikacji podpisu elektronicznego certyfikowanych w ramach Polityki jest dostępna w Centrum EUROCERT http://www.EuroCERT.pl.

W przypadku certyfikatów wydawanych w ramach Polityki, dane do składania i weryfikacji bezpiecznych podpisów elektronicznych mogą być generowane przez wnioskodawcę lub przez producenta w procesie wytwórczym komponentu technicznego.

W przypadku generowania przez producenta. wygenerowanie tych danych następuje pod kontrolą osoby do tego upoważnionej. Spełnienie wymogów bezpieczeństwa zagwarantowane jest odpowiednimi umowami. W szczególności, zapewnia się stosowanie środków ochrony fizycznej wszystkich pomieszczeń, w którym znajdują się elementy systemu teleinformatycznego służącego do tworzenia danych służące do

składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego. Środki te obejmują co najmniej instalacje systemów kontroli dostępu, systemu ochrony przeciwpożarowej oraz systemu alarmowego włamania i napadu klasy SA3 lub wyższej, zgodnie z właściwą Polską Normą.

W procesie wydawania kwalifikowanego certyfikatu w ramach Polityki, dane służące do składania bezpiecznego podpisu elektronicznego są generowane w komponencie technicznym i nie pojawiają się w żadnej postaci w systemach teleinformatycznych Centrum EUROCERT .

Dane do składania poświadczenia elektronicznego są przechowywane w komponentach technicznych spełniających wymagania jednej z wymienionych norm: ITSEC v. 1.2 poziom 3 lub bezpieczniejszy, FIPS 140 poziom 3 lub bezpieczniejszy, albo ISO/IEC 1540 poziom EAL4 lub bezpieczniejszy

5.4.2 Wykorzystywanie danych do składania bezpiecznego podpisu elektronicznego

Centrum EUROCERT wymaga, żeby do składania podpisu weryfikowanego kwalifikowanym certyfikatem wydanym w ramach Polityki było stosowane bezpieczne urządzenie do składania podpisu, wymienione na wcześniej wspomnianej liście.

Użycie danych do składania bezpiecznego podpisu elektronicznego z wykorzystaniem urządzeń innych niż wyszczególnione na liście bezpiecznych urządzeń służących do składania podpisu elektronicznego następuje na wyłączną odpowiedzialność Subskrybenta. Centrum EUROCERT nie ponosi odpowiedzialności za szkody powstałe na skutek korzystania z urządzeń nie wymienionych na tej liście. Subskrybent przyjmuje także do wiadomości fakt, że zgodnie z art. 6 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. Nr 130, poz. 1450) nie można powoływać się, że podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu nie został złożony za pomocą bezpiecznych urządzeń i danych, podlegających wyłącznej kontroli osoby składającej podpis elektroniczny.

5.4.3 Zabezpieczenia systemów Centrum EUROCERT

Centrum EUROCERT zapewnia stosowanie środków ochrony fizycznej wszystkich pomieszczeń, w którym znajdują się elementy systemu teleinformatycznego służącego do świadczenia usług certyfikacyjnych wydawania kwalifikowanych certyfikatów, w szczególności wszędzie tam, gdzie są tworzone i używane dane służące do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego oraz są przechowywane informacje związane z niezaprzeczalnością podpisu elektronicznego weryfikowanego na podstawie wydanych kwalifikowanych certyfikatów, w tym umowy o świadczenie usług certyfikacyjnych. Środki te obejmują co najmniej instalacje systemów kontroli dostępu, systemu ochrony przeciwpożarowej oraz systemu alarmowego włamania i napadu klasy SA3 lub wyższej, zgodnie z właściwą Polską Normą.

Minimalne parametry algorytmów szyfrowych dopuszczonych do stosowania przez Centrum EUROCERT oraz odbiorców usług certyfikacyjnych w ramach Polityki są następujące:

- dla algorytmu RSA:
    - minimalna długość klucza, rozumianego jako moduł p*q wynosi 1020 bitów,

- długości liczb pierwszych p i q, składających się na moduł nie mogą się różnić więcej niż o 30 bitów;

- dla algorytmu DSA:
  - minimalna długość klucza, rozumianego jako moduł p wynosi 1024 bity,
  - minimalna długość parametru q, będącego dzielnikiem liczby (p-1) wynosi 160 bitów;

- dla algorytmu ECDSA i ECGDSA:
  - minimalna długość parametru g wynosi 160 bitów,
  - minimalny współczynnik r0 wynosi 10000,
  - minimalna klasa wynosi 200.

Jeśli zgłoszenia certyfikacyjne przekazywane są do Centrum EUROCERT w postaci elektronicznej, to przekaz ma miejsce w sesji zabezpieczonej algorytmami wymienionymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 (Dz. U. Nr 128 poz.1094 z dnia 12 sierpnia 2002).

Do poświadczania kwalifikowanych certyfikatów wydawanych w ramach Polityki Centrum EUROCERT wykorzystuje algorytm podpisu SHA-1 z szyfrowaniem RSA.

Centrum EUROCERT zapewnia poufność i integralność istotnych danych, związanych ze świadczeniem usług certyfikacyjnych podczas ich transmisji lub przechowywania poprzez następujące zastosowanie kluczy infrastruktury:

- integralność zgłoszeń certyfikacyjnych i danych służących do weryfikacji bezpiecznego podpisu elektronicznego, które zostaną umieszczone w kwalifikowanym certyfikacie (kluczy użytkowników) jest zapewniona poprzez opatrzenie ich podpisem elektronicznym Inspektora do spraw Rejestracji. Dane służące do składania podpisu elektronicznego przez Inspektorów do spraw Rejestracji są generowane i przechowywane w komponentach technicznych, znajdujących się pod wyłączną kontrolą każdego z Inspektorów.
- poufność transmisji zgłoszeń certyfikacyjnych jest zapewniona poprzez zestawienie szyfrowanego kanału w protokole SSL z wykorzystaniem kluczy serwera aplikacyjnego rejestracji zgłoszeń.
- integralność zapisów w dziennikach zdarzeń jest zapewniona poprzez opatrzenie wpisów w tych dziennikach poświadczeniem elektronicznym, złożonym z wykorzystaniem kluczy infrastruktury .

Do dostępu do oprogramowania służącego do weryfikacji zgłoszeń certyfikacyjnych uprawnieni są wyłącznie Inspektorzy do spraw Rejestracji. Weryfikacja ich uprawnień odbywa się z wykorzystaniem kluczy infrastruktury, znajdujących się pod ich wyłączną kontrolą.

Jeśli przy świadczeniu usług certyfikacyjnych objętych Polityką są przekazywane dane podpisane przez osobę składającą bezpieczny podpis elektroniczny, dane służące do składania bezpiecznego podpisu elektronicznego lub dane służące do składania poświadczenia elektronicznego przez Centrum EUROCERT , to klucze infrastruktury wykorzystywane do zapewnienia poufności przekazu tych danych przechowuje się w indywidualnych modułach kluczowych lub komponentach technicznych. Jeżeli do przechowywania tych danych wykorzystuje się kilka modułów kluczowych lub komponentów technicznych, to mogą znajdować się one pod kontrolą jednej lub kilku

osób i mogą zawierać te same dane związane z zapewnieniem poufności przekazywanych danych.

Centrum EUROCERT zapewnia stosowanie środków ochrony fizycznej wszystkich pomieszczeń, w którym znajdują się elementy systemu teleinformatycznego służącego do świadczenia usług certyfikacyjnych wydawania kwalifikowanych certyfikatów, w szczególności wszędzie tam, gdzie są tworzone i używane dane służące do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego oraz są przechowywane informacje związane z niezaprzeczalnością podpisu elektronicznego weryfikowanego na podstawie wydanych kwalifikowanych certyfikatów, w tym umowy o świadczenie usług certyfikacyjnych. Środki te obejmują co najmniej instalacje systemów kontroli dostępu, systemu ochrony przeciwpożarowej oraz systemu alarmowego włamania i napadu klasy SA3 lub wyższej, zgodnie z właściwą Polską Normą.

Powyższe wymagania dotyczą w szczególności Głównego Punktu Rejestracji, gdzie są tworzone dane do składania bezpiecznych podpisów elektronicznych oraz są przechowywane umowy o świadczenie usług certyfikacyjnych do czasu ich przekazania do archiwum Centrum EUROCERT . Komputery zlokalizowane w pozostałych punktach potwierdzania tożsamości podlegają ochronie, której zakres opisany jest w stosownych umowach pomiędzy Centrum EUROCERT a administratorem danego punktu.

5.5 Profile certyfikatu i listy certyfikatów unieważnionych (CRL)

5.5.1 Profil certyfikatu

Certyfikaty wydawane zgodnie z niniejszą Polityką zawierają co najmniej następujące pola:

Atrybut	Wartość
version	2 *certyfikat zgodny z wersją 3 standardu X.509*
serialNumber	*nadany przez Centrum EUROCERT , jednoznaczny w ramach tego centrum*
signature	SHA1WithRSAEncryption 1.2.840.113549.1.1.5 *nazwa algorytmu stosowanego do podpisywania certyfikatów*
issuer	*nazwa wyróżniona jednostki wystawiającej certyfikaty zgodne z niniejszą Polityką*
country (C)	PL
organisation (O)	EuroCERT sp. z o.o.
serialNumber	Nr wpisu: <nadany numer>
commonName (CN)	Centrum EuroCERT - Kwalifikowany
validity	*okres ważności certyfikatu*
notBefore	*data wystawienia certyfikatu*

notAfter	*data wygaśnięcia certyfikatu (data wystawienia certyfikatu + nie więcej niż 2 lata)*
subject	*nazwa wyróżniona Subskrybenta certyfikatu wystawionego zgodnie z niniejszą Polityką – dopuszczalna składnia atrybutu subject została przedstawiona w opisie pod tabelą*
subjectPublicKeyInfo	
algorithm	PKCS #1 RSA Encryption 1.2.840.113549.1.1.1
subjectPublicKey	*klucz publiczny Subskrybenta o długości min 1024 bity*

Pole subject musi zawierać niepustą nazwę wyróżniającą podmiotu. Zawiera ono atrybuty zawarte w następującym zbiorze atrybutów:

- countryName (nazwa kraju)
- commonName (nazwa powszechna)
- surname (nazwisko)
- givenName (imię, imiona)
- serialNumber (numer seryjny)
- organizationName (organizacja)

Uwaga: użycie atrybutu organizationName wymaga dołączenia atrybutów stateOrProvinceName localityName i postalAddress, które dotyczą podanej organizacji

- organizationalUnitName (jednostka organizacyjna)
- stateOrProvinceName (województwo)
- localityName (nazwa miejscowości)
- postalAddress (adres)
- pseudonym (pseudonim)

Uwaga: użycie atrybutu pseudonym wyklucza użycie atrybutów surname i givenName

Nazwa podmiotu stworzona w oparciu o podzbiór powyższych atrybutów musi być unikalna w obrębie domeny Centrum EUROCERT .

Pole subject musi zawierać co najmniej atrybuty wymienione w jednej z poniższych kategorii:

1) C = PL,

commonName = nazwa powszechna Subskrybenta (wartość domyślna – surname + givenName)

surname = nazwisko (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),

givenName = imię (imiona), zgodnie z informacją wpisaną w dowodzie osobistym lub paszporcie,

serialNumber = zawiera: „NIP: <NIP Subskrybenta>” albo „PESEL: <PESEL Subskrybenta>”, gdzie nazwa zapisana w <> (razem z <>) jest zastąpiona odpowiednią wartością;

2) C = PL,

commonName = nazwa powszechna Subskrybenta,

serialNumber = zawiera: „NIP: <NIP Subskrybenta >” albo „PESEL: <PESEL Subskrybenta>”, gdzie nazwa zapisana w <> (razem z <>) jest zastąpiona odpowiednią wartością;

3) C = PL,

commonName = nazwa powszechna Subskrybenta (wartość domyślna – pseudonym)

pseudonym = nazwa pod którą podmiot jest znany w swoim środowisku lub którą chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska.

5.5.1.1 Rozszerzenia X.509

W certyfikacie umieszczone są następujące rozszerzenia zgodne ze standardem X.509:

Rozszerzenie	Krytyczne	Wartość
keyUsage 2.5.29.15	TAK	
nonRepudiation	-	*klucz do realizacji niezaprzeczalności*
authorityKeyIdentifier 2.5.29.35	NIE	
keyIdentifier	-	*identyfikator klucza Centrum EUROCERT*
cRLDistributionPoint 2.5.29.31	NIE	
distributionPoint_1	-	*punkt dystrybucji #może występować wielokrotnie*
certificatePolicies	TAK	
policyIdentifier		1.3.6.1.4.1.23554.2.1

Uwaga: Centrum EUROCERT w uzgodnieniu z Subskrybentem może umieścić w kwalifikowanym certyfikacie inne, niewymienione tu informacje, umieszczając ich treść w dodatkowych polach rozszerzeń, których stosowanie jest dozwolone.

5.5.2 Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych wskazana w certyfikacie wystawionym zgodnie z niniejszą polityką zawiera:

Atrybut	Wartość
version	1 *lista zgodny z wersją 2 standardu X.509*
signature	SHA1WithRSAEncryption *nazwa algorytmu stosowanego do podpisywania listy CRL*
issuer	*nazwa wyróżniona jednostki wystawiającej certyfikaty zgodne z niniejszą Polityką*
country (C)	PL
organisation (O)	*EuroCERT sp. z o.o.*
commonName (CN)	Centrum EuroCERT - Kwalifikowany
serialNumber	Nr wpisu: <nadany numer>
thisUpdate	*data i godzina wydania listy*
nextUpdate	*data i godzina następnego wydania listy (thisUpdate + nie więcej niż 24 godziny)*
revokedCertificates	*lista odwołanych certyfikatów*
userCertificate	*numer seryjny unieważnionego certyfikatu*
revocationDate	*data i godzina unieważnienia certyfikatu*
reasonCode	*przyczyna umieszczenia certyfikatu na liście CRL*

Do przyczyn umieszczenia certyfikatu na liście zalicza się:

0.	unspecified	nieokreślona
1.	keyCompromise	kompromitacja klucza
2.	cACompromise	kompromitacja klucza CC
3.	affiliationChanged	zmiana danych Subskrybenta
4.	superseded	zastąpienie (wymiana) klucza
5.	cessationOfOperation	zaprzestanie używania certyfikatu do celu, w jakim został wydany
6.	certificateHold	certyfikat został zawieszony

6 Administrowanie Polityką

Każda z wersji Polityki obowiązuje (posiada status aktualna) do czasu opracowania i zatwierdzenia nowej wersji. Nowa wersja opracowywana jest przez pracowników Centrum EUROCERT i ze statusem w uzgodnieniu przekazana do uzgodnienia. Po otrzymaniu i uwzględnieniu uwag wynikających z uzgodnień polityka przekazywana jest do zatwierdzenia. uzyskując status w zatwierdzeniu. Po zakończeniu procedury zatwierdzania nowa wersja polityki osiąga status aktualna.

1. Zmiany w treści Polityki Certyfikacji są wykonywane przez Pracowników Centrum
2. Zmiany w treści Polityki podlegają kontroli merytorycznej osób wyznaczonych przez Kierownika Centrum Certyfikacji
3. Po wprowadzeniu zmiany w Polityce nadawany jest nowy identyfikator.
4. Nowa wersja polityki jest zatwierdzana przez Zarząd EuroCERT sp. z o.o.
5. Zatwierdzona wersja Polityki podlega niezwłocznej publikacji na stronie internetowej Centrum EUROCERT
6. Po publikacji Polityki należy dokonać uaktualnić profil certyfikatu odpowiadający danej polityce.